Aspects of Recursion Theory in Arithmetical Theories and Categories

Yan Steimle

Thesis submitted to the Faculty of Science in partial fulfillment of the requirements for the degree of
Master of Science Mathematics and Statistics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

[1]The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

Traditional recursion theory is the study of computable functions on the natural numbers. This thesis considers recursion theory in first-order arithmetical theories and categories, thus expanding the work of Ritchie and Young, Lambek, Scott, and Hofstra [25, 16, 4, 10].

We give a complete characterisation of the representability of computable functions in arithmetical theories, paying attention to the differences between intuitionistic and classical theories and between theories with and without induction. When considering recursion theory from a category-theoretic perspective, we examine syntactic categories of arithmetical theories. In this setting, we construct a strong parameterised natural numbers object and give necessary and sufficient conditions to construct a Turing category associated to an intuitionistic arithmetical theory with induction.

Acknowledgement

I would like to thank my supervisor, Prof. Philip Scott, for his support, guidance, advice, and availability. I would also like to thank Prof. Pieter Hofstra for his comments and suggestions.

I acknowledge the financial support of the University of Ottawa, NSERC, OGS, and FRQNT.

Contents

Chapter 1

Introduction

During the 1930's, logicians such as Church, Turing, Gödel, and Kleene precisely defined the notion of a computable function, which forms the mathematical foundation of modern computer science. The subject of computability theory, also known as recursion theory, was then developed by mathematical logicians and computer scientists as an independant discipline in the subsequent years [14, 16, 19].

There is a close connection between logic and category theory. Indeed, since a formal logical system can in general be reformulated categorically, questions about computable functions in various logical systems reappear in category theory and thus enable us to study recursion theory in a categorical context [16, 10].

We first consider the representability of computable functions (i.e. primitive, total, and partial recursive functions) in formal systems, more precisely in first-order theories, providing a formalisation of the basic axioms of number theory. We thus gain a better understanding of how the properties of various theories, such as the presence or absence of induction or the theory being intuitionistic or classical, affect the representability of the different kinds of computable functions in these theories. Hence, when we consider recursion theory from a category-theoretic perspective, we have a clearer idea of which conditions are necessary in order to represent the computable functions and formalise certain aspects of recursion theory in a categorical setting.

The representability of total numerical functions in first-order theories was first considered by Gödel in his 1931 paper, where he presented his famous Incompleteness Theorems, and considered subsequently by many other logicians [16].

Boolos and Jeffrey define a notion of representability of total numerical functions in first-order theories containing numerals. The authors then present the classical first-order theory Q (generally attributed to Robinson) and consider the representability of all total recursive functions in this theory. Note that Q is a relatively weak theory as it does not contain induction, and simple results of number theory such as the commutativity, associativity, and distributivity of addition and multiplication are not provable for variables in Q [2, Ch. 14].

Kleene considers the numeralwise representability of total recursive functions in both the intuitionistic and classical version of his formal system for number theory, which contains induction. He also remarks on some results that hold in a simpler version of his formal system for number theory, which corresponds to Robinson's theory and so does not contain induction [14, Ch. VIII §41, Ch. IX §48–49]. Note that the notion of numeralwise representability used by Kleene, although presented differently, corresponds to the notion used by Boolos and Jeffrey.

Mendelson defines a classical first-order theory S that is based on Peano's postulates for number theory and contains induction. In addition to a notion of representability of a total function corresponding to Kleene's notion of numeralwise representability, Mendelson considers a second notion of representability of a total function called strong representability. However, he shows that in any classical first-order theory over the language of S, a total function is (numeralwise) representable if and only if it is strongly representable, and so these two notions of representability can be used interchangeably in S. Mendelson also briefly remarks that it is possible to find weaker theories than S for which the representable functions are precisely the total recursive ones. This leads him to define the classical theory RR, which corresponds to Robinson's theory with an added axiom for the uniqueness of the remainder and does not contain induction [19, Ch. 3].

Shoenfield defines a first-order theory N that formalises a classical axiom system for the natural numbers and considers the representability of total recursive functions in N. In fact, the nonlogical axioms of N are chosen precisely in order to ensure that all total recursive functions are representable in N. Note that N is a slightly stronger theory than Robinson's theory but does not contain induction and that Shoenfield defines representability of a total function in a slightly different way from the previously mentioned authors [33, §2.6, 6.7].

The representability of partial numerical functions in first-order theories has also been considered, although not as often. Ritchie and Young generalise the notions of representability given by Mendelson [19] and obtain three notions of representability of a partial numerical function in a first-order theory of arithmetic, namely numeralwise, type-one, and strong representability. The authors then consider the relationship between the three types of representability of partial recursive functions in consistent recursively enumerable extensions of Robinson's classical theory and eventually show that the class of partial functions strongly representable in such a theory is precisely the class of partial recursive functions [25]. Ritter proves a slight generalisation of Ritchie and Young's theorem on the strong representability of partial recursive functions by considering a larger class of first-order theories, namely classical, consistent, and recursively enumerable theories in which there is a suitable notion of inequality and all recursive relations are definable (see [32, p. 120]) [26].

While all these authors have studied certain aspects of the representability of total or partial recursive functions in first-order theories, sometimes in great detail, none of them have given a complete characterisation of the representability of the three types of computable functions while taking into account the different possible notions of representability and the different kinds of first-order theories (with induction, without induction, intuitionistic, and classical). The most complete presentation is given by Ritchie and Young [25], but there are still elements missing. Indeed, while the authors do consider three different notions of representability of partial recursive functions, they only consider classical theories, where these notions of representability are essentially interchangeable. This is not the case in intuitionistic theories, where we can find partial recursive functions that are numeralwise representable but not strongly representable, as shown in Section 2.3.3. Moreover, while Ritchie and Young state theorems concerning the representability of all partial recursive functions, they only consider partial functions of a single variable in their proofs and supporting results. This is not consistent with the construction of the class of partial recursive functions as some of the partial recursive functions of a single variable are obtained from partial recursive functions of more or less than one variable via primitive recursion or partial minimisation. Furthermore, there is more information to be gained by comparing the representability of the three types of computable functions and by considering the impact of the presence or absence of induction on type-one and strong representability, particularly in the case of intuitionistic theories.

In Chapter 2, we present a more complete characterisation of the representability of computable functions by considering the primitive, total, and partial recursive functions, three different notions of representability, and three kinds of (first-order) arithmetical theories, thereby providing the missing details and information mentioned above. More precisely, we show that primitive recursive functions are numeralwise representable in all arithmetical theories and strongly representable in both arithmetical theories with induction and classical arithmetical theories (with or without induction). We also show that total and partial recursive functions are numeralwise representable in all arithmetical theories, type-one representable in arithmetical theories with induction, and strongly representable in classical arithmetical theories.

We then use the results obtained in Chapter 2 to study certain aspects of recursion theory in a categorical setting.

As seen in Chapter 2, a first-order theory must contain a formalisation of the basic axioms of number theory in order to provide a suitable setting in which to formalise certain aspects of recursion theory. Similarly, when considering recursion theory in a categorical setting, we want to formalise certain aspects of number theory in a category, especially if we want to consider the representability of computable functions in categories. We therefore consider natural numbers objects (see [16]), which allow us to formalise the concepts of natural numbers and numerical functions in a category. Turing categories are restriction categories (i.e. categories of partial morphisms) that embody certain basic principles of recursion theory such as Gödel numbering, enumeration of partial recursive functions, and parameterisation. They provide another possibility for a categorical setting in which to consider aspects of recursion theory [4, 10].

In Chapter 3, we consider two kinds of categories associated to the arithmetic theories defined in Chapter 2. We first construct the syntactic category associated to a first-order theory using a construction similar to the one in [13, §D1.4] and in [29, 30]. The notion of a syntactic category generally arises in the study of the equivalence between logic and category theory. Indeed, certain fragments of logic (Horn, regular, coherent, first-order, and geometric logic) have a sound and complete interpretation in categories with certain additional categorical structure (lex, regular, coherent, Heyting, and geometric categories, respectively). Syntactic categories are used in order to prove the completeness theorem [13, §D1.3–D1.4].

Since recursion theory is, in particular, concerned with partial recursive functions, we need a notion of partial morphism in the categories we consider. Therefore, we construct the syntactic partial map category of a theory by removing the requirement that the morphisms be total from the definition of a syntactic category. Since syntactic partial map categories are restriction categories, we thus obtain a notion of partial morphisms in syntactic categories.

We then consider how to construct a natural numbers object in the syntactic category of an arithmetical theory. A similar topic is explored in [7], where the authors study partial recursive morphisms and natural numbers objects in elementary toposes. The authors are particularly interested in the differences between the results about partial recursive morphisms in the context of general elementary toposes and about partial recursive functions in the context of sets as these differences illustrate the gap between what is true (in sets) and what is provable (in intuitionistic type theory). We consider a similar topic to the one brought up by the central questions of [7] since we are interested in some of the similarities and differences between the treatment of basic number theory and natural numbers objects in sets (equivalently, in **Set**) and in syntactic categories of arithmetical theories. However, unlike the case in [7] where the treatment of number theory and partial recursive morphisms in elementary toposes is essentially the same as the analogous treatment in sets, we need to use the results and constructions from Chapter 2 in order to formalise the concepts of natural numbers and numerical functions in syntactic categories of arithmetical theories.

We then wish to determine if we can extend this formalisation in syntactic categories of basic aspects of number theory to include a sufficient amount of central results from recursion theory to be able to construct a Turing category. As noted in [4, 10], Turing categories are restriction categories that essentially encode the ideas underlying Kleene's Parameter (S-m-n) Theorem, Enumeration Theorem. Furthermore, some basic results from recursion theory, such as the recursion theorems, are derivable from the axioms of a Turing category. We therefore consider how to formalise results such as Kleene's Normal Form, Parameter, and Enumeration Theorems in arithmetical theories in order to construct a subcategory of the syntactic partial map category $\mathscr{P}(\mathbb{T})$ associated to an arithmetical theory that is also a Turing category. In particular, in order to formalise Kleene's Normal Form and Enumeration Theorems, we define a partial version of Church's Rule that applies to provably functional but not necessarily provably total formulas.

A notable example of a Turing category in the context of sets is the category **Comp**($\mathbb{N}$) of finite powers of $\mathbb{N}$ and tuples of partial recursive functions. Hence, given an arithmetical theory $\mathbb{T}$ for which we have constructed a natural numbers object N in the syntactic category $\mathscr{C}(\mathbb{T})$, we consider in particular subcategories of $\mathscr{P}(\mathbb{T})$ whose objects are finite powers of N and determine what properties the morphisms must satisfy in order to yield a Turing category.

Eventually, we would hope to use the results in Chapters 2 and 3 to continue the work of Lambek, Scott, and Román on the representability of computable functions in categories with a natural numbers object [16, 28, 10], in particular by considering the representability of partial recursive functions in cartesian and cartesian closed categories with equalisers and a natural numbers object. Unfortunately, we did not have time to accomplish any significant work on this subject, but we mention some ideas in Chapter 4.

Chapter 2

The representability of computable functions in arithmetical theories

We characterise the representability of computable functions in first-order theories. In order to be able to consider the representability of numerical functions, we need to formalise the basic axioms of number theory in first-order theories. Consequently, we define (first-order) arithmetical theories, which provide a framework for the formalisation of number theory.

In Section 2.1, we give a construction of the three classes of computable functions, namely the primitive, total, and partial recursive functions; in Section 2.2, we define arithmetical theories; in Section 2.3, we define several notions of representability of partial numerical functions in arithmetical theories; finally, in Section 2.4, we present a characterisation of the representability of primitive, total, and partial recursive functions in arithmetical theories.

2.1 Recursive functions and predicates

2.1.1 Numerical functions

We follow the treatment of numerical functions in [16, 31, 19, 11] and, to a lesser extent, in [33].

In order to simplify notation, we may use bold-face letters to denote sequences of variables or natural numbers. Sequences are always assumed to be of the correct length given the context.

Definition 2.1.1.1 (Numerical functions and constants) Let $k \geq 0$. A *partial (numerical) function* f from $\mathbb{N}^k$ to $\mathbb{N}$, denoted $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, is a set-theoretic mapping from some subset $D_f \subseteq \mathbb{N}^k$ to $\mathbb{N}$, where D_f is called the *domain (of definition)* of f. Note that D_f may be empty, in which case f is the *completely undefined function* from $\mathbb{N}^k$ to $\mathbb{N}$. Moreover, if $D_f = \mathbb{N}^k$, then f is a set-theoretic function from $\mathbb{N}^k$ to $\mathbb{N}$, denoted $f : \mathbb{N}^k \to \mathbb{N}$, and called a *total (numerical) function* from $\mathbb{N}^k$ to $\mathbb{N}$.

Let $\mathbf{n} \in \mathbb{N}^k$. If $\mathbf{n} \in D_f$, we say that f is *defined at* $\mathbf{n}$ or that $f(\mathbf{n})$ is *defined*, denoted $f(\mathbf{n})\downarrow$. If $\mathbf{n} \notin D_f$, we say that f is *undefined at* $\mathbf{n}$ or that $f(\mathbf{n})$ is *undefined*, denoted $f(\mathbf{n})\uparrow$. □

We now consider the case when $k = 0$, in which case $\mathbb{N}^k = \mathbb{N}^0 = \{*\}$, where $*$ denotes the empty sequence.

Definition 2.1.1.2 For each *numerical constant* (i.e. fixed natural number) $n \in \mathbb{N}$, we obtain a total function $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$ defined by $\underline{n}(*) = n$. Conversely, if $f : \mathbb{N}^0 \to \mathbb{N}$ is a total function, then $f(*)$ is some constant $n \in \mathbb{N}$, and so f is in fact the function $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$. Hence, the total functions from $\mathbb{N}^0$ to $\mathbb{N}$ correspond exactly to numerical constants in $\mathbb{N}$, and so we may refer to total functions $f : \mathbb{N}^0 \to \mathbb{N}$ as *(total) constants*.

Now consider the more general case when $f : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ is a partial function. By analogy to the total case, we call f a *partial constant*. Two possible cases arise. If $D_f = \mathbb{N}^0$, then f is a total constant as defined above, that is, $f = \underline{n}$ for some $n \in \mathbb{N}$. In this case, we may write $f\downarrow$ to indicate that f is total. If instead $D_f = \varnothing$, then f is the completely undefined function from $\mathbb{N}^0$ to $\mathbb{N}$ and we may write $f\uparrow$ to indicate this. □

Note that in order to deal with partiality and possible undefinedness when considering partial functions, we use *Kleene equality*, denoted $\simeq$ (see [14, §63, pp. 327–328], where $\simeq$ is called *weak equality*). For example, if $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and $g : \mathbb{N}^j \dashrightarrow \mathbb{N}$ are partial functions, then for all $\mathbf{m} \in \mathbb{N}^k$ and $\mathbf{n} \in \mathbb{N}^j$, $f(\mathbf{m}) \simeq g(\mathbf{n})$ if and only if one of the two following statements is true:

(i) $f(\mathbf{m})\downarrow$, $g(\mathbf{n})\downarrow$, and $f(\mathbf{m}) = g(\mathbf{n})$

(ii) $f(\mathbf{m})\uparrow$ and $g(\mathbf{n})\uparrow$.

Hence, two partial functions $f, g : \mathbb{N}^k \dashrightarrow \mathbb{N}$ are equal (as partial functions), denoted $f = g$, if and only if $f(\mathbf{m}) \simeq g(\mathbf{m})$ for all $\mathbf{m} \in \mathbb{N}^k$. That is to say, $f = g$ if and only if f and g have the same domain of definition and are equal when defined.

Let $k \geq 0$. Note that subsets of $\mathbb{N}^k$ are often called either relations or predicates and are presented in several equivalent ways in the literature [33, 19, 14]. We shall generally refer to subsets of $\mathbb{N}^k$ as *predicates on* $\mathbb{N}^k$ (or k*-ary predicates on* $\mathbb{N}$). As in [33, pp. 10, 108], for any $E \subseteq \mathbb{N}^k$, we often write $E(\mathbf{m})$ and $\neg E(\mathbf{m})$ instead of $\mathbf{m} \in E$ and $\mathbf{m} \notin E$, respectively. Similarly, given $E_1, E_2 \subseteq \mathbb{N}^k$ for some $k \geq 0$, we may write $E_1 \wedge E_2$ and $E_1 \vee E_2$ instead of $E_1 \cap E_2$ and $E_1 \cup E_2$, respectively.

Given a predicate P on $\mathbb{N}^k$, we can associate to P a k-ary function $K_P : \mathbb{N}^k \to \mathbb{N}$, called the *characteristic function of* P (also known as the *representing function* in [33]), which is defined by

$$K_P(\mathbf{m}) = \begin{cases} 0 & \text{if } P(\mathbf{m}) \\ 1 & \text{if } \neg P(\mathbf{m}) \end{cases}$$

for all $\mathbf{m} \in \mathbb{N}^k$. We can identify predicates $P \subseteq \mathbb{N}^k$ with functions $f : \mathbb{N}^k \to \mathbb{N}$ such that $f(\mathbb{N}^k) \subseteq \{0, 1\}$. Therefore, in order to completely specify a predicate on $\mathbb{N}^k$, it suffices to give its characteristic function.

2.1.2 Primitive, total, and partial recursive functions

We can now define primitive recursive, recursive, and partial recursive functions, following [16, pp. 253–255], [19, pp. 171–172, 322–323], [11, pp. 2–5, 19–21], and, to a lesser extent, [33, pp. 108–109, 144–147].

Definition 2.1.2.1 (Basic functions) The following functions are called the *basic functions*.

(I) The *zero constant* $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$ given by $\underline{0}(*) = 0$.

(II) The *successor function* $s : \mathbb{N} \to \mathbb{N}$ given by $s(n) = n + 1$ for all $n \in \mathbb{N}$.

(III) The *projection functions* (or *projections*) $U_i^k : \mathbb{N}^k \to \mathbb{N}$ for $1 \leq i \leq k$, given by $U_i^k(n_1, \dots, n_k) = n_i$ for all $(n_1, \dots, n_k) \in \mathbb{N}^k$. □

Note that instead of the zero constant $\underline{0}$, the *zero function* $Z : \mathbb{N} \to \mathbb{N}$ given by $Z(n) = 0$ for all $n \in \mathbb{N}$ is often taken as a basic function (see for example [11]). However, if we take Z instead of $\underline{0}$ as a basic function, we have no way of constructing 0-ary functions from the basic functions using only substitution and primitive recursion as defined below. Hence, we cannot show that constants (i.e. 0-ary functions) are primitive recursive. Therefore, we choose to use $\underline{0}$ as a basic function. Z can then be obtained from $\underline{0}$ and U_2^2 by primitive recursion as shown in Lemma 2.1.2.8 and can thus be shown to be primitive recursive even when it is not taken as a basic function.

Definition 2.1.2.2 (μ-operator) Let $\dots n \dots$ be some statement containing n that is either true or false for any given $n \in \mathbb{N}$. Then, $\mu_n(\dots n \dots)$ is the least $n \in \mathbb{N}$ such that $\dots n \dots$ is true and $\dots m \dots$ makes sense for all $m < n$; it is undefined if there is no such n. μ_n is called the *μ-operator*. We mostly consider the following cases:

(i) $\dots n \dots$ is of the form $g(\mathbf{m}, n) = 0$ for some partial function $g : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ (where $k \geq 0$). In this case,

$$\mu_n(g(\mathbf{m}, n) = 0) \simeq \begin{cases} \text{the least } n \text{ s.t. } g(\mathbf{m}, n) \simeq 0 \text{ and } g(\mathbf{m}, p)\downarrow \ \forall p < n & \text{if it exists} \\ \uparrow & \text{otherwise} \end{cases}$$

Note that the symbol "$\uparrow$" in the definition above indicates that $\mu_n(g(\mathbf{m}, n) = 0)$ is undefined in the second case.

If we add the restriction that g must be total and that, for each $\mathbf{m} \in \mathbb{N}^k$, there must exist some n for which $g(\mathbf{m}, n) = 0$, we may call μ_n a *total* μ-operator. If we add no such restriction, μ_n may be called a *partial* μ-operator. Note that the total μ-operator is a special case of the partial one. If we wish to emphasize the fact that we are dealing with the total μ-operator, we may denote it by μ_n^*. Note further that in the case of the total μ-operator μ_n^*, the condition that $g(\mathbf{m}, p)$ be defined for all $p < n$ is redundant as $g(\mathbf{m}, p)$ is defined for all possible $p \in \mathbb{N}$. Hence, for each $\mathbf{m} \in \mathbb{N}^k$, we may simply define $\mu_n^*(g(\mathbf{m}, n) = 0)$ to be the least n such that $g(\mathbf{m}, n) = 0$. As such an n always exists, $\mu_n^*(g(\mathbf{m}, n) = 0)$ is then defined for all $\mathbf{m} \in \mathbb{N}^k$.

(ii) $\ldots n \ldots$ is of the form $R(\mathbf{m}, n)$ for some predicate R on $\mathbb{N}^{k+1}$ (where $k \geq 0$). Then,

$$\mu_n R(\mathbf{m}, n) \simeq \begin{cases} \text{the least } n \text{ s.t. } R(\mathbf{m}, n) & \text{if it exists} \\ \uparrow & \text{otherwise} \end{cases}$$

Similarly to case (i), if we add the restriction that for all $\mathbf{m} \in \mathbb{N}^k$ there must exist an n for which $R(\mathbf{m}, n)$, then $\mu_n R(\mathbf{m}, n)$ is defined for all $\mathbf{m} \in \mathbb{N}^k$. We thus obtain a total μ-operator, which can again be denoted by μ_n^*. If we add no such restriction, μ_n is once more called a partial μ-operator. □

Definition 2.1.2.3 The following are the *recursion schemes* that allow us to construct new functions from given functions. We define most of the schemes so that they can be applied to both total and partial functions. However, we note that schemes (S), (PR) and (TM), when applied to total functions, yield only total functions. So, in particular, $\simeq$ can be replaced by $=$ in rules (S) and (PR) if they are applied to total functions (see [11, p. 21] for more details).

(S) *Substitution* (sometimes called *generalised composition*): let $n \geq 1$ and $k \geq 0$ and let $g : \mathbb{N}^n \dashrightarrow \mathbb{N}$ and $h_i : \mathbb{N}^k \dashrightarrow \mathbb{N}$ $(1 \leq i \leq n)$ be partial functions. Then, the partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, defined by

$$f(\mathbf{m}) \simeq g(h_1(\mathbf{m}), \ldots, h_n(\mathbf{m}))$$

for all $\mathbf{m} \in \mathbb{N}^k$, is said to be obtained from $g, h_1, \ldots, h_n$ by *substitution*.

Note that the domain of definition of f is given by the set

$$D_f = \left\{\mathbf{m} \in \mathbb{N}^k \;\middle|\; h_i(\mathbf{m})\downarrow \text{ for all } 1 \leq i \leq n \text{ and } g(h_1(\mathbf{m}), \ldots, h_n(\mathbf{m}))\downarrow\right\}.$$

Hence, if $g, h_1, \ldots, h_n$ are total, then so is f.

Note also that in the special case when $n = 1$, we obtain the usual notion of composition of functions since $f(\mathbf{m}) \simeq g(h_1(\mathbf{m}))$ for all $\mathbf{m} \in \mathbb{N}^k$ and so $f = g \circ h_1$.

(PR) *Primitive Recursion*: let $k \geq 0$ and let $g : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and $h : \mathbb{N}^{k+2} \dashrightarrow \mathbb{N}$ be partial functions. Then, the partial function $f : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$, defined by

$$f(\mathbf{m}, 0) \simeq g(\mathbf{m})$$

$$f(\mathbf{m}, n+1) \simeq h(\mathbf{m}, n, f(\mathbf{m}, n))$$

for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$, is said to be obtained from g and h by *primitive recursion*. The variables in the list $\mathbf{m}$ are said to be the *parameters* of the recursion and the variable n is said to be the *recursion variable*.

Consider the case $k = 0$. In this case, $f : \mathbb{N} \dashrightarrow \mathbb{N}$ is defined from a partial constant $\tilde{c}$ (corresponding to a partial function $\tilde{c} : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ where we write $\tilde{c}$ for $\tilde{c}(*)$) and a partial function $h : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ by

$$f(0) \simeq \tilde{c}$$
$$f(n+1) \simeq h(n, f(n))$$

for all $n \in \mathbb{N}$ and is said to be obtained from $\tilde{c}$ and h by primitive recursion. Note that if $\tilde{c}\uparrow$, f is the totally undefined function on $\mathbb{N}$.

Note also that if g, h (respectively, $\tilde{c}, h$) are total, then so is f.

(TM) *Total minimisation*: let $k \geq 0$ and let $g : \mathbb{N}^{k+1} \to \mathbb{N}$ be a total function such that for each $\mathbf{m} \in \mathbb{N}^k$, there is at least one $n \in \mathbb{N}$ such that $g(\mathbf{m}, n) = 0$. Then, the total function $f : \mathbb{N}^k \to \mathbb{N}$, defined by

$$f(\mathbf{m}) = \mu_n^*(g(\mathbf{m}, n) = 0)$$

for all $\mathbf{m} \in \mathbb{N}^k$, is said to be obtained from g by *total minimisation* or *via the total μ-operator*.

(PM) *Partial minimisation*: let $k \geq 0$ and let $g : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ be a partial function. Then, the partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, defined by

$$f(\mathbf{m}) \simeq \mu_n(g(\mathbf{m}, n) = 0)$$

for all $\mathbf{m} \in \mathbb{N}^k$, is said to be obtained from g by *partial minimisation* or *via the partial μ-operator*. □

Note that, when considering partial minimisation applied to a partial function $g : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$, the condition in Definition 2.1.2.2 (ii) stating that $g(\mathbf{m}, p)$ be defined for all values $p < n$ cannot be omitted. See [11, p. 20] and [33, p. 146] for more details.

Definition 2.1.2.4 [16, p. 253] Let $\mathbf{C}$ be a set of (partial) numerical functions. We say that $\mathbf{C}$ is *closed under* some scheme σ, if any (partial) function f obtained via a finite number of applications of the scheme σ to other (partial) functions in $\mathbf{C}$ is an element of $\mathbf{C}$. Equivalently, $\mathbf{C}$ is closed under a scheme σ if and only if any (partial) function f obtained via a single application of σ to other (partial) functions in $\mathbf{C}$ is an element of $\mathbf{C}$. □

Definition 2.1.2.5 (Primitive, total, and partial recursive functions) Let $k \geq 0$.

(i) A partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is called *primitive recursive* if it can be obtained from the basic functions via a finite number of applications of substitution (S) and primitive recursion (PR). Equivalently, the set of *primitive recursive functions* is the smallest set of partial numerical functions containing the basic functions and closed under schemes (S) and (PR).

(ii) A partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is called *total recursive* if it can be obtained from the basic functions via a finite number of applications of substitution (S), primitive recursion (PR), and total minimisation (TM). Equivalently, the set of *total recursive functions* is the smallest set of partial numerical functions containing the basic functions and closed under schemes (S), (PR), and (TM).

(iii) A function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is called *partial recursive* if it can be obtained from the basic functions via a finite number of applications of substitution (S), primitive recursion (PR), and partial minimisation (PM). Equivalently, the set of *partial recursive functions* is the smallest set of partial numerical functions containing the basic functions and closed under the schemes (S), (PR), and (PM). □

Note that as stated in the Church-Turing Thesis (see for instance [16, §III.1]), the partial recursive functions are precisely the intuitively computable functions, and hence we may use the term "computable functions" as a general term encompassing the primitive, total, and partial recursive functions.

Since the basic functions are total and applying schemes (S), (PR), and (TM) to total functions yields only total functions, we immediately obtain the following result.

Proposition 2.1.2.6 *Any partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ that is primitive recursive or total recursive is in fact a total function. Hence, we may restrict the definitions of primitive recursive and total recursive functions (and of the sets of such functions) to total numerical functions.*

By construction, all primitive recursive functions are total recursive and all total recursive functions are partial recursive. Moreover, as shown in [19, pp. 330, Corollary 5.8], all partial recursive functions that are total are in fact total recursive. Hence, the set of total recursive functions is equal to the set of all partial recursive functions that are in fact total.

In [33], there is an equivalent characterisation of the total recursive functions that does not use the primitive recursion scheme (PR).

Definition 2.1.2.7 [33, p. 109] The class of total recursive functions is the smallest class of numerical functions closed under substitution (S) and total minimisation (TM) that contains the projections $U_i^k : \mathbb{N}^k \to \mathbb{N}$ for all $k \geq 1$, addition $+ : \mathbb{N}^2 \to \mathbb{N}$, multiplication $\cdot : \mathbb{N}^2 \to \mathbb{N}$, and the characteristic function of the inequality predicate $K_< : \mathbb{N}^2 \to \mathbb{N}$. □

Lemma 2.1.2.8 *The* zero function $Z : \mathbb{N} \to \mathbb{N}$ *given by* $Z(n) = 0$ *for all* $n \in \mathbb{N}$ *is primitive recursive.*

PROOF Consider the basic functions $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$ and $U_2^2 : \mathbb{N}^2 \to \mathbb{N}$. Then $Z : \mathbb{N} \to \mathbb{N}$ is obtained from $\underline{0}$ and U_2^2 by primitive recursion since

$$Z(0) = 0 = \underline{0}(*)$$

and

$$Z(n+1) = U_2^2(n, Z(n))$$

for all $n \in \mathbb{N}$. Therefore, Z is primitive recursive. ■

Note that when we have a minimisation scheme available, we can obtain the zero constant $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$ by minimising over the projection $U_1^1 : \mathbb{N} \to \mathbb{N}$. Hence, taking either the zero constant $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$ or the zero function $Z : \mathbb{N} \to \mathbb{N}$ as a basic function yields the same sets of total recursive and partial recursive functions. It is only when considering the set of primitive recursive functions that the choice of $\underline{0}$ or Z as a basic function makes a difference since we can obtain Z from $\underline{0}$ as in Lemma 2.1.2.8, but not conversely, as remarked following Definition 2.1.2.1.

Lemma 2.1.2.9 *All partial constants* $\tilde{c} : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ *are partial recursive. In particular, a partial constant is either the undefined function from* $\mathbb{N}^0$ *to* $\mathbb{N}$ *or is a total constant of the form* $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$ *for some* $n \in \mathbb{N}$*, and hence primitive recursive.*

PROOF Let $n \in \mathbb{N}$. Then, $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$ is primitive recursive (and so also partial recursive) as it is obtained from the basic functions $\underline{0}$ and S by n applications of substitution. Therefore, all total constants are primitive recursive.

If $\tilde{c} : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ is a partial constant, then either $\tilde{c}\downarrow$, in which case $\tilde{c}$ is primitive (and hence also partial) recursive as noted above. If $\tilde{c}\uparrow$, then $\tilde{c}$ is the completely undefined function from $\mathbb{N}^0$ to $\mathbb{N}$ and can be obtained from the primitive recursive function $S \circ Z : \mathbb{N} \to \mathbb{N}$ by partial minimisation. Hence, it is partial recursive. Thus, all partial constants are partial recursive. ■

2.1.3 Recursive and recursively enumerable predicates

Definition 2.1.3.1 Let P be a predicate on $\mathbb{N}^k$. Then, P is said to be a *primitive (total) recursive predicate* if its characteristic function K_P is a primitive (total, respectively) recursive k-ary function. Note that a total recursive predicate is often simply called a *recursive* predicate. □

We can now generalise the notion of a recursively enumerable set to predicates on $\mathbb{N}^k$ for any $k \geq 0$.

Definition 2.1.3.2 Let $k \geq 0$. A predicate $E \subseteq \mathbb{N}^k$ is *recursively enumerable* (*r.e.*) if there exists a primitive recursive predicate $R \subseteq \mathbb{N}^{k+1}$ such that for all $\mathbf{m} \in \mathbb{N}^k$,

$$E(\mathbf{m}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } R(\mathbf{m}, n).$$

There are in fact many equivalent characterisations of recursively enumerable predicates, as shown below.

Proposition 2.1.3.3 [14, 33, 19] *Let $k \geq 0$. The following are equivalent for any $E \subseteq \mathbb{N}^k$:*

(i) E is recursively enumerable (as in Definition 2.1.3.2).

(ii) There exists a primitive recursive function $f : \mathbb{N}^{k+1} \to \mathbb{N}$ such that for all $\mathbf{m} \in \mathbb{N}$,

$$E(\mathbf{m}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } f(\mathbf{m}, n) = 0.$$

(iii) There exists a total recursive predicate $R \subseteq \mathbb{N}^{k+1}$ such that for all $\mathbf{m} \in \mathbb{N}^k$,

$$E(\mathbf{m}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } R(\mathbf{m}, n).$$

(iv) There exists a total recursive function $f : \mathbb{N}^{k+1} \to \mathbb{N}$ such that for all $\mathbf{m} \in \mathbb{N}$,

$$E(\mathbf{m}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } f(\mathbf{m}, n) = 0.$$

(v) E is the domain of a partial recursive function $g : \mathbb{N}^k \dashrightarrow \mathbb{N}$.

(vi) The function $\tilde{K}_E : \mathbb{N}^k \dashrightarrow \mathbb{N}$ defined by

$$\tilde{K}_E(\mathbf{m}) = \begin{cases} 0 & \text{if } E(\mathbf{m}) \\ \uparrow & \text{if } \neg E(\mathbf{m}) \end{cases}$$

for all $\mathbf{m} \in \mathbb{N}^k$ is a partial recursive function. Note that $\tilde{K}_E$ is called the semi-characteristic function *of E in* [11].

Proof See [33, p. 122], [19, pp. 329–331, 346–347], and [14, pp. 281–282, 306–307].■

Lemma 2.1.3.4 *Let $k \geq 1$, let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial recursive function, and let $n_0 \in \mathbb{N}$. Then, the preimage of n_0 under f, namely the set $f^{-1}(\{n_0\}) \subseteq \mathbb{N}^k$, is recursively enumerable.*

Proof Since $\{n_0\}$ is a finite set, it is primitive recursive and so is its characteristic function $K_{\{n_0\}} : \mathbb{N} \to \mathbb{N}$. Now consider the partial recursive function $h : \mathbb{N} \dashrightarrow \mathbb{N}$ obtained from $U_1^2 : \mathbb{N}^2 \to \mathbb{N}$ by partial minimisation, that is, h is defined by

$$h(p) \simeq \mu_n(U_1^2(p, n) = 0) \simeq \begin{cases} 0 & \text{if } p = 0 \\ \uparrow & \text{if } p \neq 0 \end{cases}$$

for all $p \in \mathbb{N}$. Now consider the partial function $h \circ K_{\{n_0\}} \circ f : \mathbb{N}^k \dashrightarrow \mathbb{N}$. It is partial recursive as it is the composition of partial recursive functions. We wish to determine the domain of definition of $h \circ K_{\{n_0\}} \circ f$. So, let $\mathbf{m} \in \mathbb{N}^k$ and note that

$$(h \circ K_{\{n_0\}} \circ f)(\mathbf{m}) \simeq h(K_{\{n_0\}}(f(\mathbf{m}))).$$

If $\mathbf{m} \in f^{-1}(\{n_0\})$, then

$$\begin{aligned} h(K_{\{n_0\}}(f(\mathbf{m}))) &\simeq h(K_{\{n_0\}}(n_0)) \\ &\simeq h(0) \\ &\simeq 0. \end{aligned}$$

If $\mathbf{m} \in \mathbb{N}^k \setminus f^{-1}(\{n_0\})$, then either $f(\mathbf{m}) \uparrow$, or $f(\mathbf{m}) \simeq p$ for some $p \neq n_0$. In the first case, $h(K_{\{n_0\}}(f(\mathbf{m})))$ is undefined since $f(\mathbf{m})$ is itself undefined. In the second case, we have that

$$\begin{aligned} h(K_{\{n_0\}}(f(\mathbf{m}))) &\simeq h(K_{\{n_0\}}(p)) \text{ where } p \notin \{n_0\} \\ &\simeq h(1), \end{aligned}$$

where $h(1)$ is undefined by definition of h. So, for all $\mathbf{m} \in \mathbb{N}^k$, $(h \circ K_{\{n_0\}} \circ f)(\mathbf{m})$ is defined if and only if $\mathbf{m} \in f^{-1}(\{n_0\})$. Hence, $f^{-1}(\{n_0\})$ is the domain of definition of the partial recursive function $h \circ K_{\{n_0\}} \circ f$, and therefore $f^{-1}(\{n_0\})$ is recursively enumerable by Proposition 2.1.3.3. ■

2.2 Arithmetical Theories

We largely follow [14, §16–18] and [33, pp. 14–15] for the notions of first-order language and first-order theory. We make a distinction between intuitionistic and classical first-order theories. As explained following Definition A.2.0.5, we assume without loss of generality that every classical first-order theory $\mathbb{T}$ contains the following axiom scheme for the rule of the excluded middle:

(EM) $A \vee \neg A$, where A is any formula of $\mathbb{T}$.

See Appendix A for a presentation of first-order languages and theories as well as the relevant notation and terminology.

In order to define arithmetical theories, we first need to consider recursively enumerable theories, for which it is necessary to construct a Gödel numbering for each first-order theory.

2.2.1 Gödel numbering, recursively axiomatised theories, and r.e. theories

Given a theory $\mathbb{T}$ over a language $\mathscr{L}$, we will associate to $\mathbb{T}$ a fixed *Gödel numbering*, which is an assignment of a *Gödel number* (also called *expression number* in [33, §6.6]) to each expression (term and formula) of $\mathbb{T}$. As remarked at the beginning of

Section A.2 in Appendix A, the first-order theories we consider are formally defined in terms of axioms and rules of inference as in [14, §19–23]. This is similar to the situation in [33, §2.6], although the choice of logical axioms and rules of inference differs. Hence, we can proceed in an analogous manner to the one in [33, §6.6] in order to assign a (distinct) *symbol number* $SN(\sigma)$ to each symbol $\sigma \in \Sigma_{\mathscr{L}}$ and a (distinct) *Gödel number* $\ulcorner e \urcorner$ to each expression $e \in TERM_{\mathscr{L}} \cup FOR_{\mathscr{L}}$. As in [33, §6.6, p. 126], we extend the numbering to finite sequences of expressions and, for each finite sequence $e_1, \ldots, e_k$ of expressions of $\mathbb{T}$, we let $\langle \ulcorner e_1 \urcorner, \ldots, \ulcorner e_k \urcorner \rangle$ be the Gödel number of the sequence $e_1, \ldots, e_k$, where $\langle \cdot \rangle$ denotes sequence numbers as in [33, §6.4]. We let $GNLA_{\mathbb{T}}$ be the set of Gödel numbers of nonlogical axioms of $\mathbb{T}$, $GTHM_{\mathbb{T}}$ be the set of Gödel numbers of theorems of $\mathbb{T}$, and $GFOR_{\mathbb{T}}$ be the set of Gödel numbers of formulas of $\mathbb{T}$ (equivalently, of formulas of $\mathscr{L}$). If $n \in GFOR_{\mathbb{T}}$, we let γ_n denote the formula with Gödel number n. Hence, $\ulcorner \gamma_n \urcorner = n$ for all $n \in GFOR_{\mathbb{T}}$ and, for each formula φ of $\mathbb{T}$,

$$\gamma_{\ulcorner \varphi \urcorner} \underset{\text{def}}{\equiv} \varphi.$$

Henceforth, we suppose that each theory $\mathbb{T}$ we consider has associated to it a fixed Gödel numbering obtained via the above construction.

Lemma 2.2.1.1 *Let $\mathbb{T}$ be a theory. Then, there exists a total recursive function $neg : \mathbb{N} \to \mathbb{N}$ such that*

$$neg(n) = \begin{cases} \ulcorner \neg \gamma_n \urcorner & \textit{if } GFOR_{\mathbb{T}}(n) \\ n & \textit{otherwise} \end{cases}$$

for all $n \in \mathbb{N}$. That is, $neg(n)$ is the Gödel number of the negation of the formula with Gödel number n if such a formula exists and n otherwise.

Now let $k \geq 0$, let $x_1, \ldots, x_k, y$ be fixed variables of $\mathbb{T}$, and let $\mathbf{x}$ denote the list $x_1, \ldots, x_k$ (if $k = 0$, we consider $\mathbf{x}$ as being omitted). Then, there exists a total recursive function $g : \mathbb{N}^{k+1} \to \mathbb{N}$ such that

$$g(\mathbf{m}, n) = \begin{cases} \ulcorner \gamma_n \left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}, \frac{\overline{n}}{y} \right] \urcorner & \textit{if } GFOR_{\mathbb{T}}(n) \\ n & \textit{otherwise} \end{cases}$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$. That is, $g(\mathbf{m}, n)$ is the Gödel number of $\gamma_n \left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}, \frac{\overline{n}}{y} \right]$ if γ_n exists and n otherwise.

Proof In order to construct the functions $neg : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N}^k \to \mathbb{N}$, we proceed similarly to the constructions in [33, §6.6]. Note first that we can proceed similarly to [33, §6.6, p. 124, D)] to show that $GFOR_{\mathbb{T}}$ is a total recursive predicate on $\mathbb{N}$. The function $neg : \mathbb{N} \to \mathbb{N}$ is then defined by

$$neg(n) = \begin{cases} \langle SN(\neg) \rangle * n & \text{if } GFOR_{\mathbb{T}}(n) \\ n & \text{otherwise} \end{cases}$$

for all $n \in \mathbb{N}$, where $\langle\cdot\rangle$ denotes sequence numbers as in [33, §6.4] and $* : \mathbb{N}^2 \to \mathbb{N}$ is the concatenation of sequences as defined on [33, §6.4, p. 117]. Then, since $GFOR_{\mathbb{T}}$ is a total recursive predicate and the functions relating to sequence numbers in [33, §6.4] are total recursive, $neg : \mathbb{N} \to \mathbb{N}$ as defined above is total recursive. Moreover, neg satisfies the desired property.

Now let $k \geq 0$ and fix $k+1$ variables $\mathbf{x}, y$ in $\mathbb{T}$. By extending and adapting the definition of the total recursive function $Sub : \mathbb{N}^3 \to \mathbb{N}$ in [33, §6.6, p. 124, E)], we can obtain a total recursive function $Sub_k : \mathbb{N}^{2k+3} \to \mathbb{N}$ such that

$$Sub_k(\ulcorner\varphi\urcorner, \ulcorner z_0\urcorner, \ldots \ulcorner z_k\urcorner, \ulcorner t_0\urcorner, \ldots, \ulcorner t_k\urcorner) = \ulcorner\varphi\left[\frac{t_0}{z_0}, \ldots \frac{t_k}{z_k}\right]\urcorner$$

for all formulas φ, (distinct) variables $z_0, \ldots, z_k$, and terms $t_0, \ldots, t_k$ in $\mathbb{T}$, and such that $Sub_k(n, \mathbf{m}, \mathbf{p}) = n$ if $n \notin GFOR_{\mathbb{T}}$. Then, we can define a total recursive function $g : \mathbb{N}^k \to \mathbb{N}$ satisfying the desired property by letting

$$g(\mathbf{m}, n) = Sub_k(n, \ulcorner x_1\urcorner, \ldots, \ulcorner x_k\urcorner, \ulcorner y\urcorner, \ulcorner\overline{m_1}\urcorner, \ldots, \ulcorner\overline{m_k}\urcorner, \ulcorner\overline{n}\urcorner)$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$. ■

As remarked at the beginning of Section A.2, a formal proof of a formula φ in a theory $\mathbb{T}$ is a finite sequence of formulas of $\mathbb{T}$ such that φ is the last formula in the sequence and each formula in the sequence is either an axiom of $\mathbb{T}$ or follows from one or more of the previous formulas by one of the rules of inference of $\mathbb{T}$. Since proofs in $\mathbb{T}$ are finite sequences of formulas of $\mathbb{T}$, each proof has a Gödel number, as we have extended Gödel numbering to finite sequences of formulas of $\mathbb{T}$. We wish to consider the so-called *proof predicate* on $\mathbb{T}$, which is a binary predicate on $\mathbb{T}$ that determines, for all $n, m \in \mathbb{N}$, whether or not m is the Gödel number of a proof of γ_n. However, note that while the functions in Lemma 2.2.1.1 are definable and total recursive for any first-order theory, this proof predicate is only total recursive when $\mathbb{T}$ has the additional property of being a recursively axiomatised theory.

Definition 2.2.1.2 (see also [33, pp. 125–126]) Let $\mathbb{T}$ be a theory, let $GNLA_{\mathbb{T}}$ be the set of Gödel numbers of the nonlogical axioms of $\mathbb{T}$, and let $GTHM_{\mathbb{T}}$ be the set of Gödel numbers of theorems of $\mathbb{T}$. We say that $\mathbb{T}$ is

(i) *finitely axiomatised* if $GNLA_{\mathbb{T}}$ is finite.

(ii) *primitive recursively axiomatised* if $GNLA_{\mathbb{T}}$ is primitive recursive.

(iii) *recursively axiomatised* if $GNLA_{\mathbb{T}}$ is total recursive.

(iv) an *r.e. theory* if $GTHM_{\mathbb{T}}$ is recursively enumerable.

The theory $\mathbb{T}'$ is an *r.e. extension* of $\mathbb{T}$ if $\mathbb{T}'$ is an extension of $\mathbb{T}$ and $\mathbb{T}'$ is an r.e. theory. □

Note that if $\mathbb{T}$ is finitely axiomatised, then $\mathbb{T}$ is (primitive) recursively axiomatised. We can now define the proof predicate of any recursively axiomatised theory $\mathbb{T}$.

Lemma 2.2.1.3 *Let $\mathbb{T}$ be a recursively axiomatised theory. Then, there exists a total recursive binary predicate $Pr \subseteq \mathbb{N}^2$ such that for all $n, m \in \mathbb{N}$,*

$$Pr(n, m) \text{ if and only if } GFOR_{\mathbb{T}}(n) \text{ and } m \text{ is the Gödel number of a proof of } \ulcorner \gamma_n \urcorner.$$

Pr is called the proof predicate *of $\mathbb{T}$. If $\mathbb{T}$ is primitive recursively axiomatised, then Pr is primitive recursive.*

PROOF The method in [33, §6.6, p. 126] can be adapted to show that such a total recursive proof predicate exists for each recursively axiomatised theory $\mathbb{T}$. The case when $\mathbb{T}$ is primitive recursively axiomatised is considered in [33, p. 137]. ■

As shown in [33, §6.6, p. 126], it follows from Lemma 2.2.1.3 that if $\mathbb{T}$ is a recursively axiomatised theory, then $\mathbb{T}$ is an r.e. theory. Indeed, if $\mathbb{T}$ is recursively axiomatised, then Pr is total recursive and we have that

$$GTHM_{\mathbb{T}}(n) \text{ if and only if there exists an } m \in \mathbb{N} \text{ such that } Pr(n, m)$$

for all $n \in \mathbb{N}$. Thus, $GTHM_{\mathbb{T}}$ is recursively enumerable by Proposition 2.1.3.3. Conversely, Craig's Lemma [8] states that any r.e. theory can be (primitive) recursively axiomatised. In other words, any r.e. theory is equivalent to a (primitive) recursively axiomatised theory.

2.2.2 Arithmetical theories

2.2.2.1 Definitions

Definition 2.2.2.1 Let $\mathscr{L}_{\mathbb{M}}$ be the first-order language with the following symbols:

(i) Predicate symbols: there are no nonlogical predicate symbols. The only predicate symbol of $\mathscr{L}_{\mathbb{M}}$ is the binary predicate symbol $=$ for equality that is present as a logical symbol in every first-order language.

(ii) Function symbols:

  (a) Individual constants (0-ary function symbols): 0 (zero)

  (b) Unary function symbols: S (successor)

  (c) Binary function symbols: $+$ (addition) and $\cdot$ (multiplication), both of which are placed in infix notation and associated to the left by default. □

Let $\mathscr{L}$ be any extension of $\mathscr{L}_{\mathbb{M}}$. Note that $+$ and $\cdot$ are by default associated to the left in terms of $\mathscr{L}$. Hence, for example, the term $(x+y)+z$ can be written as $x+y+z$, but no more parentheses can be omitted from the term $x \cdot (y \cdot z)$. Furthermore, if $t_1, \ldots, t_n$ are terms of $\mathscr{L}$, we can denote the term $t_1 + t_2 + \ldots t_n$, that is, the term $(\ldots((t_1+t_2)+t_3)+\ldots+t_n)$, by $\sum_{i=1}^{n} t_i$, and the term $t_1 \cdot \ldots \cdot t_n$ by $\prod_{i=1}^{n} t_i$.

We wish to consider theories in which we can formalise basic results of number theory. We first define a theory $\mathbb{M}$ that contains enough structure in order to consider the basic notions of number theory such as successors, addition, multiplication, and inequality and to ensure that some basic number-theoretic properties and results hold. For example, we wish to ensure that every variable, and hence every term, is either zero or a successor of another term. Since we wish to keep the theory as simple as possible without rendering proofs in the theory needlessly complicated, we have not included axioms for induction in $\mathbb{M}$, but have instead added some axioms in order to ensure directly that inequality works as expected in $\mathbb{M}$. This will also enable us to make a distinction between theories with induction and theories without induction. Note also that the axioms given for the theory $\mathbb{M}$ are largely inspired from the ones for Shoenfield's classical theory N for the natural numbers (see [33, p. 22]).

Definition 2.2.2.2 Let $\mathbb{M}$ be the theory over $\mathscr{L}_{\mathbb{M}}$ obtained by taking the following formulas as the nonlogical axioms.

(M1) $S(x) \neq 0$

(M2) $S(x) = S(y) \Rightarrow x = y$

(M3) $x + 0 = x$

(M4) $x + S(y) = S(x+y)$

(M5) $x \cdot 0 = 0$

(M6) $x \cdot S(y) = x + (x \cdot y)$

(M7) $x = 0 \vee (\exists y)(x = S(y))$

(M8) $(\exists w)(x + S(w) = y) \vee x = y \vee (\exists w)(y + S(w) = x)$

Let $\mathbb{M}_C$ be the classical version of $\mathbb{M}$, that is, $\mathbb{M}_C$ is the *classical* theory specified by taking (M1)–(M8) as the logical axioms ($\mathbb{M}_C$ is obtained from $\mathbb{M}$ by adding the axiom scheme (EM) – see Appendix A for more details). □

Note that $\mathbb{M}_C$ corresponds to Shoenfield's theory N for the natural numbers (see [33, p. 22]). Note also that $\mathbb{M}$ is finitely axiomatised and hence is both recursively axiomatised and an r.e. theory as remarked in Section 2.2.1.

We consider the theory $\mathbb{M}$ to be the theory having the minimal amount of structure for our purposes without creating unnecessary complications. Consequently, we define arithmetical theories to be extensions of $\mathbb{M}$, as these theories will then also contain sufficient structure in order to consider basic number theory.

Definition 2.2.2.3 (Arithmetical theory) A *(first-order) arithmetical theory* is any first-order theory $\mathbb{T}$ that is a consistent r.e. extension of $\mathbb{M}$. In particular, $\mathbb{M}$ is an r.e. theory as noted above and, since the standard model $\mathbb{N}$ is clearly a model of $\mathbb{M}$, $\mathbb{M}$ is consistent. Thus, $\mathbb{M}$ is a consistent r.e. extension of itself and hence an arithmetical theory.

An *intuitionistic arithmetical theory* is an intuitionistic theory $\mathbb{T}$ that is also an arithmetical theory (i.e. a consistent r.e. extension of $\mathbb{M}$). A *classical arithmetical theory* is a classical theory $\mathbb{T}$ that is also an arithmetical theory. Equivalently, a classical arithmetical theory is a theory $\mathbb{T}$ that is a consistent r.e. extension of $\mathbb{M}_C$. □

Since $\mathbb{M}$, as it is presented in Definition 2.2.2.2 above, is recursively axiomatised and any r.e. theory can be recursively axiomatised (see Section 2.2.1), we can assume without loss of generality that all arithmetical theories are recursively axiomatised. We then obtain a total recursive proof predicate for all arithmetical theories by Lemma 2.2.1.3, which will be useful in order to prove results in Section 2.4.4.

We shall introduce binary predicate symbols $<$ and $\leq$ for inequality as defined symbols in all arithmetical theories $\mathbb{T}$.

Definition 2.2.2.4 Let $\mathbb{T}$ be an arithmetical theory. We introduce the defined binary predicate symbols $<$ and $\leq$ in $\mathbb{T}$ via the following definitions:

> Let t, s be terms of $\mathbb{T}$. Then, we let $t < s$ abbreviate the formula
>
> $$(\exists w)(t + S(w) = s),$$
>
> where w is any new variable not occurring in either s or t, and we let $t \leq s$ abbreviate the formula
>
> $$t < s \vee t = s.$$

Note that, as in the case of unique existence, these abbreviations are only defined up to change of bound variables. However, this does not cause any problems since formulas are provably equivalent to any of their variants (see Appendix A). □

It follows that we may rewrite axiom (M8) using the new defined symbol $<$, thus obtaining

(M8) $x < y \vee x = y \vee y < x$.

Note that addition isn't commutative for variables in $\mathbb{M}$ (by a similar argument to the one in [2, p. 161]) and hence addition isn't commutative for variables in general in arithmetical theories. Consequently, we have defined the inequality symbol in an arithmetical theory as

$$t < s \underset{\text{def}}{\equiv} (\exists w)(t + S(w) = s)$$

and not as

$$t < s \underset{\text{def}}{\equiv} (\exists w)(S(w) + t = s)$$

because we need axiom (M4), which defines addition in arithmetical theories together with axiom (M3), to be compatible with the definition of $<$ and axiom (M4) is

$$x + S(y) = S(x + y)$$

and not

$$S(x) + y = S(x + y).$$

Furthermore, the definition of $<$ and $\leq$ given in Definition 2.2.2.4 corresponds to the one in [14, §39, p. 187].

In order to properly consider number theory in arithmetical theories, we need a notion of numerals.

Definition 2.2.2.5 Let $\mathscr{L}$ be a first-order language containing the unary function symbol S and the constant 0 (e.g. the language $\mathscr{L}_{\mathbb{M}}$ or any of its extensions). The term $S^k(0)$ of $\mathscr{L}$, obtained by applying S to 0 k times, is called the k^{th} *numeral* (of $\mathscr{L}$) and is denoted by $\overline{k}$.

More precisely, we have the following inductive definition:

(i) $S^0(0)$ is the term 0 and can also be denoted $\overline{0}$.

(ii) For all $m \in \mathbb{N}$, $S^{m+1}(0)$ is the term $S(\overline{m})$ and is denoted $\overline{m+1}$.

The numerals of $\mathscr{L}$ are then the terms $\overline{k}$ for all $k \in \mathbb{N}$. □

As mentioned in Section 2.1.1, we may use bold-face letters to denote sequences of variables or natural numbers. We may do the same for sequences of numerals in an arithmetical theory $\mathbb{T}$. For example, if we denote the sequence $n_1, \ldots, n_k$ of natural numbers by $\mathbf{n}$, then the corresponding sequence $\overline{n_1}, \ldots, \overline{n_k}$ of numerals is denoted by $\overline{\mathbf{n}}$.

Let $\mathbb{T}$ be any arithmetical theory. Note that we included axiom (M7) in the definition of $\mathbb{M}$ as we wished to ensure that every term in $\mathbb{T}$ was either equal to zero or was the successor of some other term, even in intuitionistic arithmetical theories. Indeed, it follows from axiom (M1) (without using axioms (M7)–(M8)) that

$$\vdash (\exists y)(x = S(y)) \Rightarrow x \neq 0 \tag{2.2.1}$$

holds in $\mathbb{T}$. Moreover, we can use induction on $m \in \mathbb{N}$ in order to show that the converse implication of (2.2.1) is provable for numerals, i.e. that for all $m \in \mathbb{N}$,

$$\vdash (\exists y)(\overline{m} = S(y)) \Leftrightarrow \overline{m} \neq 0$$

holds in $\mathbb{T}$. Again, this is provable without using axioms (M7)–(M8). However, in order to ensure that the converse implication of (2.2.1) is provable for variables in $\mathbb{T}$, i.e. that

$$\vdash (\exists y)(x = S(y)) \Leftrightarrow x \neq 0 \tag{2.2.2}$$

holds in $\mathbb{T}$, we need to either have induction on variables in $\mathbb{T}$ or have an axiom precisely for this purpose. Since we did not want all of our arithmetical theories to have induction, we chose the latter option instead. Hence, we included axiom (M7) in Definition 2.2.2.3, from which it follows that (2.2.2) holds in $\mathbb{T}$.

Axiom (M8) was included in the definition of $\mathbb{M}$ not only in order to resolve certain issues involving the definition of inequality, but also in order to ensure that the theory $\mathbb{M}_C$ was equivalent to Shoenfield's theory N [33, p. 22]. It is to be noted that axiom (M8), or some formula provably equivalent to axiom (M8), needs to be explicitly given as an axiom of $\mathbb{M}$ in order to ensure that (M8) is provable in any arithmetical theory. Indeed, as can be inferred from the discussion in [33, pp. 204–205], it is not possible to prove that (M8) follows from the axioms (M1)–(M7) in a general arithmetical theory $\mathbb{T}$ without some form of induction on variables in $\mathbb{T}$.

2.2.2.2 Basic results

We have the following basic results on numerals in arithmetical theories.

Lemma 2.2.2.6 *Let $\mathbb{T}$ be any arithmetical theory. Then, for all $m, n \in \mathbb{N}$:*

(i) If $m \neq n$, then $\vdash \overline{m} \neq \overline{n}$.

(ii) $\vdash \overline{m} = \overline{n}$ if and only if $m = n$

(iii) $\vdash \overline{m+n} = \overline{m} + \overline{n}$ and $\vdash \overline{m \cdot n} = \overline{m} \cdot \overline{n}$.

Since addition and multiplication are commutative, associative, distributive, and have units in $\mathbb{N}$, it follows by (ii) and (iii) that the same is provably true for numerals in $\mathbb{T}$.

Proof (i) See [33, p. 127] and [19, p. 158, Prop 3.6 (a)(i)].

(ii) If $m = n$, then $\overline{m}$ and $\overline{n}$ are the same term of $\mathbb{T}$, and so $\vdash \overline{m} = \overline{n}$ by (=-I). (ii) then follows from (i) and the consistency of $\mathbb{T}$.

(iii) See [19, p. 158, Prop 3.6 (a)(ii)]. ∎

Lemma 2.2.2.7 *Let $\mathbb{T}$ be an arithmetical theory.*

(i) Let $n \in \mathbb{N}$. Then, $\vdash x + \overline{n} = S^n(x)$, where we define $S^0(x)$ to be x and we define $S^n(x)$ inductively in the same way that $S^n(0)$ was defined in Definition 2.2.2.5.

(ii) $\vdash x \cdot \overline{n} = \sum_{i=1}^{n} x$. In particular, $\vdash x \cdot \overline{1} = x$.

PROOF (i) The result in obtained by induction on n, axioms (M4) and (M3), and Definition 2.2.2.5.

(ii) These results follow from the definition of addition and multiplication via axioms (M3)–(M6) and the fact that $+$ and $\cdot$ are associated to the left by default, as remarked following Definition 2.2.2.1. ∎

Although we can show that, in any arithmetical theory $\mathbb{T}$, $+$ and $\cdot$ have the usual properties of addition and multiplication (commutativity, associativity, distributivity, units, etc.) for numerals, the same is not necessarily true in general for variables. Indeed, as remarked previously, $+$ is not commutative in general for variables.

We now consider some useful basic results involving the inequality symbols that hold in any arithmetical theory.

Proposition 2.2.2.8 *Let $\mathbb{T}$ be an arithmetical theory.*

(L1) $\neg(x < 0)$

(L2) $\vdash x < S(y) \Leftrightarrow x \leq y$

(L3) For all $m \in \mathbb{N}$ such that $m > 0$,

$$\vdash x < \overline{m} \Leftrightarrow x = 0 \vee x = \overline{1} \vee \ldots \vee x = \overline{m-1}.$$

It thus follows that, for all $m \in \mathbb{N}$,

$$\vdash x < S(\overline{m}) \Leftrightarrow x = 0 \vee \ldots \vee x = \overline{m}.$$

(L4) For all $m \in \mathbb{N}$,

$$\vdash x \leq \overline{m} \Leftrightarrow x = 0 \vee \ldots \vee x = \overline{m}.$$

(L5) Both $<$ and $\leq$ are provably transitive in $\mathbb{T}$.

(L6) $\vdash x < S(x)$

(L7) $\vdash S(x) \leq y \Rightarrow x < y$

(L8) $\vdash 0 \leq x$ *and* $\vdash x \neq 0 \Leftrightarrow \overline{1} \leq x$

PROOF (L1) It follows from axiom (M4), axiom (M1), ($\exists$-E), and ($\neg$-I) that

$$\vdash \neg(\exists w)(x + S(w) = 0)$$

holds in $\mathbb{T}$. We thus have

$$\vdash \neg(x < 0)$$

by Definition 2.2.2.4, as required..

(L2) See [14, §39, Theorem 26, *138a.] and note that the induction axiom is not used to prove this result.

(L3) First note that if $m > 0$, then $m-1 \in \mathbb{N}$ and $\overline{m}$ is the term $S(\overline{m-1})$ by Definition 2.2.2.5. Hence, the first version follows from induction on $m \in \mathbb{N}$, (L2), and the Equivalence Theorem (Theorem A.3.0.7) applied during the induction step. The second version then follows from the fact that $S(m)$ is the term $\overline{m+1}$ and that $m+1 > 0$ for all $m \in \mathbb{N}$.

(L4) The case for $m = 0$ follows from (L1) and ($\vee$-E). The case for $m > 0$ follows from (L3) by the Equivalence Theorem.

(L5) See [14, §39, Theorem 26, *134a.–d.] and note that the induction axiom is not used to prove these results.

(L6) By (M3), we obtain

$$\vdash x + 0 = x,$$

from which it follows by (M4) that

$$\vdash x + S(0) = S(x).$$

Hence, we obtain

$$\vdash (\exists w)(x + S(w) = S(x)),$$

that is,

$$\vdash x < S(x),$$

by ($\exists$-I).

(L7) Since $\vdash x < S(x)$ by (L6), we obtain $\vdash S(x) = y \Rightarrow x < y$. Since, in addition, $<$ is transitive by (L5), we obtain $\vdash S(x) < y \Rightarrow x < y$. Hence, $\vdash S(x) \leq y \Rightarrow x < y$ follows by ($\vee$-E) and ($\Rightarrow$-I).

(L8) We obtain

$$\vdash 0 \leq x$$

from (L1), (M8), and ($\vee$-E).

Towards proving the second result, we first obtain

$$x \neq 0, x < \overline{1} \vdash x = 0$$

by (L3), from which it follows that

$$x \neq 0 \vdash \neg(x < \overline{1}).$$

Since we also have

$$\vdash \overline{1} \leq x \vee x < \overline{1}$$

by (M8) and the associativity of $\vee$, it thus follows by ($\vee$-E) that

$$x \neq 0 \vdash \overline{1} \leq x.$$

Conversely, we obtain

$$\overline{1} \leq x, \overline{1} + S(a) = x \stackrel{a}{\vdash} S(\overline{1} + a) = x$$

by (M4), from which it follows by (M1), ($\exists$-E), and the definition of $<$ that

$$\overline{1} \leq x \vdash x \neq 0.$$

Hence, we obtain

$$\vdash x \neq 0 \Leftrightarrow \overline{1} \leq x$$

as required. ■

2.2.2.3 Arithmetical theories with induction

In general, there is no induction on variables in the arithmetical theories given by Definition 2.2.2.3. However, in order to have an arithmetical theory corresponding to Peano arithmetic in the classical case and Heyting arithmetic in the intuitionisic case, we need to add induction on variables. We define the theory $\mathbb{H}$ for arithmetic following the construction of Shoenfield's theory P [33, p. 204], Mendelson's theory S [19, p. 150], and Kleene's formal system for number theory [14, §19].

Definition 2.2.2.9 Let $\mathbb{H}$ be the intuitionistic theory over the language $\mathscr{L}_{\mathbb{M}}$ with the nonlogical axioms (M1)–(M8) of $\mathbb{M}$ and the following infinite axiom scheme for induction: for every formula A of $\mathscr{L}_{\mathbb{M}}$,

$$\text{(IND)} \quad \left(A\left[\tfrac{0}{x}\right] \wedge (\forall x)\left(A \Rightarrow A\left[\tfrac{S(x)}{x}\right]\right)\right) \Rightarrow A. \qquad \square$$

Note that the standard model $\mathbb{N}$ is a model for $\mathbb{H}$ and hence $\mathbb{H}$ is consistent. Note also that, as remarked in the proof of Lemma 2.2.1.1, the set $GFOR_{\mathbb{H}}$ of Gödel numbers of formulas of $\mathbb{H}$ is recursively enumerable. Since the axiom scheme (IND) is indexed by the formulas of $\mathbb{H}$ as defined above, we can thus follow a procedure similar to the one in [33, §6.6] (where certain sets of formulas are shown to be total recursive) in order to show that the set of Gödel numbers of the formulas in the axiom scheme (IND) is total recursive. It thus follows that the set $GNLA_{\mathbb{H}}$ of Gödel numbers of nonlogical axioms of $\mathbb{H}$ is total recursive, that is, that $\mathbb{H}$ is recursively axiomatised. Hence, as remarked in Section 2.2.1, it follows that $\mathbb{H}$ is an r.e. theory, and so $\mathbb{H}$ is in fact an arithmetical theory as in Definition 2.2.2.3. Furthermore, the classical theory

$\mathbb{H}_C$ obtained from $\mathbb{H}$ corresponds to Shoenfield's theory P for Peano arithmetic [33, p. 204] and $\mathbb{H}$ itself corresponds to Heyting arithmetic. The theories $\mathbb{H}$ and $\mathbb{H}_C$ also correspond to the intuitionistic and classical versions of Kleene's formal system for number theory defined in [14, Ch. IV].

Definition 2.2.2.10 If $\mathbb{T}$ is a consistent recursively enumerable extension of $\mathbb{H}$, then $\mathbb{T}$ is said to be an *arithmetical theory with induction*, or to *have induction*. Equivalently, an arithmetical theory $\mathbb{T}$ has induction if and only if all of the formulas in the scheme (IND) are provably true in $\mathbb{T}$. □

Note that $\mathbb{H}$ is itself an arithmetical theory with induction. Moreover, since $\mathbb{H}$ is also an arithmetical theory as defined in Definition 2.2.2.3, the same is true for any consistent r.e. extension of $\mathbb{H}$. That is to say, all arithmetical theories with induction defined in Definition 2.2.2.10 are in particular arithmetical theories as in Definition 2.2.2.3.

In order to use the axiom (IND) in practice, we have the following derived rule, the proof of which is self-evident, in any arithmetical theory with induction.

Lemma 2.2.2.11 *Let $\mathbb{T}$ be an arithmetical theory with induction, let A be a formula of $\mathbb{T}$, and let Γ be any finite set of formulas of $\mathbb{T}$. Then,*

$$\textit{if } \Gamma \vdash A\left[\tfrac{0}{x}\right] \textit{ and } \vdash A \Rightarrow A\left[\tfrac{S(x)}{x}\right], \textit{ then } \vdash A.$$

This rule will be referred to as induction (on variables) *in $\mathbb{T}$ or sometimes as (IND).*

Using induction on variables, most basic results of number theory can be formalised in any arithmetical theory with induction, although it is important to verify if the results are intuitionistically valid or not. Adapting the arguments in [19] and [14], we obtain the following results.

Note first that since the postulates for number theory given in [14, Ch. IV, §19] hold in any arithmetical theory with induction, the results on induction, equality, arithmetic laws, and order properties in [14, Ch. VIII, §38–39] hold in any arithmetical theory with induction. We present some of these results in Proposition 2.2.2.12.

Proposition 2.2.2.12 *Let $\mathbb{T}$ be an arithmetical theory with induction. The following results hold in $\mathbb{T}$.*

(i) On variables, $+$ and $\cdot$ have units 0 and $\overline{1}$, respectively, and are commutative, associative, and distributive.

(ii) The cancellation law for addition:

$$\vdash (x + z = y + z) \Rightarrow x = y.$$

(iii) The cancellation law for multiplication:

$$\vdash z \neq 0 \wedge (x \cdot z = y \cdot z) \Rightarrow x = y.$$

(iv) The following results involving the order relation in $\mathbb{T}$*:*

$$\begin{aligned}
&\vdash \neg(x < x) \\
&\vdash S(x) \leq y \Leftrightarrow x < y \\
&\vdash \neg(x < y \wedge y < x) \\
&\vdash \neg(x < y) \Leftrightarrow y \leq x \\
&\vdash x < y \Leftrightarrow \neg(y \leq x) \\
&\vdash x \leq x + y \\
&\vdash x \neq 0 \Rightarrow y \leq y \cdot x
\end{aligned}$$

(v) $\vdash \neg(\exists y)(x < y \wedge y < S(x))$

PROOF Parts (i)–(iii) hold by [14, Ch. VIII, §39, Thm 25] and part (iv) holds by [14, Ch. VIII, §39, Thm 26]. Part (v) is proved using the fifth result in part (iv), (L2) from Proposition 2.2.2.8, (¬-I), and (∃-E). ■

By Proposition 2.2.2.12 and the remaining results in [14, Ch. VIII, §38–39], it follows that most basic number-theoretic results concerning the natural numbers endowed with the usual ordering are provable for variables in any arithmetical theory with induction, provided that they are intuitionistically valid. We shall generally refer to Proposition 2.2.2.12 when using this fact.

2.3 Notions of representability of numerical functions and predicates in arithmetical theories

The notion of representability of total functions and predicates has been considered quite frequently in the literature (see for example [31, 16, 19, 26, 25, 33, 2]). The notion of representability of partial functions and recurslively enumerable predicates has also been considered, albeit less frequently (see for example [25, 31, 24, 32]). It turns out that, although the presentation and terminology used for notions of representability of numerical functions and predicates in first-order theories vary in the literature, these notions are generally equivalent to one of the notions of representability given in Definition 2.3.1.1 and Definition 2.3.2.1, thus motivating our choice of definitions.

2.3.1 Representability of numerical functions

We define the representability of partial functions in an arithmetical theory based on the various notions of representability of total and partial functions defined in [31, 16, 19, 26, 25, 14].

Definition 2.3.1.1 Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. For $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ any partial function and $\varphi(\mathbf{x}, y)$ any formula of $\mathbb{T}$ with exactly $k+1$ free variables, we define the following four conditions for representability:

(P1) For all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$, $f(\mathbf{m}) \simeq n$ if and only if $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$.

(P2) For all $\mathbf{m} \in \mathbb{N}^k$, $\vdash \varphi(\overline{\mathbf{m}}, y) \wedge \varphi(\overline{\mathbf{m}}, z) \Rightarrow y = z$.

(P3) $\vdash \varphi(\mathbf{x}, y) \wedge \varphi(\mathbf{x}, z) \Rightarrow y = z$.

(P4) $\vdash (\exists y)\varphi(\mathbf{x}, y)$.

For the partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, if there exists a formula $\varphi(\mathbf{x}, y)$ in $\mathbb{T}$ with exactly $k+1$ free variables such that

(i) conditions (P1) and (P2) hold, then f is *numeralwise representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x}, y)$);

(ii) conditions (P1) and (P3) hold, then f is *type-one representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x}, y)$);

(iii) conditions (P1), (P3), and (P4) hold, then f is *strongly representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x}, y)$). □

Note that a formula $\varphi(\mathbf{x}, y)$ of an arithmetical theory $\mathbb{T}$ with exactly $k+1$ free variables satisfies both of conditions (P3) and (P4) if and only if it satisfies the condition

(P4') $\vdash (\exists! y)\varphi(\mathbf{x}, y)$.

Hence, the following result follows immediately.

Lemma 2.3.1.2 *Let $\mathbb{T}$ be an arithmetical theory, let $k \geq 0$, and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial function. Then, a formula $\varphi(\mathbf{x}, y)$ of $\mathbb{T}$ with exactly $k+1$ free variables strongly represents f in $\mathbb{T}$ if and only if $\varphi(\mathbf{x}, y)$ satisfies conditions (P1) and (P4').*

Remark 2.3.1.3 (Conventions for variables in representing formulas) We use the following conventions concerning (candidates for) representing formulas in an arithmetical theory $\mathbb{T}$.

(i) If $\mathbf{x}$ is a list of variables, $|\mathbf{x}|$ denotes its length. It is understood that any lists of variables are of the appropriate length given the context.

(ii) We allow the use of logical connectives, quantifiers and equality to be used with lists of variables, with the understanding that everything is defined componentwise, and, in the case of equality, that the lists have the same length. For example, if $\mathbf{x}, \mathbf{y}$ represent the lists $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ of variables respectively, then $(\forall \mathbf{x})$ denotes $(\forall x_1) \ldots (\forall x_n)$ and $\mathbf{x} = \mathbf{y}$ denotes $x_1 = y_1 \wedge \ldots \wedge x_n = y_n$. See Appendix A for more details.

(iii) Although we usually write $\varphi(\mathbf{x})$ to mean that the free variables of the formula $\varphi(\mathbf{x})$, if any, are *among* the variables in the list $\mathbf{x}$, if $\varphi(\mathbf{x})$ is a (candidate for) a representing formula of some partial function, we use the convention that the free variables of $\varphi(\mathbf{x})$ are *exactly* the variables in the list $\mathbf{x}$ unless specified otherwise. However, we may always omit the list of free variables and simply refer to $\varphi(\mathbf{x})$ as φ; this does not mean that φ is a closed formula (i.e. that φ has no free variables).

(iv) We consider formulas of a theory $\mathbb{T}$ to be equal up to change of bound variables.

(v) Once a (representing) formula $\varphi(\mathbf{x})$ has been specified together with its list of free variables $\mathbf{x}$, we use the usual convention that $\varphi(\mathbf{u})$ denotes $\varphi\left[\frac{\mathbf{u}}{\mathbf{x}}\right]$ for any list of variables $\mathbf{u}$ such that $|\mathbf{u}| = |\mathbf{x}|$ (note that the variables in the list $\mathbf{u}$ need not be pairwise distinct from each other or from the variables in the list $\mathbf{x}$). In this situation, we assume that $\mathbf{u}$ is free for $\mathbf{x}$ in φ (that is, that the substitution $\varphi\left[\frac{\mathbf{u}}{\mathbf{x}}\right]$ is possible) as we can always change the bound variables of $\varphi(\mathbf{x})$ if necessary by part (iv). Moreover, by Remark A.3.0.8, if $\varphi(\mathbf{x})$ numeralwise, type-one, or strongly represents some partial function f in $\mathbb{T}$, then the same is true for $\varphi(\mathbf{u})$ for any list $\mathbf{u}$ of distinct variables such that $|\mathbf{x}| = |\mathbf{u}|$. □

When considering total functions, it suffices to use a weaker version of condition (P1). Moreover, it is not necessary to use Kleene equality in the case of total functions.

Lemma 2.3.1.4 *Let $\mathbb{T}$ be an arithmetical theory, let $k \geq 0$, let $f : \mathbb{N}^k \to \mathbb{N}$ be a total function, and let $\varphi(\mathbf{x}, y)$ be a formula of $\mathbb{T}$ with exactly $k+1$ free variables. We consider two alternate conditions for representability:*

(P1') For all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$, if $f(\mathbf{m}) = n$, then $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$.

(P2') For all $\mathbf{m} \in \mathbb{N}^k$, $\vdash (\exists! y)\varphi(\overline{\mathbf{m}}, y)$.

Then,

(i) if one of conditions (P2) and (P3) holds, then condition (P1) holds if and only if condition (P1') holds;

(ii) f is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$ if and only if conditions (P1') and (P2') hold.

Hence, when considering the representability of total functions, we can replace condition (P1) by condition (P1').

Proof (i) Suppose that one of conditions (P2) and (P3) holds for f and $\varphi(\mathbf{x}, y)$. Note that condition (P1) clearly implies condition (P1'). Now suppose that condition (P1') is satisfied. It remains to show that, for all $\mathbf{m} \in \mathbb{N}^k$, if $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$, then $f(\mathbf{m}) = n$. So, let $\mathbf{m} \in \mathbb{N}^k$ and suppose that $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$ holds. Since f

is total, $f(\mathbf{m})$ is defined, and so $\vdash \varphi(\overline{\mathbf{m}}, \overline{f(\mathbf{m})})$ by condition (P1'). Hence, it follows by either one of conditions (P2) and (P3) that $\vdash \overline{f(\mathbf{m})} = \overline{n}$. It then follows by Lemma 2.2.2.6 that $f(\mathbf{m}) = n$. Hence, condition (P1) is satisfied.

(ii) Suppose that f is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$. By part (i), condition (P1') is satisfied. Let $\mathbf{m} \in \mathbb{N}^k$. By condition (P1'), $\vdash \varphi(\overline{\mathbf{m}}, \overline{f(\mathbf{m})})$, and so $\vdash (\exists y)\varphi(\overline{\mathbf{m}}, y)$ follows by ($\exists$-I). Hence, we obtain $\vdash (\exists! y)\varphi(\overline{\mathbf{m}}, y)$ by condition (P2), ($\forall$-I), and ($\wedge$-I). Hence, condition (P2') is also satisfied.

Suppose conversely that conditions (P1') and (P2') hold. By part (i), condition (P1) holds. Furthermore, condition (P2) follows from condition (P2') by ($\wedge$-E) and ($\forall$-E). Hence, f is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$. ■

Hence, when considering the representability of total functions, we shall generally use condition (P1') instead of condition (P1).

It follows from Lemma 2.3.1.4 that, when we are considering total functions, the notions of numeralwise and strong representability defined in Definition 2.3.1.1 are equivalent to the notions of numeralwise and strong representability in [16, 19], although in [19] numeralwise representability is simply called "representability" instead. Indeed, in [16, 19], numeralwise representability is defined using conditions (P1') and (P2') and strong representability is defined using conditions (P1') and (P4'). The three notions of representability in Definition 2.3.1.1 correspond to the homonymous notions in [25], although the representability conditions in Definition 2.3.1.1 are not formulated in exactly the same way as the ones in [25]. Shoenfield does not consider the representability of partial functions and his notion of representability of total functions (see [33]) is presented somewhat differently to what is found in [16, 19, 25].

Lemma 2.3.1.5 *Let $\mathbb{T}$ be an arithmetical theory and let $\varphi(\mathbf{x}, y)$ be a formula of $\mathbb{T}$ with exactly $k+1$ free variables. Then, condition (P3) implies condition (P2). Hence, if a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is strongly representable in $\mathbb{T}$ by a formula $\varphi(\mathbf{x}, y)$, then f is also type-one and numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$. Similarly, if f is type-one representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$, f is also numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$.*

Proof We obtain condition (P2) from condition (P3) by the Substitution Theorem (Theorem A.3.0.6). The remainder of the statement clearly follows from this fact and Definition 2.3.1.1. ■

Proposition 2.3.1.6 *Let $\mathbb{T}$ be an arithmetical theory, $k \geq 0$, $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ a partial function, and $\varphi(\mathbf{x}, y)$ and $\psi(\mathbf{x}, y)$ two formulas of $\mathbb{T}$ containing free exactly the same $k+1$ free variables. If $\vdash \varphi(\mathbf{x}, y) \Leftrightarrow \psi(\mathbf{x}, y)$, then any one of the conditions (P1)–(P4) is true for $\varphi(\mathbf{x}, y)$ if and only if the same condition is true for $\psi(\mathbf{x}, y)$. Consequently, $\varphi(\mathbf{x}, y)$ numeralwise (type-one, strongly, resp.) represents f in $\mathbb{T}$ if and only if the same is true for $\psi(\mathbf{x}, y)$.*

By Remark 2.3.1.3, it follows that the above statement also holds if we replace $\psi(\mathbf{x}, y)$ by $\psi(\mathbf{u}, v)$ where $\mathbf{u}, v$ is any list of $k+1$ distinct variables.

PROOF This result follows from the Equivalence Theorem (Theorem A.3.0.7) and the Substitution Theorem (Theorem A.3.0.6). ∎

2.3.2 Representability of predicates

We can also define a notion of representability of predicates in arithmetical theories. The following definitions are adapted from [24, 32, 25, 33], albeit with a change in terminology.

Definition 2.3.2.1 Let $\mathbb{T}$ be an arithmetical theory and $k \geq 0$. For $E \subseteq \mathbb{N}^k$ any k-ary predicate on $\mathbb{N}$ and $\varphi_E(\mathbf{x})$ any formula in $\mathbb{T}$ with exactly k free variables, we define the following conditions for representability:

(A) For all $\mathbf{m} \in \mathbb{N}^k$, $E(\mathbf{m})$ if and only if $\vdash \varphi_E(\overline{\mathbf{m}})$.

(B) For all $\mathbf{m} \in \mathbb{N}^k$,

if $E(\mathbf{m})$, then $\vdash \varphi_E(\overline{\mathbf{m}})$; and

if $\neg E(\mathbf{m})$, then $\vdash \neg\varphi_E(\overline{\mathbf{m}})$.

(C) $\vdash \varphi_E(\mathbf{x}) \vee \neg\varphi_E(\mathbf{x})$

For the predicate $E \subseteq \mathbb{N}^k$, if there exists a formula $\varphi(\mathbf{x})$ in $\mathbb{T}$ with exactly k free variables such that

(i) condition (A) is satisfied, then E is *weakly representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x})$);

(ii) condition (B) is satisfied, then E is *numeralwise representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x})$);

(iii) conditions (B) and (C) are satisfied, then E is *strongly representable* in $\mathbb{T}$ (by $\varphi(\mathbf{x})$). □

Note that the conventions in Remark 2.3.1.3 also apply to (candidates for) representing formulas of predicates.

Lemma 2.3.2.2 *Let $k \geq 0$, let E be a k-ary relation on $\mathbb{N}$, let $K_E : \mathbb{N}^k \to \mathbb{N}$ be the characteristic function of E, and let $\mathbb{T}$ be an arithmetical theory.*

(i) If E is strongly representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$, then E is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$.

(ii) If E is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$, then E is weakly representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$.

(iii) The following statements are equivalent:

(a) E is numeralwise representable in $\mathbb{T}$.

(b) K_E *is type-one representable in* $\mathbb{T}$.

(c) K_E *is numeralwise representable in* $\mathbb{T}$.

(iv) E *is strongly representable in* $\mathbb{T}$ *if and only if* K_E *is strongly representable in* $\mathbb{T}$.

(v) If $\mathbb{T}$ *is classical and* E *is numeralwise representable in* $\mathbb{T}$ *by* $\varphi(\mathbf{x})$*, then* E *is also strongly representable in* $\mathbb{T}$ *by* $\varphi(\mathbf{x})$.

Note that the results in parts (iii) and (iv) above motivate choice of terminology for the representability of predicates in Definition 2.3.2.1.

Proof (i) If E is strongly representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$, then condition (B) is satisfied and so E is also numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$.

(ii) Condition (A) follows from condition (B) by the consistency of $\mathbb{T}$. Therefore, if E is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$, it follows that E is weakly representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$.

(iii) Recall that the characteristic function $K_E : \mathbb{N}^k \to \mathbb{N}$ of E is defined by

$$K_E(\mathbf{m}) = \begin{cases} 0 & \text{if } E(\mathbf{m}) \\ 1 & \text{if } \neg E(\mathbf{m}) \end{cases}$$

for all $\mathbf{m} \in \mathbb{N}^k$.

(a) $\Rightarrow$ (b): Suppose that E is numeralwise representable in $\mathbb{T}$ by the formula $\varphi(\mathbf{x})$ and define

$$\varphi'(\mathbf{x}, y) \underset{\text{def}}{\equiv} (\varphi(\mathbf{x}) \wedge y = 0) \vee (\neg\varphi(\mathbf{x}) \wedge y = \overline{1}).$$

We show that $\varphi'(\mathbf{x}, y)$ type-one represents K_E in $\mathbb{T}$. Let $\mathbf{m} \in \mathbb{N}^k$ and $n = K_E(\mathbf{m})$. If $E(\mathbf{m})$, then $n = K_E(\mathbf{m}) = 0$ and $\vdash \varphi(\overline{\mathbf{m}})$ by condition (B) for the representability of E. Since $\vdash \overline{n} = 0$ by Lemma 2.2.2.6, we obtain $\vdash \varphi'(\overline{\mathbf{m}}, \overline{n})$ by ($\wedge$-I) and ($\vee$-I). If $\neg E(\mathbf{m})$, then $n = K_E(\mathbf{m}) = 1$ and we have $\vdash \neg\varphi(\overline{\mathbf{m}}) \wedge \overline{n} = \overline{1}$ by condition (B) for the representability of E and Lemma 2.2.2.6. Hence, we again obtain $\vdash \varphi'(\overline{\mathbf{m}}, \overline{n})$, and so condition (P1') for the representability of K_E is satisfied. Towards condition (P3) for $\varphi'(\mathbf{x}, y)$, note that $\varphi(\mathbf{x})$ and $\neg\varphi(\mathbf{x})$ cannot both be true simultaneously as $\mathbb{T}$ is consistent. Hence, we obtain that

$$\varphi'(\mathbf{x}, y) \wedge \varphi'(\mathbf{x}, z) \vdash (\varphi(\mathbf{x}) \wedge y = 0 \wedge z = 0) \vee (\neg\varphi(\mathbf{x}) \wedge y = \overline{1} \wedge z = \overline{1})$$

by the definition of φ', ($\vee$-E), and the rules for conjunction in $\mathbb{T}$. It thus follows by ($\vee$-E), (=-E), and ($\Rightarrow$-I) that

$$\vdash \varphi'(\mathbf{x}, y) \wedge \varphi'(\mathbf{x}, z) \Rightarrow y = z,$$

and so condition (P3) for $\varphi'(\mathbf{x}, y)$ is satisfied. Hence, $\varphi'(\mathbf{x}, y)$ type-one represents K_E in $\mathbb{T}$.

(b) $\Rightarrow$ (c): As shown in Lemma 2.3.1.5, if K_E is type-one representable in $\mathbb{T}$, then K_E is also numeralwise representable in $\mathbb{T}$.

(c) $\Rightarrow$ (a): Suppose that K_E is numeralwise representable in $\mathbb{T}$ by a formula $\psi(\mathbf{x}, y)$. We show that the formula $\psi(\mathbf{x}, 0)$ numeralwise represents E in $\mathbb{T}$. Let $\mathbf{m} \in \mathbb{N}^k$ and suppose that $E(\mathbf{m})$. Then, $K_E(\mathbf{m}) = 0$, and so we obtain $\vdash \psi(\overline{\mathbf{m}}, 0)$ by condition (P1') for ψ. Now suppose instead that $\neg E(\mathbf{m})$. Then, $K_E(\mathbf{m}) = 1$, and so we obtain $\vdash \psi(\overline{\mathbf{m}}, \overline{1})$ by condition (P1') for ψ. It then follows by condition (P2) for ψ that

$$\psi(\overline{\mathbf{m}}, 0) \vdash 0 = \overline{1},$$

from which it follows by axiom (M1) and ($\perp$-I) that

$$\psi(\overline{\mathbf{m}}, 0) \vdash \perp.$$

Hence, we obtain $\vdash \neg\psi(\overline{\mathbf{m}}, 0)$ by ($\neg$-I). Therefore, the formula $\psi(\mathbf{x}, 0)$ satisfies condition (B) and so numeralwise represents E in $\mathbb{T}$.

(iv) Suppose that $\varphi(\mathbf{x})$ strongly represents E in $\mathbb{T}$ and define

$$\varphi'(\mathbf{x}, y) \underset{\text{def}}{\equiv} (\varphi(\mathbf{x}) \wedge y = 0) \vee (\neg\varphi(\mathbf{x}) \wedge y = \overline{1})$$

as in the proof of part (iii). We wish to show that $\varphi'(\mathbf{x}, y)$ strongly represents K_E in $\mathbb{T}$. The arguments showing that part (iii) (a) implies part (iii) (b) once more show that $\varphi'(\mathbf{x})$ satisfies conditions (P1') and (P3). It remains to show that condition (P4) is satisfied for $\varphi'(\mathbf{x})$. Since $\varphi(\mathbf{x})$ strongly represents E in $\mathbb{T}$, condition (C) for $\varphi(\mathbf{x})$, namely

$$\vdash \varphi(\mathbf{x}) \vee \neg\varphi(\mathbf{x}),$$

holds in $\mathbb{T}$. Moreover, we obtain

$$\varphi(\mathbf{x}) \vdash \varphi'(\mathbf{x}, 0)$$

by (=-I), ($\wedge$-I), and ($\vee$-I), from which it follows by ($\exists$-I) that

$$\varphi(\mathbf{x}) \vdash (\exists y)\varphi'(\mathbf{x}, y).$$

Similarly, we obtain

$$\neg\varphi(\mathbf{x}) \vdash (\exists y)\varphi'(\mathbf{x}, y),$$

and so it follows by condition (C) for $\varphi(\mathbf{x})$ and ($\vee$-E) that

$$\vdash (\exists y)\varphi'(\mathbf{x}, y)$$

holds in $\mathbb{T}$. Hence, condition (P4) holds for $\varphi'(\mathbf{x}, y)$, and so $\varphi'(\mathbf{x}, y)$ indeed strongly represents K_E in $\mathbb{T}$.

Conversely, suppose that K_E is strongly representable in $\mathbb{T}$ by a formula $\psi(\mathbf{x}, y)$. We show that the formula $\psi(\mathbf{x}, 0)$ strongly represents E in $\mathbb{T}$. As in the proof that part (iii) (c) implies part (iii) (a), we have that $\psi(\mathbf{x}, 0)$ satisfies condition (B) for the representability of E. Furthermore, we have $\vdash (\exists y)\psi(\mathbf{x}, y)$ by condition (P4) for ψ, from which we obtain $\overset{a}{\vdash} \psi(\mathbf{x}, a)$ for some a. By (DE), we have $\overset{a}{\vdash} a = 0 \vee a \neq 0$ for this a, and hence $\vdash \psi(\mathbf{x}, 0) \vee \neg\psi(\mathbf{x}, 0)$ is obtained by using condition (P3) for ψ. Thus, condition (C) for $\psi(\mathbf{x}, 0)$ holds, and so $\psi(\mathbf{x}, 0)$ strongly represents E in $\mathbb{T}$.

(v) Suppose that $\mathbb{T}$ is classical and that E is numeralwise representable in $\mathbb{T}$ by $\varphi(\mathbf{x})$. Since $\mathbb{T}$ is classical, we thus obtain

$$\vdash \varphi(\mathbf{x}) \vee \neg\varphi(\mathbf{x})$$

by (EM), and so condition (C) for $\varphi(\mathbf{x})$ is satisfied. Hence, $\varphi(\mathbf{x})$ in fact strongly represents E in $\mathbb{T}$. ■

Definition 2.3.2.3 Let $\mathbb{T}$ be an arithmetical theory and let $E_1, E_2 \subseteq \mathbb{N}^k$ be two predicates. We say that E_1, E_2 are *exactly separable in* $\mathbb{T}$ if there exists a formula $\varphi(\mathbf{x})$ with exactly k free variables such that $\varphi(\mathbf{x})$ and $\neg\varphi(\mathbf{x})$ weakly represent E_1 and E_2 in $\mathbb{T}$, respectively. In this case, we say that $\varphi(\mathbf{x})$ *exactly separates* E_1 *and* E_2 *in* $\mathbb{T}$.

Using the definition of weak representability of predicates from Definition 2.3.2.1, we obtain that $\varphi(\mathbf{x})$ exactly separates E_1 and E_2 in $\mathbb{T}$ if and only if, for all $\mathbf{m} \in \mathbb{N}^k$,

$E_1(\mathbf{m})$ if and only if $\vdash \varphi(\overline{\mathbf{m}})$; and
$E_2(\mathbf{m})$ if and only if $\vdash \neg\varphi(\overline{\mathbf{m}})$. □

Note that since $\mathbb{T}$ is consistent, we cannot have both of $\vdash \varphi(\overline{\mathbf{m}})$ and $\vdash \neg\varphi(\overline{\mathbf{m}})$ for the same $\mathbf{m} \in \mathbb{N}^k$. Hence, for two relations to be exactly separable in $\mathbb{T}$, they must at the very least be disjoint.

We have an analogous result to Proposition 2.3.1.6 for representing formulas of predicates which is proved in the same way as Proposition 2.3.1.6.

Proposition 2.3.2.4 *Let* $\mathbb{T}$ *be an arithmetical theory and let* $k \geq 0$.

(i) Let E *be a* k*-ary predicate on* $\mathbb{N}$ *and let* $\varphi(\mathbf{x})$ *and* $\psi(\mathbf{x})$ *be two formulas of* $\mathbb{T}$ *containing free exactly the same* k *variables. Then,* $\varphi(\mathbf{x})$ *weakly (numeralwise, strongly, resp.) represents* E *in* $\mathbb{T}$ *if and only if the same is true for* $\psi(\mathbf{x})$.

(ii) Let E_1, E_2 *be two* k*-ary predicates on* $\mathbb{N}$ *and let* $\varphi(\mathbf{x})$ *and* $\psi(\mathbf{x})$ *be two formulas of* $\mathbb{T}$ *containing free exactly the same* k *variables. Then,* $\varphi(\mathbf{x})$ *exactly separates* E_1 *and* E_2 *in* $\mathbb{T}$ *if and only if the same is true for* $\psi(\mathbf{x})$.

2.3.3 The consequences of the Existence Property

In classical arithmetical theories, the different notions of representability turn out to be essentially interchangeable. Indeed, it is shown in [19, §3.2] that a total recursive function is numeralwise representable in a classical arithmetical theory if and only if it is strongly representable in this theory. Similarly, it is shown in [25, §3] that a partial recursive function is numeralwise representable if and only if it is type-one representable if and only if it is strongly representable in a classical arithmetical theory.

This is not the case for intuitionistic arithmetical theories however. In an intuitionistic arithmetical theory $\mathbb{T}$, the subclasses of partial recursive functions that are numeralwise, type-one, and strongly representable in $\mathbb{T}$ do not necessarily coincide, and hence there is an actual distinction between the different notions of representability in intuitionistic arithmetical theories. Therefore, as shown in Section 2.4, the classes of representable partial functions may differ between intuitionistic and classical arithmetical theories for certain kinds of representability.

This difference between intuitionistic and classical arithmetical theories is due to the Existence Property, which is satisfied in an arithmetical theory if and only if it is intuitionistic (see Theorem 2.3.3.6). Thus, we consider here how the Existence Property being satisfied or not affects the representability of partial functions in an arithmetical theory.

Definition 2.3.3.1 Let $\mathbb{T}$ be an arithmetical theory. Then, $\mathbb{T}$ is said to *satisfy the Existence Property* if the following property holds for $\mathbb{T}$:

(EP) For every formula φ in $\mathbb{T}$ and every variable x, if $\vdash (\exists x)\varphi$, then there exists an $n \in \mathbb{N}$ such that $\vdash \varphi\left[\frac{\overline{n}}{x}\right]$. □

Lemma 2.3.3.2 *Let $\mathbb{T}$ be an arithmetical theory. Then, $\mathbb{T}$ satisfies the Existence Property as stated in Definition 2.3.3.1 if and only if $\mathbb{T}$ satisfies the following generalised version of the Existence Property:*

For every formula φ in $\mathbb{T}$ and every list $\mathbf{x}$ of distinct variables of length $k = |\mathbf{x}| \geq 1$, if $\vdash (\exists \mathbf{x})\varphi$, then there exists $\mathbf{m} \in \mathbb{N}^k$ such that $\vdash \varphi\left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}\right]$.

Proof Note that (EP) is the special case of the generalised version when $k = 1$. Hence, if $\mathbb{T}$ satisfies the generalised version, then $\mathbb{T}$ satisfies (EP).

Now suppose that $\mathbb{T}$ satisfies (EP). We proceed by induction on $k \geq 1$ to show that $\mathbb{T}$ satisfies the generalised version. As noted above, $\mathbb{T}$ satisfies the generalised version for $k = 1$. Now suppose that $\mathbb{T}$ satisfies the generalised version for some $k \geq 1$. Let φ be a formula in $\mathbb{T}$, let $x_0, \ldots, x_k$ be $k+1$ distinct variables in $\mathbb{T}$ and let $\mathbf{x}$ denote the list $x_1, \ldots, x_k$. Suppose that $\vdash (\exists x_0, \mathbf{x})\varphi$ holds in $\mathbb{T}$. By (EP), there exists an $m_0 \in \mathbb{N}$ such that $\vdash (\exists \mathbf{x})\varphi\left[\frac{\overline{m_0}}{x_0}\right]$ holds in $\mathbb{T}$. By the induction hypothesis, it follows that there exists $\mathbf{m} \in \mathbb{N}^k$ such that $\vdash \varphi\left[\frac{\overline{m_0}}{x_0}, \frac{\overline{\mathbf{m}}}{\mathbf{x}}\right]$ holds in $\mathbb{T}$. Hence, the generalised version holds for all $k \geq 1$. ∎

We can henceforth treat both versions of the Existence Property given in Definition 2.3.3.1 and Lemma 2.3.3.2 as being interchangeable and so shall refer to both as (EP).

We now consider the impact of the Existence Property on the representability of partial recursive functions in arithmetical theories. Given any partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ and arithmetical theory $\mathbb{T}$, we wish to be able to determine whether or not f is numeralwise, type-one, or strongly representable in $\mathbb{T}$. For each notion of representability, we need to give a formula $\varphi(\mathbf{x}, y)$ such that condition (P1) holds, that is, such that for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$, $f(\mathbf{m}) \simeq n$ if and only if $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$. Since f is a partial function, it is functional as a binary relation between $\mathbb{N}^k$ and $\mathbb{N}$. Since conditions (P2) and (P3) express the fact that φ is provably functional in $\mathbb{T}$, these conditions make sense even when f is a non-total function. The problem arises when we consider condition (P4) for φ, namely

$$\vdash (\exists y)\varphi(\mathbf{x}, y),$$

which expresses the fact that φ is provably total in $\mathbb{T}$. Hence, by the Substitution Theorem, it follows that for φ to satisfy condition (P4), the statement

for all $\mathbf{m} \in \mathbb{N}^k$, $\vdash (\exists y)\varphi(\overline{\mathbf{m}}, y)$

must hold. However, since f is a partial function, it is not necessarily total, and so the statement

for each $\mathbf{m} \in \mathbb{N}^k$, there exists an $n \in \mathbb{N}$ such that $f(\mathbf{m}) \simeq n$

is not necessarily true. Now suppose that $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is non-total and $\mathbf{m} \in \mathbb{N}^k$ is such that $f(\mathbf{m})\uparrow$, that is, there does not exist an $n \in \mathbb{N}$ for which $f(\mathbf{m}) \simeq n$. For f to be strongly representable in an arithmetical theory $\mathbb{T}$, we must find a formula $\varphi(\mathbf{x}, y)$ in $\mathbb{T}$ such that

(i) $\vdash (\exists y)\varphi(\overline{\mathbf{m}}, y)$ holds; and

(ii) there does not exist an $n \in \mathbb{N}$ for which

$$\vdash \varphi(\overline{\mathbf{m}}, \overline{n}) \tag{2.3.1}$$

holds.

Indeed, if there did exist an $n \in \mathbb{N}$ for which (2.3.1) holds, it would follow by condition (P1) that $f(\mathbf{m}) \simeq n$ for this $n \in \mathbb{N}$, thus contradicting our above assumption. Note that if $\mathbb{T}$ satisfies the Existence Property (that is, if $\mathbb{T}$ is intuitionistic), then there can be no formula $\varphi(\mathbf{x}, y)$ in $\mathbb{T}$ satisfying (i) and (ii) above. Therefore, the notion of strong representability of partial functions in intuitionistic arithmetical theories doesn't make sense as we cannot require unique existence for variables when the partial function may not be defined on certain inputs. For ease of reference, we summarise this observation in the following result.

Theorem 2.3.3.3 *No non-total function can be strongly representable in an intuitionistic arithmetical theory.*

However, if the Existence Property fails for $\mathbb{T}$ (that is, if $\mathbb{T}$ is classical), then it is not necessarily impossible to find a formula $\varphi(\mathbf{x}, y)$ satisfying (i) and (ii) above, and so it makes sense to consider the strong representability of partial functions in classical arithmetical theories.

We now wish to show that an arithmetical theory $\mathbb{T}$ satisfies the Existence Property if and only if it is intuitionsitic, as claimed above. If $\mathbb{T}$ is a classical arithmetical theory, we can find a counter-example showing that (EP) fails for $\mathbb{T}$. In fact we can show that the completely undefined function from $\mathbb{N}^k$ to $\mathbb{N}$ (for any $k \geq 0$) is strongly representable in any classical arithmetical theory, thus giving a concrete example showing that Theorem 2.3.3.3 only holds for intuitionistic theories. We first need a preliminary result.

Lemma 2.3.3.4 *Let $\mathbb{T}$ be an arithmetical theory. Let A, B be formulas of $\mathbb{T}$ and let x be a variable that does not occur free in either of A and B. Then, the formulas*

$$A \vee B,$$

$$(\exists x)((x = 0 \Rightarrow A) \wedge (x \neq 0 \Rightarrow B)),$$

and

$$(\exists x)((x = 0 \Rightarrow A) \wedge (x \neq 0 \Rightarrow B) \wedge x < \overline{2})$$

are provably equivalent in $\mathbb{T}$.

Proof The proof is straightforward and similar to the one in [35, §1.3.7]. ∎

Lemma 2.3.3.5 *Let $\mathbb{T}$ be a classical arithmetical theory. Then, there exists a formula $\varphi(x)$ in $\mathbb{T}$ with unique free variable x such that $\vdash (\exists x)\varphi(x)$ and, for all $n \in \mathbb{N}$, $\nvdash \varphi(\overline{n})$.*

Proof By Gödel's Incompleteness Theorem, since $\mathbb{T}$ is a consistent theory, there exists a closed undecidable formula in $\mathbb{T}$. That is to say, there exists a closed formula G in $\mathbb{T}$ such that $\nvdash G$ and $\nvdash \neg G$. Define

$$\varphi(x) \underset{\text{def}}{\equiv} (x = 0 \Rightarrow G) \wedge (x \neq 0 \Rightarrow \neg G).$$

Since $\mathbb{T}$ is classical, we obtain

$$\vdash G \vee \neg G$$

by (EM). Since G is a closed formula and so does not contain x free, it follows by Lemma 2.3.3.4 that

$$\vdash (G \vee \neg G) \Leftrightarrow (\exists x)\varphi(x)$$

holds in $\mathbb{T}$, and so we obtain

$$\vdash (\exists x)\varphi(x).$$

Now let $n \in \mathbb{N}$ and observe that either $n = 0$ or $n \neq 0$. Suppose that $\vdash \varphi(\overline{n})$. If $n = 0$, we obtain $\vdash \overline{n} = 0$ by Lemma 2.2.2.6, and so

$$\vdash G$$

follows from $\vdash \varphi(\overline{n})$ by ($\wedge$-E) and ($\Rightarrow$-E). This is a contradiction as G is undecidable in $\mathbb{T}$. If instead $n \neq 0$, we obtain $\vdash \overline{n} \neq 0$ by Lemma 2.2.2.6, and so

$$\vdash \neg G$$

follows from $\vdash \varphi(\overline{n})$ by ($\wedge$-E) and ($\Rightarrow$-E). This is again a contradiction. Hence, for all $n \in \mathbb{N}$, $\nvdash \varphi(\overline{n})$. ■

Theorem 2.3.3.6 *Let $\mathbb{T}$ be an arithmetical theory. If $\mathbb{T}$ is intuitionistic, then $\mathbb{T}$ satisfies the Existence Property. If $\mathbb{T}$ is classical, the Existence Property fails for $\mathbb{T}$.*

Proof If $\mathbb{T}$ is intuitionistic, then $\mathbb{T}$ satisfies (EP) (see for example [16] or [35, §1.11.2]).

Now suppose $\mathbb{T}$ is classical. Then, by Lemma 2.3.3.5, the Existence Property fails for $\mathbb{T}$. ■

In classical arithmetical theories, the Existence Property fails and Theorem 2.3.3.3 does not hold. Hence, it makes sense to consider the strong representability of partial functions in classical arithmetical theories, as illustrated by the following example concerning the completely undefined functions on any number $k \geq 0$ of variables.

Example 2.3.3.7 Let $k \geq 0$, and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be the completely undefined function on k variables. Then, f is strongly representable in any classical arithmetical theory. □

Proof Let $\mathbb{T}$ be a classical arithmetical theory, let G be the closed undecidable formula from Lemma 2.3.3.5, and define

$$\varphi_k(\mathbf{x}, y) \underset{\text{def}}{\equiv} \mathbf{x} = \mathbf{x} \wedge (y = 0 \Rightarrow G) \wedge (y \neq 0 \Rightarrow \neg G) \wedge y < \overline{2}.$$

Note that if $k = 0$, the list $\mathbf{x}$ is empty and hence omitted, yielding the formula

$$\varphi_0(y) \underset{\text{def}}{\equiv} (y = 0 \Rightarrow G) \wedge (y \neq 0 \Rightarrow \neg G) \wedge y < \overline{2}.$$

We claim that $\varphi_k(\mathbf{x}, y)$ strongly represents f in $\mathbb{T}$.

(P1) Let $\mathbf{m} \in \mathbb{N}^k$ and suppose to the contrary that there exists an $n \in \mathbb{N}$ such that $\vdash \varphi_k(\overline{\mathbf{m}}, \overline{n})$ holds. We then obtain

$$\vdash (\overline{n} = 0 \Rightarrow G) \wedge (\overline{n} \neq 0 \Rightarrow \neg G)$$

by ($\wedge$-E). This is impossible as shown in the proof of Lemma 2.3.3.5. Since f is completely undefined, we thus have $f(\mathbf{m}) \not\simeq n$ and $\nvdash \varphi_k(\overline{\mathbf{m}}, \overline{n})$ for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$, and so condition (P1) holds for f and $\varphi_k(\mathbf{x}, y)$ in $\mathbb{T}$.

(P3) By Proposition 2.2.2.8, we have

$$\vdash y < \overline{2} \Leftrightarrow y = 0 \vee y = \overline{1},$$

and so we obtain

$$\varphi_k(\mathbf{x}, y) \wedge \varphi_k(\mathbf{x}, z) \vdash (y = 0 \vee y = \overline{1}) \wedge (z = 0 \vee z = \overline{1}).$$

Consequently, we obtain

$$\varphi_k(\mathbf{x}, y) \wedge \varphi_k(\mathbf{x}, z), y \neq z \vdash G \wedge \neg G$$

using (M1) and ($\Rightarrow$-E), and so

$$\varphi_k(\mathbf{x}, y) \wedge \varphi_k(\mathbf{x}, z) \vdash y = z$$

follows by ($\neg$-I), (DE), and ($\vee$-E). Thus, condition (P3) for φ_k follows by ($\Rightarrow$-I).

(P4) Now note that since $\vdash x_i = x_i$ for all $1 \leq i \leq k$ by (=-I), a straightforward argument using ($\exists$-E), ($\wedge$-E) and ($\wedge$-I) shows that

$$\vdash (\exists y)\varphi_k(\mathbf{x}, y) \Leftrightarrow (\exists y)((y = 0 \Rightarrow G) \wedge (y \neq 0 \Rightarrow \neg G) \wedge y < \overline{2}).$$

Hence, by Lemma 2.3.3.4, it follows that

$$\vdash (\exists y)\varphi_k(\mathbf{x}, y) \Leftrightarrow (G \vee \neg G).$$

Since $\mathbb{T}$ is classical, we obtain $\vdash G \vee \neg G$ by (EM), and so we obtain $\vdash (\exists y)\varphi_k(\mathbf{x}, y)$. Hence, condition (P4) for φ_k is satisfied.

Thus, $\varphi_k(\mathbf{x}, y)$ indeed strongly represents the completely undefined function f in $\mathbb{T}$. ∎

2.4 Representability theorems

We can now characterise the representability of primitive, total, and partial recursive functions in arithmetical theories. We consider three types of arithmetical theories, namely general arithmetical theories, arithmetical theories with induction, and classical arithmetical theories (with or without induction). For each of the three classes of computable functions, we determine if the functions are numeralwise, type-one, or strongly representable in arithmetical theories of each type. We first consider the representability of primitive recursive functions (Section 2.4.1). We then examine the representability of partial recursive functions (Section 2.4.2) and obtain the corresponding results about the representability of total recursive functions as a consequence (Section 2.4.3). Finally, we show that any partial function that is representable in an arithmetical theory must be partial recursive (Section 2.4.4).

2.4.1 Primitive recursive functions

2.4.1.1 Basic functions and of functions obtained by substitution

We first show that the basic functions are strongly representable in all arithmetical theories and consider the representability of certain other primitive recursive functions and predicates.

Proposition 2.4.1.1 *Let $\mathbb{T}$ be any arithmetical theory. The basic functions are strongly representable in $\mathbb{T}$.*

PROOF We show that the basic functions given in Definition 2.1.2.1 are strongly representable in $\mathbb{T}$.

(I) Consider the zero constant $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$ defined by $\underline{0}(*) = 0$. Define

$$\varphi_{\underline{0}}(y) \underset{\text{def}}{\equiv} y = 0.$$

We show that $\underline{0}$ is strongly representable in $\mathbb{T}$ by $\varphi_{\underline{0}}(y)$. For the unique element $* \in \mathbb{N}^0$, we have that $\underline{0}(*) = 0$ and we obtain $\vdash 0 = 0$, that is $\vdash \varphi_{\underline{0}}(0)$, by (=-I). So, condition (P1') is satisfied. Moreover, we obtain $\vdash (\exists! y)(y = 0)$ from $\vdash 0 = 0$ and the properties of equality in $\mathbb{T}$. Hence, condition (P4') is satisfied, and so $\varphi_{\underline{0}}(y)$ strongly represents $\underline{0}$ in $\mathbb{T}$ by Lemma 2.3.1.2.

(II) Consider the successor function $s : \mathbb{N} \to \mathbb{N}$ defined by $s(n) = n + 1$ for all $n \in \mathbb{N}$. Define

$$\varphi_s(x, y) \underset{\text{def}}{\equiv} y = S(x).$$

We show that $\varphi_s(x, y)$ strongly represents s in $\mathbb{T}$. Suppose that $n, m \in \mathbb{N}$ are such that $s(n) = m$. Then, $m = n + 1$, and so $\overline{m}$ is the term $S(\overline{n})$ by Definition 2.2.2.5. We thus obtain $\vdash \overline{m} = S(\overline{n})$ by (=-I), and so condition (P1') is satisfied. Moreover, we obtain

$$\vdash (y = S(x) \wedge z = S(x)) \Rightarrow y = z$$

by (=-E) and ($\Rightarrow$-I) and we obtain

$$\vdash (\exists y)(y = S(x))$$

by (=-I) and ($\exists$-I). Hence, conditions (P3) and (P4) for φ_s are satisfied, and so the formula $\varphi_s(x, y)$ indeed strongly represents s in $\mathbb{T}$.

(III) Let $k \geq 1$ and let $1 \leq i \leq k$. Consider the projection function $U_i^k : \mathbb{N}^k \to \mathbb{N}$ defined by $U_i^k(n_1, \ldots, n_k) = n_i$ for all $(n_1, \ldots, n_k) \in \mathbb{N}$. Define

$$\varphi(\mathbf{x}, y) \underset{\text{def}}{\equiv} \mathbf{x} = \mathbf{x} \wedge y = x_i.$$

We show that $\varphi(\mathbf{x}, y)$ strongly represents U_i^k in $\mathbb{T}$. Let $\mathbf{n} \in \mathbb{N}^k$ and $m \in \mathbb{N}$ and suppose that $U_i^k(\mathbf{n}) = m$. Then, $m = n_i$ by definition, and so we obtain $\vdash \overline{m} = \overline{n_i}$. We thus obtain $\vdash \varphi(\overline{\mathbf{n}}, \overline{m})$ by (=-I) and ($\wedge$-I). Hence, condition (P1') is satisfied.

We obtain $\vdash \mathbf{x} = \mathbf{x} \wedge x_i = x_i$ by (=-I) and ($\wedge$-I), and so $\vdash (\exists y)\varphi(\mathbf{x}, y)$ follows by ($\exists$-I). We also obtain

$$\vdash \varphi(\mathbf{x}, y) \wedge \varphi(\mathbf{x}, z) \Rightarrow y = z$$

by the properties of equality in $\mathbb{T}$, and so conditions (P4) and (P3) for φ are satisfied. Hence, $\varphi(\mathbf{x}, y)$ strongly represents U_i^k in $\mathbb{T}$. ∎

Note that the formulas given in Proposition 2.4.1.1 also type-one and numeralwise represent the basic functions in any arithmetic theory $\mathbb{T}$ as shown in Lemma 2.3.1.5.

Corollary 2.4.1.2 *Let $\mathbb{T}$ be an arithmetical theory. For each $n \in \mathbb{N}$, the 0-ary constant function $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$, which is primitive recursive by Lemma 2.1.2.9, is strongly representable in $\mathbb{T}$ by the formula $y = \overline{n}$.*

Proof An analogous argument to the one in the proof of Proposition 2.4.1.1 for the zero constant $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$, replacing 0 by n, shows that $\underline{n} : \mathbb{N}^0 \to \mathbb{N}$ is strongly representable in $\mathbb{T}$ by the formula $y = \overline{n}$. ∎

Furthermore, $Z_k : \mathbb{N}^k \to \mathbb{N}$, the constant zero function on k variables defined by $Z_k(\mathbf{n}) = 0$ for all $\mathbf{n} \in \mathbb{N}^k$, is also primitive recursive and strongly representable in any arithmetical theory $\mathbb{T}$, as shown below.

Lemma 2.4.1.3 *Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. Then, $Z_k : \mathbb{N}^k \to \mathbb{N}$ is strongly representable in $\mathbb{T}$ by the formula*

$$\varphi_{Z_k}(\mathbf{x}, y) \underset{\text{def}}{\equiv} \mathbf{x} = \mathbf{x} \wedge y = 0.$$

Note that $Z_0 : \mathbb{N}^0 \to \mathbb{N}$ is the zero constant, also denoted $\underline{0} : \mathbb{N}^0 \to \mathbb{N}$, and that $Z_1 : \mathbb{N} \to \mathbb{N}$ is the usual zero function on $\mathbb{N}$, also denoted $Z : \mathbb{N} \to \mathbb{N}$.

Proof If $k = 0$, $Z_0 = \underline{0}$ is strongly representable in $\mathbb{T}$ by the formula $\varphi_{\underline{0}}(y) \underset{\text{def}}{\equiv} y = 0$ as shown in the proof of Proposition 2.4.1.1.

Let $k \geq 1$. Suppose that $\mathbf{n} \in \mathbb{N}^k$ and note that $Z_k(\mathbf{n}) = 0$. We obtain $\vdash \overline{\mathbf{n}} = \overline{\mathbf{n}} \wedge 0 = 0$ by (=-I) and ($\wedge$-I), and so condition (P1') is satisfied for $\varphi_{Z_k}(\mathbf{x}, y)$.

We obtain $\vdash \mathbf{x} = \mathbf{x} \wedge 0 = 0$ by (=-I) and ($\wedge$-I). Hence, it follows by ($\exists$-I) that $\vdash (\exists y)\varphi_{Z_k}(\mathbf{x}, y)$, and so condition (P4) is satisfied for φ_{Z_k}. We also obtain

$$\varphi_{Z_k}(\mathbf{x}, y) \wedge \varphi_{Z_k}(\mathbf{x}, z) \vdash y = 0 \wedge z = 0$$

by ($\wedge$-E) and ($\wedge$-I), from which

$$\vdash \varphi_{Z_k}(\mathbf{x}, y) \wedge \varphi_{Z_k}(\mathbf{x}, z) \Rightarrow y = z$$

follows by (=-E) and ($\Rightarrow$-I). Hence, condition (P3) for φ_{Z_k} is satisfied, and so φ_{Z_k} indeed strongly represents Z_k in $\mathbb{T}$. ∎

We now consider the representability of functions obtained by substitution.

Proposition 2.4.1.4 *Let $\mathbb{T}$ be any arithmetical theory and let $g : \mathbb{N}^n \to \mathbb{N}$ and $h_i : \mathbb{N}^k \to \mathbb{N}$ (for all $1 \leq i \leq n$) be total functions strongly (type-one, numeralwise) representable in $\mathbb{T}$. Let the total function $f : \mathbb{N}^k \to \mathbb{N}$ be obtained from $g, h_1, \ldots, h_n$ by the substitution scheme (S). Then, f is strongly (type-one, numeralwise, resp.) representable in $\mathbb{T}$.*

PROOF We first prove the result for strong representability. Suppose that g and the h_i are strongly representable in $\mathbb{T}$. Then, there exists a formula $\varphi_i(x_1, \ldots, x_k, y_i)$ that strongly represents h_i in $\mathbb{T}$ for all $1 \leq i \leq n$ and a formula $\psi(y_1, \ldots, y_n, z)$ in $\mathbb{T}$ that strongly represents g in $\mathbb{T}$ (note that by Remark 2.3.1.3 we may assume that each φ_i contains the same variables $x_1, \ldots, x_k$ free and that the variables x_j, y_i, z are all pairwise distinct). Let $\mathbf{x}$ denote the list $x_1, \ldots, x_k$ and let $\mathbf{y}$ denote the list $y_1, \ldots, y_n$. Define

$$\theta(\mathbf{x}, z) \underset{\text{def}}{\equiv} (\exists \mathbf{y})(\varphi_1(\mathbf{x}, y_1) \wedge \ldots \wedge \varphi_n(\mathbf{x}, y_n) \wedge \psi(\mathbf{y}, z)).$$

We wish to show that $\theta(\mathbf{x}, z)$ strongly represents f in $\mathbb{T}$.

(P1') Let $\mathbf{m} \in \mathbb{N}^k$ and $p \in \mathbb{N}$, and suppose that $f(\mathbf{m}) = p$. Let $q_i = h_i(\mathbf{m})$ for all $1 \leq i \leq n$ and let $\mathbf{q}$ denote the list $q_1, \ldots, q_n$. Then, since f is obtained from $g, h_1, \ldots, h_n$ by substitution, we have that $g(\mathbf{q}) = p$. As $\varphi_1, \ldots, \varphi_n, \psi$ strongly represent the total functions $h_1, \ldots, h_n, g$, respectively, in $\mathbb{T}$, we then obtain by condition (P1') for these formulas and ($\wedge$-I) that

$$\vdash \varphi_1(\overline{\mathbf{m}}, \overline{q_1}) \wedge \ldots \wedge \varphi_n(\overline{\mathbf{m}}, \overline{q_n}) \wedge \psi(\overline{\mathbf{q}}, \overline{p}).$$

Then, ($\exists$-I) yields

$$\vdash (\exists \mathbf{y})(\varphi_1(\overline{\mathbf{m}}, y_1) \wedge \ldots \wedge \varphi_n(\overline{\mathbf{m}}, y_n) \wedge \psi(\mathbf{y}, \overline{p})),$$

that is,

$$\vdash \theta(\overline{\mathbf{m}}, \overline{p}).$$

Hence, condition (P1') for θ is satisfied.

(P3) We show condition (P3) for θ via the following derivation in $\mathbb{T}$.

1		$\theta(\mathbf{x}, z) \wedge \theta(\mathbf{x}, u)$	
2	$\mathbf{c}, \mathbf{d}$	$\varphi_1(\mathbf{x}, c_1) \wedge \ldots \wedge \varphi_n(\mathbf{x}, c_n) \wedge \psi(\mathbf{c}, z)$	
3		$\varphi_1(\mathbf{x}, d_1) \wedge \ldots \wedge \varphi_n(\mathbf{x}, d_n) \wedge \psi(\mathbf{d}, u)$	
4		$c_i = d_i$ for all $1 \leq i \leq n$	Condition (P3) for φ_i $(1 \leq i \leq n)$, 2, 3
5		$\psi(\mathbf{d}, z)$	(=-E), 4, 2
6		$z = u$	Condition (P3) for ψ, 3, 5
7		$z = u$	($\wedge$-E), ($\exists$-E), 1, 2–6
8		$\theta(\mathbf{x}, z) \wedge \theta(\mathbf{x}, u) \Rightarrow z = u$	($\Rightarrow$-I), 1–7

(P4) We show condition (P4) for θ via the following derivation in $\mathbb{T}$.

1		$(\exists y_i)\varphi_i(\mathbf{x}, y_i)$ for all $1 \leq i \leq n$	Condition (P4) for φ_i for all $1 \leq i \leq n$
2	$\mathbf{b}$	$\varphi_i(\mathbf{x}, b_i)$ for all $1 \leq i \leq n$	
3		$(\exists z)\psi(\mathbf{b}, z)$	Condition (P4) for ψ
4	a	$\psi(\mathbf{b}, a)$	
5		$\varphi_1(\mathbf{x}, b_1) \wedge \ldots \wedge \varphi_n(\mathbf{x}, b_n) \wedge \psi(\mathbf{b}, a)$	($\wedge$-I), 2, 4
6		$(\exists z)\theta(\mathbf{x}, z)$	($\exists$-I),Definition of θ, 5
7		$(\exists z)\theta(\mathbf{x}, z)$	($\exists$-E), 3, 4–6
8		$(\exists z)\theta(\mathbf{x}, z)$	($\exists$-E), 1, 2–7

Hence, $\theta(\mathbf{x}, z)$ satisfies conditions (P1'), (P3), and (P4), and so strongly represents f in $\mathbb{T}$.

We have shown above that condition (P3) for θ follows from condition (P3) for the φ_i and ψ. Hence, if the h_i and g are type-one representable by the φ_i and ψ, respectively, then f is type-one representable by θ. Moreover, the analogous result for numeralwise representability is easily obtained by adapting the proof of condition (P3) for θ above to show condition (P2) instead, where we use the fact that the h_i are total and so $\vdash \varphi_i(\overline{\mathbf{m}}, \overline{h_i(\mathbf{m})})$ for each $\mathbf{m} \in \mathbb{N}^k$ and $1 \leq i \leq n$ in order to be able to use condition (P2) for ψ instead of condition (P3) for ψ. ∎

By Propositions 2.4.1.1 and 2.4.1.4, the basic functions and all functions obtained from them by substitution are strongly representable in any arithmetical theory. In order to characterise the representability of primitive recursive functions, we would, in particular, like to determine if the primitive recursive functions are strongly representable in certain kinds of arithmetical theories. It remains to consider the representability of functions obtained by primitive recursion from strongly representable functions.

2.4.1.2 Examples of representability of primitive recursive functions

We now consider the representability of certain primitive recursive functions that will be useful in order to show the representability of all primitive recursive functions in certain kinds of arithmetical theories.

Proposition 2.4.1.5 *Let $j, k \geq 1$, let $f : \mathbb{N}^k \to \mathbb{N}$ and $h : \{1, \ldots, k\} \to \{1, \ldots, j\}$ be total functions, and let $g : \mathbb{N}^j \to \mathbb{N}$ be defined by*

$$g(m_1, \ldots, m_j) = f(m_{h(1)}, \ldots, m_{h(k)})$$

for all $m_1, \ldots, m_j \in \mathbb{N}$.

(i) If f is primitive (total) recursive, then so is g.

(ii) Let $\mathbb{T}$ be an arithmetical theory, let f be numeralwise (type-one, strongly) representable in $\mathbb{T}$ by the formula $\varphi_f(x_1, \ldots, x_k, y)$, and let $u_1, \ldots, u_j$ be new variables not occurring in φ_f. If h is surjective, define

$$\varphi_g(u_1, \ldots, u_j, y) \underset{\text{def}}{\equiv} \varphi_f(u_{h(1)}, \ldots, u_{h(k)}, y).$$

If h is not surjective, let $i_1, \ldots, i_n$ be, in order, the indices in the set $\{1, \ldots, j\} \setminus h(\{1, \ldots, k\})$ and define

$$\varphi_g(u_1, \ldots, u_j, y) \underset{\text{def}}{\equiv} \varphi_f(u_{h(1)}, \ldots, u_{h(k)}, y) \wedge \left(\bigwedge_{\ell=1}^{n} u_{i_\ell} = u_{i_\ell} \right).$$

Then, g is numeralwise (type-one, strongly, resp.) representable in $\mathbb{T}$ by the formula $\varphi_g(u_1, \ldots, u_j, y)$.

Proof (i) See [19, Prop. 3.14, pp. 172–173].

(ii) It suffices to consider the case when h is surjective. The case when h is not surjective is proved by a similar argument, in which we modify the representing formula φ_g slightly in order to ensure that it has exactly $j + 1$ free variables as required in Definition 2.3.1.1.

So, suppose that h is surjective and that f is strongly representable in $\mathbb{T}$ by $\varphi_f(x_1, \ldots, x_k, y)$.

Let $m_1, \ldots, m_j \in \mathbb{N}$ and let $p = g(m_1, \ldots, m_j) = f(m_{h(1)}, \ldots, m_{h(k)})$. By condition (P1') for φ_f, we have that

$$\vdash \varphi_f(\overline{m_{h(1)}}, \ldots, \overline{m_{h(k)}}, \overline{p}),$$

that is

$$\vdash \varphi_g(\overline{m_1}, \ldots, \overline{m_j}, \overline{p}).$$

Hence, condition (P1') for φ_g is satisfied.

By condition (P4') for φ_f, we have that

$$\vdash (\exists! y)\varphi_f(x_1, \ldots, x_k, y).$$

Since $u_1, \ldots, u_j$ are new variables not occurring in φ_f, it follows by the Substitution Theorem that

$$\vdash (\exists! y)\varphi_f(u_{h(1)}, \ldots, u_{h(k)}, y),$$

that is

$$\vdash (\exists! y)\varphi_g(u_1, \ldots, u_j, y)$$

holds in $\mathbb{T}$. Hence, condition (P4') for φ_g is satisfied, and so g is strongly representable in $\mathbb{T}$ by φ_g.

An analogous argument shows that if φ_f satisfies condition (P3) (but not necessarily condition (P4)), then so does φ_g. Moreover, if φ_f satisfies condition (P2) (but not necessarily conditions (P3) or (P4)), then so does φ_g. Hence, the result also holds for type-one and numeralwise representability. ∎

Next, we consider polynomial functions and their representability.

Definition 2.4.1.6 Let $\mathbb{T}$ be an arithmetical theory.

(i) Let x be any variable of $\mathbb{T}$. We define the term x^n of $\mathbb{T}$ for all $n \geq 1$ by the following inductive definition.

(1) x^1 is the term x

(2) x^{n+1} is the term $x^n \cdot x$ for all $n \geq 1 \in \mathbb{N}$.

Note that we extend this definition in the obvious way in order to define t^n for any term t of $\mathbb{T}$ and any $n \geq 1$.

(ii) Let $k \geq 1$ and let $p(\mathbf{v}) = p(v_1, \ldots, v_k)$ be a polynomial expression in the k variables $v_1, \ldots, v_k$ with coefficients in $\mathbb{N}$. Note that the variables need not all appear in the polynomial expression.

Let $\mathbf{x}$ be the list $x_1, \ldots, x_k$ of k distinct variables in $\mathbb{T}$. We define the term $\hat{p}(\mathbf{x})$ of $\mathbb{T}$ corresponding to $p(\mathbf{v})$ to be the term obtained by replacing each power of an indeterminate v_i^j be the corresponding term x_i^j in $\mathbb{T}$, replacing each natural number a appearing in p by the corresponding numeral $\overline{a}$ in $\mathbb{T}$, and replacing addition and multiplication in p by the function symbols $+$ and $\cdot$ in $\mathbb{T}$. Note that although we do not change the order of addition in p when constructing $\hat{p}$, we agree to multiply on the right by numerals in $\mathbb{T}$ whenever possible, in light of Lemma 2.2.2.7. That is to say, if for example $p(v_1, v_2)$ is the expression $v_1(3v_2 + 2)$, then the corresponding term $\hat{p}(x_1, x_2)$ is the term $x_1 \cdot ((x_2 \cdot \overline{3}) + \overline{2})$, and not the term $x_1 \cdot ((\overline{3} \cdot x_2) + \overline{2})$.

(iii) Let $k \geq 0$, let $p(\mathbf{v})$ and $q(\mathbf{v})$ be two polynomial expressions in k variables with coefficients in $\mathbb{N}$, let $\bigcirc \in \{=, <, \leq\}$, and let E be the k-ary predicate on $\mathbb{N}$ defined by

$$E(\mathbf{m}) \text{ if and only if } p(\mathbf{m}) \bigcirc q(\mathbf{m})$$

for all $\mathbf{m} \in \mathbb{N}^k$. Any such predicate shall be called a *simple polynomial predicate*. If each of the variables in the list $\mathbf{v}$ appears with a non-zero exponent in at least one term of $p(\mathbf{v})$ or $q(\mathbf{v})$ with a non-zero coefficient, we allow ourselves to simply say that E is the predicate $p(\mathbf{m}) \bigcirc q(\mathbf{m})$.

Let $\mathbf{x}$ be the list $x_1, \ldots, x_k$ of distinct variables in $\mathbb{T}$. Let $\hat{p}(\mathbf{x})$, $\hat{q}(\mathbf{x})$ be the terms of $\mathbb{T}$ corresponding to the polynomial expressions p and q, respectively, as defined in part (ii). We define the formula of $\mathbb{T}$ corresponding to E to be

$$\mathbf{E}(\mathbf{x}) \underset{\text{def}}{\equiv} \hat{p}(\mathbf{x}) \bigcirc \hat{q}(\mathbf{x}),$$

where we take $\bigcirc$ to be the appropriate predicate or defined symbol in $\mathbb{T}$.

(iv) Let $k \geq 0$. The k-ary *polynomial predicates* on $\mathbb{N}$ and their corresponding formulas in $\mathbb{T}$ are given by the following inductive definition (all predicates mentioned are assumed to be k-ary).

- Any simple polynomial predicate E is a polynomial predicate and its corresponding formula is $\mathbf{E}(\mathbf{x})$ as defined in part (iii).
- If E is a polynomial predicate with corresponding formula $\varphi_E(\mathbf{x})$, then $\neg E$ is a polynomial predicate with corresponding formula $\neg\varphi_E(\mathbf{x})$ (recall that $\neg E$ corresponds to $\mathbb{N}^k \setminus E$).
- If E_1, E_2 are two polynomial predicates with corresponding formulas $\varphi_{E_1}(\mathbf{x})$ and $\varphi_{E_2}(\mathbf{x})$, respectively, then $E_1 \wedge E_2$ and $E_1 \vee E_2$ are polynomial predicates with corresponding formulas $\varphi_{E_1}(\mathbf{x}) \wedge \varphi_{E_2}(\mathbf{x})$ and $\varphi_{E_1}(\mathbf{x}) \vee \varphi_{E_2}(\mathbf{x})$, respectively (recall that $\wedge$ and $\vee$ correspond to $\cap$ and $\cup$, respectively). □

Proposition 2.4.1.7 *Let $\mathbb{T}$ be an arithmetical theory.*

(i) *Let $k \geq 1$, let p be a polynomial expression in k variables such that each variable appears at least once with a non-zero exponent in a term of p with a non-zero coefficient, and let $f_p : \mathbb{N}^k \to \mathbb{N}$ be the* polynomial function *defined by*

$$f_p(\mathbf{m}) = p(\mathbf{m})$$

for all $\mathbf{m} \in \mathbb{N}^k$. Let $\mathbf{x}$ be the list $x_1, \ldots, x_k$ of distinct variables in $\mathbb{T}$. Then, f_p is strongly representable in $\mathbb{T}$ by the formula

$$\varphi_{f_p}(\mathbf{x}, y) \underset{\text{def}}{\equiv} y = \hat{p}(\mathbf{x}),$$

where $\hat{p}(\mathbf{x})$ is the term corresponding to $p(\mathbf{v})$ as defined in Definition 2.4.1.6.

(ii) *The formula $x = y$ strongly represents the equality predicate $m = n$ in $\mathbb{T}$. The formulas $x < y$ and $x \leq y$ numeralwise represent the predicates $m < n$ and $m \leq n$, respectively, in $\mathbb{T}$. If $\mathbb{T}$ has induction, $x < y$ and $x \leq y$ strongly represent the predicates $m < n$ and $m \leq n$, respectively, in $\mathbb{T}$.*

(iii) *Let $k \geq 0$ and let E be the k-ary simple polynomial predicate on $\mathbb{N}$ defined by*

$$E(\mathbf{m}) \textit{ if and only if } p(\mathbf{m}) \bigcirc q(\mathbf{m}),$$

where $p(\mathbf{v})$ and $q(\mathbf{v})$ are two polynomial expressions on k variables with coefficients in $\mathbb{N}$ such that each of the variables in the list $\mathbf{v}$ appears with a non-zero exponent in at least one term of $p(\mathbf{v})$ or $q(\mathbf{v})$ with a non-zero coefficient and where $\bigcirc \in \{=, <, \leq\}$. Define

$$\varphi_E(\mathbf{x}) \underset{\text{def}}{\equiv} \mathbf{E}(\mathbf{x}),$$

where $\mathbf{E}(\mathbf{x})$ is the formula corresponding to E as defined in Definition 2.4.1.6. If $\bigcirc$ is $=$, then $\varphi_E(\mathbf{x})$ strongly represents E in $\mathbb{T}$. If $\bigcirc \in \{<, \leq\}$, then $\varphi_E(\mathbf{x})$ numeralwise represents E in $\mathbb{T}$. If $\mathbb{T}$ has induction, $\varphi_E(\mathbf{x})$ strongly represents E in $\mathbb{T}$ in all cases.

Proof (i) Let $\mathbf{m} \in \mathbb{N}^k$ and let $n = f_p(\mathbf{m}) = p(\mathbf{m})$. By Lemma 2.2.2.6, we obtain $\vdash \overline{p(\mathbf{m})} = \hat{p}(\overline{\mathbf{m}})$, that is, $\vdash \overline{n} = \hat{p}(\overline{\mathbf{m}})$. Hence, condition (P1') for φ_{f_p} is satisfied. Since $\hat{p}(\mathbf{x})$ is a term of $\mathbb{T}$, we obtain $\vdash \hat{p}(\mathbf{x}) = \hat{p}(\mathbf{x})$ by (=-I). Hence, $\vdash (\exists y)(y = \hat{p}(\mathbf{x}))$ follows by ($\exists$-I). Moreover, we obtain

$$\vdash (y = \hat{p}(\mathbf{x}) \wedge z = \hat{p}(\mathbf{x})) \Rightarrow y = z$$

by (=-E) and ($\Rightarrow$-I). Thus, conditions (P4) and (P3) for φ_{f_p} are satisfied, and so φ_{f_p} strongly represents f_p in $\mathbb{T}$.

(ii) We first show that $x = y$ strongly represents the equality predicate $m = n$ in $\mathbb{T}$. Let $m, n \in \mathbb{N}$. By Lemma 2.2.2.6, if $m = n$, then $\vdash \overline{m} = \overline{n}$ in $\mathbb{T}$, and if $m \neq n$, then $\vdash \neg(\overline{m} = \overline{n})$ in $\mathbb{T}$. Hence, condition (B) is satisfied. Furthermore, we obtain $\vdash x = y \vee \neg(x = y)$ by (DE). Hence, condition (C) is satisfied, and so $x = y$ strongly represents the equality predicate in $\mathbb{T}$.

We now show that $x < y$ numeralwise represents the predicate $m < n$ in $\mathbb{T}$. Let $m, n \in \mathbb{N}$ and suppose that $m < n$. Then, $m - n \geq 1$ and $m + \overline{(m - n)} = n$. Since $m - n \geq 1$, $m - n - 1 \in \mathbb{N}$ and $\overline{m - n}$ is the term $S(\overline{m - n - 1})$ by definition. Hence, $\vdash \overline{m} + S(\overline{m - n - 1}) = \overline{n}$ by Lemma 2.2.2.6, and so we obtain $\vdash (\exists w)(\overline{m} + S(w) = \overline{n})$ by ($\exists$-I), that is $\vdash \overline{m} < \overline{n}$. Now suppose that $m \not< n$. If $n = 0$, we have that $\vdash \neg(\overline{m} < \overline{n})$ by (L1) from Proposition 2.2.2.8. Now suppose instead that $n > 0$. We obtain

$$\overline{m} < \overline{n} \vdash \overline{m} = 0 \vee \ldots \vee \overline{m} = \overline{n - 1}$$

by Proposition 2.2.2.8. Since $m \not< n$, it follows that, for all $r < n$, $m \neq r$ and so also $\vdash \overline{m} \neq \overline{r}$. Hence, we obtain

$$\vdash \neg(\overline{m} < \overline{n}).$$

by ($\vee$-E) and ($\neg$-I). Thus, condition (B) is satisfied and $x < y$ numeralwise represents the predicate $m < n$ in $\mathbb{T}$.

Furthermore, since $x < y$ and $x = y$ numeralwise represent the predicates $m < n$ and $m = n$, respectively, in $\mathbb{T}$ and

$$x \leq y \underset{\text{def}}{\equiv} x < y \vee x = y,$$

it follows that $x \leq y$ numeralwise represents the predicate $m \leq n$ in $\mathbb{T}$.

Now suppose that $\mathbb{T}$ has induction. In order to show that $x < y$ strongly represents $m < n$ in $\mathbb{T}$, it remains to show condition (C), that is

$$\vdash x < y \vee \neg(x < y).$$

Since we have $\vdash x < y \vee x = y \vee y < x$ by axiom (M8) and we obtain $\vdash x < y \Rightarrow x < y \vee \neg(x < y)$ by ($\vee$-I) and ($\Rightarrow$-I), it remains to show that

$$\vdash [x = y \vee y < x] \Rightarrow [x < y \vee \neg(x < y)].$$

Since $\vdash x = y \vee y < x \Leftrightarrow y \leq x$ by the commutativity of equality and disjunction in $\mathbb{T}$, it suffices to show that

$$\vdash y \leq x \Rightarrow \neg(x < y)$$

holds in $\mathbb{T}$. This holds by Proposition 2.2.2.12. Hence, condition (C) holds, and so $x < y$ strongly represents the predicate $m < n$ in $\mathbb{T}$.

As before, since $x < y$ and $x = y$ strongly represent the predicates $m < n$ and $m = n$, respectively, in the arithmetical theory $\mathbb{T}$ with induction, it follows that $x \leq y$ strongly represents the predicate $m \leq n$ in $\mathbb{T}$.

(iii) Suppose first that $\bigcirc$ is $=$, that is, that E is of the form $p(\mathbf{m}) = q(\mathbf{m})$. Since $\vdash \overline{p(\mathbf{m})} = \hat{p}(\overline{\mathbf{m}})$ and $\vdash \overline{q(\mathbf{m})} = \hat{q}(\overline{\mathbf{m}})$ from the proof of part (i) and $x = y$ strongly represents the equality predicate in $\mathbb{T}$ as shown in part (ii), it follows from the Substitution Theorem that

$$\varphi_E(\mathbf{x}) \underset{\text{def}}{\equiv} \hat{p}(\mathbf{x}) = \hat{q}(\mathbf{x})$$

strongly (and so also numeralwise) represents E in $\mathbb{T}$.

Similarly, if $\bigcirc \in \{<, \leq\}$, it follows from part (ii) that $\varphi_E(\mathbf{x})$ numeralwise represents E in $\mathbb{T}$ and, if $\mathbb{T}$ has induction, that $\varphi_E(\mathbf{x})$ strongly represents E in $\mathbb{T}$. ■

In particular, we can draw the following conclusions from Proposition 2.4.1.7.

Corollary 2.4.1.8 *Let $\mathbb{T}$ be any arithmetical theory.*

(i) $y = x_1 + x_2$ *strongly represents addition in* $\mathbb{T}$.

(ii) $y = x_1 \cdot x_2$ *strongly represents multiplication in* $\mathbb{T}$.

(iii) $y = x \cdot \overline{m}$ *strongly represents multiplication by the constant* m *in* $\mathbb{T}$.

(iv) $y = x^2$, *that is,* $y = x \cdot x$, *strongly represents squaring in* $\mathbb{T}$.

(v) $y = x$ *strongly represents the identity function* $\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ *in* $\mathbb{T}$.

(vi) If $p(\mathbf{v})$ *is any polynomial expression on* k *variables,* $v_{i_1}, \ldots, v_{i_\ell}$ *are, in order, the variables in the list* $\mathbf{v}$ *that do not appear with a non-zero exponent in any term of* p *with a non-zero coefficient, and* $f_p : \mathbb{N}^k \to \mathbb{N}$ *is the polynomial function defined by* $f(\mathbf{m}) = p(\mathbf{m})$ *for all* $\mathbf{m} \in \mathbb{N}$, *then* f_p *is strongly representable in* $\mathbb{T}$ *by the formula*

$$\varphi_{f_p}(\mathbf{x}, y) \underset{\text{def}}{\equiv} y = \hat{p}(\mathbf{x}) \wedge \left(\bigwedge_{j=1}^{\ell} x_{i_j} = x_{i_j} \right).$$

(vii) Let $p(\mathbf{v}), q(\mathbf{v})$ *be two polynomial expressions on* k *variables, let* $v_{i_1}, \ldots, v_{i_\ell}$ *be, in order, the variables in the list* $\mathbf{v}$ *that do not appear with a non-zero exponent in any term of* p *or* q *with a non-zero coefficient, let* $\bigcirc \in \{=, <, \leq\}$, *let* E *be the* k*-ary predicate on* $\mathbb{N}$ *defined by*

$$E(\mathbf{m}) \textit{ if and only if } p(\mathbf{m}) \bigcirc q(\mathbf{m})$$

for all $\mathbf{m} \in \mathbb{N}$*, and define*

$$\varphi_E(\mathbf{x}) \underset{\text{def}}{\equiv} \mathbf{E}(\mathbf{x}) \wedge \left(\bigwedge_{j=1}^{\ell} x_{i_j} = x_{i_j} \right).$$

If $\bigcirc$ *is* $=$, $\varphi_E(\mathbf{x})$ *strongly represents* E *in* $\mathbb{T}$*. If* $\bigcirc \in \{<, \leq\}$, $\varphi_E(\mathbf{x})$ *numeralwise represents* E *in* $\mathbb{T}$*. If* $\mathbb{T}$ *has induction,* $\varphi_E(\mathbf{x})$ *strongly represents* E *in* $\mathbb{T}$ *in all cases.*

(viii) The constant function $c_n^k : \mathbb{N}^k \to \mathbb{N}$*, defined by* $c_n^k(\mathbf{m}) = n$ *for all* $\mathbf{m} \in \mathbb{N}^k$*, is strongly representable in any arithmetical theory* $\mathbb{T}$ *by the formula*

$$\varphi_{c_n^k}(\mathbf{x}, y) \underset{\text{def}}{\equiv} y = \overline{n} \wedge \left(\bigwedge_{i=1}^{k} x_i = x_i \right).$$

Proof Parts (i)–(v) follow directly from Proposition 2.4.1.7 (i) and parts (vi)–(viii) follow from Propositions 2.4.1.7 and 2.4.1.5. ■

We now consider the representability of functions obtained by restriction.

Lemma 2.4.1.9 *Let* $\mathbb{T}$ *be an arithmetical theory. Let* $k \geq 0$ *and let* $f : \mathbb{N}^{k+1} \to \mathbb{N}$ *be a primitive recursive function that is strongly (type-one, numeralwise) representable in* $\mathbb{T}$ *by the formula* $\varphi(z, \mathbf{x}, y)$ *(where* $\mathbf{x}$ *is the sequence* $x_1, \ldots, x_k$ *when* $k > 0$ *and is non-existent when* $k = 0$*). Let* $n \in \mathbb{N}$ *be fixed. Then, the function* $f_n : \mathbb{N}^k \to \mathbb{N}$*, given by* $f_n(\mathbf{m}) = f(n, \mathbf{m})$ *for all* $\mathbf{m} \in \mathbb{N}^k$*, is primitive recursive and strongly (type-one, numeralwise, repsectively) representable in* $\mathbb{T}$ *via the formula* $\varphi(\overline{n}, \mathbf{x}, y)$*.*

Proof We first show that f_n is primitive recursive. If $k = 0$, we have that $f_n = \underline{f(n)} : \mathbb{N}^0 \to \mathbb{N}$ which is primitive recursive by Lemma 2.1.2.9. If $k \geq 1$, we let $g := S^n \circ Z \circ U_k^1 : \mathbb{N}^k \to \mathbb{N}$ and note that $g(\mathbf{m}) = n$ for all $\mathbf{m} \in \mathbb{N}^k$. Moreover, g is primitive recursive as it is obtained from the primitive recursive function Z and the basic functions S and U_k^1 by successive applications of the substitution scheme (S). Then, we have that

$$f_n(\mathbf{m}) = f(n, m_1, \ldots, m_k) = f(g(\mathbf{m}), U_k^1(\mathbf{m}), \ldots, U_k^k(\mathbf{m}))$$

for all $\mathbf{m} \in \mathbb{N}$, and so f_n is obtained from the primitive recursive functions $f, g, U_k^1, \ldots, U_k^k$ by substitution, whence f_n is primitive recursive.

We now suppose that f is strongly representable in $\mathbb{T}$ by $\varphi(z, \mathbf{x}, y)$. Suppose that $\mathbf{m} \in \mathbb{N}^k$, and let $p = f_n(\mathbf{m})$. Then, by the definition of f_n, $f(n, \mathbf{m}) = p$, and so $\vdash \varphi(\overline{n}, \overline{\mathbf{m}}, \overline{p})$ by condition (P1') for f. Hence, condition (P1') holds for f_n and $\varphi(\overline{n}, \mathbf{x}, y)$. By condition (P4') for $\varphi(z, \mathbf{x}, y)$, we obtain that $\vdash (\exists! y)\varphi(z, \mathbf{x}, y)$. By the

Substitution Theorem, we then obtain that $\vdash (\exists! y)\varphi(\overline{n}, \mathbf{x}, y)$. Thus, condition (P4') holds for $\varphi(\overline{n}, \mathbf{x}, y)$, and so $\varphi(\overline{n}, \mathbf{x}, y)$ strongly represents f_n in $\mathbb{T}$.

A similar argument shows that if $\varphi(z, \mathbf{x}, y)$ type-one (numeralwise) represents f in $\mathbb{T}$, then $\varphi(\overline{n}, \mathbf{x}, y)$ type-one (numeralwise, respectively) represents f_n in $\mathbb{T}$. ∎

2.4.1.3 Gödel's beta-function and the encoding of sequences

From Propositions 2.4.1.1 and 2.4.1.4, we see that it suffices to express the definitions of the basic functions and of the substitution scheme (S) as formulas in an arithmetical theory $\mathbb{T}$ in order to show that the basic functions and functions obtained by substitution are strongly representable in $\mathbb{T}$. It is tempting to proceed in a similar manner for functions obtained via the primitive recursion scheme (PR). For example, consider $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$, two functions strongly representable in $\mathbb{T}$ as total functions, and $f : \mathbb{N}^{k+1} \to \mathbb{N}$ the function obtained from g, h by primitive recursion. Thus, f is defined by

$$\begin{aligned} f(\mathbf{m}, 0) &= g(\mathbf{m}) \\ f(\mathbf{m}, n+1) &= h(\mathbf{m}, n, f(\mathbf{m}, n)) \end{aligned} \tag{2.4.1}$$

for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$. We wish to show that f is strongly representable in $\mathbb{T}$ as a total function. Let $\mathbf{x}$ denote the list $x_1, \ldots, x_k$ of variables and $\mathbf{v}$ denote the list v_1, v_2, v_3 of variables. Let $\varphi(\mathbf{x}, y), \psi(\mathbf{x}, \mathbf{v})$ strongly represent g, h in $\mathbb{T}$, respectively. We might then define

$$\theta(\mathbf{x}, u, w) \underset{\text{def}}{\equiv} (\exists y)(u = 0 \wedge w = y \wedge \varphi(\mathbf{x}, y)) \vee (\exists \mathbf{v})(u = S(v_1) \wedge w = v_3 \wedge \psi(\mathbf{x}, \mathbf{v}))$$

and hope to show that $\theta(\mathbf{x}, u, w)$ strongly represents f in $\mathbb{T}$, as it seems to be a fairly straightforward way of expressing the primitive recursion scheme by a formula in $\mathbb{T}$. It turns out that $\theta(\mathbf{x}, u, w)$ does indeed satisfy conditions (P1) and (P4), but a problem arises when we try to prove condition (P3), that is $\vdash \theta(\mathbf{x}, u, w) \wedge \theta(\mathbf{x}, u, w') \Rightarrow w = w'$. Indeed, in the case when $u \neq 0$, we obtain $u = S(a_1) \wedge w = a_3 \wedge \psi(\mathbf{x}, \mathbf{a})$ and $u = S(b_1) \wedge w' = b_3 \wedge \psi(\mathbf{x}, \mathbf{b})$ for some $\mathbf{a}, \mathbf{b}$. It then follows by axiom (M2) that $a_1 = b_1$, but we have no information on a_2 and b_2, and so cannot show that $a_2 = b_2$. Since we cannot show that $a_2 = b_2$, we cannot use condition (P3) for ψ in order to deduce that $a_3 = b_3$, from which it would follow that $w = w'$. Hence, we need to include more information about v_2 in θ in order to be able to show condition (P3) for θ. However, the only information we have about v_2 is that it corresponds to the argument $f(\mathbf{m}, n)$ passed to h in (2.4.1), and so we would somehow need to define $\theta(\mathbf{x}, u, w)$ as

$$(\exists y)(u = 0 \wedge w = y \wedge \varphi(\mathbf{x}, y)) \vee (\exists \mathbf{v})(u = S(v_1) \wedge w = v_3 \wedge \theta(\mathbf{x}, v_1, v_2) \wedge \psi(\mathbf{x}, \mathbf{v})).$$

Since we cannot define θ in terms of itself, we need another way of expressing how v_2 is obtained in $\theta(\mathbf{x}, u, w)$.

When computing $f(\mathbf{m}, n)$ for given $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$, we can consider the finite sequence

$$a_0 = g(\mathbf{m}), a_1 = h(\mathbf{m}, 0, a_0), a_2 = h(\mathbf{m}, 1, a_1), \ldots, \\ a_k = h(\mathbf{m}, k-1, a_{k-1}), \ldots, a_n = h(\mathbf{m}, n-1, a_{n-1}) \quad (2.4.2)$$

We can then obtain $f(\mathbf{m}, n)$ by taking the last element in the sequence (2.4.2). Note that we never needed to apply f in order to compute the elements in the sequence, but that we do need to be able to keep track of the index k. That is to say, we must know how many times we have already applied g and h, as we need to know whether to apply g or h and, when applying h, we must also know the value of $k-1$ in order to be able to compute $a_k = h(\mathbf{m}, k-1, a_{k-1})$. Therefore, if we can encode the finite sequence (2.4.2) as a function of $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$ and then strongly represent this function in $\mathbb{T}$ using the representing formulas of g and h, but without using a representing formula for f, we will be able to express how v_2 is obtained in θ, thus yielding a formula that will strongly represent f in $\mathbb{T}$. It will then follow that, if $\mathbb{T}$ is an arithmetical theory in which we can strongly represent encodings as detailed above, all functions obtained via primitive recursion from functions strongly representable in $\mathbb{T}$ are themselves strongly representable in $\mathbb{T}$, and so we will be able to show that all primitive recursive functions are strongly representable in $\mathbb{T}$.

Therefore, we must consider the encoding and representation of sequences, which we shall do via Gödel's β-function. Various authors such as Shoenfield [33], Mendelson [19], Boolos and Jeffrey [2], and Kleene [14] consider Gödel's β-function, although they consider different versions of it. Kleene and Mendelson define β as a function of three variables [14, 19] and Shoenfield and Boolos and Jeffrey [33, 2] define β as a function of two variables. We shall use a construction, adapted from [14, 19], of the β-function as a function of three variables.

Let $\mathrm{rm} : \mathbb{N}^2 \to \mathbb{N}$, the *remainder* function, be defined by:

(i) $\mathrm{rm}(m, 0) = m$ for all $m \in \mathbb{N}$;

(ii) $\mathrm{rm}(m, n)$ is the remainder upon division of m by n for all $m, n \in \mathbb{N}$ such that $n \neq 0$.

Then, rm is primitive recursive [19, pp. 174–175] and n divides m if and only if $\mathrm{rm}(m, n) = 0$ [14, p. 202]. Adapting the argument in [14, pp. 202–203] and [19, pp. 164–165,184] yields the following result on the representability of the remainder function in arithmetical theories.

Lemma 2.4.1.10 *Let $\mathbb{T}$ be an arithmetical theory and let* $\mathrm{rm} : \mathbb{N}^2 \to \mathbb{N}$ *be the remainder function as defined above. Define*

$$\delta(x, y, z) \underset{\text{def}}{\equiv} (\exists u)(u \leq x \land x = y \cdot u + z \land z < y) \lor (y = 0 \land z = x).$$

Then, rm *is numeralwise representable in* $\mathbb{T}$ *by* $\delta(x, y, z)$*. If* $\mathbb{T}$ *has induction,* rm *is strongly representable in* $\mathbb{T}$ *by* $\delta(x, y, z)$*.*

Proof See Appendix C for a detailed proof. ∎

Now let $\beta : \mathbb{N}^3 \to \mathbb{N}$ be defined by

$$\beta(c, d, i) = \mathrm{rm}(c, (i + 1)d + 1)$$

for all $c, d, i \in \mathbb{N}$ [14, p. 243, 19, p. 184]. Then, β is primitive recursive as it is obtained from addition, multiplication, and rm by substitution. It also satisfies the following property, which enables the encoding of finite sequences of any length.

Lemma 2.4.1.11 (Gödel's $\boldsymbol{\beta}$-function Lemma) [19, p. 184, Lemma 3.23] *Let* $\beta : \mathbb{N}^3 \to \mathbb{N}$ *be the primitive recursive function defined by*

$$\beta(c, d, i) = \mathrm{rm}(c, (i + 1)d + 1)$$

for all $c, d, i \in \mathbb{N}$ *as above. Then, for any sequence* $a_0, a_1, \ldots, a_n \in \mathbb{N}$ *(where* $n \geq 0$*), there exist* $c, d \in \mathbb{N}$ *such that* $\beta(c, d, i) = a_i$ *for all* $0 \leq i \leq n$*. These numbers* c *and* d *are said to* encode *the sequence* $a_0, \ldots, a_n$ (via β)*.*

The function β defined above can be represented in arithmetical theories as follows.

Lemma 2.4.1.12 *Let* $\mathbb{T}$ *be an arithmetical theory, let* $\mathbf{x}$ *be the list* x_1, x_2, x_3*, and let* $\Lambda(\mathbf{x}, y)$ *be the formula*

$$\delta(x_1, (x_3+\overline{1})\cdot x_2+\overline{1}, y) \underset{\text{def}}{\equiv} (\exists u) \left[u \leq x_1 \wedge x_1 = ((x_3 + \overline{1}) \cdot x_2 + \overline{1}) \cdot u + y \wedge y < (x_3 + \overline{1}) \cdot x_2 + \overline{1}\right].$$

Then, $\Lambda(\mathbf{x}, y)$ *numeralwise represents* β *in* $\mathbb{T}$*. If* $\mathbb{T}$ *has induction, then* $\Lambda(\mathbf{x}, y)$ *strongly represents* β *in* $\mathbb{T}$*.*

Proof Let $\mathbb{T}$ be any arithmetical theory. Consider the primitive recursive function on $\mathbb{N}^3$ given by $(c, d, i) \mapsto (i + 1)d + 1$ in $\mathbb{T}$. It is equal to the polynomial function $f_p : \mathbb{N}^3 \to \mathbb{N}$ corresponding to the polynomial $p(v_1, v_2, v_3) = (v_3 + 1)v_2 + 1$, which has corresponding term $(x_3 + \overline{1}) \cdot x_2 + \overline{1}$ in $\mathbb{T}$, as noted in Definition 2.4.1.6. By Corollary 2.4.1.8, the formula

$$\varphi(\mathbf{x}, v) \underset{\text{def}}{\equiv} v = (x_3 + \overline{1}) \cdot x_2 + \overline{1} \wedge x_1 = x_1$$

strongly, and so also numeralwise, represents f_p in $\mathbb{T}$. Hence, by Proposition 2.4.1.4 and Lemma 2.4.1.10, the formula

$$(\exists v)(\varphi(\mathbf{x}, v) \wedge \delta(x_1, v, y))$$

numeralwise represents β in $\mathbb{T}$ and, if $\mathbb{T}$ has induction, strongly represents β in $\mathbb{T}$.

It follows from the definition of $\varphi(\mathbf{x}, v)$ and the rules for equality and $\exists$, that

$$\vdash (\exists v)(\varphi(\mathbf{x}, v) \wedge \delta(x_1, v, y)) \Leftrightarrow \delta(x_1, (x_3 + \overline{1}) \cdot x_2 + \overline{1}, y).$$

Hence, by Proposition 2.3.1.6, $\Lambda(\mathbf{x}, y) \underset{\text{def}}{\equiv} \delta(x_1, (x_3 + \overline{1}) \cdot x_2 + \overline{1}, y)$ numeralwise represents β in $\mathbb{T}$ and, if $\mathbb{T}$ has induction, strongly represents β in $\mathbb{T}$. ∎

2.4.1.4 Functions obtained by primitive recursion

We can use Gödel's β-function and its representing function Λ in order to show that functions obtained from strongly representable functions by primitive recursion (PR) are themselves strongly representable in arithmetical theories with induction, via an argument somewhat similar to the one in [19, pp. 185–187].

Note that we show this result only for strong representability for reasons given directly after Lemma 2.4.1.13.

Lemma 2.4.1.13 *Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. Let $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$ be total functions and let $f : \mathbb{N}^{k+1} \to \mathbb{N}$ be obtained from g, h by primitive recursion. Suppose that g and h are numeralwise representable in $\mathbb{T}$ by the formulas $\varphi_g(\mathbf{x}, u)$ and $\varphi_h(\mathbf{x}, v_1, v_2, v_3)$, respectively. Let $\Theta(\mathbf{x}, y, z, q_0, q_1)$ be the formula*

$$(\exists u)(\Lambda(q_0, q_1, 0, u) \wedge \varphi_g(\mathbf{x}, u)) \wedge \Lambda(q_0, q_1, y, z) \wedge \\ (\forall w)[w < y \Rightarrow (\exists v)(\exists v')(\Lambda(q_0, q_1, w, v) \wedge \Lambda(q_0, q_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))],$$

where Λ is the representing formula for β given in Lemma 2.4.1.12, and define

$$\rho(\mathbf{x}, y, z) \underset{\text{def}}{\equiv} (\exists q_0)(\exists q_1)\Theta(\mathbf{x}, y, z, q_0, q_1).$$

Then, $\rho(\mathbf{x}, y, z)$ satisfies condition (P1') for the representability of f in $\mathbb{T}$.

Proof Let $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$ and let $p = f(\mathbf{m}, n)$. Then, we can write down the sequence

$$a_0 = g(\mathbf{m}), a_1 = h(\mathbf{m}, 0, a_0), a_2 = h(\mathbf{m}, 1, a_1), \ldots, a_n = h(\mathbf{m}, n-1, a_{n-1}),$$

that is, the sequence $(a_i)_{i=0}^n$ defined by

$$a_i := \begin{cases} g(\mathbf{m}) & \text{if } i = 0 \\ h(\mathbf{m}, i-1, a_{i-1}) & \text{if } i \geq 1 \end{cases}. \tag{2.4.3}$$

Since $(a_i)_{i=0}^n$ is a finite sequence in $\mathbb{N}$, there exist $c, d \in \mathbb{N}$ such that $\beta(c, d, i) = a_i$ for all $0 \leq i \leq n$ by Lemma 2.4.1.11. Furthermore, by definition of the function f and of the sequence (a_i), we have that $a_n = f(\mathbf{m}, n) = p$. We show that $\vdash \Theta(\overline{\mathbf{m}}, \overline{n}, \overline{p}, \overline{c}, \overline{d})$. Since c, d encode the sequence (a_i) and Λ numeralwise represents β in $\mathbb{T}$ by Lemma 2.4.1.12, we have that $\vdash \Lambda(\overline{c}, \overline{d}, 0, \overline{g(\mathbf{m})})$ and $\vdash \Lambda(\overline{c}, \overline{d}, \overline{n}, \overline{p})$. Since φ_g numeralwise represents g in $\mathbb{T}$, we have that $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{g(\mathbf{m})})$. Thus, we obtain

$$\vdash (\exists u)(\Lambda(\overline{c}, \overline{d}, 0, u) \wedge \varphi_g(\overline{\mathbf{m}}, u)) \wedge \Lambda(\overline{c}, \overline{d}, \overline{n}, \overline{p}) \tag{2.4.4}$$

by ($\exists$-I) and ($\wedge$-I). If $n = 0$, then $\overline{n}$ is the term 0 in $\mathbb{T}$ and so $w < \overline{n}$ is provably false in $\mathbb{T}$ by Proposition 2.2.2.8. Hence, we obtain

$$\vdash (\forall w)(w < \overline{n} \Rightarrow (\exists v)(\exists v')(\Lambda(\overline{c}, \overline{d}, w, v) \wedge \Lambda(\overline{c}, \overline{d}, S(w), v') \wedge \varphi_h(\overline{\mathbf{m}}, w, v, v'))) \tag{2.4.5}$$

by (Con), (⇒-I), and (∀-I). If $n \neq 0$, we obtain

$$\vdash w < \overline{n} \Leftrightarrow w = 0 \vee \ldots \vee w = \overline{n-1}$$

by Proposition 2.2.2.8. Now suppose that $j < n$. Then, $\beta(c, d, j) = a_j$ and $\beta(c, d, j+1) = a_{j+1} = h(\mathbf{m}, j, a_j)$. Since φ_h numeralwise represents h in $\mathbb{T}$ and $\vdash \overline{j+1} = S\left(\overline{j}\right)$ by the definition of numerals, we obtain

$$\vdash \Lambda(\overline{c}, \overline{d}, \overline{j}, \overline{a_j}) \wedge \Lambda(\overline{c}, \overline{d}, S(\overline{j}), \overline{a_{j+1}}) \wedge \varphi_h(\overline{\mathbf{m}}, \overline{j}, \overline{a_j}, \overline{a_{j+1}}).$$

It thus follows that, for all $0 \leq j < n$,

$$w = \overline{j} \vdash (\exists v)(\exists v')(\Lambda(\overline{c}, \overline{d}, w, v) \wedge \Lambda(\overline{c}, \overline{d}, S(w), v') \wedge \varphi_h(\overline{\mathbf{m}}, w, v, v')).$$

Therefore, we obtain (2.4.5) for $n \geq 0$ by (∨-E), (⇒-I), and (∀-I), and so in fact (2.4.5) holds in all possible cases.

Then, $\vdash \Theta(\overline{\mathbf{m}}, \overline{n}, \overline{p}, \overline{c}, \overline{d})$ follows from (2.4.4) and (2.4.5) by (∧-I), and so we obtain $\vdash \rho(\overline{\mathbf{m}}, \overline{n}, \overline{p})$ by (∃-I). Therefore, condition (P1') for $\rho(\mathbf{x}, y, z)$ is satisfied. ∎

Now note that if we could show that the formula $\rho(\mathbf{x}, y, z)$ in Lemma 2.4.1.13 satisfies condition (P2), it would follow that functions obtained by primitive recursion from numeralwise representable functions are themselves numeralwise representable in any arithmetical theory $\mathbb{T}$. However, the following problem occurs when trying to show condition (P2) for $\rho(\mathbf{x}, y, z)$ when $\mathbb{T}$ is not assumed to have induction. Let $(\mathbf{m}, n) \in \mathbb{N}^k$. Since $\mathbb{T}$ is an arbitrary arithmetical theory, it does not necessarily satisfy (EP), and so there do not necessarily exist $n_0, n_1, m_0, m_1 \in \mathbb{N}$ such that

$$\rho(\overline{\mathbf{m}}, \overline{n}, z) \wedge \rho(\overline{\mathbf{m}}, \overline{n}, z') \vdash \Theta(\overline{\mathbf{m}}, \overline{n}, z, \overline{n_0}, \overline{n_1}) \wedge \Theta(\overline{\mathbf{m}}, \overline{n}, z', \overline{m_0}, \overline{m_1}) \tag{2.4.6}$$

holds in $\mathbb{T}$. If there did exist such $n_0, n_1, m_0, m_1 \in \mathbb{N}$, we could use condition (P2) for Λ in order to conclude from (2.4.6) that

$$\rho(\overline{\mathbf{m}}, \overline{n}, z) \wedge \rho(\overline{\mathbf{m}}, \overline{n}, z') \vdash z = z' \tag{2.4.7}$$

holds in $\mathbb{T}$. However, instead of (2.4.6), we obtain

$$\rho(\overline{\mathbf{m}}, \overline{n}, z) \wedge \rho(\overline{\mathbf{m}}, \overline{n}, z') \overset{a_0, a_1, b_0, b_1}{\vdash} \Theta(\overline{\mathbf{m}}, \overline{n}, z, a_0, a_1) \wedge \Theta(\overline{\mathbf{m}}, \overline{n}, z', b_0, b_1) \tag{2.4.8}$$

for some arbitrary a_0, a_1, b_0, b_1. We therefore require condition (P3) for Λ instead of condition (P2) in order to obtain (2.4.7) from (2.4.8). Recall from Lemma 2.4.1.12 that we have only proved that Λ satisfies condition (P3) when $\mathbb{T}$ has induction, in which case Λ in fact strongly represents β in $\mathbb{T}$. Furthermore, to show that the primitive recursive functions are strongly representable in a certain theory, we only need to consider the representability of functions obtained by primitive recursion from strongly representable functions, as noted at the end of Section 2.4.1.1. Therefore, we only consider strong representability and arithmetical theories with induction in this section. Theories without induction and other types of representability will be considered later using a different approach.

So, let $\mathbb{T}$ be an arithmetical theory with induction. We wish to use the formulas from Lemma 2.4.1.13 in order to show that functions obtained by primitive recursion from strongly representable functions are themselves strongly representable in $\mathbb{T}$. In particular, we wish to use induction on y in $\mathbb{T}$ to show condition (P4) for $\rho(\mathbf{x}, y, z)$, namely $\vdash (\exists z)\rho(\mathbf{x}, y, z)$. In order to establish the base case, that is, in order to prove

$$\vdash (\exists z)\rho(\mathbf{x}, 0, z),$$

we need to be able to formalise in $\mathbb{T}$ the process of encoding sequences of length one via β. In order to establish the induction step, that is, in order to prove

$$\vdash (\exists z)\rho(\mathbf{x}, y, z) \Rightarrow (\exists z)\rho(\mathbf{x}, S(y), z),$$

we need to formalise in $\mathbb{T}$ the process of encoding sequences obtained by appending an element to a previously encoded sequence. To do so, it suffices to show that

$$\vdash (\forall x)(\exists u)(\exists v)\Lambda(u, v, 0, x) \tag{2.4.9}$$

and

$$\vdash (\forall y, u, v, x)(\exists u', v')[(\forall w)(w \leq y \Rightarrow (\exists z)(\Lambda(u, v, w, z) \wedge \Lambda(u', v', w, z))) \wedge \Lambda(u', v', S(y), x)], \tag{2.4.10}$$

hold in $\mathbb{T}$, as stated in [14, §49]. (2.4.9) formalises the existence of encodings of sequences of length one and thus allows us to establish the base case. We can prove that (2.4.9) holds in $\mathbb{T}$ by constructing primitive recursive functions that give an encoding for sequences of length one and then representing them in $\mathbb{T}$, as shown in Lemma 2.4.1.14. (2.4.10) allows us to establish the induction step. As stated in [14, §49, Remark 1], an analogous result is proved in Hilbert and Bernays (1934, pp. 401–419) for another formal system, and so it can be inferred that (2.4.10) holds in both the classical and intuitionistic formal system for number theory in [14] (see Remark 1, §49 and the discussion preceding Example 9, §74 in [14]). Since our arithmetical theories with induction correspond to extensions of the formal system for number theory in [14] as noted after Definition 2.2.2.10, we may conclude that the same result holds in our case. That is to say, we assume that (2.4.10) holds in any arithmetical theory with induction.

Lemma 2.4.1.14 *Let $\mathbb{T}$ be an arithmetical theory with induction and let Λ be the formula strongly representing β in $\mathbb{T}$, as defined in Lemma 2.4.1.12. Then,*

$$\vdash (\forall x)(\exists u)(\exists v)\Lambda(u, v, 0, x)$$

holds in $\mathbb{T}$.

Proof Note that $\beta(0,0,0) = \mathrm{rm}(0,1) = 0$ and so the pair $(0,0)$ is an encoding of the sequence (0) via β. Furthermore, for all $n \geq 1$, we have that $\beta(2n+1, n, 0) = \mathrm{rm}(2n+1, n+1) = n$ as $2n+1 = (n+1) \cdot 1 + n$, where $n < n+1$. Hence, the pair $(2n+1, n)$ is an encoding of the sequence (n) via β. We shall show that the same is provably true for variables in $\mathbb{T}$, that is, we shall show that

$$\vdash \Lambda(0,0,0,0)$$

and

$$\vdash x \neq 0 \Rightarrow \Lambda(x + S(x), x, 0, x).$$

Since $\beta(0,0,0) = 0$, it follows by condition (P1') for Λ that $\vdash \Lambda(0,0,0,0)$ holds in $\mathbb{T}$, from which we obtain

$$\vdash x = 0 \Rightarrow (\exists u)(\exists v)\Lambda(u, v, 0, x).$$

Furthermore, using the properties of inequality, multiplication, and addition in $\mathbb{T}$ from Propositions 2.2.2.8 and 2.2.2.12 and Lemma 2.2.2.7, we obtain

$$x \neq 0 \vdash \overline{1} \leq x + S(x) \wedge x + S(x) = S(x) \cdot \overline{1} + x \wedge x < x + S(x)$$

and

$$\vdash S(x) = (0 + \overline{1}) \cdot x + \overline{1}.$$

Hence, we obtain

$$x \neq 0 \vdash \delta(x + S(x), (0 + \overline{1}) \cdot x + \overline{1}, x)$$

by ($\exists$-I) and (=-E), and so

$$\vdash x \neq 0 \Rightarrow \Lambda(x + S(x), x, 0, x)$$

follows by the definition of Λ from Lemma 2.4.1.12 and ($\Rightarrow$-I). Since we obtain $\vdash x = 0 \vee x \neq 0$ by (DE), it follows by ($\vee$-E) and ($\forall$-I) that

$$\vdash (\forall x)(\exists u)(\exists v)\Lambda(u, v, 0, x)$$

holds in $\mathbb{T}$. ■

Thus, (2.4.9) indeed holds in any arithmetical theory with induction. Note that, in the proof of Lemma 2.4.1.14, we only need induction in $\mathbb{T}$ in order to establish that addition and multiplication are commutative on variables in $\mathbb{T}$. If we instead added the commutativity of addition and multiplication on variables as axioms in an arithmetical theory $\mathbb{T}$ without induction (similarly to the treatment of Robinson's theory in [14]), we could prove that Lemma 2.4.1.14 holds in such an arithmetical theory.

We also present an equivalent formulation of (2.4.10), as it is more appropriate in certain situations.

Lemma 2.4.1.15 *Let $\mathbb{T}$ be an arithmetical theory and let Λ be the formula strongly representing β in $\mathbb{T}$, as defined in Lemma 2.4.1.12. Then,*

$$\begin{aligned}\vdash (\exists u', v')[(\forall w)(w \le y \Rightarrow (\exists z)(\Lambda(u,v,w,z) \wedge \Lambda(u',v',w,z))) \wedge \Lambda(u',v',S(y),x)] \\ \Leftrightarrow (\exists u', v')[(\forall w,z)(w \le y \wedge \Lambda(u,v,w,z) \Rightarrow \Lambda(u',v',w,z)) \wedge \Lambda(u',v',S(y),x)].\end{aligned} \tag{2.4.11}$$

Hence, (2.4.10) *holds in $\mathbb{T}$ if and only if*

$$\vdash (\forall y,u,v,x)(\exists u',v')[(\forall w,z)(w \le y \wedge \Lambda(u,v,w,z) \Rightarrow \Lambda(u',v',w,z)) \wedge \Lambda(u',v',S(y),x)] \tag{2.4.12}$$

does.

Proof It follows from conditions (P3) and (P4) for Λ that

$$\begin{aligned}\vdash (\forall w)(w \le y \Rightarrow (\exists z)(\Lambda(u,v,w,z) \wedge \Lambda(u',v',w,z))) \\ \Leftrightarrow (\forall w,z)(w \le y \wedge \Lambda(u,v,w,z) \Rightarrow \Lambda(u',v',w,z))\end{aligned}$$

holds in $\mathbb{T}$. Hence, (2.4.11) follows by the Equivalence Theorem (Theorem A.3.0.7). Therefore, again by the Equivalence Theorem, (2.4.10) holds in $\mathbb{T}$ if and only if (2.4.12) does. ∎

By Lemma 2.4.1.15, since we assume that (2.4.10) holds in all arithmetical theories with induction, we may henceforth also assume that (2.4.12) holds in all arithmetical theories with induction.

We can now consider the strong representability of functions obtained by primitive recursion in arithmetical theories with induction.

Proposition 2.4.1.16 *Let $\mathbb{T}$ be an arithmetical theory with induction, let $k \ge 0$, and let $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$ be total functions that are strongly representable in $\mathbb{T}$ by the formulas $\varphi_g(\mathbf{x}, u)$ and $\varphi_h(\mathbf{x}, v_1, v_2, v_3)$, respectively. Let $f : \mathbb{N}^{k+1} \to \mathbb{N}$ be obtained from g, h by primitive recursion. As in Lemma 2.4.1.13, let $\Theta(\mathbf{x}, y, z, q_0, q_1)$ be the formula*

$$\begin{aligned}(\exists u)(\Lambda(q_0,q_1,0,u) \wedge \varphi_g(\mathbf{x},u)) \wedge \Lambda(q_0,q_1,y,z) \wedge \\ (\forall w)[w < y \Rightarrow (\exists v)(\exists v')(\Lambda(q_0,q_1,w,v) \wedge \Lambda(q_0,q_1,S(w),v') \wedge \varphi_h(\mathbf{x},w,v,v'))],\end{aligned}$$

where Λ is the representing formula for β given in Lemma 2.4.1.12, and define

$$\rho(\mathbf{x}, y, z) \underset{\text{def}}{\equiv} (\exists q_0)(\exists q_1)\Theta(\mathbf{x}, y, z, q_0, q_1).$$

Then, $\rho(\mathbf{x}, y, z)$ strongly represents f in $\mathbb{T}$.

Proof We sketch the main ideas of the proof. For full details, see Appendix C.

By Lemma 2.4.1.13, condition (P1') holds for $\rho(\mathbf{x}, y, z)$ and f in $\mathbb{T}$. Furthermore, since $\mathbb{T}$ has induction, Λ strongly represents β in $\mathbb{T}$ by Lemma 2.4.1.12.

In order to show that condition (P3) holds for ρ, we first show

$$\vdash \Theta(\mathbf{x}, y, z, u_0, v_0) \wedge \Theta(\mathbf{x}, y, z', u_0', v_0') \Rightarrow (\forall p)(\forall r)(\Lambda(u_0, v_0, p, r) \wedge p \leq y \Rightarrow \Lambda(u_0', v_0', p, r)) \tag{2.4.13}$$

by induction on the variable p in $\mathbb{T}$. (2.4.13) states that u_0, v_0 and u_0', v_0' encode the same sequence. Indeed, both sequences have initial parameters $\mathbf{x}$, last index y, and are constructed using the same formulas φ_g and φ_h. Hence, we can use condition (P3) for φ_g, φ_h, and Λ to show (2.4.13). We then obtain condition (P3) for ρ using (2.4.13) and condition (P3) for Λ.

In order to show condition (P4) for ρ, we proceed by induction on y in $\mathbb{T}$. As noted in the discussion preceding Lemma 2.4.1.14, we use (2.4.9) to show

$$\vdash (\exists z)\rho(\mathbf{x}, 0, z)$$

and (2.4.10) to show

$$\vdash (\exists z)\rho(\mathbf{x}, y, z) \Rightarrow (\exists z)\rho(\mathbf{x}, S(y), z).$$

We then obtain

$$\vdash (\exists z)\rho(\mathbf{x}, y, z)$$

by induction on y in $\mathbb{T}$, and so condition (P4) holds for ρ in $\mathbb{T}$.

Thus, $\rho(\mathbf{x}, y, z)$ satisfies conditions (P1'), (P3), and (P4), and hence strongly represents the function $f : \mathbb{N}^{k+1} \to \mathbb{N}$ in $\mathbb{T}$. ∎

It follows immediately from Proposition 2.4.1.16 that for any arithmetical theory $\mathbb{T}$ with induction, the class of total functions strongly representable in $\mathbb{T}$ is closed under primitive recursion.

2.4.1.5 Numeralwise and type-one representability of total recursive functions

We wish to show that all primitive recursive functions are numeralwise representable in any arithmetical theory in order to completely characterise the representability of primitive recursive functions in such theories.

As noted in Section 2.4.1.4, it does not seem possible to prove Proposition 2.4.1.16 for numeralwise representability in arithmetical theories without induction. We shall instead show that all total recursive functions are numeralwise representable in any arithmetical theory and conclude that all primitive recursive functions are numeralwise representable in any arithmetical theory.

Since Definition 2.1.2.7 gives an alternate characterisation of the class of total recursive functions without referring to the primitive recursion scheme (PR), we can show that all total recursive functions are numeralwise representable in any arithmetical theory without having to give an explicit construction for functions obtained by primitive recursion. We do, however, need to consider the representability of functions obtained by total minimisation. We first consider the more general case of partial minimisation applied to total functions.

Lemma 2.4.1.17 *Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. Let $g : \mathbb{N}^{k+1} \to \mathbb{N}$ be a total function that is numeralwise representable in $\mathbb{T}$ by the formula $\varphi_g(\mathbf{x}, y, z)$ and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be obtained from g by partial minimisation. That is to say, f is defined by*

$$f(\mathbf{m}) \simeq \mu_n(g(\mathbf{m}, n) = 0)$$

for all $\mathbf{m} \in \mathbb{N}^k$. Then, f is type-one representable in $\mathbb{T}$ by the formula

$$\psi(\mathbf{x}, u) \underset{\text{def}}{\equiv} \varphi_g(\mathbf{x}, u, 0) \wedge (\forall w)(w < u \Rightarrow \neg\varphi_g(\mathbf{x}, w, 0)).$$

Proof In order to show that condition (P3) holds for $\psi(\mathbf{x}, u)$ in $\mathbb{T}$, take both $\psi(\mathbf{x}, u)$ and $\psi(\mathbf{x}, v)$ as premisses. We obtain $\varphi_g(\mathbf{x}, u, 0)$ and $\varphi_g(\mathbf{x}, v, 0)$ from $\psi(\mathbf{x}, u)$ and $\psi(\mathbf{x}, v)$, respectively. If we suppose additionally that $u < v$, we obtain $\neg\varphi_g(\mathbf{x}, u, 0)$ from $\psi(\mathbf{x}, v)$, a contradiction. Supposing $v < u$ yields an analogous contradiction, and so it must follow that $u = v$. Hence, condition (P3) holds for $\psi(\mathbf{x}, u)$ in $\mathbb{T}$.

It remains to show condition (P1). Let $\mathbf{m} \in \mathbb{N}^k$ and $p \in \mathbb{N}$. Recall that since g is total, $f(\mathbf{m})$ is defined if and only if there exists an $n \in \mathbb{N}$ such that $g(\mathbf{m}, n) = 0$. Suppose first that $f(\mathbf{m}) \simeq p$. By the definition of f, it follows that $g(\mathbf{m}, p) = 0$ and so $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{p}, 0)$ by condition (P1') for φ_g. It remains to show that

$$\vdash (\forall w)(w < \overline{p} \Rightarrow \neg\varphi_g(\overline{\mathbf{m}}, w, 0)) \tag{2.4.14}$$

There are two cases to consider.

Case 1: Suppose that $p = 0$. Since $\overline{p}$ is the term 0, it follows by Proposition 2.2.2.8 that $\vdash \neg(w < \overline{p})$. Hence, we obtain $\vdash (\forall w)(w < \overline{p} \Rightarrow \neg\varphi_g(\overline{\mathbf{m}}, w, 0))$ by (Con), ($\Rightarrow$-I), and ($\forall$-I).

Case 2: Suppose that $p \neq 0$. Then, by definition of f, $g(\mathbf{m}, n) \neq 0$ for all $n < p$. Hence, for all $n < p$, we have that $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{n}, \overline{g(\mathbf{m}, n)})$, and so $\vdash \neg\varphi_g(\overline{\mathbf{m}}, \overline{n}, 0)$, by condition (P2) for φ_g and Lemma 2.2.2.6. Thus, for all $n < p$, we obtain $\vdash w = \overline{n} \Rightarrow \neg\varphi_g(\mathbf{x}, w, 0)$. Since we also have $\vdash w < \overline{p} \Leftrightarrow w = 0 \vee \ldots \vee w = \overline{p-1}$ by Proposition 2.2.2.8, it follows by ($\vee$-E), ($\Rightarrow$-I), and ($\forall$-I) that $\vdash (\forall w)(w < \overline{p} \Rightarrow \neg\varphi_g(\mathbf{x}, w, 0))$ holds in $\mathbb{T}$.

Hence, (2.4.14) holds, and so we obtain $\vdash \psi(\overline{\mathbf{m}}, \overline{p})$ by ($\wedge$-I).

Now suppose that $f(\mathbf{m}) \not\simeq p$ and suppose to the contrary that $\vdash \psi(\overline{\mathbf{m}}, \overline{p})$. Since $f(\mathbf{m}) \not\simeq p$, either $f(\mathbf{m})\downarrow$ but $f(\mathbf{m}) \neq p$, or $f(\mathbf{m})\uparrow$. In the first case, we have that

$\vdash \psi(\overline{\mathbf{m}},\overline{f(\mathbf{m})})$ and so we obtain $\vdash \overline{f(\mathbf{m})} = \overline{p}$ from condition (P3) for ψ. But $f(\mathbf{m}) \neq p$, and so this is a contradiction by Lemma 2.2.2.6. In the second case, $f(\mathbf{m})\uparrow$. Since g is a total function, it follows that for each $n \in \mathbb{N}$, $g(\mathbf{m}, n) \neq 0$. In particular, $g(\mathbf{m}, p) \neq 0$ and we obtain $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{p}, \overline{g(\mathbf{m}, p)})$ by condition (P1') for φ_g. Furthermore, we obtain $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{p}, 0)$ from $\vdash \psi(\overline{\mathbf{m}}, \overline{p})$ by ($\wedge$-E). Hence, it follows by condition (P2) for φ_g that $\vdash \overline{g(\mathbf{m}, p)} = 0$. But $g(\mathbf{m}, p) \neq 0$, and so this is a contradiction by Lemma 2.2.2.6. We thus obtain $\nvdash \psi(\overline{\mathbf{m}}, \overline{p})$ in both cases. Therefore, condition (P1) holds in $\mathbb{T}$ for $\psi(\mathbf{x}, u)$, and so $\psi(\mathbf{x}, u)$ type-one represents f in $\mathbb{T}$. ∎

Note that the proof of condition (P1) for ψ in Lemma 2.4.1.17 fails when g is allowed to be any partial function, even if we require g to be strongly representable in $\mathbb{T}$ by φ_g. Indeed, in order to obtain the last contradiction, we obtained $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{p}, \overline{g(\mathbf{m}, p)})$ by condition (P1') for φ_g and then gained a contradiction since $g(\mathbf{m}, p) \neq 0$. However, if we let g be non-total, then the best we can obtain in the case when $g(\mathbf{m}, p)\uparrow$ is $\vdash (\exists z)\varphi_g(\overline{\mathbf{m}}, \overline{p}, z)$ by condition (P4) for φ_g, provided that φ_g strongly represents g in $\mathbb{T}$. However, by condition (P1') for φ_g, there will not exist an $n \in \mathbb{N}$ such that $\vdash \varphi_g(\overline{\mathbf{m}}, \overline{p}, \overline{n})$ (and in particular, the Existence Property cannot hold for $\mathbb{T}$ since otherwise the non-total function g cannot be strongly representable in $\mathbb{T}$). Hence, we cannot use the argument at the end of the proof of Lemma 2.4.1.17 in order to gain a contradiction, and so the proof fails when g is allowed to be a non-total function.

Corollary 2.4.1.18 *Let $\mathbb{T}$ be an arithmetical theory. The class of total numerical functions numeralwise (type-one, respectively) representable in $\mathbb{T}$ is closed under total minimisation.*

Proof This follows from Lemma 2.4.1.17 and Lemma 2.3.1.5 as total minimisation is a special case of partial minimisation and yields only total functions. ∎

Theorem 2.4.1.19 *Let $\mathbb{T}$ be an arithmetical theory. All total recursive functions are numeralwise representable in $\mathbb{T}$.*

Proof By Definition 2.1.2.7, in order to show that all total recursive functions are numeralwise representable in $\mathbb{T}$, it suffices to show that U_i^k for $k \geq i \geq 1$, $+$, $\cdot$, and $K_<$ are numeralwise representable in $\mathbb{T}$ and that the class of total numerical functions numeralwise representable in $\mathbb{T}$ is closed under substitution and total minimisation.

By Proposition 2.4.1.1, the projection functions $U_i^k : \mathbb{N}^k \to \mathbb{N}$ are strongly representable in $\mathbb{T}$ for all $k \geq i \geq 1$. By Corollary 2.4.1.8, addition and multiplication are strongly representable in $\mathbb{T}$. Hence, the projections, addition, and multiplication are also numeralwise representable in $\mathbb{T}$. Since $K_< : \mathbb{N}^2 \to \mathbb{N}$ is the characteristic function of the inequality predicate $m < n$, $K_<$ is defined by

$$K(m, n) = \begin{cases} 0 & \text{if } m < n \\ 1 & \text{if } m \not< n \end{cases}$$

By Proposition 2.4.1.7, the predicate $m < n$ is numeralwise representable in $\mathbb{T}$ by the formula $x < y$. Hence, by Lemma 2.3.2.2, it follows that $K_<$ is numeralwise representable in $\mathbb{T}$ by the formula

$$\varphi_{K_<}(x, y, z) \underset{\text{def}}{\equiv} (x < y \wedge z = 0) \vee (\neg(x < y) \wedge z = \overline{1}).$$

By Proposition 2.4.1.4 and Corollary 2.4.1.18, the class of total functions that are numeralwise representable in $\mathbb{T}$ is closed under substitution and total minimisation. Hence, all total recursive functions are numeralwise representable in $\mathbb{T}$. ■

Corollary 2.4.1.20 *Let $\mathbb{T}$ be an arithmetical theory. All total recursive predicates on $\mathbb{N}$ are numeralwise representable in $\mathbb{T}$.*

Proof This follows directly from Theorem 2.4.1.19 and Lemma 2.3.2.2. ■

Lemma 2.4.1.21 *Let $\mathbb{T}$ be an arithmetical theory. If $\mathbb{T}$ is either classical or has induction, then the functions U_i^k for $k \geq i \geq 1$, $+$, $\cdot$, and $K_<$ given as basic functions for the class of total recursive functions in Definition 2.1.2.7 are strongly representable in $\mathbb{T}$.*

Proof Let $\mathbb{T}$ be an arithmetical theory. As noted in the proof of Theorem 2.4.1.19, the projection functions, addition, and multiplication are strongly representable in $\mathbb{T}$.

As shown in the proof of Theorem 2.4.1.19, $K_<$ is numeralwise representable in $\mathbb{T}$ by the formula

$$\varphi_{K_<}(x, y, z) \underset{\text{def}}{\equiv} (x < y \wedge z = 0) \vee (\neg(x < y) \wedge z = \overline{1}).$$

Now suppose that

$$\vdash x < y \vee \neg(x < y) \tag{2.4.15}$$

holds in $\mathbb{T}$. Then, a treatment by cases and ($\vee$-E) yields

$$\vdash \varphi_{K_<}(x, y, z) \wedge \varphi_{K_<}(x, y, w) \Rightarrow z = w,$$

and so $\varphi_{K_<}(x, y, z)$ satisfies condition (P3) in $\mathbb{T}$. Furthermore, it follows from (2.4.15) by ($\vee$-E), (=-I), and ($\exists$-I) that

$$\vdash (\exists z)\varphi_{K_<}(x, y, z)$$

holds in $\mathbb{T}$, and so condition (P4) for $\varphi_{K_<}$ holds in $\mathbb{T}$. Therefore, if (2.4.15) holds in $\mathbb{T}$, then $K_<$ is strongly representable in $\mathbb{T}$ by $\varphi_{K_<}$.

Note that if $\mathbb{T}$ is classical, then (2.4.15) holds in $\mathbb{T}$ by (EM). Moreover, if $\mathbb{T}$ has induction (but is not necessarily classical), then

$$\vdash \neg(x < y) \Leftrightarrow y \leq x$$

holds in $\mathbb{T}$ by Proposition 2.2.2.12. Since we obtain

$$\vdash x < y \vee y \leq x$$

from axiom (M8), it then follows by the Equivalence Theorem that (2.4.15) holds in $\mathbb{T}$. Hence, if $\mathbb{T}$ is either classical or has induction, then $K_<$ is strongly representable in $\mathbb{T}$ by $\varphi_{K_<}$ as shown above, which completes the proof. ■

Theorem 2.4.1.22 *Let $\mathbb{T}$ be either a classical arithmetical theory or an arithmetical theory with induction. All total recursive functions are type-one representable in $\mathbb{T}$.*

Proof By 2.4.1.21, U_i^k for $k \geq i \geq 1$, $+$, $\cdot$, and $K_<$ are strongly representable in $\mathbb{T}$. Hence, they are also type-one representable in $\mathbb{T}$. By Proposition 2.4.1.4 and Corollary 2.4.1.18, the class of total functions type-one representable in $\mathbb{T}$ is closed under substitution and total minimisation. Therefore, it follows from Definition 2.1.2.7 that all total recursive functions are type-one representable in $\mathbb{T}$. ■

2.4.1.6 Characterisation of the representability of primitive recursive functions

We can now characterise the representability of primitive recursive functions in general arithmetical theories and in arithmetical theories with induction. For classical arithmetical theories (with or without induction), we present an intermediate result, but will obtain a stronger result later as a consequence of the representability theorems for partial recursive functions.

Theorem 2.4.1.23 *Let $\mathbb{T}$ be an arithmetical theory.*

(i) All primitive recursive functions are numeralwise representable in $\mathbb{T}$.

(ii) If $\mathbb{T}$ has induction, all primitive recursive functions are strongly representable in $\mathbb{T}$.

(iii) If $\mathbb{T}$ is classical (but does not necessarily have induction), all primitive recursive functions are type-one representable in $\mathbb{T}$.

Proof (i) By Theorem 2.4.1.19, all total recursive functions are numeralwise representable in $\mathbb{T}$. Since all primitive recursive functions are in fact total recursive functions, they are all numeralwise representable in $\mathbb{T}$.

(ii) Now suppose that $\mathbb{T}$ has induction. By Proposition 2.4.1.1, the basic functions are strongly representable in $\mathbb{T}$. By Proposition 2.4.1.4 and Proposition 2.4.1.16, the class of functions that are strongly representable in $\mathbb{T}$ is closed under substitution and primitive recursion. Hence, all primitive recursive functions are strongly representable in $\mathbb{T}$.

(iii) Similarly to part (i), this follows from Theorem 2.4.1.22. ■

Corollary 2.4.1.24 *Let $\mathbb{T}$ be an arithmetical theory. All primitive recursive predicates are numeralwise representable in $\mathbb{T}$. If $\mathbb{T}$ has induction, all primitive recursive predicates are strongly representable in $\mathbb{T}$.*

Proof This follows from Theorem 2.4.1.23 and Lemma 2.3.2.2. ■

2.4.2 Partial recursive functions

We wish to characterise the representability of partial recursive functions in the three types of arithmetical theories we consider. We will prove the following three theorems.
Theorem (2.4.2.6) *Let $\mathbb{T}$ be an arithmetical theory with induction. All partial recursive functions are type-one representable in $\mathbb{T}$.*

Theorem (2.4.2.8) *Let $\mathbb{T}$ be a classical arithmetical theory. All partial recursive functions are strongly representable in $\mathbb{T}$.*

Theorem (2.4.2.10) *Let $\mathbb{T}$ be an arithmetical theory. All partial recursive functions are numeralwise representable in $\mathbb{T}$.*

A key element needed to prove Theorems 2.4.2.6, 2.4.2.8, and 2.4.2.10 is the Kleene Normal Form Theorem.
Theorem 2.4.2.1 (Kleene Normal Form Theorem) [16, p. 255] *There exist a primitive recursive function $U : \mathbb{N} \to \mathbb{N}$ and, for each $k \geq 1$, a primitive recursive $(k+2)$-ary predicate $T_k(e, \mathbf{m}, n)$ on $\mathbb{N}$ such that, for any partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ $(k \geq 1)$, there exists a number $e \in \mathbb{N}$ such that*

$$f(\mathbf{m}) \simeq U(\mu_n T_k(e, \mathbf{m}, n))$$

for all $\mathbf{m} \in \mathbb{N}^k$.

Note that the predicates T_k for all $k \geq 1$ are called the (k-*ary*) *Kleene T-predicates* and that U is sometimes referred to as the *output function*.

It follows from Theorem 2.4.2.1 that, if we consider the characteristic function $K_{T_k} : \mathbb{N}^{k+2} \to \mathbb{N}$ of T_k for some $k \geq 1$, we have that K_{T_k} is primitive recursive and, for each partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, there exists an $e \in \mathbb{N}$ such that $f(\mathbf{m}) \simeq U(\mu_n(K_{T_k}(e, \mathbf{m}, n) = 0))$ for all $\mathbf{m} \in \mathbb{N}^k$. Hence, we immediately obtain the following alternate statement of the Kleene Normal Form Theorem.
Corollary 2.4.2.2 (Kleene Normal Form Theorem, alternate version) *There exist a primitive recursive function $U : \mathbb{N} \to \mathbb{N}$ and, for each $k \geq 1$, a primitive recursive function $T'_k : \mathbb{N}^{k+2} \to \mathbb{N}$ such that, for any partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ $(k \geq 1)$, there exists a number $e \in \mathbb{N}$ such that*

$$f(\mathbf{m}) \simeq U(\mu_n(T'_k(e, \mathbf{m}, n) = 0))$$

for all $\mathbf{m} \in \mathbb{N}^k$.

It follows from Corollary 2.4.2.2 that, in order to prove Theorems 2.4.2.6, 2.4.2.8, and 2.4.2.10, it suffices to consider the following:

(i) the representability of primitive recursive functions;

(ii) the representability of functions obtained from total functions by partial minimisation; and

(iii) the possible undefinedness of partial recursive functions on certain inputs.

We have already dealt with (i) and (ii). Indeed, by Theorem 2.4.1.23, all primitive recursive functions, and so in particular U and T'_k from Corollary 2.4.2.2, are numeralwise representable in all arithmetical theories, type-one representable in all classical arithmetical theories, and strongly representable in all arithmetical theories with induction. Furthermore, by Lemma 2.4.1.9, the function $T'_{k,e} : \mathbb{N}^{k+1} \to \mathbb{N}$ obtained from T'_k by fixing the first input to be some $e \in \mathbb{N}$ is also primitive recursive, and so representable in arithmetical theories according to Theorem 2.4.1.23. By Lemma 2.4.1.17, functions obtained by partial minimisation from numeralwise representable total functions are type-one representable in all arithmetical theories.

It remains to consider (iii), namely undefinedness of partial recursive functions on certain inputs. In order to deal with possible undefinedness on certain inputs, we can restrict the inputs we have to consider to the domain of definition using weak representability (see Definition 2.3.2.1). We wish to show that all recursively enumerable k-ary predicates on $\mathbb{N}$ are weakly representable in all arithmetical theories by generalising the argument in [32]. We begin with a preliminary result that generalises the one in [32, §4].

Lemma 2.4.2.3 *Let $\mathbb{T}$ be an arithmetical theory. Let $k, j \geq 0$ and let $E_1 \subseteq \mathbb{N}^k$ and $E_2 \subseteq \mathbb{N}^{k+j}$ be recursively enumerable predicates on $\mathbb{N}$. There exists a formula $\varphi(\mathbf{x}, \mathbf{u})$ in $\mathbb{T}$ with exactly $k + j$ free variables such that, for all $\mathbf{m} \in \mathbb{N}^k$ and $\mathbf{p} \in \mathbb{N}^j$,*

if $E_1(\mathbf{m})$ and $\neg E_2(\mathbf{m}, \mathbf{p})$, then $\vdash \varphi(\overline{\mathbf{m}}, \overline{\mathbf{p}})$; and

if $\neg E_1(\mathbf{m})$ and $E_2(\mathbf{m}, \mathbf{p})$, then $\vdash \neg\varphi(\overline{\mathbf{m}}, \overline{\mathbf{p}})$.

In fact, since $\mathbb{T}$ is consistent, we obtain

if $E_1(\mathbf{m})$ and $\neg E_2(\mathbf{m}, \mathbf{p})$, then $\vdash \varphi(\overline{\mathbf{m}}, \overline{\mathbf{p}})$; and

if $\neg E_1(\mathbf{m})$ and $E_2(\mathbf{m}, \mathbf{p})$, then $\nvdash \varphi(\overline{\mathbf{m}}, \overline{\mathbf{p}})$.

Proof Since E_1 and E_2 are recursively enumerable predicates, there exist primitive recursive predicates $F_1 \subseteq \mathbb{N}^{k+1}$ and $F_2 \subseteq \mathbb{N}^{k+j+1}$ such that

$$E_1(\mathbf{m}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } F_1(\mathbf{m}, n)$$

and

$$E_2(\mathbf{m}, \mathbf{p}) \text{ iff there exists an } n \in \mathbb{N} \text{ such that } F_2(\mathbf{m}, \mathbf{p}, n)$$

for all $\mathbf{m} \in \mathbb{N}^k$ and $\mathbf{p} \in \mathbb{N}^j$ by Proposition 2.1.3.3 (note that if $j = 0$, then $\mathbf{p}$ is the empty list and so can be omitted). By Corollary 2.4.1.24, there exist formulas $\psi_1(\mathbf{x}, y)$ and $\psi_2(\mathbf{x}, \mathbf{u}, y)$ that numeralwise represent F_1 and F_2 in $\mathbb{T}$, respectively.

Define

$$\varphi(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists y)(\psi_1(\mathbf{x},y) \wedge (\forall z)(z \leq y \Rightarrow \neg\psi_2(\mathbf{x},\mathbf{u},z)).$$

We will show that for all $\mathbf{m} \in \mathbb{N}^k$ and $\mathbf{p} \in \mathbb{N}^j$,

if $E_1(\mathbf{m})$ and $\neg E_2(\mathbf{m},\mathbf{p})$, then $\vdash \varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$; and

if $\neg E_1(\mathbf{m})$ and $E_2(\mathbf{m},\mathbf{p})$, then $\vdash \neg\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$.

Note that, since $\mathbb{T}$ is consistent, $\vdash \neg\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$ implies that $\nvdash \varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$. Hence, it will follow that

if $\neg E_1(\mathbf{m})$ and $E_2(\mathbf{m},\mathbf{p})$, then $\nvdash \varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$.

Let $\mathbf{m} \in \mathbb{N}^k$ and $\mathbf{p} \in \mathbb{N}^j$. Suppose first that $E_1(\mathbf{m})$ and $\neg E_2(\mathbf{m},\mathbf{p})$. Then, there exists an $n_1 \in \mathbb{N}$ such that $F_1(\mathbf{m},n_1)$ and for all $n_2 \in \mathbb{N}$, $\neg F_2(\mathbf{m},\mathbf{p},n_2)$. Hence, we obtain $\vdash \psi_1(\overline{\mathbf{m}},\overline{n_1})$ and $\vdash \neg\psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},\overline{n_2})$ for all $n_2 \in \mathbb{N}$ by condition (B) for the representability of F_1 and F_2, respectively, in $\mathbb{T}$. We thus obtain

$$\vdash z = \overline{r} \Rightarrow \neg\psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},z)$$

for all $r \leq n_1$. Since

$$\vdash z \leq \overline{n_1} \Leftrightarrow z = 0 \vee \ldots \vee z = \overline{n_1}$$

by Proposition 2.2.2.8, it then follows by ($\vee$-E), ($\Rightarrow$-I), and ($\forall$-I) that

$$\vdash (\forall z)(z \leq \overline{n_1} \Rightarrow \neg\psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},z)).$$

We then obtain $\vdash \varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$ by ($\wedge$-I) and ($\exists$-I).

Suppose instead that $\neg E_1(\mathbf{m})$ and $E_2(\mathbf{m},\mathbf{p})$. So, there exists an $n_2 \in \mathbb{N}$ such that $F_2(\mathbf{m},\mathbf{p},n_2)$ and, for all $n_1 \in \mathbb{N}$, $\neg F_1(\mathbf{m},n_1)$. Hence, we obtain $\vdash \psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},\overline{n_2})$ and $\vdash \neg\psi_1(\overline{\mathbf{m}},\overline{n_1})$ for all $n_1 \in \mathbb{N}$ by condition (B) for the representability of F_2 and F_1, respectively, in $\mathbb{T}$. Taking $\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$ as a premiss, we have

$$\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}}) \overset{a}{\vdash} \psi_1(\overline{\mathbf{m}},a) \wedge (\forall z)(z \leq a \Rightarrow \neg\psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},a)) \tag{2.4.16}$$

for some arbitrary a. By axiom (M8), we have $\overset{a}{\vdash} \overline{n_2} \leq a \vee a \leq \overline{n_2}$. If we suppose that $\overline{n_2} \leq a$, we obtain

$$\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}}), \overline{n_2} \leq a \overset{a}{\vdash} \neg\psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},\overline{n_2})$$

from (2.4.16) by ($\Rightarrow$-E), a contradiction since $\vdash \psi_2(\overline{\mathbf{m}},\overline{\mathbf{p}},\overline{n_2})$ holds in $\mathbb{T}$. If we suppose instead that $a \leq \overline{n_2}$, then $a = \overline{r}$ for some $0 \leq r \leq n_2$ by Proposition 2.2.2.8. We then obtain

$$\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}}), a = \overline{r} \overset{a}{\vdash} \psi_1(\overline{\mathbf{m}},\overline{r})$$

from (2.4.16) by (=-E), which is again a contradiction as $r \in \mathbb{N}$ and so $\vdash \neg\psi_1(\overline{\mathbf{m}},\overline{r})$ holds in $\mathbb{T}$. It thus follows by ($\vee$-E) and ($\neg$-I) that $\vdash \neg\varphi(\overline{\mathbf{m}},\overline{\mathbf{p}})$ holds in $\mathbb{T}$, which completes the proof. ∎

Note that Lemma 2.4.2.3 still holds when one or both of E_1 and E_2 are empty and when one or both of k and j is 0, provided that any lists of variables of length 0 are considered as omitted.

The fact that all recursively enumerable predicates are weakly representable in any arithmetical theory turns out to be a consequence of a more general result about the exact separability of recursively enumerable predicates in arithmetical theories, the proof of which is adapted from the proof of a similar result in [32] on exact separability of recursively enumerable sets in formal theories. For the definition of exact separability of predicates in an arithmetical theory, see Definition 2.3.2.3.

Lemma 2.4.2.4 *Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. Any two disjoint k-ary recursively enumerable predicates on $\mathbb{N}$ are exactly separable in $\mathbb{T}$.*

Proof Let $E_1, E_2 \subseteq \mathbb{N}^k$ be recursively enumerable and disjoint. Suppose first that $k = 0$. Note that there are two possible 0-ary recursively enumerable predicates on $\mathbb{N}$, namely $\varnothing$ and $\mathbb{N}^0 = \{*\}$ itself. Without loss of generality, it suffices to consider two cases. Suppose first that $E_1 = E_2 = \varnothing$. By Gödel's Incompleteness Theorem, there exists a closed undecidable formula G in $\mathbb{T}$. Then, we have $\nvdash G$ and $\nvdash \neg G$ in $\mathbb{T}$. Therefore, since $* \in \varnothing$ is false, both G and $\neg G$ weakly represent $\varnothing$ in $\mathbb{T}$. Hence, $\varnothing$ is exactly separable from itself in $\mathbb{T}$ by G. Now suppose that $E_1 = \mathbb{N}^0$ and $E_2 = \varnothing$. Consider the closed and provably true formula $\top \underset{\text{def}}{\equiv} 0 = 0$ of $\mathbb{T}$. Since $* \in \mathbb{N}^0$ is true and $\top$ is provable in $\mathbb{T}$, $\mathbb{N}^0$ is weakly representable in $\mathbb{T}$ by $\top$. Moreover, since $\nvdash \neg\top$ by the consistency of $\mathbb{T}$, $\neg\top$ weakly represents $\varnothing$ in $\mathbb{T}$. Hence, $\mathbb{N}^0$ and $\varnothing$ are exactly separable in $\mathbb{T}$ by $\top$. So, any two disjoint 0-ary recursively enumerable predicates on $\mathbb{N}$ are exactly separable in $\mathbb{T}$.

Now suppose that $k \geq 1$, let $x_1, \ldots, x_k, y$ be distinct fixed variables in $\mathbb{T}$, and let $\mathbf{x}$ denote the list $x_1, \ldots, x_k$. Recall from Section 2.2.1 that the Gödel number of a formula φ in $\mathbb{T}$ is denoted by $\ulcorner\varphi\urcorner$ and that the formula with Gödel number n is denoted by γ_n. Moreover, by Lemma 2.2.1.1, given the variables $\mathbf{x}, y$ that we have fixed, we can construct a total recursive function $g : \mathbb{N}^{k+1} \to \mathbb{N}$ such that $g(\mathbf{m}, n)$ is either the Gödel number of the formula $\gamma_n\left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}, \frac{\overline{n}}{y}\right]$ if γ_n exists (i.e. if n is the Gödel number of some formula of $\mathbb{T}$), or n itself if n is not the Gödel number of any formula of $\mathbb{T}$. That is to say, for each $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$, we have

$$g(\mathbf{m}, n) = \begin{cases} \ulcorner\gamma_n\left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}, \frac{\overline{n}}{y}\right]\urcorner & \text{if } GFOR_{\mathbb{T}}(n) \\ n & \text{if } \neg GFOR_{\mathbb{T}}(n) \end{cases}.$$

Now let $D_2 \subseteq \mathbb{N}^{k+1}$ be the predicate defined by

$$D_2(\mathbf{m}, n) \text{ if and only if } GTHM_{\mathbb{T}}(g(\mathbf{m}, n)) \tag{2.4.17}$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$, where we recall that $GTHM_{\mathbb{T}}$ is the set of Gödel numbers of theorems of $\mathbb{T}$. Note that $GTHM_{\mathbb{T}} \subseteq \mathbb{N}$ is recursively enumerable as $\mathbb{T}$ is a recursively enumerable theory and that g is a total recursive function. Hence, a straightforward argument using Proposition 2.1.3.3 shows that D_2 is also a recursively enumerable predicate on $\mathbb{N}$.

By Lemma 2.2.1.1, we also have a total recursive function $neg : \mathbb{N} \to \mathbb{N}$ such that

$$neg(n) = \begin{cases} \ulcorner \neg\gamma_n \urcorner & \text{if } GFOR_{\mathbb{T}}(n) \\ n & \text{otherwise} \end{cases}$$

for all $n \in \mathbb{N}$. Since $neg \circ g$ is the composition of two total recursive functions, it is total recursive. Hence, analogously to D_2, the predicate $D_1 \subseteq \mathbb{N}^{k+1}$ given by

$$D_1(\mathbf{m}, n) \text{ if and only if } GTHM_{\mathbb{T}}(neg(g(\mathbf{m}, n)))$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$ is a recursively enumerable predicate on $\mathbb{N}$.

We define two new predicates $H_i \subseteq \mathbb{N}^{k+1}$ $(i = 1, 2)$ as follows: for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$,

$$H_i(\mathbf{m}, n) \text{ if and only if } E_i(\mathbf{m}) \text{ or } D_i(\mathbf{m}, n).$$

Since E_i and D_i are recursively enumerable, it again follows by a straightforward argument that H_i is recursively enumerable for $i = 1, 2$.

We can now apply Lemma 2.4.2.3 to the two recursively enumerable predicates $H_1, H_2 \subseteq \mathbb{N}^{k+1}$ and obtain a formula $\varphi(\mathbf{x}, y)$ in $\mathbb{T}$ such that, for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$,

$$\text{if } H_1(\mathbf{m}, n) \text{ and } \neg H_2(\mathbf{m}, n), \text{ then } \vdash \varphi(\overline{\mathbf{m}}, \overline{n})$$

and

$$\text{if } \neg H_1(\mathbf{m}, n) \text{ and } H_2(\mathbf{m}, n), \text{ then } \vdash \neg\varphi(\overline{\mathbf{m}}, \overline{n}).$$

By the definition of the H_i and the D_i $(i = 1, 2)$, it follows that, for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$,

$$\text{if } [E_1(\mathbf{m}) \text{ or } GTHM_{\mathbb{T}}(neg(g(\mathbf{m}, n)))] \text{ and not } [E_2(\mathbf{m}) \text{ or } GTHM_{\mathbb{T}}(g(\mathbf{m}, n))], \text{ then } \vdash \varphi(\overline{\mathbf{m}}, \overline{n})$$

and

$$\text{if not } [E_1(\mathbf{m}) \text{ or } GTHM_{\mathbb{T}}(neg(g(\mathbf{m}, n)))] \text{ and } [E_2(\mathbf{m}) \text{ or } GTHM_{\mathbb{T}}(g(\mathbf{m}, n))], \text{ then } \vdash \neg\varphi(\overline{\mathbf{m}}, \overline{n}).$$

Now let q be the Gödel number of $\varphi(\mathbf{x}, y)$, that is, $q = \ulcorner \varphi(\mathbf{x}, y) \urcorner$. Then, for all $\mathbf{m} \in \mathbb{N}$, $g(\mathbf{m}, q) = \ulcorner \varphi(\overline{\mathbf{m}}, \overline{q}) \urcorner$. If we define

$$\psi(\mathbf{x}) \underset{\text{def}}{\equiv} \varphi(\mathbf{x}, \overline{q}),$$

we thus obtain

$$GTHM_{\mathbb{T}}(g(\mathbf{m}, q)) \text{ if and only if } \vdash \psi(\overline{\mathbf{m}})$$

and

$$GTHM_{\mathbb{T}}(neg(g(\mathbf{m}, q))) \text{ if and only if } \vdash \neg\psi(\overline{\mathbf{m}}).$$

Hence, we obtain that, for all $\mathbf{m} \in \mathbb{N}^k$,

$$\text{if } (E_1(\mathbf{m}) \text{ or } \vdash \neg\psi(\overline{\mathbf{m}})) \text{ and not } (E_2(\mathbf{m}) \text{ or } \vdash \psi(\overline{\mathbf{m}})), \text{ then } \vdash \psi(\overline{\mathbf{m}}) \tag{2.4.18}$$

and

$$\text{if not } (E_1(\mathbf{m}) \text{ or } \vdash \neg\psi(\overline{\mathbf{m}})) \text{ and } (E_2(\mathbf{m}) \text{ or } \vdash \psi(\overline{\mathbf{m}})), \text{ then } \vdash \neg\psi(\overline{\mathbf{m}}). \tag{2.4.19}$$

We will show that $\psi(\mathbf{x})$ exactly separates E_1 and E_2 in $\mathbb{T}$, that is, that $\psi(\mathbf{x})$ weakly represents E_1 in $\mathbb{T}$ and $\neg\psi(\mathbf{x})$ weakly represents E_2 in $\mathbb{T}$. Suppose first that neither of E_1, E_2 is empty. We obtain

$$\text{if } (E_1(\mathbf{m}) \text{ or } \vdash \neg\psi(\overline{\mathbf{m}})), \neg E_2(\mathbf{m}), \text{ and } \nvdash \psi(\overline{\mathbf{m}}), \text{ then } \vdash \psi(\overline{\mathbf{m}}) \tag{2.4.20}$$

and

$$\text{if } \neg E_1(\mathbf{m}), \nvdash \neg\psi(\overline{\mathbf{m}}), \text{ and } (E_2(\mathbf{m}) \text{ or } \vdash \psi(\overline{\mathbf{m}})), \text{ then } \vdash \neg\psi(\overline{\mathbf{m}}) \tag{2.4.21}$$

for all $\mathbf{m} \in \mathbb{N}^k$ from (2.4.18) and (2.4.19). Let $\mathbf{m} \in \mathbb{N}^k$ and suppose first that $E_1(\mathbf{m})$. Since E_1, E_2 are disjoint, we then have $\neg E_2(\mathbf{m})$. If $\nvdash \psi(\overline{\mathbf{m}})$, it follows by (2.4.20) that $\vdash \psi(\overline{\mathbf{m}})$, a contradiction. So, we must have that $\vdash \psi(\overline{\mathbf{m}})$. Conversely, suppose that $\vdash \psi(\overline{\mathbf{m}})$. As $\mathbb{T}$ is consistent, it follows that $\nvdash \neg\psi(\overline{\mathbf{m}})$. Now suppose additionally that $\neg E_1(\mathbf{m})$. It then follows by (2.4.21) that $\vdash \neg\psi(\overline{\mathbf{m}})$, a contradiction. So, $E_1(\mathbf{m})$ must hold.

Now suppose that $E_2(\mathbf{m})$. Then $\neg E_1(\mathbf{m})$ as E_1, E_2 are disjoint. If $\nvdash \neg\psi(\overline{\mathbf{m}})$, it follows by (2.4.21) that $\vdash \neg\psi(\overline{\mathbf{m}})$, a contradiction. Hence, $\vdash \neg\psi(\overline{\mathbf{m}})$. Conversely, suppose that $\vdash \neg\psi(\overline{\mathbf{m}})$. As $\mathbb{T}$ is consistent, we have that $\nvdash \psi(\overline{\mathbf{m}})$. Since $\neg E_2(\mathbf{m})$ implies by (2.4.20) that $\vdash \psi(\overline{\mathbf{m}})$, a contradiction, it follows that $E_2(\mathbf{m})$.

Therefore, $\psi(\mathbf{x})$ and $\neg\psi(\mathbf{x})$ weakly represent E_1 and E_2, respectively, in $\mathbb{T}$.

Now suppose that $E_1 = \varnothing$, but $E_2 \neq \varnothing$. Then note that H_1 is simply D_1 as $E_1(\mathbf{m})$ is false for all $\mathbf{m} \in \mathbb{N}^k$. Hence, we obtain

$$\text{if } \vdash \neg\psi(\overline{\mathbf{m}}), \neg E_2(\mathbf{m}), \text{ and } \nvdash \psi(\overline{\mathbf{m}}), \text{ then } \vdash \psi(\overline{\mathbf{m}}) \tag{2.4.22}$$

and

$$\text{if } \nvdash \neg\psi(\overline{\mathbf{m}}), \text{ and } (E_2(\mathbf{m}) \text{ or } \vdash \psi(\overline{\mathbf{m}})), \text{ then } \vdash \neg\psi(\overline{\mathbf{m}}) \tag{2.4.23}$$

for all $\mathbf{m} \in \mathbb{N}^k$ from (2.4.18) and (2.4.19). An analogous argument to the one above shows that $\neg\psi(\mathbf{x})$ weakly represents E_2. Since $E_1 = \varnothing$, in order for $\psi(\mathbf{x})$ to weakly represent E_1, we must have that $\nvdash \psi(\overline{\mathbf{m}})$ for all $\mathbf{m} \in \mathbb{N}^k$. So, let $\mathbf{m} \in \mathbb{N}^k$ and suppose that $\vdash \psi(\overline{\mathbf{m}})$. If $\nvdash \neg\psi(\overline{\mathbf{m}})$, it follows by (2.4.23) that $\vdash \neg\psi(\overline{\mathbf{m}})$, a contradiction. So, it must be true that $\vdash \neg\psi(\overline{\mathbf{m}})$. But $\mathbb{T}$ is consistent, and so this contradicts the fact that $\vdash \psi(\overline{\mathbf{m}})$ holds. Hence, $\nvdash \psi(\overline{\mathbf{m}})$. Therefore, $\psi(\mathbf{x})$ weakly represents $E_1 = \varnothing$.

Now suppose that $E_1 = E_2 = \varnothing$. Then, note that H_i is simply D_i for $i = 1, 2$. Hence, we obtain

$$\text{if} \vdash \neg\psi(\overline{\mathbf{m}}) \text{ and} \nvdash \psi(\overline{\mathbf{m}}), \text{ then} \vdash \psi(\overline{\mathbf{m}}) \tag{2.4.24}$$

and

$$\text{if} \nvdash \neg\psi(\overline{\mathbf{m}}), \vdash \psi(\overline{\mathbf{m}}), \text{ then} \vdash \neg\psi(\overline{\mathbf{m}}) \tag{2.4.25}$$

for all $\mathbf{m} \in \mathbb{N}^k$ from (2.4.18) and (2.4.19). Thus, for all $\mathbf{m} \in \mathbb{N}^k$, both $\nvdash \psi(\overline{\mathbf{m}})$ and $\nvdash \neg\psi(\overline{\mathbf{m}})$ hold, whence $\psi(\mathbf{x})$ and $\neg\psi(\mathbf{x})$ both weakly represent $\varnothing$.

Hence, in all possible cases, $\psi(\mathbf{x})$ exactly separates E_1 and E_2 in $\mathbb{T}$, which completes the proof. ∎

Since Lemma 2.4.2.4 holds even in the case when one or both of the recursively enumerable relations considered is empty, we obtain our desired result on the weak representability of recursively enumerable predicates as a consequence.

Lemma 2.4.2.5 *Let $\mathbb{T}$ be an arithmetical theory and let $k \geq 0$. Then, all k-ary recursively enumerable predicates on $\mathbb{N}$ are weakly representable in $\mathbb{T}$.*

Proof Let $E \subseteq \mathbb{N}^k$ be recursively enumerable. Note that $\varnothing \subseteq \mathbb{N}^k$ is also recursively enumerable and disjoint from E. Therefore, by Lemma 2.4.2.4, there exists a formula $\psi(\mathbf{x})$ with exactly k free variables that exactly separates E and $\varnothing$ in $\mathbb{T}$. By the definition of exact separability in Definition 2.3.2.3, it follows in particular that $\psi(\mathbf{x})$ weakly represents E in $\mathbb{T}$. ∎

We can now adapt the ideas in the proof of [25, Theorem 3.6] to prove Theorem 2.4.2.6.

Theorem 2.4.2.6 *Let $\mathbb{T}$ be an arithmetical theory with induction. All partial recursive functions are type-one representable in $\mathbb{T}$.*

Proof We first consider partial functions $f : \mathbb{N}^0 \dashrightarrow \mathbb{N}$, that is, partial constants. Note that by the proof of Lemma 2.1.2.9, f is either a total constant, in which case it is primitive recursive, or f is the 0-ary completely undefined function. In the first case, f is strongly representable in $\mathbb{T}$ by Theorem 2.4.1.23, and hence is also type-one representable in $\mathbb{T}$. In the second case, the completely undefined function $f : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ is type-one representable in $\mathbb{T}$ by the formula $y = y \wedge \bot$ (as noted in Appendix A, $\bot \underset{\text{def}}{\equiv} 0 \neq 0$ and is both closed and provably false in $\mathbb{T}$). Indeed, condition (P1) holds since f is nowhere defined and $\nvdash \overline{n} = \overline{n} \wedge \bot$ for all $n \in \mathbb{N}$. Furthermore, condition (P3) is obtained by using ($\bot$-E). Hence, all partial constants are type-one representable in $\mathbb{T}$.

Now let $k \geq 1$ and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial recursive function. By Corollary 2.4.2.2, there exist primitive recursive functions $U : \mathbb{N} \to \mathbb{N}$, $T'_k : \mathbb{N}^{k+2} \to \mathbb{N}$ and an $e \in \mathbb{N}$ such that $f(\mathbf{m}) \simeq U(\mu_n(T'_k(e, \mathbf{m}, n) = 0))$ for all $\mathbf{m} \in \mathbb{N}^k$. By Theorem 2.4.1.23, there exist formulas $\varphi(z, y)$ and $\psi(u, \mathbf{x}, z, w)$ that strongly (and so in fact type-one) represent U and T'_k, respectively, in $\mathbb{T}$. By Lemma 2.4.1.9, the function $T'_{k,e} : \mathbb{N}^{k+1} \to \mathbb{N}$, given by $T'_{k,e}(\mathbf{m}, n) = T'_k(e, \mathbf{m}, n)$ for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$, is also primitive recursive and is type-one representable in $\mathbb{T}$ by the formula $\psi(\overline{e}, \mathbf{x}, z, w)$. Hence, by Lemma 2.4.1.17, the function $g : \mathbb{N}^k \dashrightarrow \mathbb{N}$ obtained from $T'_{k,e}$ by partial minimisation, i.e. given by

$$g(\mathbf{m}) \simeq \mu_n(T'_{k,e}(\mathbf{m}, n) = T'_k(e, \mathbf{m}, n) = 0)$$

for all $\mathbf{m} \in \mathbb{N}^k$, is type-one representable in $\mathbb{T}$ by some formula $\sigma(\mathbf{x}, z)$. Now let $D_f \subseteq \mathbb{N}^k$ be the domain of f. Note that since f is a partial recursive function, D_f is a recursively enumerable k-ary predicate on $\mathbb{N}$ by Proposition 2.1.3.3. Hence, there exists a formula $\eta(\mathbf{x})$ that weakly represents D_f in $\mathbb{T}$ by Lemma 2.4.2.5.

Define

$$\theta(\mathbf{x}, y) \underset{\text{def}}{\equiv} \eta(\mathbf{x}) \wedge (\exists z)(\sigma(\mathbf{x}, z) \wedge \varphi(z, y)).$$

We claim that $\theta(\mathbf{x}, y)$ type-one represents f in $\mathbb{T}$.

Condition (P3) for $\theta(\mathbf{x}, y)$ follows from condition (P3) for σ and φ by an analogous argument to the one in the proof of Proposition 2.4.1.4.

It remains to show condition (P1). Let $\mathbf{m} \in \mathbb{N}^k$ and $p \in \mathbb{N}$. Suppose first that $f(\mathbf{m}) \simeq p$. Then, $f(\mathbf{m})\downarrow$ and so $\mathbf{m} \in D_f$. Hence, $\vdash \eta(\overline{\mathbf{m}})$ as $\eta(\mathbf{x})$ weakly represents D_f in $\mathbb{T}$. Also,

$$p = f(\mathbf{m}) = U(\mu_n(T'_k(e, \mathbf{m}, n) = 0)) = U(g(\mathbf{m})),$$

where $g(\mathbf{m})$ is defined. Hence, we have

$$\vdash \sigma\left(\overline{\mathbf{m}}, \overline{g(\mathbf{m})}\right) \wedge \varphi\left(\overline{g(\mathbf{m})}, \overline{p}\right)$$

by condition (P1) for σ and φ. Thus, we obtain

$$\vdash \eta(\overline{\mathbf{m}}) \wedge (\exists z)(\sigma(\overline{\mathbf{m}}, z) \wedge \varphi(z, \overline{p})),$$

that is,

$$\vdash \theta(\overline{\mathbf{m}}, \overline{p}),$$

by ($\exists$-I) and ($\wedge$-I).

Now suppose conversely that $\vdash \theta(\overline{\mathbf{m}}, \overline{p})$. We obtain $\vdash \eta(\overline{\mathbf{m}})$ by ($\wedge$-E), and so $\mathbf{m} \in D_f$ since $\eta(\mathbf{x})$ weakly represents D_f in $\mathbb{T}$. Therefore, $f(\mathbf{m})\downarrow$, and so $f(\mathbf{m}) \in \mathbb{N}$. Replace p with $f(\mathbf{m})$ in the above argument shows that $\vdash \theta(\overline{\mathbf{m}}, \overline{f(\mathbf{m})})$. But then we obtain $\vdash \overline{p} = \overline{f(\mathbf{m})}$ by condition (P3) for θ. Hence, it follows by Lemma 2.2.2.6 that $f(\mathbf{m}) \simeq p$.

Hence, condition (P1) holds for f and $\theta(\mathbf{x}, y)$, from which it follows that f is indeed type-one representable in $\mathbb{T}$ by $\theta(\mathbf{x}, y)$.

Therefore, all partial recursive functions are type-one representable in $\mathbb{T}$. ∎

Corollary 2.4.2.7 *Let $\mathbb{T}$ be a classical arithmetical theory. All partial recursive functions are type-one representable in $\mathbb{T}$.*

Proof Note that in the proof of Theorem 2.4.2.6, the fact that the theory $\mathbb{T}$ considered there had induction was only used in order to obtain from Theorem 2.4.1.23 (ii) formulas that strongly represent U and T'_k in $\mathbb{T}$. In fact, the arguments in the proof of Theorem 2.4.2.6 would still hold if U and T'_k were merely type-one representable in $\mathbb{T}$ since we never used condition (P4) for the formulas φ and ψ representing U and T'_k, respectively, in $\mathbb{T}$ in the proof.

If $\mathbb{T}$ is a classical arithmetical theory (with or without induction), Theorem 2.4.1.23 (iii) yields formulas $\varphi(z, y)$ and $\psi(u, \mathbf{x}, z, w)$ that type-one represent U and T'_k in $\mathbb{T}$. Hence, since induction in $\mathbb{T}$ is used nowhere else in the proof of Theorem 2.4.2.6, the same proof shows that all partial recursive functions are type-one representable in the classical arithmetical theory $\mathbb{T}$. ■

By Theorem 2.3.3.3, it is not possible to strongly represent all partial recursive functions in *intuitionistic* arithmetical theories, even in those with induction. However, we can show that all partial recursive functions are strongly representable in all *classical* arithmetical theories. In order to deal with the undefinedness of partial functions on certain inputs in the context of strong representability, we need to use the more general result in Lemma 2.4.2.4 on exact separability of recursively enumerable predicates instead of the result in Lemma 2.4.2.5 on weak representability of recursively enumerable predicates.

We adapt the argument in the proof of [25, Theorem 3.2] in order to prove Theorem 2.4.2.8.

Theorem 2.4.2.8 *Let $\mathbb{T}$ be a classical arithmetical theory. All partial recursive functions are strongly representable in $\mathbb{T}$.*

Proof First note that any partial recursive function $f : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ is either a total constant or the completely undefined partial function on $\mathbb{N}^0$. If f is a total constant, it is primitive recursive and so strongly representable in $\mathbb{T}$ by Theorem 2.4.1.23. If f is completely undefined, then f is strongly representable in $\mathbb{T}$ by the formula given in Example 2.3.3.7.

We now consider the partial recursive functions on $\mathbb{N}^k$ for $k \geq 1$. Let $k \geq 1$, let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial recursive function, and let $n_0, n_1 \in \mathbb{N}$ be distinct natural numbers. Then, the preimages

$$f^{-1}(\{n_0\}), f^{-1}(\{n_1\}) \subseteq \mathbb{N}^k$$

are two disjoint recursively enumerable predicates by Lemma 2.1.3.4. Therefore, by Lemma 2.4.2.4, there exists a formula $\sigma(\mathbf{x})$ in $\mathbb{T}$ that exactly separates $f^{-1}(\{n_0\})$ and $f^{-1}(\{n_1\})$ in $\mathbb{T}$. That is to say, $\sigma(\mathbf{x})$ and $\neg\sigma(\mathbf{x})$ weakly represent $f^{-1}(\{n_0\})$ and $f^{-1}(\{n_1\})$, respectively, in $\mathbb{T}$.

Furthermore, by Corollary 2.4.2.7, since f is partial recursive and $\mathbb{T}$ is classical, there exists a formula $\varphi(\mathbf{x}, y)$ in $\mathbb{T}$ that type-one represents f in $\mathbb{T}$. Define

$$\psi(\mathbf{x}) \underset{\text{def}}{\equiv} (\exists z)\varphi(\mathbf{x}, z) \wedge \neg\varphi(\mathbf{x}, \overline{n_0}) \wedge \neg\varphi(\mathbf{x}, \overline{n_1})$$

and

$$\theta(\mathbf{x}, y) \underset{\text{def}}{\equiv} (\psi(\mathbf{x}) \wedge \varphi(\mathbf{x}, y)) \vee (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \wedge y = \overline{n_0}) \vee (\neg\psi(\mathbf{x}) \wedge \neg\sigma(\mathbf{x}) \wedge y = \overline{n_1}).$$

We will now show that $\theta(\mathbf{x}, y)$ strongly represents f in $\mathbb{T}$.

We first show condition (P1) for $\theta(\mathbf{x}, y)$. Let $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$ and suppose that $f(\mathbf{m}) \simeq n$. We obtain $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$ by condition (P1) for $\varphi(\mathbf{x}, y)$, and so we obtain $\vdash (\exists z)\varphi(\overline{\mathbf{m}}, z)$ by ($\exists$-I). We consider three separate cases.

Case 1: Suppose first that $n \neq n_0$ and $n \neq n_1$. Then, by Lemma 2.2.2.6, it follows that $\vdash \overline{n} \neq \overline{n_0}$ and $\vdash \overline{n} \neq \overline{n_1}$. So, by condition (P3) for $\varphi(\mathbf{x}, y)$ and the fact that $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$, it follows that $\vdash \neg\varphi(\overline{\mathbf{m}}, \overline{n_0})$ and $\vdash \neg\varphi(\overline{\mathbf{m}}, \overline{n_1})$. Thus, $\vdash \psi(\overline{\mathbf{m}})$ holds, from which we obtain $\vdash \psi(\overline{\mathbf{m}}) \wedge \varphi(\overline{\mathbf{m}}, \overline{n})$ by ($\wedge$-I). We then obtain $\vdash \theta(\overline{\mathbf{m}}, \overline{n})$ by ($\vee$-I).

Case 2: Suppose that $n = n_0$. Then, $\vdash \varphi(\overline{\mathbf{m}}, \overline{n_0})$ follows by condition (P1) for $\varphi(\mathbf{x}, y)$. We thus obtain

$$\psi(\overline{\mathbf{m}}) \vdash \neg\varphi(\overline{\mathbf{m}}, \overline{n_0}) \wedge \varphi(\overline{\mathbf{m}}, \overline{n_0})$$

by ($\wedge$-E) and ($\wedge$-I), and so $\vdash \neg\psi(\overline{\mathbf{m}})$ follows by ($\neg$-I). Moreover, $\mathbf{m} \in f^{-1}(\{n_0\})$. Since $\sigma(\mathbf{x})$ weakly represents $f^{-1}(\{n_0\})$ in $\mathbb{T}$, we thus obtain $\vdash \sigma(\overline{\mathbf{m}})$. By (=-I) and ($\wedge$-I) we then obtain

$$\vdash \neg\psi(\overline{\mathbf{m}}) \wedge \sigma(\overline{\mathbf{m}}) \wedge \overline{n_0} = \overline{n_0},$$

from which it follows that $\vdash \theta(\overline{\mathbf{m}}, \overline{n_0})$ by ($\vee$-I).

Case 3: Now suppose instead that $n = n_1$. A similar argument as in Case 2, noting that $\neg\sigma(\mathbf{x})$ weakly represents $f^{-1}(\{n_1\})$, shows that

$$\vdash \neg\psi(\overline{\mathbf{m}}) \wedge \neg\sigma(\overline{\mathbf{m}}) \wedge \overline{n_1} = \overline{n_1},$$

from which we obtain $\vdash \theta(\overline{\mathbf{m}}, \overline{n_1})$ by ($\vee$-I).

In all possible cases, $f(\mathbf{m}) \simeq n$ implies $\vdash \theta(\overline{\mathbf{m}}, \overline{n})$. It remains to show the converse. So, suppose that $\vdash \theta(\overline{\mathbf{m}}, \overline{n})$. We reason once more by cases.

Case 1: Suppose first that $n \neq n_0$ and $n \neq n_1$. It follows that $\vdash \overline{n} \neq \overline{n_0}$ and $\vdash \overline{n} \neq \overline{n_1}$ by Lemma 2.2.2.6. We then obtain

$$\vdash \neg(\neg\psi(\overline{\mathbf{m}}) \wedge \sigma(\overline{\mathbf{m}}) \wedge \overline{n} = \overline{n_0})$$

and
$$\vdash \neg(\neg\psi(\overline{\mathbf{m}}) \wedge \neg\sigma(\overline{\mathbf{m}}) \wedge \overline{n} = \overline{n_1})$$
using ($\neg$-I). Since $\vdash \theta(\overline{\mathbf{m}}, \overline{n})$ holds by assumption, we then obtain
$$\vdash \psi(\overline{\mathbf{m}}) \wedge \varphi(\overline{\mathbf{m}}, \overline{n})$$
by ($\vee$-E), and so $\vdash \varphi(\overline{\mathbf{m}}, \overline{n})$ follows by ($\wedge$-E). Since $\varphi(\mathbf{x}, y)$ type-one represents f in $\mathbb{T}$, it follows by condition (P1) for $\varphi(\mathbf{x}, y)$ that $f(\mathbf{m}) \simeq n$.

Case 2: Suppose that $n = n_0$. We have $\vdash \overline{n_0} = \overline{n_0}$ by (=-I). In addition, since $n_0 \neq n_1$, we have that $\vdash \overline{n_0} \neq \overline{n_1}$ by Lemma 2.2.2.6. It follows that
$$\vdash \neg(\neg\psi(\overline{\mathbf{m}}) \wedge \neg\sigma(\overline{\mathbf{m}}) \wedge \overline{n_0} = \overline{n_1})$$
by ($\neg$-I). Furthermore, we have that
$$\psi(\overline{\mathbf{m}}) \wedge \varphi(\overline{\mathbf{m}}, \overline{n_0}) \vdash \varphi(\overline{\mathbf{m}}, \overline{n_0}) \wedge \neg\varphi(\overline{\mathbf{m}}, \overline{n_0})$$
by the definition of ψ and the rules for conjunction. Hence,
$$\vdash \neg(\psi(\overline{\mathbf{m}}) \wedge \varphi(\overline{\mathbf{m}}, \overline{n_0}))$$
follows by ($\neg$-I). Since $\vdash \theta(\overline{\mathbf{m}}, \overline{n_0})$ holds by assumption,
$$\vdash \neg\psi(\overline{\mathbf{m}}) \wedge \sigma(\overline{\mathbf{m}}) \wedge \overline{n_0} = \overline{n_0}$$
follows by ($\vee$-E). Applying ($\wedge$-E) then yields $\vdash \sigma(\overline{\mathbf{m}})$. Since $\sigma(\mathbf{x})$ weakly represents $f^{-1}(\{n_0\})$ in $\mathbb{T}$, it follows that $\mathbf{m} \in f^{-1}(\{n_0\})$, that is, that $f(\mathbf{m}) \simeq n_0$.

Case 3: Suppose instead that $n = n_1$. A similar argument to the one in Case 2, using the fact that $\neg\sigma(\mathbf{x})$ weakly represents $f^{-1}(\{n_1\})$ in $\mathbb{T}$, shows that $f(\mathbf{m}) \simeq n_1$.

Hence, $\vdash \theta(\overline{\mathbf{m}}, \overline{n})$ implies $f(\mathbf{m}) \simeq n$ in all possible cases. Therefore, condition (P1) holds for θ and f in $\mathbb{T}$.

We now show that $\theta(\mathbf{x}, y)$ satisfies condition (P4'), that is, we show $\vdash (\exists! y)\theta(\mathbf{x}, y)$. First note that by (EM) (and the commutativity of $\vee$ in $\mathbb{T}$), we obtain $\vdash \neg\psi(\mathbf{x}) \vee \psi(\mathbf{x})$ and $\vdash \neg\sigma(\mathbf{x}) \vee \sigma(\mathbf{x})$. Hence, we have that
$$\vdash \neg\psi(\mathbf{x}) \Leftrightarrow \neg\psi(\mathbf{x}) \wedge (\neg\sigma(\mathbf{x}) \vee \sigma(\mathbf{x}))$$
by ($\wedge$-E) and ($\Leftrightarrow$-I), and so we obtain
$$\vdash (\neg\psi(\mathbf{x}) \wedge (\neg\sigma(\mathbf{x}) \vee \sigma(\mathbf{x}))) \vee \psi(\mathbf{x})$$
by the Equivalence Theorem. It thus follows by the distributivity of $\wedge$ over $\vee$ in $\mathbb{T}$ that
$$\vdash (\neg\psi(\mathbf{x}) \wedge \neg\sigma(\mathbf{x})) \vee (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x})) \vee \psi(\mathbf{x}) \tag{2.4.26}$$
holds in $\mathbb{T}$. We claim that the following three provability results hold in $\mathbb{T}$:

(i) $\vdash \psi(\mathbf{x}) \Rightarrow (\exists! y)\theta(\mathbf{x}, y)$

(ii) $\vdash (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x})) \Rightarrow (\exists! y)\theta(\mathbf{x}, y)$

(iii) $\vdash (\neg\psi(\mathbf{x}) \wedge \neg\sigma(\mathbf{x})) \Rightarrow (\exists! y)\theta(\mathbf{x}, y)$

Note that $\vdash (\exists! y)\theta(\mathbf{x}, y)$ follows from (2.4.26) and (i)–(iii) by ($\vee$-E). Hence, it suffices to show that (i)–(iii) hold in $\mathbb{T}$ in order to show that $\theta(\mathbf{x}, y)$ satisfies condition (P4') in $\mathbb{T}$.

(i) We obtain $\psi(\mathbf{x}) \vdash (\exists z)\varphi(\mathbf{x}, z)$ by ($\wedge$-E). Moreover, we obtain

$$\psi(\mathbf{x}), \varphi(\mathbf{x}, a) \vdash^{a} (\psi(\mathbf{x}) \wedge \varphi(\mathbf{x}, a)) \vee (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \wedge a = \overline{n_0}) \vee (\neg\psi(\mathbf{x}) \wedge \neg\sigma(\mathbf{x}) \wedge a = \overline{n_0})$$

by ($\vee$-I). We then obtain

$$\psi(\mathbf{x}), \varphi(\mathbf{x}, a) \vdash^{a} (\exists y)\theta(\mathbf{x}, y)$$

by ($\exists$-I), from which it follows by ($\exists$-E) that

$$\psi(\mathbf{x}) \vdash (\exists y)\theta(\mathbf{x}, y).$$

We also obtain

$$\psi(\mathbf{x}), \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \vdash (\psi(\mathbf{x}) \wedge \varphi(\mathbf{x}, y)) \wedge (\psi(\mathbf{x}) \wedge \varphi(\mathbf{x}, u))$$

by applying ($\vee$-E) to both $\theta(\mathbf{x}, y)$ and $\theta(\mathbf{x}, u)$. It follows by ($\wedge$-E) and ($\wedge$-I) that

$$\psi(\mathbf{x}), \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \vdash \varphi(\mathbf{x}, y) \wedge \varphi(\mathbf{x}, u),$$

and so we obtain

$$\psi(\mathbf{x}) \vdash \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \Rightarrow y = u$$

by condition (P3) for $\varphi(\mathbf{x}, y)$ and ($\Rightarrow$-I).

Therefore, we obtain $\vdash \psi(\mathbf{x}) \Rightarrow (\exists! y)\theta(\mathbf{x}, y)$ by ($\forall$-I), ($\wedge$-I), and ($\Rightarrow$-I).

(ii) We obtain $\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \vdash \neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \wedge \overline{n_0} = \overline{n_0}$ by (=-I) and ($\wedge$-I), and so it follows by ($\vee$-I) that $\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \vdash \theta(\mathbf{x}, \overline{n_0})$. Hence, it follows by ($\exists$-I) that $\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \vdash (\exists y)\theta(\mathbf{x}, y)$.

Furthermore, we obtain

$$\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}), \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \vdash (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \wedge y = \overline{n_0}) \wedge (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \wedge u = \overline{n_0})$$

by ($\vee$-E) as in the proof of (i). It follows that

$$\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}), \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \vdash y = \overline{n_0} \wedge u = \overline{n_0},$$

and so we obtain

$$\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x}) \vdash \theta(\mathbf{x}, y) \wedge \theta(\mathbf{x}, u) \Rightarrow y = u$$

by (=-E) and ($\Rightarrow$-I).

Thus, we obtain $\vdash (\neg\psi(\mathbf{x}) \wedge \sigma(\mathbf{x})) \Rightarrow (\exists! y)\theta(\mathbf{x}, y)$ by ($\forall$-I), ($\wedge$-I), and ($\Rightarrow$-I).

(iii) An analogous argument to the proof of (ii), using n_1 instead of n_0, shows that

$$\vdash (\neg\psi(\mathbf{x}) \wedge \neg\sigma(\mathbf{x})) \Rightarrow (\exists! y)\theta(\mathbf{x}, y).$$

Thus, $\theta(\mathbf{x}, y)$ satisfies condition (P4'), and hence strongly represents f in $\mathbb{T}$. ■

Note that Theorem 2.4.2.8 holds only for classical arithmetical theories. Indeed, by Theorem 2.3.3.3, it is impossible to strongly represent non-total functions in intuitionistic arithmetical theories.

Furthermore, we now obtain a stronger result than the one in Theorem 2.4.1.23 (iii) about the representability of primitive recursive functions in classical arithmetical theories.

Corollary 2.4.2.9 *Let $\mathbb{T}$ be a classical arithmetical theory. All primitive recursive functions are strongly representable in $\mathbb{T}$.*

Proof This result follows directly from Theorem 2.4.2.8 as primitive recursive functions are in particular partial recursive functions. ■

The proof of Theorem 2.4.2.6 can be adapted to prove that all partial recursive functions are numeralwise representable in any arithmetical theory (even in the absence of induction).

Theorem 2.4.2.10 *Let $\mathbb{T}$ be an arithmetical theory. All partial recursive functions are numeralwise representable in $\mathbb{T}$.*

Proof The same argument as in the proof of Theorem 2.4.2.6 shows that all partial recursive functions $\mathbb{N}^0 \dashrightarrow \mathbb{N}$ are type-one, and so also numeralwise, representable in $\mathbb{T}$.

Let $k \geq 1$, let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial recursive function, and let $e \in \mathbb{N}$ be the natural number given by Corollary 2.4.2.2 and satisfying

$$f(\mathbf{m}) \simeq U(\mu_n(T'_k(e, \mathbf{m}, n) = 0)) \simeq U(\mu_n(T'_{k,e}(\mathbf{m}, n) = 0))$$

for all $\mathbf{m} \in \mathbb{N}^k$, as in the proof of Theorem 2.4.2.6. By Theorem 2.4.1.23, we obtain formulas $\varphi(z, y)$ and $\psi_e(\mathbf{x}, z, w)$ that numeralwise represent U and $T'_{k,e}$ in $\mathbb{T}$. Hence, by Lemma 2.4.1.17, we again obtain a formula $\sigma(\mathbf{x}, z)$ that type-one, and so also numeralwise, represents the function $g : \mathbb{N}^k \dashrightarrow \mathbb{N}$ obtained from $T'_{k,e}$ by partial minimisation. Furthermore, we also obtain a formula $\eta(\mathbf{x})$ that weakly represents the domain D_f of f in $\mathbb{T}$ by Lemma 2.4.2.5. Hence, we can show that the formula

$$\theta(\mathbf{x}, y) \underset{\text{def}}{\equiv} \eta(\mathbf{x}) \wedge (\exists z)(\sigma(\mathbf{x}, z) \wedge \varphi(z, y))$$

from the proof of Theorem 2.4.2.6 numeralwise represents f in $\mathbb{T}$.

We first show that condition (P2) holds in $\mathbb{T}$ for $\theta(\mathbf{x}, y)$. First note that, since $f(\mathbf{m}) \simeq U(g(\mathbf{m}))$ for all $\mathbf{m} \in \mathbb{N}^k$ and U is total, $f(\mathbf{m})\downarrow$ if and only if $g(\mathbf{m})\downarrow$. Hence, the domains of g and f are equal (that is, $D_g = D_f$), and so $\eta(\mathbf{x})$ also weakly represents the domain of g in $\mathbb{T}$. Let $\mathbf{m} \in \mathbb{N}^k$ and suppose that $\vdash \theta(\overline{\mathbf{m}}, y)$. We obtain $\vdash \eta(\overline{\mathbf{m}})$ by ($\wedge$-E), and so $\mathbf{m} \in D_g$ as $\eta(\mathbf{x})$ weakly represents $D_f = D_g$. Hence, $g(\mathbf{m})\downarrow$ and so we obtain $\vdash \sigma(\overline{\mathbf{m}}, \overline{g(\mathbf{m})})$ by condition (P1) for σ and g. We can then use condition (P2) for σ and φ to show that condition (P2) holds for θ in $\mathbb{T}$ via an argument similar to the one used for condition (P3) in the proof of Proposition 2.4.1.4.

Furthermore, note that in the proof of Theorem 2.4.2.6, although condition (P3) for $\theta(\mathbf{x}, y)$ is used in order to show that $\theta(\mathbf{x}, y)$ satisfies condition (P1), condition (P2) for $\theta(\mathbf{x}, y)$ is actually sufficient. Hence, the same argument holds here, and so $\theta(\mathbf{x}, y)$ satisfies condition (P1). Thus, $\theta(\mathbf{x}, y)$ numeralwise represents f in $\mathbb{T}$.

Therefore, all partial recursive functions are numeralwise representable in $\mathbb{T}$. ∎

2.4.3 Total recursive functions

We have already shown in Theorem 2.4.1.19 and Theorem 2.4.1.22 that all total recursive functions are numeralwise representable in all arithmetical theories and type-one representable in all classical arithmetical theories. Using the results on the representability of partial recursive functions from Section 2.4.2, we can completely characterise the representability of total recursive functions in arithmetical theories as follows.

Theorem 2.4.3.1 *Let $\mathbb{T}$ be an arithmetical theory.*

(i) All total recursive functions are numeralwise representable in $\mathbb{T}$.

(ii) If $\mathbb{T}$ has induction, then all total recursive functions are type-one representable in $\mathbb{T}$.

(iii) If $\mathbb{T}$ is classical (with or without induction), then all total recursive functions are strongly representable in $\mathbb{T}$.

Proof (i) This is simply Theorem 2.4.1.19, which was included here for completeness.

(ii) This follows from Theorem 2.4.2.6 as all total recursive functions are in fact partial recursive functions.

(iii) Analogously to part (ii), this follows from Theorem 2.4.2.8. ∎

2.4.4 Representable functions are partial recursive

In Theorems 2.4.2.6, 2.4.2.8, and 2.4.2.10, we have shown that, if a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is partial recursive, then it is numeralwise representable in all arithmetical theories, type-one representable in all arithmetical theories with induction, and strongly representable in all classical arithmetical theories. We now wish to show that the converses of Theorems 2.4.2.6, 2.4.2.8, and 2.4.2.10 hold. In order to do so, it suffices to show that if a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is numeralwise representable in an arithmetical theory $\mathbb{T}$, then it is in fact partial recursive.

We first need to consider a recursive bijective pairing function. One such function is the Cantor pairing function discussed in [2, 34].

Lemma 2.4.4.1 [2, 34] *Consider the* Cantor pairing function $J : \mathbb{N}^2 \to \mathbb{N}$ *defined by*

$$J(m,n) := \frac{(m+n)(m+n+1)}{2} + m = \frac{(m+n)^2 + (m+n) + 2m}{2}$$

for all $m, n \in \mathbb{N}$*. Then,* J *is a primitive recursive bijection from* $\mathbb{N}^2$ *to* $\mathbb{N}$*. Moreover, the* inverse pairing functions $J_1, J_2 : \mathbb{N} \to \mathbb{N}$ *defined by*

$$J_1(p) = \mu_{m \leq p}(\exists n \leq p)(J(m,n) = p)$$

and

$$J_2(p) = \mu_{n \leq p}(\exists m \leq p)(J(m,n) = p)$$

for all $p \in \mathbb{N}$ *are primitive recursive and satisfy*

$$J_1(J(m,n)) = m,$$

$$J_2(J(m,n)) = n,$$

and

$$J(J_1(p), J_2(p)) = p$$

for all $m, n, p \in \mathbb{N}$*. In other words, the function* $\langle J_1, J_2 \rangle : \mathbb{N} \to \mathbb{N}^2$ *is the set-theoretic inverse of* $J : \mathbb{N}^2 \to \mathbb{N}$*.*

Proof See [34, pp. 20–21, 63–64] and [2, pp. 164–165]. ■

Theorem 2.4.4.2 *Let* $\mathbb{T}$ *be an arithmetical theory, let* $k \geq 0$*, and let* $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ *be a partial function. If* f *is numeralwise representable in* $\mathbb{T}$*, then* f *is partial recursive.*

Proof As mentioned after Definition 2.2.2.3, we assume without loss of generality that every arithmetical theory is recursively axiomatised. Hence, by Lemma 2.2.1.3, $\mathbb{T}$ has a total recursive proof predicate $Pr \subseteq \mathbb{N}^2$ such that, for all $n, m \in \mathbb{N}$,

$$Pr(n,m) \text{ if and only if } GFOR_{\mathbb{T}}(n) \text{ and } m \text{ is the Gödel number of a proof of } \ulcorner \gamma_n \urcorner.$$

Let $k \geq 0$ and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial function that is numeralwise representable in $\mathbb{T}$ by the formula $\varphi(\mathbf{x}, y)$. Let z be a new variable not occurring in φ. Then, for the $k+2$ fixed variables $\mathbf{x}, y, z$, we obtain a total recursive function $g : \mathbb{N}^{k+2} \to \mathbb{N}$ such that

$$g(\mathbf{m}, n, p) = \begin{cases} \ulcorner \gamma_p \left[\frac{\overline{\mathbf{m}}}{\mathbf{x}}, \frac{\overline{n}}{y}, \frac{\overline{p}}{z} \right] \urcorner & \text{if } GFOR_{\mathbb{T}}(p) \\ p & \text{otherwise} \end{cases}.$$

for all $(\mathbf{m}, n, p) \in \mathbb{N}^{k+2}$ by Lemma 2.2.1.1. Let $q = \ulcorner \varphi(\mathbf{x}, y) \urcorner$. Then, $\gamma_q \underset{\text{def}}{\equiv} \varphi$ and, since z does not occur in φ, we have that

$$g(\mathbf{m}, n, q) = \ulcorner \varphi(\overline{\mathbf{m}}, \overline{n}) \urcorner$$

for all $\mathbf{m} \in \mathbb{N}^k$ and $n \in \mathbb{N}$. Note that the function $g_q : \mathbb{N}^{k+1} \to \mathbb{N}$ obtained from g by fixing the last argument to be q is total recursive by an argument similar to the one in Lemma 2.4.1.9. Since $\varphi(\mathbf{x}, y)$ numeralwise represents f in $\mathbb{T}$, it thus follows that, for all $\mathbf{m} \in \mathbb{N}^k$,

$$\begin{aligned} f(\mathbf{m}) &\simeq J_1(\mu_n Pr(\ulcorner \varphi(\overline{\mathbf{m}}, \overline{J_1(n)}) \urcorner, J_2(n))) \\ &\simeq J_1(\mu_n Pr(g(\mathbf{m}, J_1(n), q), J_2(n))) \\ &\simeq J_1(\mu_n (K_{Pr}(g_q(\mathbf{m}, J_1(n)), J_2(n)) = 0)). \end{aligned}$$

Thus, f is obtained from the primitive recursive functions J_1 and J_2 and the total recursive functions g_q and K_{Pr} by substitution and partial minimisation, and hence is a partial recursive function. ∎

Corollary 2.4.4.3 *Let $\mathbb{T}$ be an arithmetical theory, let $k \geq 0$, and let $\varphi(\mathbf{x}, y)$ be a formula of $\mathbb{T}$ with exactly $k+1$ free variables satisfying condition (P2), (P3), or (P4'). Then, there exists a unique partial recursive function $f_\varphi : \mathbb{N}^k \dashrightarrow \mathbb{N}$ that is numeralwise, type-one, or strongly, respectively, representable in $\mathbb{T}$ by $\varphi(\mathbf{x}, y)$. Moreover, if $\mathbb{T}$ is intuitionistic and $\varphi(\mathbf{x}, y)$ satisfies condition (P4'), then f_φ must be total.*

Proof The existence and uniqueness of f_φ, as well as its numeralwise representability by φ, follow directly from the proof of Theorem 2.4.4.2. If φ satisfies condition (P3) ((P4'), respectively), then φ in fact type-one (strongly, respectively) represents f_φ in $\mathbb{T}$. Moreover, if $\mathbb{T}$ is intuitionistic and $\varphi(\mathbf{x}, y)$ satisfies condition (P4') (equivalently, both of conditions (P3) and (P4)), then $\varphi(\mathbf{x}, y)$ strongly represents f_φ in $\mathbb{T}$. Since no non-total function is strongly representable in the intuitionistic theory $\mathbb{T}$ as noted in Section 2.3.3, it follows that f_φ must be total. ∎

We can thus summarise the results on the representability of partial recursive functions in arithmetical theories as follows.

Theorem 2.4.4.4 *Let $\mathbb{T}$ be an arithmatical theory, let $k \geq 0$, and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial function.*

(i) f is numeralwise representable in $\mathbb{T}$ if and only if it is partial recursive.

(ii) If $\mathbb{T}$ has induction, then f is type-one representable in $\mathbb{T}$ if and only if it is partial recursive.

(iii) If $\mathbb{T}$ is classical, then f is strongly representable in $\mathbb{T}$ if and only if it is partial recursive.

Proof Since a formula $\varphi(\mathbf{x}, y)$ that strongly or type-one represents a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ in an arithmetical theory $\mathbb{T}$ also numeralwise represents f in $\mathbb{T}$, these results follow directly from Theorems 2.4.2.6, 2.4.2.8, 2.4.2.10, and 2.4.4.2. ■

2.5 Conclusion

In this chapter, we have characterised the representability of primitive, total, and partial recursive functions in three types of arithmetical theories. Primitive recursive functions are numeralwise representable in all arithmetical theories and strongly representable in both arithmetical theories with induction and classical arithmetical theories (with or without induction). Total and partial recursive functions are numeralwise representable in all arithmetical theories, type-one representable in arithmetical theories with induction, and strongly representable in classical arithmetical theories. Furthermore, if a partial numerical function is numeralwise, type-one, or strongly representable in an arithmetical theory, then it must be partial recursive.

There remain a few unanswered questions. Firstly, partial recursive functions are not in general strongly representable in intuitionistic arithmetical theories with induction. Indeed, as explained in Section 2.3.3, non-total functions cannot be strongly represented in intuitionistic arithmetical theories because of the Existence Property. However, we have not yet established whether or not the total recursive functions are strongly representable in intuitionistic arithmetical theories with induction. Since the primitive recursive functions are strongly representable in intuitionistic arithmetical theories with induction, it only remains to determine whether or not the class of total functions strongly representable in an intuitionistic arithmetical theory with induction is closed under total minimisation. The issue here lies with the least number principle, which is not valid intuitionistically in general except for decidable formulas.

Secondly, we can ask if full induction is necessary in order to strongly represent all primitive recursive functions in an arithmetical theory or if a weaker form of induction on a restricted class of formulas, such as the class of Σ_1 formulas for example, would be sufficient. In particular, we would need to determine the exact necessary conditions an arithmetical theory must satisfy for the β-function to be strongly representable and for (2.4.9) and (2.4.10) to hold in this arithmetical theory (see [34] for a definition of Σ_1 formulas and for more information on this topic).

Chapter 3

Syntactic categories of first-order theories

We construct syntactic and syntactic partial map categories of arithmetical theories and consider aspects of number theory and recursion theory in this setting.

In Section 3.1 we define syntactic and syntactic partial map categories of general (first-order) theories and give constructions of some of the additional categorical structure contained in these categories. In particular, we show that the syntactic categories of a theory $\mathbb{T}$ is a regular category and that the syntactic partial map category of $\mathbb{T}$ is a cartesian restriction category. In Section 3.2, we give a construction of a strong natural numbers object in the syntactic category of an arithmetical theory with induction. In Section 3.3, we consider recursion theory in the setting of syntactic categories of arithmetical theories by considering necessary and sufficient conditions for certain subcategories of a syntactic partial map category of an arithmetical theory with induction to be a Turing category.

3.1 Syntactic and syntactic partial map categories of general first-order theories

3.1.1 Syntactic categories

3.1.1.1 Definition and basic results

In order to construct a syntactic category for an arithmetical theory $\mathbb{T}$, we first construct one for any first-order theory (either intuitionistic or classical). Our construction is similar to the construction of a syntactic category of a cartesian theory in [13, §D1.4] and to the construction of the regular category associated with an intuitionistic theory over a (possibly multi-sorted) language in [29] and [30].

Definition 3.1.1.1 Let $\mathbb{T}$ be a theory. We define the relation of $\mathbb{T}$-*provable* (or simply *provable*) *equivalence* on the formulas of $\mathbb{T}$ as follows. Let φ, ψ be formulas of $\mathbb{T}$. Then,

$$\varphi \sim \psi \text{ if and only if } \vdash \varphi \Leftrightarrow \psi.$$

This is clearly an equivalence relation on the formulas of $\mathbb{T}$. The equivalence class of a formula φ under provable equivalence is denoted by $\lceil \varphi \rceil$. □

We can now define the syntactic category of a theory $\mathbb{T}$.

Definition 3.1.1.2 The *syntactic category* $\mathscr{C}(\mathbb{T})$ of a theory $\mathbb{T}$ has the following elements:

Objects: The objects of $\mathscr{C}(\mathbb{T})$ are the formulas of $\mathbb{T}$.

Morphisms: The morphisms of $\mathscr{C}(\mathbb{T})$ are equivalence classes of formulas that are provably functional relations between the domain and codomain formulas in the following sense. Let $A(\mathbf{x})$ and $B(\mathbf{y})$ be objects of $\mathscr{C}(\mathbb{T})$ having as free variables exactly those in the lists $\mathbf{x}$ and $\mathbf{y}$ of distinct variables, respectively. An equivalence class of formulas of $\mathbb{T}$ under the equivalence relation defined in Definition 3.1.1.1 is a morphism from $A(\mathbf{x})$ to $B(\mathbf{y})$ if and only if it is an equivalence class of a formula F in $\mathbb{T}$ satisfying the following conditions:

(i) (Variable condition) The variables $\mathbf{x}$ occurring free in A also occur free in F. Suppose without loss of generality that $y_1, \ldots, y_k$ are the distinct variables forming the list $\mathbf{y}$ of free variables of B, where $k = |\mathbf{y}|$. Then, there is a corresponding list $v_1, \ldots, v_k$, denoted $\mathbf{v}$, of distinct new variables (that is, none of the v_i occur in A or B) such that each v_i occurs free in F. There are no other variables occurring free in the formula F, and hence we may denote it by $F(\mathbf{x}, \mathbf{v})$.

(ii) (Defining conditions) The following provability results, called the *defining conditions* (for a morphism from $A(\mathbf{x})$ to $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$), hold in $\mathbb{T}$.

(1) $\vdash F(\mathbf{x}, \mathbf{v}) \Rightarrow A(\mathbf{x}) \wedge B(\mathbf{v})$

(2) $\vdash A(\mathbf{x}) \Rightarrow (\exists \mathbf{v}) F(\mathbf{x}, \mathbf{v})$

(3) $\vdash F(\mathbf{x}, \mathbf{v}) \wedge F(\mathbf{x}, \mathbf{v}') \Rightarrow \mathbf{v} = \mathbf{v}'$

In practice, the following equivalent formulation of defining conditions (1)–(3) may be used.

(1) $F(\mathbf{x}, \mathbf{v}) \vdash A(\mathbf{x}) \wedge B(\mathbf{v})$

(2) $A(\mathbf{x}) \vdash (\exists \mathbf{v}) F(\mathbf{x}, \mathbf{v})$

(3) $F(\mathbf{x}, \mathbf{v}) \wedge F(\mathbf{x}, \mathbf{v}') \vdash \mathbf{v} = \mathbf{v}'$

Note also that, if B has no free variables, we have morphisms of the form $\ulcorner F(\mathbf{x}) \urcorner : A(\mathbf{x}) \to B$, where defining condition (2) for $F(\mathbf{x})$ becomes

$$\vdash A(\mathbf{x}) \Rightarrow F(\mathbf{x})$$

and where defining condition (3) for $F(\mathbf{x})$ is vacuously true, and so simply omitted in practice.

Notational conventions: The conventions for representing formulas detailed in Remark 2.3.1.3 also apply to formulas that are objects of $\mathscr{C}(\mathbb{T})$ or representatives of morphisms in $\mathscr{C}(\mathbb{T})$. Part (iv) is justified by Remark 3.1.1.8 below.

Moreover, we shall generally use letters x, y, z to denote the free variables of objects of $\mathscr{C}(\mathbb{T})$ and use the corresponding letters u, v, w, respectively, to denote the free variables in the representatives of morphisms corresponding to the free variables in their codomains. For example, a representative of a morphism from $A(\mathbf{y})$ to $B(\mathbf{x})$ will be of the form $F(\mathbf{y}, \mathbf{u})$ and a representative of a morphism from $C(\mathbf{x})$ to $D(\mathbf{z})$ will be of the form $G(\mathbf{x}, \mathbf{w})$. Furthermore, we only consider a formula $F(\mathbf{x}, \mathbf{v})$ as a candidate for a representative of a morphism from $A(\mathbf{x})$ to $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$ if the variable condition is satisfied, that is, if $\mathbf{v}$ is a list of distinct new variables such that $|\mathbf{v}| = |\mathbf{y}|$. Hence, we generally do not need to consider the variable condition explicitly as it is always understood to be satisfied whenever applicable.

Composition of morphisms: Note that we shall use diagrammatic order for the composition of morphisms in $\mathscr{C}(\mathbb{T})$. To make the distinction from the usual (i.e. functional) order clear, we shall use a semi-colon as the composition symbol when in diagrammatic order and either a circle or no symbol for the usual order. Suppose that $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner$ and $\ulcorner G(\mathbf{y}, \mathbf{w}) \urcorner$ are two morphisms in $\mathscr{C}(\mathbb{T})$ forming the diagram

$$A(\mathbf{x}) \xrightarrow{\ulcorner F(\mathbf{x},\mathbf{v}) \urcorner} B(\mathbf{y}) \xrightarrow{\ulcorner G(\mathbf{y},\mathbf{w}) \urcorner} C(\mathbf{z}) \ .$$

Their composite is defined to be $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner ; \ulcorner G(\mathbf{y}, \mathbf{w}) \urcorner := \ulcorner F(\mathbf{x}, \mathbf{v}); G(\mathbf{y}, \mathbf{w}) \urcorner$, where $F(\mathbf{x}, \mathbf{v}); G(\mathbf{y}, \mathbf{w})$, also denoted $(F; G)(\mathbf{x}, \mathbf{w})$, is the formula

$$(\exists \mathbf{q})(F(\mathbf{x}, \mathbf{q}) \wedge G(\mathbf{q}, \mathbf{w})).$$

Note that the variables in the list $\mathbf{q}$ are distinct from those in the lists $\mathbf{x}$ and $\mathbf{w}$.

Identity morphisms: Let $A(\mathbf{x})$ be an object of $\mathscr{C}(\mathbb{T})$ and define

$$\mathrm{id}_A(\mathbf{x}, \mathbf{u}) \underset{\mathrm{def}}{\equiv} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}.$$

Then, $\ulcorner \mathrm{id}_A(\mathbf{x}, \mathbf{u}) \urcorner : A(\mathbf{x}) \to A(\mathbf{x})$, i.e. the morphism

$$A(\mathbf{x}) \xrightarrow{\ulcorner A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \urcorner} A(\mathbf{x}) \ ,$$

is the identity morphism on $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. □

Remark 3.1.1.3 Note that the way we have defined morphisms in Definition 3.1.1.2 may seem needlessly complicated. Indeed, we want $\mathscr{C}(\mathbb{T})$ to be the category whose objects are formulas of $\mathbb{T}$ and whose morphisms are $\mathbb{T}$-provable equivalence classes of $\mathbb{T}$-provably functional relations between them. Hence, at first glance, it would seem to be appropriate to define a morphism from $A(\mathbf{x})$ to $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$ to be of the form $\lceil F(\mathbf{x},\mathbf{y})\rceil$, where $F(\mathbf{x},\mathbf{y})$ contains exactly the variables in the set $\{\mathbf{x},\mathbf{y}\}$ free and satisfies defining conditions analogous to the ones in Definition 3.1.1.2 (obtained by replacing $\mathbf{v}$ by $\mathbf{y}$ therein).

Suppose for the moment that we define morphisms of $\mathscr{C}(\mathbb{T})$ in this alternative manner. A problem arises when we consider morphisms on an object $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Indeed, according to the alternative definition of a morphism in $\mathscr{C}(\mathbb{T})$ given above, a morphism from $A(\mathbf{x})$ to itself would be of the form $\lceil F(\mathbf{x})\rceil$, where $F(\mathbf{x})$ contains exactly the variables in the list $\mathbf{x}$ free. But then it is no longer possible to express conditions for $F(\mathbf{x})$ to be a $\mathbb{T}$-provably functional relation from $A(\mathbf{x})$ to $A(\mathbf{x})$ as we can no longer distinguish between the variables occurring free in the domain and those occurring free in the codomain. Naturally, if $\mathbf{y}$ is a list of distinct variables disjoint from $\mathbf{x}$ such that $|\mathbf{y}| = |\mathbf{x}|$, $A(\mathbf{x})$ and $A(\mathbf{y})$ are $\mathbb{T}$-provably equivalent. A morphism $\lceil F(\mathbf{x},\mathbf{y})\rceil : A(\mathbf{x}) \to A(\mathbf{y})$ would then capture the desired notion of a morphism on $A(\mathbf{x})$, as $A(\mathbf{x})$ and $A(\mathbf{y})$ are the same formula up to change of variables and it is possible to express conditions for $F(\mathbf{x},\mathbf{y})$ to be a $\mathbb{T}$-provably functional relation from $A(\mathbf{x})$ to $A(\mathbf{y})$. Hence, in order to fix the problem arising from morphisms on a single object, we could require that morphisms in $\mathscr{C}(\mathbb{T})$ be of the form $\lceil F(\mathbf{x},\mathbf{y})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$, where $\mathbf{x}$ and $\mathbf{y}$ are disjoint lists of variables.

However, if we adopt this solution, another problem arises. Indeed, it then becomes impossible to define genuine identity morphisms in $\mathscr{C}(\mathbb{T})$, as we can no longer define morphisms $A(\mathbf{x}) \to A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Instead, we only have morphisms from $A(\mathbf{x})$ to an object that is $\mathbb{T}$-provable equivalent (and hence presumably isomorphic in $\mathscr{C}(\mathbb{T})$) to $A(\mathbf{x})$. We could conceivably fix this new problem by defining objects of $\mathscr{C}(\mathbb{T})$ to be equivalence classes of formulas of $\mathbb{T}$ under some equivalence relation under which $A(\mathbf{x})$ and $A(\mathbf{y})$ are related whenever $\mathbf{y}$ is a list of distinct variables disjoint from $\mathbf{x}$ and $|\mathbf{y}| = |\mathbf{x}|$. This would need to be a different equivalence relation from the equivalence relation given by $\mathbb{T}$-provable equivalence of formulas as defined in Definition 3.1.1.1, as otherwise all theorems of $\mathbb{T}$ would be equivalent and hence would all correspond to the same object of $\mathscr{C}(\mathbb{T})$, which would somewhat defeat the purpose of constructing $\mathscr{C}(\mathbb{T})$ to begin with. Since determining what this object-equivalence relation should be and dealing with two distinct kinds of equivalence classes in $\mathscr{C}(\mathbb{T})$ seems needlessly complicated, we chose instead to define morphisms in $\mathscr{C}(\mathbb{T})$ as in Definition 3.1.1.2. We then only need to deal with one kind of equivalence class and we can define a genuine identity morphism from $A(\mathbf{x})$ to itself for each object $A(\mathbf{x})$. Moreover, since $A(\mathbf{x})$ and $A(\mathbf{y})$ (where the variables in the list $\mathbf{y}$ are distinct and $|\mathbf{y}| = |\mathbf{x}|$) can be shown to be isomorphic in $\mathscr{C}(\mathbb{T})$ (see Remark 3.1.1.8), we can still use these objects interchangeably in $\mathscr{C}(\mathbb{T})$. However, we can now make the distinction that, while $A(\mathbf{x})$ and $A(\mathbf{y})$ are always *isomorphic* objects in $\mathscr{C}(\mathbb{T})$, they are only *equal* as objects of $\mathscr{C}(\mathbb{T})$ when $\mathbf{x}$ and $\mathbf{y}$ denote the same list of variables. □

We make the following remark on the free variables occurring in the representatives of morphisms in syntactic categories.

Remark 3.1.1.4 Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$, let $A(\mathbf{x})$ and $B(\mathbf{y})$ be two objects of $\mathscr{C}(\mathbb{T})$, and let $\mathbf{v}$ be a list of distinct new variables not occurring in either A or B such that $|\mathbf{v}| = |\mathbf{y}|$. We can assume without loss of generality that the representative of any morphism in $\mathscr{C}(\mathbb{T})$ has as free variables exactly those in the set $\{\mathbf{x}, \mathbf{v}\}$. Indeed, as defined in Definition 3.1.1.2, the variables in the list $\mathbf{x}$ of free variables of A occur free in the representative of any morphism from A to B. Moreover, for any morphism $\lceil F(\mathbf{x}, \mathbf{v}') \rceil$ from $A(\mathbf{x})$ to $B(\mathbf{y})$, we can assume without loss of generality that none of the variables in the list $\mathbf{v}$ occur as bound variables in F. Indeed, we can always replace the bound variables of F with new variables not already occurring in F. We thus obtain a variant F' of F, which is provably equivalent to F in $\mathbb{T}$, and hence is such that $\lceil F'(\mathbf{x}, \mathbf{v}') \rceil = \lceil F(\mathbf{x}, \mathbf{v}') \rceil$ as morphisms in $\mathscr{C}(\mathbb{T})$ from $A(\mathbf{x})$ to $B(\mathbf{y})$. We then obtain $\vdash F(\mathbf{x}, \mathbf{v}') \Leftrightarrow F(\mathbf{x}, \mathbf{v})$ in $\mathbb{T}$ by the Substitution Theorem, and so in fact $\lceil F(\mathbf{x}, \mathbf{v}') \rceil = \lceil F(\mathbf{x}, \mathbf{v}) \rceil$ as morphisms in $\mathscr{C}(\mathbb{T})$ from $A(\mathbf{x})$ to $B(\mathbf{y})$. In particular, it follows that whenever we consider parallel morphisms in $\mathscr{C}(\mathbb{T})$, we may without loss of generality assume that their representatives have exactly the same free variables.

In fact, by the same argument, we can say more generally that whenever we consider several morphisms in $\mathscr{C}(\mathbb{T})$ with the same codomain $C(\mathbf{z})$, we can assume without loss of generality that the chosen representatives of the morphisms into $C(\mathbf{z})$ have the same free variables $\mathbf{w}$ corresponding to the variables $\mathbf{z}$ of the codomain, regardless of the domain of the morphisms. □

We must verify that for each theory $\mathbb{T}$, $\mathscr{C}(\mathbb{T})$ as defined in Definition 3.1.1.2 is indeed a category.

Proposition 3.1.1.5 *Let $\mathbb{T}$ be a first-order theory. Then, $\mathscr{C}(\mathbb{T})$ is a category.*

Proof In order to prove this result, we must show that composition in $\mathscr{C}(\mathbb{T})$ is well-defined and that $\mathscr{C}(\mathbb{T})$ satisfies the axioms of a category. Similar results are shown in [29, 30, 13], and so we omit some of the details.

We first verify that composition of morphisms in $\mathscr{C}(\mathbb{T})$ is a well-defined operation. So, suppose we have the following morphisms in $\mathscr{C}(\mathbb{T})$:

$$A(\mathbf{x}) \xrightarrow{\lceil F_1(\mathbf{x},\mathbf{v}) \rceil = \lceil F_2(\mathbf{x},\mathbf{v}) \rceil} B(\mathbf{y}) \xrightarrow{\lceil G_1(\mathbf{y},\mathbf{w}) \rceil = \lceil G_2(\mathbf{y},\mathbf{w}) \rceil} C(\mathbf{z}), \ .$$

By Remark 3.1.1.4, we can assume that F_1 and F_2 have the same free variables, and similarly for G_1 and G_2. We obtain $\lceil F_1; G_1 \rceil = \lceil F_2; G_2 \rceil$, and so in fact $\lceil F_1 \rceil ; \lceil G_1 \rceil = \lceil F_2 \rceil ; \lceil G_2 \rceil$, from the Equivalence Theorem.

It remains to show that $(F_1; G_1)(\mathbf{x}, \mathbf{w})$ satisfies defining conditions (1)–(3) for a morphism from $A(\mathbf{x})$ to $C(\mathbf{z})$ in $\mathscr{C}(\mathbb{T})$.

(1) Defining condition (1) for $F_1; G_1$ follows from defining condition (1) for both F_1 and G_1.

(2) We have

$$A(\mathbf{x}) \vdash (\exists \mathbf{v}) F_1(\mathbf{x}, \mathbf{v})$$

by defining condition (2) for F_1. We then obtain

$$A(\mathbf{x}), F_1(\mathbf{x}, \mathbf{a}) \stackrel{\mathbf{a}}{\vdash} B(\mathbf{a})$$

by defining condition (1) for F_1, and so

$$A(\mathbf{x}), F_1(\mathbf{x}, \mathbf{a}) \stackrel{\mathbf{a}}{\vdash} (\exists \mathbf{w}) G_1(\mathbf{a}, \mathbf{w})$$

follows by defining condition (2) for G_1. We thus obtain

$$\vdash A(\mathbf{x}) \Rightarrow (\exists \mathbf{w})(\exists \mathbf{q})(F_1(\mathbf{x}, \mathbf{q}) \wedge G_1(\mathbf{q}, \mathbf{w}))$$

using the rules for $\exists$ and ($\Rightarrow$-I), and so defining condition (2) is satisfied.

(3) Defining condition (3) for $F_1; G_1$ follows from defining condition (3) for both F_1 and G_1.

Hence, $\lceil F_1; G_1 \rceil = \lceil F_1 \rceil ; \lceil G_1 \rceil$ is indeed a morphism from A to C in $\mathscr{C}(\mathbb{T})$, whence composition in $\mathscr{C}(\mathbb{T})$ is well-defined.

Next, we show that $\mathscr{C}(\mathbb{T})$ satisfies the axioms of a category. We must show that $\lceil \mathrm{id}_A \rceil$ is indeed a morphism of $\mathscr{C}(\mathbb{T})$ for each object A of $\mathscr{C}(\mathbb{T})$, that composition is associative, and that the identity morphisms are units for composition. Let $A(\mathbf{x})$ be an object of $\mathscr{C}(\mathbb{T})$. Recall that

$$\mathrm{id}_A(\mathbf{x}, \mathbf{u}) \underset{\mathrm{def}}{\equiv} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}.$$

We now verify the defining conditions (1)–(3) for id_A.

(1) We obtain

$$A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \vdash A(\mathbf{x}) \wedge A(\mathbf{u})$$

by (=-E), and so defining condition (1) follows by ($\Rightarrow$-I).

(2) We obtain $\vdash \mathbf{x} = \mathbf{x}$ by (=-I), and so

$$\vdash A(\mathbf{x}) \Rightarrow (\exists \mathbf{u})(A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u})$$

follows by ($\wedge$-I), ($\exists$-I), and ($\Rightarrow$-I). Hence, defining condition (2) is satisfied.

(3) We obtain
$$(\mathbf{x} = \mathbf{u}), (\mathbf{x} = \mathbf{u}') \vdash \mathbf{u} = \mathbf{u}'$$
by (=-E). It thus follows that
$$\vdash (A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}) \wedge (A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}') \Rightarrow \mathbf{u} = \mathbf{u}',$$
and so defining condition (3) is satisfied.

Consequently, $\lceil \mathrm{id}_A(\mathbf{x}, \mathbf{u}) \rceil$ is indeed a morphism on $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$.

Now suppose we have the following diagram in $\mathscr{C}(\mathbb{T})$:
$$A(\mathbf{x}) \xrightarrow{\lceil F(\mathbf{x},\mathbf{v}) \rceil} B(\mathbf{y}) \xrightarrow{\lceil G(\mathbf{y},\mathbf{w}) \rceil} C(\mathbf{z}) \xrightarrow{\lceil H(\mathbf{z},\mathbf{u}') \rceil} D(\mathbf{x}') \ .$$
It follows from the rules for $\exists$ that
$$\vdash (\exists \mathbf{p}) \left[(\exists \mathbf{q})(F(\mathbf{x}, \mathbf{q}) \wedge G(\mathbf{q}, \mathbf{p})) \wedge H(\mathbf{p}, \mathbf{u}') \right] \Leftrightarrow (\exists \mathbf{q}) \left[F(\mathbf{x}, \mathbf{q}) \wedge (\exists \mathbf{p})(G(\mathbf{q}, \mathbf{p}) \wedge H(\mathbf{p}, \mathbf{u}')) \right]$$
holds in $\mathbb{T}$. Hence, we have that $\lceil (F; G); H \rceil = \lceil F; (G; H) \rceil$, and so composition of morphisms is associative in $\mathscr{C}(\mathbb{T})$. Moreover, both the formula $(F; G); H$ and the formula $F; (G; H)$ are provably equivalent in $\mathbb{T}$ to the formula
$$(F; G; H)(\mathbf{x}, \mathbf{u}') \underset{\text{def}}{\equiv} (\exists \mathbf{q}, \mathbf{p})(F(\mathbf{x}, \mathbf{q}) \wedge G(\mathbf{q}, \mathbf{p}) \wedge H(\mathbf{p}, \mathbf{u}')).$$
Generalising, we obtain that the composition of the $n \geq 2$ morphisms
$$\lceil F_1 \rceil : A_1(\mathbf{x^{(1)}}) \to A_2(\mathbf{x^{(2)}}), \ldots, \lceil F_n \rceil : A_n(\mathbf{x^{(n)}}) \to A_{n+1}(\mathbf{x^{(n+1)}})$$
in $\mathscr{C}(\mathbb{T})$, regardless of the way in which the composition is associated, is in fact equal to the morphism
$$\lceil F_1; \ldots; F_n \rceil : A_1(\mathbf{x^{(1)}}) \to A_{n+1}(\mathbf{x^{(n+1)}}),$$
where we define
$$(F_1; \ldots; F_n)(\mathbf{x^{(1)}}, \mathbf{u^{(n+1)}}) \underset{\text{def}}{\equiv}$$
$$(\exists \mathbf{q^{(1)}}, \ldots, \mathbf{q^{(n-1)}})(F_1(\mathbf{x^{(1)}}, \mathbf{q^{(1)}}) \wedge F_2(\mathbf{q^{(1)}}, \mathbf{q^{(2)}}) \wedge \ldots \wedge F_n(\mathbf{q^{(n-1)}}, \mathbf{u^{(n+1)}})).$$

Thus, we may henceforth assume without loss of generality that the representative of the composite of any finite number $n \geq 2$ of morphisms in $\mathscr{C}(\mathbb{T})$ is constructed in the above manner.

We now wish to show that the identity morphisms are units for composition. Consider a morphism $\lceil F(\mathbf{x}, \mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$. We must show that $\lceil F \rceil = \lceil \mathrm{id}_A; F \rceil$ and $\lceil F \rceil = \lceil F; \mathrm{id}_B \rceil$. Since $\wedge$ is associative in $\mathbb{T}$, it suffices to show that
$$\vdash F(\mathbf{x}, \mathbf{v}) \Leftrightarrow (\exists \mathbf{q})(A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{q} \wedge F(\mathbf{q}, \mathbf{v})) \tag{3.1.1}$$

and

$$\vdash F(\mathbf{x},\mathbf{v}) \Leftrightarrow (\exists \mathbf{q})(F(\mathbf{x},\mathbf{q}) \wedge B(\mathbf{q}) \wedge \mathbf{q} = \mathbf{v}) \tag{3.1.2}$$

hold in $\mathbb{T}$.

To show that (3.1.1) holds, note that we obtain

$$F(\mathbf{x},\mathbf{v}) \vdash A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{x} \wedge F(\mathbf{x},\mathbf{v})$$

by defining condition (1) for F, (=-I), and ($\wedge$-I). It thus follows by ($\exists$-I) and ($\Rightarrow$-I) that

$$\vdash F(\mathbf{x},\mathbf{v}) \Rightarrow (\exists \mathbf{q})(A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{q} \wedge F(\mathbf{q},\mathbf{v})).$$

We also obtain that

$$(\exists \mathbf{q})(A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{q} \wedge F(\mathbf{q},\mathbf{v})) \vdash F(\mathbf{x},\mathbf{v})$$

by ($\exists$-E), ($\wedge$-E), and (=-E). Hence, (3.1.1) follows and the proof of (3.1.2) is analogous. Thus, the identity morphisms are units for composition, and so $\mathscr{C}(\mathbb{T})$ indeed satisfies the axioms of a category. ■

Remark 3.1.1.6 For any theory $\mathbb{T}$, $\mathscr{C}(\mathbb{T})$ is similar to the category **Set** since we can think of an object $A(\mathbf{x})$ as the set $\{\mathbf{x} \mid \vdash A(\mathbf{x})\}$, that is, the set of all $\mathbf{x}$ for which $A(\mathbf{x})$ is provable, and we can think of the $\mathbb{T}$-provably total and functional representative $F(\mathbf{x},\mathbf{v})$ of a morphism $\ulcorner F(\mathbf{x},\mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ as the graph of a function $f : \{\mathbf{x} \mid \vdash A(\mathbf{x})\} \to \{\mathbf{v} \mid \vdash B(\mathbf{v})\}$. □

Lemma 3.1.1.7 *Let $\mathbb{T}$ be a theory and let $\mathscr{C}(\mathbb{T})$ be its syntactic category. If two objects of $\mathscr{C}(\mathbb{T})$ contain exactly the same number of free variables and are provably equivalent in $\mathbb{T}$, then they are isomorphic in $\mathscr{C}(\mathbb{T})$.*

Proof Let $A(\mathbf{x})$ and $B(\mathbf{y})$ be two objects of $\mathscr{C}(\mathbb{T})$ such that $|\mathbf{x}| = |\mathbf{y}|$ and suppose that they are provably equivalent in $\mathbb{T}$, that is, that

$$\vdash A(\mathbf{x}) \Leftrightarrow B(\mathbf{y})$$

holds in $\mathbb{T}$. We wish to show that $A(\mathbf{x})$ and $B(\mathbf{y})$ are isomorphic in $\mathscr{C}(\mathbb{T})$. Note first that we can assume without loss of generality that none of the variables in the list $\mathbf{x}$ occur as bound variables in B and that none of the variables in the list $\mathbf{y}$ occur as bound variables in A.

Define

$$F(\mathbf{x},\mathbf{v}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{v}$$

and

$$G(\mathbf{y},\mathbf{u}) \underset{\text{def}}{\equiv} B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{u}.$$

By comparison with identity morphisms of $\mathscr{C}(\mathbb{T})$, it is clear that $\ulcorner F(\mathbf{x},\mathbf{v})\urcorner$ is a morphism from $A(\mathbf{x})$ to $B(\mathbf{y})$ and that $\ulcorner G(\mathbf{y},\mathbf{u})\urcorner$ is a morphism from $B(\mathbf{y})$ to $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$, and so we obtain the diagram

$$A(\mathbf{x}) \underset{\ulcorner G(\mathbf{y},\mathbf{u})\urcorner}{\overset{\ulcorner F(\mathbf{x},\mathbf{v})\urcorner}{\rightleftarrows}} B(\mathbf{y})$$

in $\mathscr{C}(\mathbb{T})$. A straightforward argument shows that $\ulcorner G(\mathbf{y},\mathbf{u})\urcorner$ is the inverse of $\ulcorner H(\mathbf{x},\mathbf{v})\urcorner$, and so $A(\mathbf{x})$ and $B(\mathbf{y})$ are indeed isomorphic in $\mathscr{C}(\mathbb{T})$. ■

Remark 3.1.1.8 Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$, let $A(\mathbf{x})$ be a formula of $\mathbb{T}$, and let $A'(\mathbf{x})$ be a variant of $A(\mathbf{x})$ (that is, $A'(\mathbf{x})$ is obtained from $A(\mathbf{x})$ by possibly changing one or more of the bound variables of $A(\mathbf{x})$). It follows from Lemma 3.1.1.7 that $A(\mathbf{x})$ and $A'(\mathbf{x})$ are isomorphic in $\mathscr{C}(\mathbb{T})$. Hence, we can consider formulas to be equal up to change of bound variables in the context of syntactic categories.

Moreover, if $\mathbf{y}$ is any list of distinct variables that satisfies $|\mathbf{y}| = |\mathbf{x}|$ and is free for $\mathbf{x}$ in A, then $A(\mathbf{x})$ and $A(\mathbf{y})$ are provably equivalent in $\mathbb{T}$, and so isomorphic in $\mathscr{C}(\mathbb{T})$, by Lemma 3.1.1.7. Hence, $A(\mathbf{x})$ and $A(\mathbf{y})$ can be considered to effectively be the same object of $\mathscr{C}(\mathbb{T})$, and so in fact the exact choice of variables (both bound and free) occurring in an object of $\mathscr{C}(\mathbb{T})$ is largely irrelevant. □

3.1.1.2 Monomorphisms and subobjects in syntactic categories

We wish to characterise monomorphisms and subobjects in syntactic categories. Although the definition of a monomorphism in an arbitrary category is stated at the categorical level (see Definition B.0.0.1 in Appendix B), in the case of the syntactic category of a theory $\mathbb{T}$, we can give an equivalent condition at the level of the underlying theory $\mathbb{T}$.

Lemma 3.1.1.9 *Let $\mathbb{T}$ be a theory and let $\ulcorner F(\mathbf{x},\mathbf{v})\urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism in $\mathscr{C}(\mathbb{T})$. Then, $\ulcorner F(\mathbf{x},\mathbf{v})\urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ is a monomorphism in $\mathscr{C}(\mathbb{T})$ if and only if, for all parallel morphisms $\ulcorner G(\mathbf{z},\mathbf{u})\urcorner, \ulcorner H(\mathbf{z},\mathbf{u})\urcorner : C(\mathbf{z}) \to A(\mathbf{x})$ into $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$,*

$$\vdash [(G;F)(\mathbf{z},\mathbf{v}) \Leftrightarrow (H;F)(\mathbf{z},\mathbf{v})] \Rightarrow [G(\mathbf{z},\mathbf{u}) \Leftrightarrow H(\mathbf{z},\mathbf{u})] \tag{3.1.3}$$

holds in $\mathbb{T}$.

Proof The proof is straightforward and thus omitted. ■

As in any category, there is a notion of equivalence of monomorphisms in syntactic categories, as well as a notion of subobjects (see [18] for a general categorical definition). More specifically, we have the following definitions.

Definition 3.1.1.10 Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$ and let C be an object of $\mathscr{C}(\mathbb{T})$.

(i) Let $\lceil F \rceil : A \to C$ and $\lceil G \rceil : B \to C$ be two monomorphisms in $\mathscr{C}(\mathbb{T})$. $\lceil F \rceil$ and $\lceil G \rceil$ are said to be *equivalent* in $\mathscr{C}(\mathbb{T})$ if there exists an isomorphism $\lceil H \rceil : A \to B$ in $\mathscr{C}(\mathbb{T})$ such that $\lceil H; G \rceil = \lceil F \rceil$, as in the diagram

$$\begin{array}{ccc} A & \xrightarrow{\lceil F \rceil} & C \\ {\scriptstyle \lceil H \rceil}\downarrow & \nearrow{\scriptstyle \lceil G \rceil} & \\ B & & \end{array} \quad . \tag{3.1.4}$$

Equivalently, $\lceil F \rceil$ and $\lceil G \rceil$ are equivalent in $\mathscr{C}(\mathbb{T})$ if there exist morphisms $\lceil H \rceil : A \to B$ and $\lceil J \rceil : B \to A$ in $\mathscr{C}(\mathbb{T})$ such that $\lceil H; G \rceil = \lceil F \rceil$ and $\lceil J; F \rceil = \lceil G \rceil$.

(ii) A *subobject* of C is an equivalence class of monomorphisms into C under the above equivalence relation. Note that we usually identify a subobject of C with (the domain of) one of its representatives, and consider it to be defined up to equivalence of monomorphisms.

(iii) There is a partial order relation on subobjects of C defined as follows. Let $[\lceil F \rceil : A \to C]$ and $[\lceil G \rceil : B \to C]$ be two subobjects of C. Then, $[\lceil F \rceil] \leq [\lceil G \rceil]$ if and only if there exists a morphism $\lceil H \rceil : A \to B$ such that $\lceil F \rceil = \lceil H; G \rceil$. Note that $\lceil F \rceil$ and $\lceil G \rceil$ are equivalent as monomorphisms if and only if $[\lceil F \rceil] \leq [\lceil G \rceil]$ and $[\lceil G \rceil] \leq [\lceil F \rceil]$. □

Lemma 3.1.1.11 *Let $\mathbb{T}$ be a theory and $\mathscr{C}(\mathbb{T})$ its syntactic category. Any morphism in $\mathscr{C}(\mathbb{T})$ of the form*

$$A(\mathbf{x}) \xrightarrow{\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{w} \rceil} B(\mathbf{z}) \ ,$$

where $|\mathbf{x}| = |\mathbf{z}| = |\mathbf{w}|$, is a monomorphism.

Proof By hypothesis, $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{w} \rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$, so we do not need to verify the defining conditions. Suppose that we have two morphisms $\lceil G(\mathbf{y}, \mathbf{u}) \rceil, \lceil H(\mathbf{y}, \mathbf{u}) \rceil : C(\mathbf{y}) \to A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ making the diagram

$$C(\mathbf{y}) \underset{\lceil H(\mathbf{y},\mathbf{u}) \rceil}{\overset{\lceil G(\mathbf{y},\mathbf{u}) \rceil}{\rightrightarrows}} A(\mathbf{x}) \xrightarrow{\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{w} \rceil} B(\mathbf{z}) \tag{3.1.5}$$

commute. By defining condition (1) for G, (=-I), and ($\wedge$-I), we obtain

$$G(\mathbf{y}, \mathbf{u}) \vdash G(\mathbf{y}, \mathbf{u}) \wedge (A(\mathbf{u}) \wedge \mathbf{u} = \mathbf{u}),$$

from which

$$G(\mathbf{y}, \mathbf{u}) \vdash (\exists \mathbf{q})(G(\mathbf{y}, \mathbf{q}) \wedge (A(\mathbf{q}) \wedge \mathbf{q} = \mathbf{u}))$$

follows by (∃-I). Since diagram (3.1.5) commutes, it follows that

$$G(\mathbf{y},\mathbf{u}) \vdash (\exists \mathbf{q})(H(\mathbf{y},\mathbf{q}) \wedge (A(\mathbf{q}) \wedge \mathbf{q} = \mathbf{u})),$$

and so we obtain

$$G(\mathbf{y},\mathbf{u}) \vdash H(\mathbf{y},\mathbf{u})$$

by (∃-E) and (=-E). An analogous argument yields

$$H(\mathbf{y},\mathbf{u}) \vdash G(\mathbf{y},\mathbf{u}),$$

and so $\lceil G(\mathbf{y},\mathbf{u}) \rceil = \lceil H(\mathbf{y},\mathbf{u}) \rceil$. Consequently, $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{w} \rceil : A(\mathbf{x}) \to B(\mathbf{z})$ is indeed a monomorphism in $\mathscr{C}(\mathbb{T})$. ■

Recall the analogy between **Set** and syntactic categories mentioned in Remark 3.1.1.6. Since monomorphisms in **Set** are injective, it is therefore natural to ask if representatives of monomorphisms in $\mathscr{C}(\mathbb{T})$ are provably injective in $\mathbb{T}$.

Lemma 3.1.1.12 *Let $\mathbb{T}$ be a theory and let $\lceil F(\mathbf{x},\mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be a monomorphism in $\mathscr{C}(\mathbb{T})$. Then, $\lceil F(\mathbf{x},\mathbf{v}) \rceil$ is provably injective in $\mathbb{T}$, that is to say,*

$$\vdash F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v}) \Rightarrow \mathbf{x} = \mathbf{x}'$$

holds in $\mathbb{T}$.

Proof Let $\mathbf{x}'$ be any list of variables such that $|\mathbf{x}'| = |\mathbf{x}|$. Define

$$C(\mathbf{x},\mathbf{x}') \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge A(\mathbf{x}'),$$

$$G(\mathbf{x},\mathbf{x}',\mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge A(\mathbf{x}') \wedge \mathbf{x} = \mathbf{u},$$

and

$$H(\mathbf{x},\mathbf{x}',\mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge A(\mathbf{x}') \wedge \mathbf{x}' = \mathbf{u}.$$

It is straightforward to show that $\lceil H \rceil$ and $\lceil G \rceil$ are morphisms from $C(\mathbf{x},\mathbf{x}')$ to $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Consequently, we can consider the following diagram in $\mathscr{C}(\mathbb{T})$:

$$C(\mathbf{x},\mathbf{x}') \underset{\lceil H(\mathbf{x},\mathbf{x}',\mathbf{u}) \rceil}{\overset{\lceil G(\mathbf{x},\mathbf{x}',\mathbf{u}) \rceil}{\rightrightarrows}} A(\mathbf{x}) \xrightarrow{\lceil F(\mathbf{x},\mathbf{v}) \rceil} B(\mathbf{y}) \ .$$

Since $\lceil F(\mathbf{x},\mathbf{v}) \rceil$ is a monomorphism in $\mathscr{C}(\mathbb{T})$ and $\lceil G(\mathbf{x},\mathbf{x}',\mathbf{u}) \rceil$ and $\lceil H(\mathbf{x},\mathbf{x}',\mathbf{u}) \rceil$ are parallel morphisms into $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$,

$$\vdash [(G;F)(\mathbf{x},\mathbf{x}',\mathbf{v}) \Leftrightarrow (H;F)(\mathbf{x},\mathbf{x}',\mathbf{v})] \Rightarrow [G(\mathbf{x},\mathbf{x}',\mathbf{u}) \Leftrightarrow H(\mathbf{x},\mathbf{x}',\mathbf{u})] \qquad (3.1.6)$$

holds in $\mathbb{T}$ by Lemma 3.1.1.9. We then have the following derivation in $\mathbb{T}$.

1	$F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v})$	
2	$A(\mathbf{x}) \wedge A(\mathbf{x}')$	Defining condition (1) for F, 1
3	$(A(\mathbf{x}) \wedge A(\mathbf{x}') \wedge \mathbf{x} = \mathbf{x}) \wedge F(\mathbf{x},\mathbf{v})$	(=-I), ($\wedge$-I), 1, 2
4	$(G;F)(\mathbf{x},\mathbf{x}',\mathbf{v})$	($\exists$-I), Definition of G, 3
5	$(H;F)(\mathbf{x},\mathbf{x}',\mathbf{v})$	Analogous argument, 3–4
6	$(G;F)(\mathbf{x},\mathbf{x}',\mathbf{v}) \Leftrightarrow (H;F)(\mathbf{x},\mathbf{x}',\mathbf{v})$	($\Rightarrow$-I), ($\wedge$-I), 4, 5
7	$G(\mathbf{x},\mathbf{x}',\mathbf{u}) \Leftrightarrow H(\mathbf{x},\mathbf{x}',\mathbf{u})$	(3.1.6), ($\Rightarrow$-E), 6
8	$G(\mathbf{x},\mathbf{x}',\mathbf{x}') \Leftrightarrow H(\mathbf{x},\mathbf{x}',\mathbf{x}')$	Substitution Theorem, 7
9	$H(\mathbf{x},\mathbf{x}',\mathbf{x}')$	(=-I), ($\wedge$-I), Definition of H, 2
10	$G(\mathbf{x},\mathbf{x}',\mathbf{x}')$	($\Rightarrow$-E), 8, 9
11	$\mathbf{x} = \mathbf{x}'$	($\wedge$-E), 10
12	$F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v}) \Rightarrow \mathbf{x} = \mathbf{x}'$	($\Rightarrow$-I), 1–11

Therefore, we indeed obtain

$$\vdash F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v}) \Rightarrow \mathbf{x} = \mathbf{x}',$$

and so $F(\mathbf{x},\mathbf{v})$ is provably injective in $\mathbb{T}$. ■

Proposition 3.1.1.13 *Let $\mathbb{T}$ be a theory, $\mathscr{C}(\mathbb{T})$ its syntactic category, and $C(\mathbf{x})$ an object in $\mathscr{C}(\mathbb{T})$. Every monomorphism into $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ is equivalent to a monomorphism of the form*

$$A(\mathbf{x}) \xrightarrow{\ulcorner A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \urcorner} C(\mathbf{x}) \ .$$

Proof Let $C(\mathbf{x})$ be an object of $\mathscr{C}(\mathbb{T})$ and let $\ulcorner F(\mathbf{y},\mathbf{u}) \urcorner : B(\mathbf{y}) \to C(\mathbf{x})$ be a monomorphism in $\mathscr{C}(\mathbb{T})$. Define

$$\mathrm{Im}_F(\mathbf{x}) \underset{\text{def}}{\equiv} (\exists \mathbf{p}) F(\mathbf{p},\mathbf{x})$$

and

$$I_F(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} \mathrm{Im}_F(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}.$$

We claim that $\ulcorner F(\mathbf{y},\mathbf{u}) \urcorner$ is a morphism from $B(\mathbf{y})$ to $\mathrm{Im}_F(\mathbf{x})$ and $\ulcorner I_F(\mathbf{x},\mathbf{u}) \urcorner$ is a morphism from $\mathrm{Im}_F(\mathbf{x})$ to $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Since $\ulcorner F(\mathbf{y},\mathbf{u}) \urcorner : B(\mathbf{y}) \to C(\mathbf{x})$ is a morphism of $\mathscr{C}(\mathbb{T})$, $F(\mathbf{y},\mathbf{u})$ satisfies the defining conditions for a morphism from

$B(\mathbf{y})$ to $C(\mathbf{x})$. Since defining conditions (2) and (3) do not depend on the codomain, $F(\mathbf{y}, \mathbf{u})$ also satisfies defining conditions (2) and (3) for a morphism from $B(\mathbf{y})$ to $\mathrm{Im}_F(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Furthermore, we obtain

$$F(\mathbf{y}, \mathbf{u}) \vdash B(\mathbf{y})$$

by defining condition (1) for F as a morphism from B to C. We thus obtain

$$F(\mathbf{y}, \mathbf{u}) \vdash B(\mathbf{y}) \wedge (\exists \mathbf{p}) F(\mathbf{p}, \mathbf{u})$$

by ($\exists$-I) and ($\wedge$-I). Hence, $F(\mathbf{y}, \mathbf{u})$ satisfies all defining conditions for a morphism from $B(\mathbf{y})$ to $\mathrm{Im}_F(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. We obtain

$$\mathrm{Im}_F(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \vdash \mathrm{Im}_F(\mathbf{x}) \wedge C(\mathbf{u})$$

using defining condition (1) for $F(\mathbf{x}, \mathbf{u})$ as a morphism into $C(\mathbf{x})$, ($\exists$-E), and (=-E). Hence, $I_F(\mathbf{x}, \mathbf{u})$ satisfies defining condition (1) for a morphism from $\mathrm{Im}_F(\mathbf{x})$ to $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Defining conditions (2) and (3) for $I_F(\mathbf{x}, \mathbf{u})$ are obtained in a straightforward manner by using ($\exists$-I) and the rules for equality. Note further that, since

$$I_F(\mathbf{x}, \mathbf{u}) \underset{\text{def}}{\equiv} \mathrm{Im}_F(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u},$$

$\lceil I_F(\mathbf{x}, \mathbf{u}) \rceil : \mathrm{Im}_F(\mathbf{x}) \to C(\mathbf{x})$ is a monomorphism in $\mathscr{C}(\mathbb{T})$ by Lemma 3.1.1.11.

We claim that the diagram

$$\begin{array}{ccc} B(\mathbf{y}) & \xrightarrow{\lceil F(\mathbf{y},\mathbf{u}) \rceil} & C(\mathbf{x}) \\ {\scriptstyle \lceil F(\mathbf{y},\mathbf{u}) \rceil}\downarrow & \nearrow {\scriptstyle \lceil I_F(\mathbf{x},\mathbf{u}) \rceil} & \\ \mathrm{Im}_F(\mathbf{x}) & & \end{array} \tag{3.1.7}$$

commutes in $\mathscr{C}(\mathbb{T})$. Indeed, we obtain

$$F(\mathbf{y}, \mathbf{a}) \wedge ((\exists \mathbf{p}) F(\mathbf{p}, \mathbf{a}) \wedge \mathbf{a} = \mathbf{u}) \vdash^{\mathbf{a}} F(\mathbf{y}, \mathbf{u})$$

by (=-E), and so

$$(\exists \mathbf{q})(F(\mathbf{y}, \mathbf{q}) \wedge ((\exists \mathbf{p}) F(\mathbf{p}, \mathbf{q}) \wedge \mathbf{q} = \mathbf{u})) \vdash F(\mathbf{y}, \mathbf{u})$$

follows by ($\exists$-E). Moreover, we obtain

$$F(\mathbf{y}, \mathbf{u}) \vdash F(\mathbf{y}, \mathbf{u}) \wedge ((\exists \mathbf{p}) F(\mathbf{p}, \mathbf{u}) \wedge \mathbf{u} = \mathbf{u})$$

by ($\exists$-I) and (=-I), from which

$$F(\mathbf{y}, \mathbf{u}) \vdash (\exists \mathbf{q})(F(\mathbf{y}, \mathbf{q}) \wedge ((\exists \mathbf{p}) F(\mathbf{p}, \mathbf{q}) \wedge \mathbf{q} = \mathbf{u}))$$

follows by ($\exists$-I). Since

$$F(\mathbf{y},\mathbf{u}); I_F(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{q})(F(\mathbf{y},\mathbf{q}) \wedge ((\exists \mathbf{p})F(\mathbf{p},\mathbf{q}) \wedge \mathbf{q} = \mathbf{u})),$$

we thus obtain $\lceil F(\mathbf{y},\mathbf{u})\rceil = \lceil F(\mathbf{y},\mathbf{u}); I_F(\mathbf{x},\mathbf{u})\rceil$, and so diagram (3.1.7) commutes in $\mathscr{C}(\mathbb{T})$.

We now wish to show that $\lceil F(\mathbf{y},\mathbf{u})\rceil : B(\mathbf{y}) \to \mathrm{Im}_F(\mathbf{x})$ is an isomorphism. Define

$$G(\mathbf{x},\mathbf{v}) \underset{\text{def}}{\equiv} F(\mathbf{v},\mathbf{x}).$$

We claim that $\lceil G(\mathbf{x},\mathbf{v})\rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $\mathrm{Im}_F(\mathbf{x})$ to $B(\mathbf{y})$. Indeed, we obtain

$$F(\mathbf{v},\mathbf{x}) \vdash (\exists \mathbf{p})F(\mathbf{p},\mathbf{x}) \wedge B(\mathbf{v})$$

by ($\exists$-I) and defining condition (1) for $\lceil F\rceil : B \to C$. Thus, defining condition (1) for G holds. Moreover, by definition of G and Im_F, we have

$$\mathrm{Im}_F(\mathbf{x}) \underset{\text{def}}{\equiv} (\exists \mathbf{p})F(\mathbf{p},\mathbf{x}) \underset{\text{def}}{\equiv} (\exists \mathbf{p})G(\mathbf{x},\mathbf{p}).$$

Hence, it follows that

$$\mathrm{Im}_F(\mathbf{x}) \vdash (\exists \mathbf{p})G(\mathbf{x},\mathbf{p}),$$

and so defining condition (2) for G holds. Since $\lceil F(\mathbf{y},\mathbf{u})\rceil$ is a monomorphism in $\mathscr{C}(\mathbb{T})$,

$$\vdash (\forall \mathbf{u},\mathbf{y},\mathbf{y}')(F(\mathbf{y},\mathbf{u}) \wedge F(\mathbf{y}',\mathbf{u}) \Rightarrow \mathbf{y} = \mathbf{y}') \tag{3.1.8}$$

holds in $\mathscr{C}(\mathbb{T})$ by Lemma 3.1.1.12 and ($\forall$-I). Hence, we obtain

$$\vdash G(\mathbf{x},\mathbf{v}) \wedge G(\mathbf{x},\mathbf{v}') \Rightarrow \mathbf{v} = \mathbf{v}'$$

by ($\forall$-E) and the definition of G. Therefore, defining condition (3) holds for G in $\mathbb{T}$, and so $\lceil G(\mathbf{x},\mathbf{v})\rceil$ is indeed a morphism in $\mathscr{C}(\mathbb{T})$ from $\mathrm{Im}_F(\mathbf{x})$ to $B(\mathbf{y})$.

It remains to show that $\lceil G\rceil : \mathrm{Im}_F \to B$ is the inverse of $\lceil F\rceil : B \to \mathrm{Im}_F$. We easily obtain

$$\vdash (\exists \mathbf{q})(F(\mathbf{q},\mathbf{x}) \wedge F(\mathbf{q},\mathbf{u})) \Leftrightarrow (\exists \mathbf{p})F(\mathbf{p},\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$$

by using defining condition (3) for F and the rules for $\exists$ and equality. Hence, $\lceil G; F\rceil = \lceil \mathrm{id}_{\mathrm{Im}_F}\rceil$. In order to show that $\lceil F; G\rceil = \lceil \mathrm{id}_B\rceil$, we use the fact that $\lceil F\rceil : B \to C$ is a monomorphism in $\mathscr{C}(\mathbb{T})$. Consider the diagram

$$B(\mathbf{y}) \underset{\lceil \mathrm{id}_B\rceil}{\overset{\lceil F;G\rceil}{\rightrightarrows}} B(\mathbf{y}) \xrightarrow{\lceil F\rceil} C(\mathbf{x}) \tag{3.1.9}$$

in $\mathscr{C}(\mathbb{T})$. Since $\lceil \mathrm{id}_B; F\rceil = \lceil F\rceil$ as morphisms in $\mathscr{C}(\mathbb{T})$ from $B(\mathbf{y})$ to $C(\mathbf{x})$ and $\lceil F\rceil : B \to C$ is a monomorphism, it suffices to show that $\lceil F; G; F\rceil = \lceil F\rceil$ in order to conclude that $\lceil F; G \rceil = \lceil \mathrm{id}_B \rceil$. As defined in Proposition 3.1.1.5, $(F; G; F)(\mathbf{y}, \mathbf{u})$ is the formula

$$(\exists \mathbf{q}, \mathbf{q}')(F(\mathbf{y}, \mathbf{q}) \wedge G(\mathbf{q}, \mathbf{q}') \wedge F(\mathbf{q}', \mathbf{u})) \underset{\text{def}}{\equiv} (\exists \mathbf{q}, \mathbf{q}')(F(\mathbf{y}, \mathbf{q}) \wedge F(\mathbf{q}', \mathbf{q}) \wedge F(\mathbf{q}', \mathbf{u})).$$

Using (3.1.8), (=-E), and ($\exists$-E), we obtain that $(F; G; F)(\mathbf{y}, \mathbf{u}) \vdash F(\mathbf{y}, \mathbf{u})$. Furthermore, we obtain $F(\mathbf{y}, \mathbf{u}) \vdash (F; G; F)(\mathbf{y}, \mathbf{u})$ by ($\wedge$-I) and ($\exists$-I). Hence,

$$\lceil (F; G); F \rceil = \lceil F; G; F \rceil = \lceil F \rceil = \lceil \mathrm{id}_B; F \rceil,$$

and so $\lceil F; G \rceil = \lceil \mathrm{id}_B \rceil$ as $\lceil F \rceil : B \to C$ is a monomorphism. Consequently, $\lceil F \rceil : B \to \mathrm{Im}_F$ is indeed an isomorphism with inverse $\lceil G \rceil : \mathrm{Im}_F \to B$.

Since $\lceil F(\mathbf{y}, \mathbf{u}) \rceil : B(\mathbf{y}) \to \mathrm{Im}_F(\mathbf{x})$ is an isomorphism and diagram (3.1.7) commutes in $\mathscr{C}(\mathbb{T})$, it follows that $\lceil F(\mathbf{y}, \mathbf{u}) \rceil : B(\mathbf{y}) \to C(\mathbf{x})$ and $\lceil I_F(\mathbf{x}, \mathbf{u}) \rceil : \mathrm{Im}_F(\mathbf{x}) \to C(\mathbf{x})$ are equivalent as monomorphisms in $\mathscr{C}(\mathbb{T})$ by Definition 3.1.1.10. Thus, letting $A(\mathbf{x}) \underset{\text{def}}{\equiv} \mathrm{Im}_F(\mathbf{x})$, we obtain that $\lceil F(\mathbf{y}, \mathbf{u}) \rceil : B(\mathbf{y}) \to C(\mathbf{x})$ is equivalent to the monomorphism $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil : A(\mathbf{x}) \to C(\mathbf{x})$ of the required form. ∎

Remark 3.1.1.14 As usual, although subobjects of an object C in $\mathscr{C}(\mathbb{T})$ are formally defined to be equivalence classes of monomorphisms into C, in practice we consider objects A together with a specified monomorphism $A \rightarrowtail C$ to be subobjects of C. These subobjects are then defined up to equivalence of monomorphisms. By Proposition 3.1.1.13 and Lemma 3.1.1.11, we can in fact identify each subobject of an object $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ with an object $A(\mathbf{x})$ having exactly the same free variables as $C(\mathbf{x})$. The specified monomorphism chosen as a representative of the actual subobject of $C(\mathbf{x})$ can be taken to be of the form $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil : A(\mathbf{x}) \rightarrowtail C(\mathbf{x})$. Therefore, we may henceforth consider every subobject of an object $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ to be an object $A(\mathbf{x})$ with exactly the same free variables as $C(\mathbf{x})$ and with associated monomorphism $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil : A(\mathbf{x}) \to C(\mathbf{x})$, unless clearly specified otherwise.

The order relation between subobjects of a given object $C(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ may consequently be reformulated as follows. Let $A(\mathbf{x})$ and $B(\mathbf{x})$ be two subobjects of $C(\mathbf{x})$. Then, $A(\mathbf{x}) \leq B(\mathbf{x})$ if and only if there exists a morphism $\lceil F(\mathbf{x}, \mathbf{u}) \rceil : A(\mathbf{x}) \to B(\mathbf{x})$ making the diagram

$$\begin{array}{ccc} A(\mathbf{x}) & \xrightarrow{\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil} & C(\mathbf{x}) \\ {\scriptstyle \lceil F(\mathbf{x}, \mathbf{u}) \rceil}\big\downarrow & \nearrow_{\lceil B(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil} & \\ B(\mathbf{x}) & & \end{array}$$

commute in $\mathscr{C}(\mathbb{T})$, i.e. such that $\lceil A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \rceil = \lceil F(\mathbf{x}, \mathbf{u}); (B(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}) \rceil$. □

3.1.1.3 Properties of syntactic categories

We now consider some of the structure present in syntactic categories.

Proposition 3.1.1.15 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$. Then, $\mathscr{C}(\mathbb{T})$ has*

(i) a terminal object;

(ii) binary products;

(iii) binary pullbacks;

(iv) equalisers.

Proof Terminal objects and binary products in syntactic categories are briefly considered in [29, 30, 13], but we present the constructions in detail here for completeness.

(i) (Terminal object) If $\mathbb{T}$ is an arithmetical theory, we define

$$\tau \underset{\text{def}}{\equiv} \top \underset{\text{def}}{\equiv} 0 = 0,$$

and if $\mathbb{T}$ is not an arithmetical theory, we define

$$\tau \underset{\text{def}}{\equiv} (\forall y)(y = y).$$

Then, τ is a closed formula that is provably true in $\mathbb{T}$ (that is, a closed theorem of $\mathbb{T}$) and an object of $\mathscr{C}(\mathbb{T})$ without free variables. For any object $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$, define

$$!_A(\mathbf{x}) \underset{\text{def}}{\equiv} A(\mathbf{x}).$$

We claim that τ is a terminal object of $\mathscr{C}(\mathbb{T})$ and that, for any object $A(\mathbf{x}) \in \mathscr{C}(\mathbb{T})$, $\lceil !_A(\mathbf{x}) \rceil$ is the unique morphism from $A(\mathbf{x})$ to τ in $\mathscr{C}(\mathbb{T})$, which we may call the *terminating morphism* (*associated to* $A(\mathbf{x})$). As τ is a theorem of $\mathbb{T}$, we obtain $A(\mathbf{x}) \vdash A(\mathbf{x}) \wedge \tau$. Hence, defining condition (1) is satisfied. Since τ has no free variables, defining condition (3) is vacuously satisfied and no existential quantifier appears in defining condition (2). Hence, defining condition (2) is simply

$$\vdash A(\mathbf{x}) \Rightarrow A(\mathbf{x}),$$

and hence holds in $\mathbb{T}$. Thus, $\lceil !_A(\mathbf{x}) \rceil = \lceil A(\mathbf{x}) \rceil$ is indeed a morphism from $A(\mathbf{x})$ to τ in $\mathscr{C}(\mathbb{T})$. It remains to show that it is the unique such morphism.

Let $\lceil F(\mathbf{x}) \rceil : A(\mathbf{x}) \to \tau$ be a morphism in $\mathscr{C}(\mathbb{T})$. We must show that $\lceil F(\mathbf{x}) \rceil = \lceil A(\mathbf{x}) \rceil$ as morphisms in $\mathscr{C}(\mathbb{T})$ from $A(\mathbf{x})$ to τ. Defining condition (1) for F states that $\vdash F(\mathbf{x}) \Rightarrow A(\mathbf{x}) \wedge \tau$, from which it follows that $\vdash F(\mathbf{x}) \Rightarrow A(\mathbf{x})$. Moreover, since τ has no free variables, defining condition (2) for F states that

$\vdash A(\mathbf{x}) \Rightarrow F(\mathbf{x})$. Hence, it follows that $\vdash F(\mathbf{x}) \Leftrightarrow A(\mathbf{x})$, and so $\lceil F(\mathbf{x}) \rceil = \lceil A(\mathbf{x}) \rceil$ as morphisms from $A(\mathbf{x})$ to τ in $\mathscr{C}(\mathbb{T})$. Therefore, $\lceil !_A(\mathbf{x}) \rceil = \lceil A(\mathbf{x}) \rceil$ is indeed the unique morphism from $A(\mathbf{x})$ to τ in $\mathscr{C}(\mathbb{T})$. Hence, τ is a terminal object in $\mathscr{C}(\mathbb{T})$. In fact, since all terminal objects in a category are isomorphic, we may say that τ is *the* terminal object of $\mathscr{C}(\mathbb{T})$.

(ii) (Binary products) Let $A(\mathbf{x})$ and $B(\mathbf{y})$ be two objects of $\mathscr{C}(\mathbb{T})$. We wish to show that their product exists in $\mathscr{C}(\mathbb{T})$. Let $\mathbf{y}'$ be a list of variables not occurring in $A(\mathbf{x})$ such that $|\mathbf{y}'| = |\mathbf{y}|$ and $\mathbf{y}'$ is free for $\mathbf{y}$ in B. In particular, if the lists $\mathbf{y}$ and $\mathbf{x}$ are disjoint, we can assume without loss of generality that none of the variables in the list $\mathbf{y}$ occur in $A(\mathbf{x})$ (as we can always change the bound variables of A if necessary). In this case, we let $\mathbf{y}'$ be the list $\mathbf{y}$ itself. Note also that $B(\mathbf{y})$ and $B(\mathbf{y}')$ are provably equivalent in $\mathbb{T}$, and hence isomorphic in $\mathscr{C}(\mathbb{T})$ by Lemma 3.1.1.7. Define

$$\pi_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{u}$$

and

$$\pi_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge B(\mathbf{y}') \wedge \mathbf{y}' = \mathbf{v}.$$

We claim that $A(\mathbf{x}) \wedge B(\mathbf{y}')$ is the product of $A(\mathbf{x})$ and $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$ and that the corresponding projections are the morphisms $\lceil \pi_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \rceil : A(\mathbf{x}) \wedge B(\mathbf{y}') \to A(\mathbf{x})$ and $\lceil \pi_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \rceil : A(\mathbf{x}) \wedge B(\mathbf{y}') \to B(\mathbf{y})$.

We must show that π_A and π_B satisfy the defining conditions for morphisms in $\mathscr{C}(\mathbb{T})$ and that $A \wedge B$, together with $\lceil \pi_A \rceil$ and $\lceil \pi_B \rceil$, satisfies the universal property of the binary product of A and B.

By ($\wedge$-E), ($\wedge$-I) and (=-E), we obtain

$$A(\mathbf{x}) \wedge B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{u} \vdash (A(\mathbf{x}) \wedge B(\mathbf{y}')) \wedge A(\mathbf{u}),$$

from which defining condition (1) for π_A follows. We obtain

$$A(\mathbf{x}) \wedge B(\mathbf{y}') \vdash A(\mathbf{x}) \wedge B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{x}$$

by (=-I) and ($\wedge$-I). Defining condition (2) for π_A thus follows by ($\exists$-I) and ($\Rightarrow$-I). Furthermore, we obtain

$$\vdash \pi_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \wedge \pi_A(\mathbf{x}, \mathbf{y}', \mathbf{u}') \Rightarrow \mathbf{u} = \mathbf{u}'$$

from the rules for equality and ($\Rightarrow$-I), and so defining condition (3) for π_A is also satisfied. Hence, $\lceil \pi_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \rceil$ is indeed a morphism from $A(\mathbf{x}) \wedge B(\mathbf{y}')$ to $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. An analogous argument shows that $\lceil \pi_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \rceil$ is a morphism from $A(\mathbf{x}) \wedge B(\mathbf{y}')$ to $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$.

It remains to show that $A(\mathbf{x}) \wedge B(\mathbf{y}')$ satisfies the universal property of the binary product of $A(\mathbf{x})$ and $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$. Suppose that $C(\mathbf{z})$ is an object of $\mathscr{C}(\mathbb{T})$ and that $\lceil F(\mathbf{z},\mathbf{u})\rceil : C(\mathbf{z}) \to A(\mathbf{x})$ and $\lceil G(\mathbf{z},\mathbf{v})\rceil : C(\mathbf{z}) \to B(\mathbf{y})$ are two morphisms in $\mathscr{C}(\mathbb{T})$. We must show that there exists a unique morphism

$$\langle \lceil F(\mathbf{z},\mathbf{u})\rceil, \lceil G(\mathbf{z},\mathbf{v}))\rceil\rangle = \lceil \langle F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{v})\rangle \rceil : C(\mathbf{z}) \to A(\mathbf{x}) \wedge B(\mathbf{y}')$$

making the following diagram commute:

$$\begin{array}{ccccc} & & C(\mathbf{z}) & & \\ & \swarrow^{\lceil F(\mathbf{z},\mathbf{u})\rceil} & \Big\downarrow{\scriptstyle \lceil \langle F(\mathbf{z},\mathbf{u}),G(\mathbf{z},\mathbf{v})\rangle\rceil} & \searrow^{\lceil G(\mathbf{z},\mathbf{v})\rceil} & \\ A(\mathbf{x}) & \xleftarrow[\lceil \pi_A(\mathbf{x},\mathbf{y}',\mathbf{u})\rceil]{} & A(\mathbf{x}) \wedge B(\mathbf{y}') & \xrightarrow[\lceil \pi_B(\mathbf{x},\mathbf{y}',\mathbf{v})\rceil]{} & B(\mathbf{y}) \end{array} \tag{3.1.10}$$

Define

$$\langle F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{v})\rangle \underset{\text{def}}{\equiv} F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v}).$$

We first show that $\lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v})\rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $C(\mathbf{z})$ to $A(\mathbf{x}) \wedge B(\mathbf{y}')$. We obtain

$$F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v}) \vdash C(\mathbf{z}) \wedge (A(\mathbf{u}) \wedge B(\mathbf{v}))$$

from defining condition (1) for F and G and the rules for conjunction in $\mathbb{T}$. Hence, defining condition (1) for $F \wedge G$ holds. Similarly, defining condition (2) for $F \wedge G$ follows from defining condition (2) F and G, and the same for defining condition (3). Hence, $\lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v})\rceil$ is indeed a morphism from $C(\mathbf{z})$ to $A(\mathbf{x}) \wedge B(\mathbf{y}')$ in $\mathscr{C}(\mathbb{T})$.

Next, we show that diagram (3.1.10) commutes for $\lceil \langle F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{v})\rangle\rceil := \lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v})\rceil$.

Since conjunction is associative in $\mathbb{T}$, in order to show that $\lceil (F \wedge G); \pi_A\rceil = \lceil F\rceil$, it suffices to show that

$$\vdash (\exists \mathbf{q})(\exists \mathbf{p})(F(\mathbf{z},\mathbf{q}) \wedge G(\mathbf{z},\mathbf{p}) \wedge A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q} = \mathbf{u}) \Leftrightarrow F(\mathbf{z},\mathbf{u})$$

holds in $\mathbb{T}$. We have that

$$F(\mathbf{z},\mathbf{a}) \wedge G(\mathbf{z},\mathbf{b}) \wedge A(\mathbf{a}) \wedge B(\mathbf{b}) \wedge \mathbf{a} = \mathbf{u} \vdash^{\mathbf{a},\mathbf{b}} F(\mathbf{z},\mathbf{u})$$

by ($\wedge$-E) and (=-E). Hence, we obtain

$$\vdash (\exists \mathbf{q})(\exists \mathbf{p})(F(\mathbf{z},\mathbf{q}) \wedge G(\mathbf{z},\mathbf{p}) \wedge A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q} = \mathbf{u}) \Rightarrow F(\mathbf{z},\mathbf{u})$$

by (∃-E) and (⇒-I).

Conversely, we obtain $F(\mathbf{z},\mathbf{u}) \vdash C(\mathbf{z})$ by defining condition (1) for F and $C(\mathbf{z}) \vdash (\exists\mathbf{v})G(\mathbf{z},\mathbf{v})$ by defining condition (2) for G. It thus follows that $F(\mathbf{z},\mathbf{u}) \vdash (\exists\mathbf{v})G(\mathbf{z},\mathbf{v})$ by (Cut). Moreover, we obtain $G(\mathbf{z},\mathbf{b}) \stackrel{\mathbf{b}}{\vdash} B(\mathbf{b})$ by defining condition (1) for G. We thus obtain

$$F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{b}) \stackrel{\mathbf{b}}{\vdash} F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{b}) \wedge A(\mathbf{u}) \wedge B(\mathbf{b}) \wedge \mathbf{u}=\mathbf{u},$$

by defining condition (1) for F, (=-I), and (∧-I), and so it follows by (∃-I) that

$$F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{b}) \stackrel{\mathbf{b}}{\vdash} (\exists\mathbf{q})(\exists\mathbf{p})(F(\mathbf{z},\mathbf{q}) \wedge G(\mathbf{z},\mathbf{p}) \wedge A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q}=\mathbf{u}).$$

Hence, we obtain

$$\vdash F(\mathbf{z},\mathbf{u}) \Rightarrow (\exists\mathbf{q})(\exists\mathbf{p})(F(\mathbf{z},\mathbf{q}) \wedge G(\mathbf{z},\mathbf{p}) \wedge A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q}=\mathbf{u})$$

by (∃-E) and (⇒-I). Consequently, $\lceil (F \wedge G);\pi_A \rceil = \lceil F \rceil$. A similar argument shows that $\lceil (F \wedge G);\pi_B \rceil = \lceil G \rceil$, and so diagram (3.1.10) indeed commutes for $\lceil F \wedge G \rceil : C \to A \wedge B$.

It remains to show that $\lceil F \wedge G \rceil$ is the unique morphism making diagram (3.1.10) commute. Suppose that $\lceil H(\mathbf{z},\mathbf{u},\mathbf{v}) \rceil : C(\mathbf{z}) \to A(\mathbf{x}) \wedge B(\mathbf{y}')$ is another morphism of $\mathscr{C}(\mathbb{T})$ making diagram (3.1.10) commute. We must show that

$$\vdash F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v}) \Leftrightarrow H(\mathbf{z},\mathbf{u},\mathbf{v})$$

in $\mathbb{T}$. Since $\lceil H \rceil$ makes diagram (3.1.10) commute, we have that $\lceil H;\pi_A \rceil = \lceil F \rceil$ and $\lceil H;\pi_B \rceil = \lceil G \rceil$, and so $\vdash H;\pi_A \Leftrightarrow F$ and $\vdash H;\pi_B \Leftrightarrow G$. Hence, by the Equivalence Theorem, it suffices to show that

$$\vdash (H;\pi_A)(\mathbf{z},\mathbf{u}) \wedge (H;\pi_B)(\mathbf{z},\mathbf{v}) \Leftrightarrow H(\mathbf{z},\mathbf{u},\mathbf{v}),$$

where

$$(H;\pi_A)(\mathbf{z},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists\mathbf{q})(\exists\mathbf{p})(H(\mathbf{z},\mathbf{q},\mathbf{p}) \wedge (A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q}=\mathbf{u}))$$

and

$$(H;\pi_B)(\mathbf{z},\mathbf{v}) \underset{\text{def}}{\equiv} (\exists\mathbf{q}')(\exists\mathbf{p}')(H(\mathbf{z},\mathbf{q}',\mathbf{p}') \wedge (A(\mathbf{q}') \wedge B(\mathbf{p}') \wedge \mathbf{p}'=\mathbf{v})).$$

The following derivation in $\mathbb{T}$ shows that

$$\vdash (H;\pi_A)(\mathbf{z},\mathbf{u}) \wedge (H;\pi_B)(\mathbf{z},\mathbf{v}) \Rightarrow H(\mathbf{z},\mathbf{u},\mathbf{v}).$$

1		$(H;\pi_A)(\mathbf{z},\mathbf{u})$	
2		$(H;\pi_B)(\mathbf{z},\mathbf{v})$	
3	$\mathbf{a}^*,\mathbf{b}^*$	$H(\mathbf{z},\mathbf{a},\mathbf{b}) \wedge (A(\mathbf{a}) \wedge B(\mathbf{b}) \wedge \mathbf{a} = \mathbf{u})$	
4		$H(\mathbf{z},\mathbf{a}',\mathbf{b}') \wedge (A(\mathbf{a}') \wedge B(\mathbf{b}') \wedge \mathbf{b}' = \mathbf{v})$	
5		$H(\mathbf{z},\mathbf{u},\mathbf{b}) \wedge H(\mathbf{z},\mathbf{a}',\mathbf{v})$	(=-E), ($\wedge$-I), 3, 4
6		$\mathbf{u} = \mathbf{a}' \wedge \mathbf{b} = \mathbf{v}$	Defining condition (3) for H, 5
7		$H(\mathbf{z},\mathbf{u},\mathbf{v})$	($\wedge$-E), (=-E), 5, 6
8		$H(\mathbf{z},\mathbf{u},\mathbf{v})$	($\exists$-E), 1, 2, 3–7

Conversely, we obtain

$$H(\mathbf{z},\mathbf{u},\mathbf{v}) \vdash H(\mathbf{z},\mathbf{u},\mathbf{v}) \wedge (A(\mathbf{u}) \wedge B(\mathbf{v}) \wedge \mathbf{u} = \mathbf{u})$$

by defining condition (1) for H, (=-I), and ($\wedge$-I). Hence, it follows by ($\wedge$-I) and ($\exists$-I) that

$$H(\mathbf{z},\mathbf{u},\mathbf{v}) \vdash (H;\pi_A).$$

An analogous argument shows that

$$H(\mathbf{z},\mathbf{u},\mathbf{v}) \vdash (H;\pi_B),$$

and so we obtain

$$\vdash H(\mathbf{z},\mathbf{u},\mathbf{v}) \Rightarrow (H;\pi_A) \wedge (H;\pi_B).$$

Consequently, we obtain $\vdash F \wedge G \Leftrightarrow H$ as noted above, and so in fact $\lceil H \rceil = \lceil F \wedge G \rceil$. Therefore, $\lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v}) \rceil$ is indeed the unique morphism from $C(\mathbf{z})$ to $A(\mathbf{x}) \wedge B(\mathbf{y}')$ in $\mathscr{C}(\mathbb{T})$ making diagram (3.1.10) commute, whence $A(\mathbf{x}) \wedge B(\mathbf{y}')$ is indeed the product of $A(\mathbf{x})$ and $B(\mathbf{y}')$ in $\mathscr{C}(\mathbb{T})$ (up to isomorphism).

Note that, in particular, the product of $A(\mathbf{x})$ with itself obtained via the above construction is $A(\mathbf{x}) \wedge A(\mathbf{x}')$, where the variables in the list $\mathbf{x}'$ are new, and not $A(\mathbf{x}) \wedge A(\mathbf{x})$.

(iii) (Pullbacks) We now show that $\mathscr{C}(\mathbb{T})$ has pullbacks. Suppose we have the following pair of morphisms in $\mathscr{C}(\mathbb{T})$:

$$\begin{array}{ccc} & & B(\mathbf{y}) \\ & & \big\downarrow{\scriptstyle \lceil G(\mathbf{y},\mathbf{w}) \rceil} \\ A(\mathbf{x}) & \xrightarrow[\lceil F(\mathbf{x},\mathbf{w}) \rceil]{} & C(\mathbf{z}) \end{array}$$

Let $\mathbf{y}'$ be a list of distinct variables not occurring in $A(\mathbf{x})$ such that $|\mathbf{y}'| = |\mathbf{y}|$ and $\mathbf{y}'$ is free for $\mathbf{y}$ in B. As in the case of binary products in part (ii), if none of the variables in the list $\mathbf{y}$ occur in $A(\mathbf{x})$, we let $\mathbf{y}'$ be the list $\mathbf{y}$ itself and we note that $B(\mathbf{y})$ and $B(\mathbf{y}')$ are provably equivalent in $\mathbb{T}$ and isomorphic in $\mathscr{C}(\mathbb{T})$. Consider the formulas

$$A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}') \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge B(\mathbf{y}') \wedge (\forall \mathbf{w})(F(\mathbf{x}, \mathbf{w}) \Leftrightarrow G(\mathbf{y}', \mathbf{w})),$$

$$P_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{u},$$

and

$$P_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}') \wedge \mathbf{y}' = \mathbf{v}.$$

Note that $\lceil P_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \rceil$ is a morphism from $A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$ to $A(\mathbf{x})$ and $\lceil P_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \rceil$ is a morphism from $A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$ to $B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$. Indeed, we obtain $P_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \vdash A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$ and $P_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \vdash A(\mathbf{u})$ by ($\wedge$-E), (=-E), and the definition of P_A. Thus, defining condition (1) for P_A follows by ($\wedge$-I) and ($\Rightarrow$-I). We obtain $A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}') \vdash A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}') \wedge \mathbf{u} = \mathbf{u}$ by (=-I) and ($\wedge$-I), from which defining condition (2) for P_A follows by ($\exists$-I) and ($\Rightarrow$-I). Moreover, defining condition (3) for P_A follows from the properties of equality in $\mathbb{T}$. The argument for $\lceil P_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \rceil$ is analogous.

We claim that $A \underset{F,G}{\times} B$, together with the projections $\lceil P_A \rceil : A \underset{F,G}{\times} B \to A$, and $\lceil P_B \rceil : A \underset{F,G}{\times} B \to B$, is the pullback of $\lceil F \rceil$ and $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$. Note that the formulas $A \underset{F,G}{\times} B$, P_A, and P_B depend on the representatives F and G of the morphisms $\lceil F \rceil$ and $\lceil G \rceil$, respectively. However, for any other choice of representatives F' and G', we obtain formulas $A \underset{F',G'}{\times} B$, P'_A, and P'_B that contain the same number of free variables as $A \underset{F,G}{\times} B$, P_A, and P_B and are provably equivalent in $\mathbb{T}$ to $A \underset{F,G}{\times} B$, P_A, and P_B, respectively. Hence, by Lemma 3.1.1.7, $A \underset{F,G}{\times} B$ and $A \underset{F',G'}{\times} B$ are isomorphic as objects in $\mathscr{C}(\mathbb{T})$ and, furthermore, $\lceil P'_A \rceil$ and $\lceil P'_B \rceil$ correspond to $\lceil P_A \rceil$ and $\lceil P_B \rceil$, respectively, under this isomorphism. Hence, construction given above for the pullback of $\lceil F \rceil$ and $\lceil G \rceil$ and its projections is well-defined and does not depend on the chosen representatives of $\lceil F \rceil$ and $\lceil G \rceil$.

We first show that $\lceil P_A \rceil$ and $\lceil P_B \rceil$ make the diagram

$$\begin{array}{ccc} A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') & \xrightarrow{\lceil P_B(\mathbf{x},\mathbf{y}',\mathbf{v})\rceil} & B(\mathbf{y}) \\ {\scriptstyle \lceil P_A(\mathbf{x},\mathbf{y}',\mathbf{u})\rceil}\downarrow & & \downarrow{\scriptstyle \lceil G(\mathbf{y},\mathbf{w})\rceil} \\ A(\mathbf{x}) & \xrightarrow[\lceil F(\mathbf{x},\mathbf{w})\rceil]{} & C(\mathbf{z}) \end{array} \tag{3.1.11}$$

commute in $\mathscr{C}(\mathbb{T})$. We have

$$(P_A; F)(\mathbf{x}, \mathbf{y}', \mathbf{w}) \underset{\text{def}}{\equiv} (\exists \mathbf{q})((A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{q}) \wedge F(\mathbf{q}, \mathbf{w}))$$

and

$$(P_B; G)(\mathbf{x}, \mathbf{y}', \mathbf{w}) \underset{\text{def}}{\equiv} (\exists \mathbf{p})((A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{y} = \mathbf{p}) \wedge G(\mathbf{p}, \mathbf{w})).$$

We obtain

$$(A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{a}) \wedge F(\mathbf{a}, \mathbf{w}) \vdash^{\mathbf{a}} F(\mathbf{x}, \mathbf{w}) \wedge (F(\mathbf{x}, \mathbf{w}) \Leftrightarrow G(\mathbf{y}', \mathbf{w}))$$

by the rules for conjunction, (=-E), and (∀-E). Hence, it follows by (⇒-E) that

$$(A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{a}) \wedge F(\mathbf{a}, \mathbf{w}) \vdash^{\mathbf{a}} G(\mathbf{y}', \mathbf{w}),$$

from which

$$(A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{x} = \mathbf{a}) \wedge F(\mathbf{a}, \mathbf{w}) \vdash^{\mathbf{a}} (A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}') \wedge \mathbf{y}' = \mathbf{y}') \wedge G(\mathbf{y}', \mathbf{w})$$

follows by (=-I) and the rules for conjunction. We thus obtain

$$(P_A; F)(\mathbf{x}, \mathbf{y}', \mathbf{w}) \vdash (P_B; G)(\mathbf{x}, \mathbf{y}', \mathbf{w})$$

by (∃-I) and (∃-E). An analogous argument shows that

$$(P_B; G)(\mathbf{x}, \mathbf{y}', \mathbf{w}) \vdash (P_A; F)(\mathbf{x}, \mathbf{y}', \mathbf{w}),$$

and so we obtain

$$\lceil P_A; F \rceil = \lceil P_B; G \rceil .$$

Hence, diagram (3.1.11) commutes with $\lceil P_A \rceil$ and $\lceil P_B \rceil$.

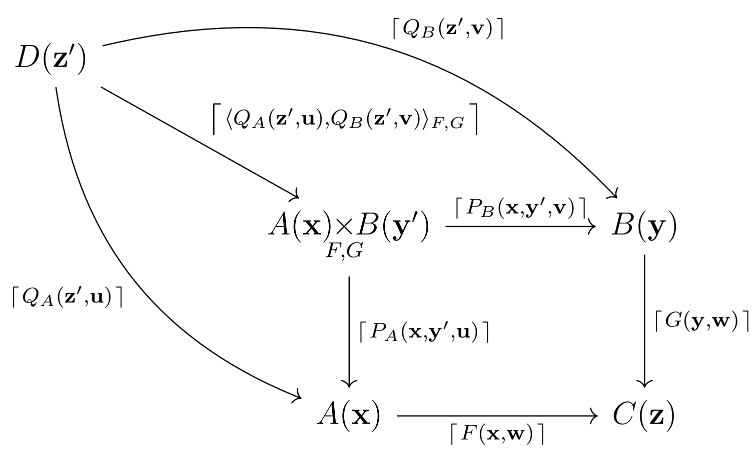
It remains to show that $A\underset{F,G}{\times}B$, together with the projections $\lceil P_A \rceil$ and $\lceil P_B \rceil$, satisfies the universal property of the pullback of $\lceil F \rceil$ and $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$. Suppose that $D(\mathbf{z}')$ is an object in $\mathscr{C}(\mathbb{T})$ and that $\ulcorner Q_A(\mathbf{z}',\mathbf{u}) \urcorner : D(\mathbf{z}') \to A(\mathbf{x})$ and $\ulcorner Q_B(\mathbf{z}',\mathbf{v}) \urcorner : D(\mathbf{z}') \to B(\mathbf{y})$ are morphisms in $\mathscr{C}(\mathbb{T})$ such that the diagram

$$\begin{CD} D(\mathbf{z}') @>{\ulcorner Q_B(\mathbf{z}',\mathbf{v}) \urcorner}>> B(\mathbf{y}) \\ @V{\ulcorner Q_A(\mathbf{z}',\mathbf{u}) \urcorner}VV @VV{\ulcorner G(\mathbf{y},\mathbf{w}) \urcorner}V \\ A(\mathbf{x}) @>>{\ulcorner F(\mathbf{x},\mathbf{w}) \urcorner}> C(\mathbf{z}) \end{CD} \tag{3.1.12}$$

commutes in $\mathscr{C}(\mathbb{T})$. We must show that there is a unique morphism

$$\langle \ulcorner Q_A(\mathbf{z}',\mathbf{u}) \urcorner , \ulcorner Q_B(\mathbf{z}',\mathbf{v}) \urcorner \rangle_{\ulcorner F \urcorner, \ulcorner G \urcorner} = \ulcorner \langle Q_A(\mathbf{z}',\mathbf{u}), Q_B(\mathbf{z}',\mathbf{v}) \rangle_{F,G} \urcorner : D(\mathbf{z}') \to A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$$

in $\mathscr{C}(\mathbb{T})$ such that the diagram



(3.1.13)

commutes. Define

$$\langle Q_A(\mathbf{z}',\mathbf{u}), Q_B(\mathbf{z}',\mathbf{v}) \rangle_{F,G} \underset{\text{def}}{\equiv} Q_A(\mathbf{z}',\mathbf{u}) \wedge Q_B(\mathbf{z}',\mathbf{v}).$$

We first show that $\ulcorner Q_A(\mathbf{z}',\mathbf{u}) \wedge Q_B(\mathbf{z}',\mathbf{v}) \urcorner$ is indeed a morphism from $D(\mathbf{z}')$ to $A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$ in $\mathscr{C}(\mathbb{T})$. By defining condition (1) for Q_A and Q_B, we obtain

$$Q_A(\mathbf{z}',\mathbf{u}) \wedge Q_B(\mathbf{z}',\mathbf{v}) \vdash D(\mathbf{z}')$$

and

$$Q_A(\mathbf{z}',\mathbf{u}) \wedge Q_B(\mathbf{z}',\mathbf{v}) \vdash A(\mathbf{u}) \wedge B(\mathbf{v}).$$

Furthermore, we obtain

$$Q_A(\mathbf{z}',\mathbf{u}) \wedge Q_B(\mathbf{z}',\mathbf{v}), F(\mathbf{u},\mathbf{w}) \vdash (Q_A; F)(\mathbf{z}',\mathbf{w})$$

by the rules for conjunction and ($\exists$-I). Since diagram (3.1.12) commutes in $\mathscr{C}(\mathbb{T})$, we have that

$$\vdash (Q_A; F)(\mathbf{z}', \mathbf{w}) \Leftrightarrow (Q_B; G)(\mathbf{z}', \mathbf{w}),$$

and so we obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}), F(\mathbf{u}, \mathbf{w}) \vdash (Q_B; G)(\mathbf{z}', \mathbf{w}).$$

We obtain

$$H(\mathbf{z}', \mathbf{u}, \mathbf{v}), F(\mathbf{u}, \mathbf{w}), Q_B(\mathbf{z}', \mathbf{b}) \wedge G(\mathbf{b}, \mathbf{w}) \vdash^{\mathbf{b}} \mathbf{b} = \mathbf{v}$$

by defining condition (3) for Q_B, and so

$$Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}), F(\mathbf{u}, \mathbf{w}) \vdash G(\mathbf{v}, \mathbf{w})$$

follows by ($\wedge$-E), (=-E) and ($\exists$-E). Hence, we obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}) \vdash F(\mathbf{u}, \mathbf{w}) \Rightarrow G(\mathbf{v}, \mathbf{w})$$

by ($\Rightarrow$-I). We obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}) \vdash G(\mathbf{v}, \mathbf{w}) \Rightarrow F(\mathbf{u}, \mathbf{w})$$

by an analogous argument, and so we obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}) \vdash A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{v})$$

by ($\forall$-I) and ($\wedge$-I). Defining condition (1) for $Q_A \wedge Q_B$ then follows by ($\wedge$-I) and ($\Rightarrow$-I). Defining conditions (2) and (3) for $Q_A \wedge Q_B$ follow from defining conditions (2) and (3), respectively, for Q_A and Q_B. Hence, $\ulcorner Q_A \wedge Q_B \urcorner$ is indeed a morphism in $\mathscr{C}(\mathbb{T})$ from D to $A \underset{F,G}{\times} B$.

In order to show that diagram (3.1.13) commutes in $\mathscr{C}(\mathbb{T})$ for $\ulcorner \langle Q_A, Q_B \rangle_{F,G} \urcorner :=$ $\ulcorner Q_A \wedge Q_B \urcorner$, it remains to show that $\ulcorner (Q_A \wedge Q_B); P_A \urcorner = \ulcorner Q_A \urcorner$ and $\ulcorner (Q_A \wedge Q_B); P_B \urcorner =$ $\ulcorner Q_B \urcorner$. We obtain

$$((Q_A \wedge Q_B); P_A)(\mathbf{z}', \mathbf{u}) \vdash Q_A(\mathbf{z}', \mathbf{u})$$

by ($\exists$-E) and (=-E). Conversely, by defining condition (1) for Q_A, we obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \vdash D(\mathbf{z}'),$$

from which

$$Q_A(\mathbf{z}', \mathbf{u}) \vdash (\exists \mathbf{v}) Q_B(\mathbf{z}', \mathbf{v})$$

follows by defining condition (2) for Q_B and (Cut). We obtain

$$Q_A(\mathbf{z}', \mathbf{u}), Q_B(\mathbf{z}', \mathbf{b}) \vdash^{\mathbf{b}} A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{b})$$

by ($\wedge$-I) and defining condition (1) for $Q_A \wedge Q_B$. Then,

$$Q_A(\mathbf{z}', \mathbf{u}), Q_B(\mathbf{z}', \mathbf{b}) \vdash^{\mathbf{b}} (Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{b})) \wedge (A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{b}) \wedge \mathbf{u} = \mathbf{u})$$

follows by ($\wedge$-I) and (=-I), and so we obtain

$$Q_A(\mathbf{z}', \mathbf{u}) \vdash ((Q_A \wedge Q_B); P_A)(\mathbf{z}', \mathbf{u})$$

by ($\exists$-I) and ($\exists$-E). Therefore, $\lceil (Q_A \wedge Q_B); P_A \rceil = \lceil Q_A \rceil$. An analogous argument shows that $\lceil (Q_A \wedge Q_B); P_B \rceil = \lceil Q_B \rceil$, and so diagram (3.1.13) commutes in $\mathscr{C}(\mathbb{T})$ for $\lceil Q_A \wedge Q_B \rceil$.

Now suppose that $\lceil J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \rceil : D(\mathbf{z}') \to A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$ is a morphism in $\mathscr{C}(\mathbb{T})$ making diagram (3.1.13) commute. We wish to show that $\lceil Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}) \rceil = \lceil J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \rceil$, that is, that

$$\vdash Q_A(\mathbf{z}', \mathbf{u}) \wedge Q_B(\mathbf{z}', \mathbf{v}) \Leftrightarrow J(\mathbf{z}', \mathbf{u}, \mathbf{v}).$$

Since diagram (3.1.13) commutes for $\lceil J \rceil$, we have

$$\vdash J; P_A \Leftrightarrow Q_A$$

and

$$\vdash J; P_B \Leftrightarrow Q_B.$$

Hence, it suffices to show that

$$\vdash (J; P_A)(\mathbf{z}', \mathbf{u}) \wedge (J; P_B)(\mathbf{z}', \mathbf{v}) \Leftrightarrow J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \tag{3.1.14}$$

holds in $\mathbb{T}$. We obtain

$$J(\mathbf{z}', \mathbf{a}, \mathbf{b}) \wedge P_A(\mathbf{a}, \mathbf{b}, \mathbf{u}), J(\mathbf{z}', \mathbf{c}, \mathbf{d}) \wedge P_B(\mathbf{c}, \mathbf{d}, \mathbf{v}) \vdash^{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}} J(\mathbf{z}', \mathbf{u}, \mathbf{b}) \wedge J(\mathbf{z}', \mathbf{c}, \mathbf{v})$$

by (=-E) and ($\wedge$-I). Hence, we obtain

$$J(\mathbf{z}', \mathbf{a}, \mathbf{b}) \wedge P_A(\mathbf{a}, \mathbf{b}, \mathbf{u}), J(\mathbf{z}', \mathbf{c}, \mathbf{d}) \wedge P_B(\mathbf{c}, \mathbf{d}, \mathbf{v}) \vdash^{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}} J(\mathbf{z}', \mathbf{u}, \mathbf{v})$$

by defining condition (3) for J and (=-E). Thus,

$$(J; P_A)(\mathbf{z}', \mathbf{u}) \wedge (J; P_B)(\mathbf{z}', \mathbf{v}) \vdash J(\mathbf{z}', \mathbf{u}, \mathbf{v})$$

follows by (∃-E). Conversely, we obtain

$$J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \vdash J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \wedge (A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{v}) \wedge \mathbf{u} = \mathbf{u})$$

by defining condition (1) for J, (=-I), and (∧-I). Thus,

$$J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \vdash (J; P_A)(\mathbf{z}', \mathbf{u})$$

follows by (∃-I). An analogous argument shows that

$$J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \vdash (J; P_B)(\mathbf{z}', \mathbf{v}),$$

and so we obtain

$$J(\mathbf{z}', \mathbf{u}, \mathbf{v}) \vdash (J; P_A)(\mathbf{z}', \mathbf{u}) \wedge (J; P_B)(\mathbf{z}', \mathbf{v}).$$

Hence, (3.1.14) holds in $\mathbb{T}$, and so $\lceil Q_A \wedge Q_B \rceil = \lceil J \rceil$. Therefore, $\lceil Q_A \wedge Q_B \rceil$ is indeed the unique morphism from D to $A \underset{F,G}{\times} B$ in $\mathscr{C}(\mathbb{T})$ making diagram (3.1.13) commute. Thus, $A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}')$, together with the projections $\lceil P_A(\mathbf{x}, \mathbf{y}', \mathbf{u}) \rceil$ and $\lceil P_B(\mathbf{x}, \mathbf{y}', \mathbf{v}) \rceil$, is indeed the pullback of $\lceil F(\mathbf{x}, \mathbf{w}) \rceil$ and $\lceil G(\mathbf{y}, \mathbf{w}) \rceil$ in $\mathscr{C}(\mathbb{T})$ (up to isomorphism), and so $\mathscr{C}(\mathbb{T})$ has all binary pullbacks.

(iv) (Equalisers) We now wish to show that $\mathscr{C}(\mathbb{T})$ has equalisers. We shall merely give the construction as the proof is similar to the proofs of parts (ii) and (iii) above. Consider the following pair of morphisms in $\mathscr{C}(\mathbb{T})$:

$$A(\mathbf{x}) \underset{\lceil G(\mathbf{x},\mathbf{v}) \rceil}{\overset{\lceil F(\mathbf{x},\mathbf{v}) \rceil}{\rightrightarrows}} B(\mathbf{y}) \ .$$

We wish to construct the equaliser of $\lceil F \rceil$ and $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$. Consider the formulas

$$E_{F,G}(\mathbf{x}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge (\forall \mathbf{w})(F(\mathbf{x}, \mathbf{w}) \Leftrightarrow G(\mathbf{x}, \mathbf{w}))$$

and

$$\xi_{F,G}(\mathbf{x}, \mathbf{u}) \underset{\text{def}}{\equiv} E_{F,G}(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u},$$

where we may drop the subscripts if no ambiguity may arise. Then, $\lceil \xi_{F,G}(\mathbf{x}, \mathbf{u}) \rceil$ is a morphism from $E_{F,G}(\mathbf{x})$ to $A(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$.

We claim that $E_{F,G}$, together with $\lceil \xi_{F,G} \rceil : E_{F,G} \to A$, is (up to isomorphism) the equaliser of $\lceil F \rceil$ and $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$. Indeed, the diagram

$$E_{F,G}(\mathbf{x}) \xrightarrow{\lceil \xi(\mathbf{x},\mathbf{u}) \rceil} A(\mathbf{x}) \underset{\lceil G(\mathbf{x},\mathbf{v}) \rceil}{\overset{\lceil F(\mathbf{x},\mathbf{v}) \rceil}{\rightrightarrows}} B(\mathbf{y}) \ , \qquad (3.1.15)$$

where $\xi \underset{\text{def}}{\equiv} \xi_{F,G}$, commutes in $\mathscr{C}(\mathbb{T})$. Furthermore, suppose that $\lceil H(\mathbf{z},\mathbf{u}) \rceil : C(\mathbf{z}) \to A(\mathbf{x})$ is a morphism in $\mathscr{C}(\mathbb{T})$ such that

$$\lceil H(\mathbf{z},\mathbf{u}); F(\mathbf{x},\mathbf{v}) \rceil = \lceil H(\mathbf{z},\mathbf{u}); G(\mathbf{x},\mathbf{v}) \rceil . \tag{3.1.16}$$

Then, the morphism $\lceil H(\mathbf{z},\mathbf{u}) \wedge E_{F,G}(\mathbf{u}) \rceil : C(\mathbf{z}) \to E_{F,G}(\mathbf{x})$ is the unique morphism from $C(\mathbf{z})$ to $E_{F,G}(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$ such that the diagram

$$\begin{array}{ccccc} E_{F,G}(\mathbf{x}) & \xrightarrow{\lceil \xi(\mathbf{x},\mathbf{u}) \rceil} & A(\mathbf{x}) & \overset{\lceil F(\mathbf{x},\mathbf{v}) \rceil}{\underset{\lceil G(\mathbf{x},\mathbf{v}) \rceil}{\rightrightarrows}} & B(\mathbf{y}) \\ {\scriptstyle \lceil H(\mathbf{z},\mathbf{u}) \wedge E_{F,G}(\mathbf{u}) \rceil} \uparrow & \nearrow {\scriptstyle \lceil H(\mathbf{z},\mathbf{u}) \rceil} & & & \\ C(\mathbf{z}) & & & & \end{array} \tag{3.1.17}$$

commutes in $\mathscr{C}(\mathbb{T})$. Thus, $E_{F,G}$, together with the morphism $\lceil \xi \rceil$, satisfies the universal property of the equaliser of $\lceil F \rceil$ and $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$. Consequently, $\mathscr{C}(\mathbb{T})$ admits all equalisers of parallel pairs of morphisms. ∎

Note that, in the spirit of Remark 3.1.1.8 and of the discussions at the beginning of the proofs of parts (ii) and (iii) of Proposition 3.1.1.15, when constructing the product of arbitrary objects $A(\mathbf{x})$ and $B(\mathbf{y})$ or the pullback of arbitrary morphisms $\lceil F(\mathbf{x},\mathbf{w}) \rceil : A(\mathbf{x}) \to C(\mathbf{z})$ and $\lceil G(\mathbf{y},\mathbf{w}) \rceil : B(\mathbf{y}) \to C(\mathbf{z})$ in the syntactic category $\mathscr{C}(\mathbb{T})$ of a theory $\mathbb{T}$, we can and will assume without loss of generality that the lists $\mathbf{x}$ and $\mathbf{y}$ are disjoint, and so we do not need to use a new list $\mathbf{y}'$ of distinct variables in the constructions of the product and pullback.

Corollary 3.1.1.16 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$. Then, $\mathscr{C}(\mathbb{T})$ is finitely complete.*

Proof By Proposition 3.1.1.15, $\mathscr{C}(\mathbb{T})$ admits a terminal object, binary products, binary pullbacks, and equalisers. Hence, $\mathscr{C}(\mathbb{T})$ is finitely complete (see Proposition B.0.0.2 in Appendix B). ∎

Lemma 3.1.1.17 *Let $\mathscr{C}(\mathbb{T})$ be a syntactic category of a theory $\mathbb{T}$ and let $\lceil F(\mathbf{x},\mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ and $\lceil F'(\mathbf{x}',\mathbf{v}') \rceil : A'(\mathbf{x}') \to B'(\mathbf{y}')$ be two morphisms in $\mathscr{C}(\mathbb{T})$. Then,*

$$\langle \lceil (\pi_A; F)(\mathbf{x},\mathbf{x}',\mathbf{v}) \rceil , \lceil (\pi_{A'}; F')(\mathbf{x},\mathbf{x}',\mathbf{v}') \rceil \rangle = \lceil F(\mathbf{x},\mathbf{v}) \wedge F'(\mathbf{x}',\mathbf{v}') \rceil$$

as morphisms in $\mathscr{C}(\mathbb{T})$ from $A \wedge A'$ to $B \wedge B'$. We denote this morphism by $\lceil F(\mathbf{x},\mathbf{v}) \rceil \times \lceil F'(\mathbf{x}',\mathbf{v}') \rceil$ and it is the product of $\lceil F \rceil$ and $\lceil F' \rceil$ in $\mathscr{C}(\mathbb{T})$.

Proof By the construction in the proof of Proposition 3.1.1.15 (ii), we obtain

$$\langle \lceil \pi_A; F \rceil , \lceil \pi_{A'}; F' \rceil \rangle = \lceil (\pi_A; F) \wedge (\pi_{A'}; F') \rceil .$$

We wish to show that

$$\lceil (\pi_A; F)(\mathbf{x},\mathbf{x}',\mathbf{v}) \wedge (\pi_{A'}; F')(\mathbf{x},\mathbf{x}',\mathbf{v}') \rceil = \lceil F(\mathbf{x},\mathbf{v}) \wedge F'(\mathbf{x}',\mathbf{v}') \rceil ,$$

that is, that

$$\vdash (\pi_A; F)(\mathbf{x}, \mathbf{x}', \mathbf{v}) \wedge (\pi_{A'}; F')(\mathbf{x}, \mathbf{x}', \mathbf{v}') \Leftrightarrow F(\mathbf{x}, \mathbf{v}) \wedge F'(\mathbf{x}', \mathbf{v}'). \tag{3.1.18}$$

We obtain

$$F(\mathbf{x}, \mathbf{v}), F'(\mathbf{x}', \mathbf{v}') \vdash (\pi_A; F)(\mathbf{x}, \mathbf{x}', \mathbf{v}) \wedge (\pi_{A'}; F')(\mathbf{x}, \mathbf{x}', \mathbf{v}')$$

by defining condition (1) for F and F', (=-I), ($\wedge$-I), and ($\exists$-I). Conversely, we obtain

$$(\pi_A; F)(\mathbf{x}, \mathbf{x}', \mathbf{v}), (\pi_{A'}; F')(\mathbf{x}, \mathbf{x}', \mathbf{v}') \vdash F(\mathbf{x}, \mathbf{v}) \wedge F'(\mathbf{x}', \mathbf{v}')$$

by ($\exists$-E), ($\wedge$-E), ($\wedge$-I), and (=-E). Hence, (3.1.18) follows by ($\wedge$-I) and ($\Rightarrow$-I), and so in fact

$$\langle \lceil \pi_A; F \rceil , \lceil \pi_{A'}; F' \rceil \rangle = \lceil F \wedge F' \rceil .$$

Furthermore, if we follow the usual construction of the product of two morphisms in a category (see for example [16]), we obtain the morphism $\langle \lceil \pi_A; F \rceil , \lceil \pi_{A'}; F' \rceil \rangle : A \wedge A' \to B \wedge B'$ as the product of $\lceil F \rceil$ and $\lceil F' \rceil$ in $\mathscr{C}(\mathbb{T})$. Hence, $\lceil F(\mathbf{x}, \mathbf{v}) \rceil \times \lceil F'(\mathbf{x}', \mathbf{v}') \rceil := \lceil F(\mathbf{x}, \mathbf{v}) \wedge F'(\mathbf{x}', \mathbf{v}') \rceil$ is indeed the product of $\lceil F \rceil$ and $\lceil F' \rceil$ in $\mathscr{C}(\mathbb{T})$. ∎

There are two operations on morphisms that arise when we consider products in categories, namely the pairing and the product. As shown in Proposition 3.1.1.15, given a pair of morphisms $\lceil F(\mathbf{z}, \mathbf{u}) \rceil : C(\mathbf{z}) \to A(\mathbf{x})$ and $\lceil G(\mathbf{z}, \mathbf{v}) \rceil : C(\mathbf{z}) \to B(\mathbf{y})$,

$$\langle \lceil F \rceil , \lceil G \rceil \rangle := \lceil F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}) \rceil : C(\mathbf{z}) \to A(\mathbf{x}) \wedge B(\mathbf{y})$$

is the pairing of $\lceil F \rceil$ and $\lceil G \rceil$, that is, the unique morphism from $C(\mathbf{z})$ to the product of $A(\mathbf{x})$ and $B(\mathbf{y})$ arising from the universal property of products. As shown in Lemma 3.1.1.17, the product of two morphisms $\lceil H(\mathbf{x}, \mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ and $\lceil H'(\mathbf{x}', \mathbf{v}') \rceil : A'(\mathbf{x}') \to B'(\mathbf{y}')$ in $\mathscr{C}(\mathbb{T})$ is the morphism

$$\lceil H(\mathbf{x}, \mathbf{v}) \rceil \times \lceil H'(\mathbf{x}', \mathbf{v}') \rceil := \lceil H(\mathbf{x}, \mathbf{v}) \wedge H'(\mathbf{x}', \mathbf{v}') \rceil : A(\mathbf{x}) \wedge A'(\mathbf{x}') \to B(\mathbf{y}) \wedge B'(\mathbf{y}').$$

We now wish to show that all syntactic categories are in fact regular categories. Since we have given a construction of pullbacks in syntactic categories in Proposition 3.1.1.15 and have characterised subobjects in syntactic categories in Remark 3.1.1.14, we can reformulate the definition of a regular category in terms of pullback-stable images (see Definition B.0.0.3 in Appendix B) in the context of syntactic categories as follows.

Definition 3.1.1.18 Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$. Then, $\mathscr{C}(\mathbb{T})$ is regular if the following conditions hold.

(i) $\mathscr{C}(\mathbb{T})$ is finitely complete.

(ii) $\mathscr{C}(\mathbb{T})$ has images: for each morphism $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$, there is a smallest subobject $\mathrm{Im}_F(\mathbf{y})$ of $B(\mathbf{y})$ with associated morphism $\lceil I_F(\mathbf{y},\mathbf{v})\rceil : \mathrm{Im}_F(\mathbf{y}) \to B(\mathbf{y})$, called the *image* of $\lceil F(\mathbf{x},\mathbf{v})\rceil$ in $\mathscr{C}(\mathbb{T})$, through which $\lceil F(\mathbf{x},\mathbf{v})\rceil$ factors, that is, such that the diagram

$$\begin{array}{ccc} A(\mathbf{x}) & \xrightarrow{\lceil F(\mathbf{x},\mathbf{v})\rceil} & B(\mathbf{y}) \\ & \searrow \quad \nearrow_{\lceil I_F(\mathbf{y},\mathbf{v})\rceil} & \\ & \mathrm{Im}_F(\mathbf{y}) & \end{array}$$

commutes in $\mathscr{C}(\mathbb{T})$ for some morphism $A(\mathbf{x}) \to \mathrm{Im}_F(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$.

(iii) Images are preserved under pullback in the following sense. Let $\lceil F(\mathbf{x},\mathbf{w})\rceil : A(\mathbf{x}) \to C(\mathbf{z})$ and $\lceil G(\mathbf{y},\mathbf{w})\rceil : B(\mathbf{y}) \to C(\mathbf{z})$ be morphisms in $\mathbb{T}$ and consider their pullback

$$\begin{array}{ccc} A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{y}) & \xrightarrow{\lceil P_B(\mathbf{x},\mathbf{y},\mathbf{v})\rceil} & B(\mathbf{y}) \\ {\scriptstyle \lceil P_A(\mathbf{x},\mathbf{y},\mathbf{u})\rceil}\downarrow & & \downarrow{\scriptstyle \lceil G(\mathbf{y},\mathbf{w})\rceil} \\ A(\mathbf{x}) & \xrightarrow[\lceil F(\mathbf{x},\mathbf{w})\rceil]{} & C(\mathbf{z}) \end{array}$$

(as remarked after Proposition 3.1.1.15, we can assume without loss of generality that the lists $\mathbf{x}$ and $\mathbf{y}$ are disjoint). Then, the pullback of $\lceil I_G(\mathbf{z},\mathbf{w})\rceil : \mathrm{Im}_G(\mathbf{z}) \to C(\mathbf{z})$ along $\lceil F(\mathbf{x},\mathbf{w})\rceil : A(\mathbf{x}) \to C(\mathbf{z})$ is $\lceil I_{P_A}(\mathbf{x},\mathbf{u})\rceil : \mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x})$, that is to say,

$$\begin{array}{ccc} \mathrm{Im}_{P_A}(\mathbf{x}) & \longrightarrow & \mathrm{Im}_G(\mathbf{z}) \\ {\scriptstyle \lceil I_{P_A}(\mathbf{x},\mathbf{u})\rceil}\downarrow & & \downarrow{\scriptstyle \lceil I_G(\mathbf{z},\mathbf{w})\rceil} \\ A(\mathbf{x}) & \xrightarrow[\lceil F(\mathbf{x},\mathbf{w})\rceil]{} & C(\mathbf{z}) \end{array}$$

is a pullback square. □

Proposition 3.1.1.19 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of a theory $\mathbb{T}$. Then, $\mathscr{C}(\mathbb{T})$ is regular.*

Proof We show that $\mathscr{C}(\mathbb{T})$ satisfies conditions (i)–(iii) of Definition 3.1.1.18, that is, that $\mathscr{C}(\mathbb{T})$ is finitely complete and has pullback-stable images.

(i) As shown in Corollary 3.1.1.16, $\mathscr{C}(\mathbb{T})$ is finitely complete.

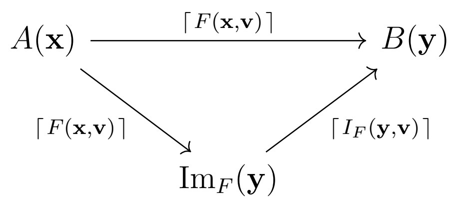
(ii) We show that $\mathscr{C}(\mathbb{T})$ has images. Let $\ulcorner F(\mathbf{x},\mathbf{v})\urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism in $\mathscr{C}(\mathbb{T})$. Define

$$\mathrm{Im}_F(\mathbf{y}) \underset{\text{def}}{\equiv} (\exists \mathbf{q})F(\mathbf{q},\mathbf{y})$$

and

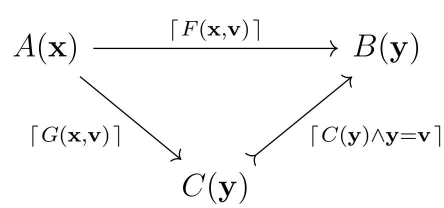
$$I_F(\mathbf{y},\mathbf{v}) \underset{\text{def}}{\equiv} \mathrm{Im}_F(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}.$$

By the same argument as in the proof of Proposition 3.1.1.13, $\ulcorner F(\mathbf{x},\mathbf{v})\urcorner : A(\mathbf{x}) \to \mathrm{Im}_F(\mathbf{y})$ and $\ulcorner I_F(\mathbf{y},\mathbf{v})\urcorner : \mathrm{Im}_F(\mathbf{y}) \to B(\mathbf{y})$ are morphisms of $\mathscr{C}(\mathbb{T})$, and the diagram



(3.1.19)

commutes in $\mathscr{C}(\mathbb{T})$. Furthermore, by Lemma 3.1.1.11, $\ulcorner I_F(\mathbf{y},\mathbf{v})\urcorner : \mathrm{Im}_F(\mathbf{y}) \to B(\mathbf{y})$ is a monomorphism. Therefore, following the discussion in Remark 3.1.1.14, $\mathrm{Im}_F(\mathbf{y})$, together with the associated monomorphism $\ulcorner I_F(\mathbf{y},\mathbf{v})\urcorner : \mathrm{Im}_F(\mathbf{y}) \to B(\mathbf{y})$, is a subobject of $B(\mathbf{y})$ making diagram (3.1.19) commute. In order to show that $\mathrm{Im}_F(\mathbf{y})$ is indeed the image of the morphism $\ulcorner F(\mathbf{x},\mathbf{y})\urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$, we must show that it is the smallest subobject of $B(\mathbf{y})$ making diagram (3.1.19) commute. By Remark 3.1.1.14, it suffices to consider subobjects of $B(\mathbf{y})$ given by an object $C(\mathbf{y})$ with associated monomorphism $\ulcorner C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}\urcorner : C(\mathbf{y}) \to B(\mathbf{y})$. Therefore, suppose $C(\mathbf{y})$ is such a subobject of $B(\mathbf{y})$ for which there exists a morphism $\ulcorner G(\mathbf{x},\mathbf{v})\urcorner : A(\mathbf{x}) \to C(\mathbf{y})$ making the diagram



(3.1.20)

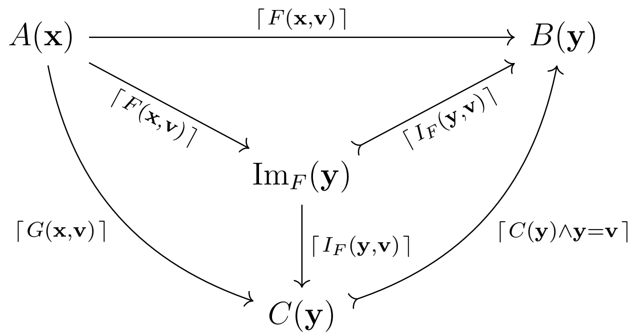
commute. It follows from the commutativity of diagram (3.1.20) that

$$\vdash F(\mathbf{x},\mathbf{v}) \Leftrightarrow (\exists \mathbf{p})(G(\mathbf{x},\mathbf{p}) \wedge (C(\mathbf{p}) \wedge \mathbf{p} = \mathbf{v}))$$

holds in $\mathbb{T}$. Hence, we obtain

$$\vdash F(\mathbf{x},\mathbf{v}) \Leftrightarrow G(\mathbf{x},\mathbf{v}) \wedge C(\mathbf{v}) \tag{3.1.21}$$

by the rules for $\exists$ and equality in $\mathbb{T}$. We claim that $\ulcorner I_F(\mathbf{y},\mathbf{v})\urcorner$ is a morphism from $\mathrm{Im}_F(\mathbf{y})$ to $C(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$ such that the diagram



(3.1.22)

commutes in $\mathscr{C}(\mathbb{T})$.

Recall that

$$I_F(\mathbf{y},\mathbf{v}) \underset{\text{def}}{\equiv} \mathrm{Im}_F(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \underset{\text{def}}{\equiv} (\exists \mathbf{q})F(\mathbf{q},\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}.$$

Hence, we obtain $I_F(\mathbf{y},\mathbf{v}) \vdash \mathrm{Im}_F(\mathbf{y})$ by ($\wedge$-E), and we obtain

$$I_F(\mathbf{y},\mathbf{v}) \vdash (\exists \mathbf{q})F(\mathbf{q},\mathbf{v})$$

by (=-E). By (3.1.21), we obtain

$$I_F(\mathbf{y},\mathbf{v}), F(\mathbf{a},\mathbf{v}) \mid\!\!\overset{\mathbf{a}}{\underline{}}\, G(\mathbf{a},\mathbf{v}) \wedge C(\mathbf{v}),$$

from which it follows by ($\wedge$-E) and ($\exists$-E) that $I_F(\mathbf{y},\mathbf{v}) \vdash C(\mathbf{v})$. Hence, we obtain

$$I_F(\mathbf{y},\mathbf{v}) \vdash \mathrm{Im}_F(\mathbf{y}) \wedge C(\mathbf{v})$$

by ($\wedge$-I), and so defining condition (1) is satisfied. Moreover, defining conditions (2) and (3) do not depend on the codomain and hence are satisfied since we have already established that $\ulcorner I_F(\mathbf{y},\mathbf{v}) \urcorner$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $\mathrm{Im}_F(\mathbf{y})$ to $B(\mathbf{y})$. Hence, $\ulcorner I_F(\mathbf{y},\mathbf{v}) \urcorner$ is indeed a morphism in $\mathscr{C}(\mathbb{T})$ from $\mathrm{Im}_F(\mathbf{y})$ to $C(\mathbf{y})$.

It remains to show that diagram (3.1.22) commutes. Since diagrams (3.1.19) and (3.1.20) commute, it suffices to show that the bottom left and right triangles of diagram (3.1.22) commute. That is to say, we must show that

$$\vdash (\exists \mathbf{p})(F(\mathbf{x},\mathbf{p}) \wedge I_F(\mathbf{p},\mathbf{v})) \Leftrightarrow G(\mathbf{x},\mathbf{v}) \tag{3.1.23}$$

and

$$\vdash (\exists \mathbf{p})(I_F(\mathbf{y},\mathbf{p}) \wedge (C(\mathbf{p}) \wedge \mathbf{p} = \mathbf{v})) \Leftrightarrow I_F(\mathbf{y},\mathbf{v}) \tag{3.1.24}$$

hold in $\mathbb{T}$. By the definition of $I_F(\mathbf{p},\mathbf{v})$, (=-E) and ($\exists$-E), we obtain

$$(\exists \mathbf{p})(F(\mathbf{x},\mathbf{p}) \wedge I_F(\mathbf{p},\mathbf{v})) \vdash F(\mathbf{x},\mathbf{v}).$$

Furthermore, by (3.1.21) and ($\wedge$-E), we obtain

$$F(\mathbf{x}, \mathbf{v}) \vdash G(\mathbf{x}, \mathbf{v}).$$

Hence, it follows by (Cut) that

$$(\exists \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge I_F(\mathbf{p}, \mathbf{v})) \vdash G(\mathbf{x}, \mathbf{v}).$$

By defining condition (1) for $\ulcorner G \urcorner$ and ($\wedge$-I), we obtain

$$G(\mathbf{x}, \mathbf{v}) \vdash G(\mathbf{x}, \mathbf{v}) \wedge C(\mathbf{v}),$$

from which it follow by (3.1.21) that

$$G(\mathbf{x}, \mathbf{v}) \vdash F(\mathbf{x}, \mathbf{v}).$$

It then follows by ($\exists$-I), ($=$-I), and ($\wedge$-I) that

$$G(\mathbf{x}, \mathbf{v}) \vdash (\exists \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge I_F(\mathbf{p}, \mathbf{v})).$$

Hence, (3.1.23) holds in $\mathbb{T}$.

By ($=$-E) and ($\exists$-E), we obtain

$$(\exists \mathbf{p})(I_F(\mathbf{y}, \mathbf{p}) \wedge (C(\mathbf{p}) \wedge \mathbf{p} = \mathbf{v})) \vdash I_F(\mathbf{y}, \mathbf{v}).$$

By defining condition (1) for $\ulcorner I_F \urcorner : \mathrm{Im}_F \to C$, ($=$-I), and ($\wedge$-I), we obtain

$$I_F(\mathbf{y}, \mathbf{v}) \vdash I_F(\mathbf{y}, \mathbf{v}) \wedge (C(\mathbf{v}) \wedge \mathbf{v} = \mathbf{v}),$$

from which

$$I_F(\mathbf{y}, \mathbf{v}) \vdash (\exists \mathbf{p})(I_F(\mathbf{y}, \mathbf{p}) \wedge (C(\mathbf{p}) \wedge \mathbf{p} = \mathbf{v}))$$

follows by ($\exists$-I). Hence, (3.1.24) holds in $\mathbb{T}$.

Therefore, diagram (3.1.22) commutes in $\mathscr{C}(\mathbb{T})$. It follows in particular that the diagram

$$\begin{array}{ccc} \mathrm{Im}_F(\mathbf{y}) & \xrightarrow{\ulcorner I_F(\mathbf{y},\mathbf{v}) \urcorner} & B(\mathbf{y}) \\ {\scriptstyle \ulcorner I_F(\mathbf{y},\mathbf{v}) \urcorner} \downarrow & \nearrow {\scriptstyle \ulcorner C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \urcorner} & \\ C(\mathbf{y}) & & \end{array}$$

commutes in $\mathscr{C}(\mathbb{T})$. As noted in Remark 3.1.1.14, it thus follows that $\mathrm{Im}_F(\mathbf{y}) \leq C(\mathbf{y})$ as subobjects of $B(\mathbf{y})$.

Therefore, $\mathrm{Im}_F(\mathbf{y})$, together with the associated monomorphism $\ulcorner I_F(\mathbf{y}, \mathbf{v}) \urcorner : \mathrm{Im}_F(\mathbf{y}) \to B(\mathbf{y})$, is the smallest subobject of $B(\mathbf{y})$ through which $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ factors, and hence is the image of $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$.

(iii) We now show that images in $\mathscr{C}(\mathbb{T})$ are stable under pullback. Let $\ulcorner F(\mathbf{x},\mathbf{w})\urcorner : A(\mathbf{x}) \to C(\mathbf{z})$ and $\ulcorner G(\mathbf{y},\mathbf{w})\urcorner : B(\mathbf{y}) \to C(\mathbf{z})$ be morphisms in $\mathbb{T}$ and consider their pullback

$$\begin{array}{ccc} A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}) & \xrightarrow{\ulcorner P_B(\mathbf{x},\mathbf{y},\mathbf{v})\urcorner} & B(\mathbf{y}) \\ {\scriptstyle \ulcorner P_A(\mathbf{x},\mathbf{y},\mathbf{u})\urcorner}\downarrow & & \downarrow{\scriptstyle \ulcorner G(\mathbf{y},\mathbf{w})\urcorner} \\ A(\mathbf{x}) & \xrightarrow[\ulcorner F(\mathbf{x},\mathbf{w})\urcorner]{} & C(\mathbf{z}) \end{array} . \tag{3.1.25}$$

By Remark 3.1.1.8 and the discussion following Proposition 3.1.1.15, we can assume without loss of generality that the lists $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ are pairwise disjoint. Let $\mathrm{Im}_G(\mathbf{z})$, with associated morphism $\ulcorner I_G(\mathbf{z},\mathbf{w})\urcorner : \mathrm{Im}_G(\mathbf{z}) \to C(\mathbf{z})$, be the image in $\mathscr{C}(\mathbb{T})$ of $\ulcorner G(\mathbf{y},\mathbf{w})\urcorner : B(\mathbf{y}) \to C(\mathbf{z})$ in $\mathscr{C}(\mathbb{T})$ and let $\mathrm{Im}_{P_A}(\mathbf{x})$, with associated morphism $\ulcorner I_{P_A}(\mathbf{x},\mathbf{u})\urcorner : \mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x})$, be the image in $\mathscr{C}(\mathbb{T})$ of $\ulcorner P_A(\mathbf{x},\mathbf{y},\mathbf{u})\urcorner : A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}) \to A(\mathbf{x})$, as defined in the proof of part (ii) above. We claim that $\ulcorner \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})\urcorner$ is a morphism from $\mathrm{Im}_{P_A}(\mathbf{x})$ to $\mathrm{Im}_G(\mathbf{z})$ in $\mathscr{C}(\mathbb{T})$ and that the diagram

$$\begin{array}{ccc} \mathrm{Im}_{P_A}(\mathbf{x}) & \xrightarrow{\ulcorner \mathrm{Im}_{P_A}(\mathbf{x})\wedge F(\mathbf{x},\mathbf{w})\urcorner} & \mathrm{Im}_G(\mathbf{z}) \\ {\scriptstyle \ulcorner I_{P_A}(\mathbf{x},\mathbf{u})\urcorner}\downarrow & & \downarrow{\scriptstyle \ulcorner I_G(\mathbf{z},\mathbf{w})\urcorner} \\ A(\mathbf{x}) & \xrightarrow[\ulcorner F(\mathbf{x},\mathbf{w})\urcorner]{} & C(\mathbf{z}) \end{array} \tag{3.1.26}$$

commutes in $\mathscr{C}(\mathbb{T})$. Recall from Proposition 3.1.1.15 and the proof of part (ii) above that

$$A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge B(\mathbf{y}) \wedge (\forall \mathbf{w})(F(\mathbf{x},\mathbf{w}) \Leftrightarrow G(\mathbf{y},\mathbf{w})),$$

$$P_A(\mathbf{x},\mathbf{y},\mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{y}) \wedge \mathbf{x} = \mathbf{u},$$

and

$$\mathrm{Im}_{P_A}(\mathbf{x}) \underset{\text{def}}{\equiv} (\exists \mathbf{q},\mathbf{p})(A(\mathbf{q})\underset{F,G}{\times}B(\mathbf{p}) \wedge \mathbf{q} = \mathbf{x}).$$

It thus follows by the rules for $\exists$ and equality that

$$\vdash \mathrm{Im}_{P_A}(\mathbf{x}) \Leftrightarrow (\exists \mathbf{p})(A(\mathbf{x})\underset{F,G}{\times}B(\mathbf{p})). \tag{3.1.27}$$

We now show that $\mathrm{Im}_{P_A} \wedge F$ satisfies defining conditions (1)–(3) for a morphism from Im_{P_A} to Im_G.

(1) We obtain $\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \vdash \mathrm{Im}_{P_A}(\mathbf{x})$ by ($\wedge$-E). By (3.1.27), it follows that

$$\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \vdash (\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p})).$$

We obtain

$$\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}), A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{b}) \vdash^{\mathbf{b}} G(\mathbf{b},\mathbf{w})$$

by ($\forall$-E), ($\wedge$-E), and ($\Rightarrow$-E), and so

$$\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \vdash (\exists \mathbf{p}) G(\mathbf{p},\mathbf{w})$$

follows by ($\exists$-I) and ($\exists$-E). Hence, we obtain

$$\vdash \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \Rightarrow \mathrm{Im}_{P_A}(\mathbf{x}) \wedge \mathrm{Im}_G(\mathbf{w})$$

by ($\wedge$-I) and ($\Rightarrow$-I), and so defining condition (1) is satisfied.

(2) By (3.1.27), we obtain $\mathrm{Im}_{P_A}(\mathbf{x}) \vdash (\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p}))$. Furthermore, we obtain

$$\mathrm{Im}_{P_A}(\mathbf{x}), A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{b}) \vdash^{\mathbf{b}} A(\mathbf{x})$$

by ($\wedge$-E), from which

$$\mathrm{Im}_{P_A}(\mathbf{x}) \vdash (\exists \mathbf{w}) F(\mathbf{x},\mathbf{w})$$

follows by defining condition (2) for F and ($\exists$-E). We then obtain

$$\mathrm{Im}_{P_A}(\mathbf{x}) \vdash (\exists \mathbf{w})(\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}))$$

by the rules for $\exists$ and ($\wedge$-I). Thus, defining condition (2) is satisfied.

(3) Defining condition (3) for $\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})$ follows from defining condition (3) for $F(\mathbf{x},\mathbf{w})$.

Hence, $\ulcorner \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \urcorner$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $\mathrm{Im}_{P_A}(\mathbf{x})$ to $\mathrm{Im}_G(\mathbf{z})$. We now show that diagram (3.1.26) commutes in $\mathscr{C}(\mathbb{T})$, that is, we show that

$$\vdash I_{P_A}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{w}) \Leftrightarrow (\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})); I_G(\mathbf{z},\mathbf{w}). \tag{3.1.28}$$

First note that by definition of I_{P_A}, we have

$$I_{P_A}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{w}) \underset{\text{def}}{\equiv} (\exists \mathbf{q})((\mathrm{Im}_{P_A}(\mathbf{x}) \wedge \mathbf{x} = \mathbf{q}) \wedge F(\mathbf{q},\mathbf{w})),$$

from which it follows that

$$\vdash I_{P_A}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{w}) \Leftrightarrow \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \tag{3.1.29}$$

by the rules for $\exists$ and equality. By definition of I_G, we have

$$(\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})); I_G(\mathbf{z},\mathbf{w}) \underset{\text{def}}{\equiv} (\exists \mathbf{r})[(\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{r})) \wedge (\mathrm{Im}_G(\mathbf{r}) \wedge \mathbf{r} = \mathbf{w})],$$

from which it follows that

$$\vdash (\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})); I_G(\mathbf{z},\mathbf{w}) \Leftrightarrow \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \wedge \mathrm{Im}_G(\mathbf{w}).$$

By the rules for $\wedge$ and defining condition (1) for $\lceil \mathrm{Im}_{P_A} \wedge F \rceil : \mathrm{Im}_{P_A} \to \mathrm{Im}_G$, we obtain

$$\vdash \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}) \wedge \mathrm{Im}_G(\mathbf{w}) \Leftrightarrow \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}).$$

Hence, it follows that

$$\vdash (\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w})); I_G(\mathbf{z},\mathbf{w}) \Leftrightarrow \mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x},\mathbf{w}). \tag{3.1.30}$$

We then obtain (3.1.28) from (3.1.29) and (3.1.30), and so diagram (3.1.26) commutes in $\mathscr{C}(\mathbb{T})$.

Now consider the pullback of $\lceil F(\mathbf{x},\mathbf{w}) \rceil : A(\mathbf{x}) \to C(\mathbf{z})$ and $\lceil I_G(\mathbf{z},\mathbf{w}) \rceil : \mathrm{Im}_G(\mathbf{z}) \to C(\mathbf{w})$ in $\mathscr{C}(\mathbb{T})$. Since the lists $\mathbf{x}$ and $\mathbf{z}$ are disjoint, by the proof of Proposition 3.1.1.15 (iii), this pullback is given by

$$\begin{array}{ccc} A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) & \xrightarrow{\lceil Q_{\mathrm{Im}_G}(\mathbf{x},\mathbf{z},\mathbf{w}) \rceil} & \mathrm{Im}_G(\mathbf{z}) \\ {\scriptstyle \lceil Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \rceil}\downarrow & & \downarrow{\scriptstyle \lceil I_G(\mathbf{z},\mathbf{w}) \rceil} \\ A(\mathbf{x}) & \xrightarrow[\lceil F(\mathbf{x},\mathbf{w}) \rceil]{} & C(\mathbf{z}) \end{array}, \tag{3.1.31}$$

where

$$A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge \mathrm{Im}_G(\mathbf{z}) \wedge (\forall \mathbf{w})(F(\mathbf{x},\mathbf{w}) \Leftrightarrow I_G(\mathbf{z},\mathbf{w})),$$

$$Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \wedge \mathbf{x} = \mathbf{u},$$

and

$$Q_{\mathrm{Im}_G}(\mathbf{x},\mathbf{z},\mathbf{w}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \wedge \mathbf{z} = \mathbf{w}.$$

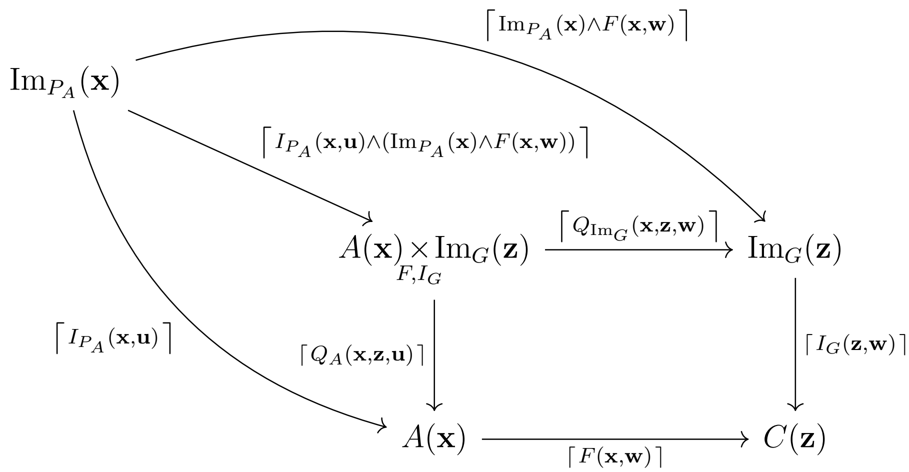
We claim that $\lceil Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \rceil : A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \to A(\mathbf{x})$ and $\lceil I_{P_A}(\mathbf{x},\mathbf{u}) \rceil : \mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x})$ are equivalent as monomorphisms into $A(\mathbf{x})$ (see Definition 3.1.1.10). Since pullbacks are defined up to isomorphism, it will then follow that $\lceil I_{P_A}(\mathbf{x},\mathbf{u}) \rceil$:

$\mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x})$ is indeed the pullback of $\ulcorner I_G(\mathbf{z}, \mathbf{w}) \urcorner$ along $\ulcorner F(\mathbf{x}, \mathbf{w}) \urcorner$ in $\mathscr{C}(\mathbb{T})$ and that diagram (3.1.26) is a pullback square.

Since diagram (3.1.31) is a pullback diagram and diagram (3.1.26) commutes, it follows from the proof of Proposition 3.1.1.15 (iii) that the morphism

$$\begin{aligned}&\ulcorner \langle I_{P_A}(\mathbf{x}, \mathbf{u}), (\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x}, \mathbf{w}))\rangle_{F, I_G} \urcorner \\ &\qquad = \ulcorner I_{P_A}(\mathbf{x}, \mathbf{u}) \wedge (\mathrm{Im}_{P_A}(\mathbf{x}) \wedge F(\mathbf{x}, \mathbf{w})) \urcorner : \mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x}) \underset{F, I_G}{\times} \mathrm{Im}_G(\mathbf{z})\end{aligned}$$

is the unique morphism in $\mathscr{C}(\mathbb{T})$ such that the diagram



(3.1.32)

commutes in $\mathscr{C}(\mathbb{T})$. Thus, $\ulcorner I_{P_A} \wedge (\mathrm{Im}_{P_A} \wedge F) \urcorner$ is such that $\ulcorner (I_{P_A} \wedge (\mathrm{Im}_{P_A} \wedge F)); Q_A \urcorner = \ulcorner I_{P_A} \urcorner$. It remains to find a morphism $\ulcorner J(\mathbf{x}, \mathbf{z}, \mathbf{u}) \urcorner : A(\mathbf{x}) \underset{F, I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \to \mathrm{Im}_{P_A}(\mathbf{x})$ such that $\ulcorner J; I_{P_A} \urcorner = \ulcorner Q_A \urcorner$. Let

$$J(\mathbf{x}, \mathbf{z}, \mathbf{u}) \underset{\text{def}}{\equiv} Q_A(\mathbf{x}, \mathbf{z}, \mathbf{u}).$$

We first show that $J(\mathbf{x}, \mathbf{z}, \mathbf{u}) \underset{\text{def}}{\equiv} Q_A(\mathbf{x}, \mathbf{z}, \mathbf{u})$ satisfies defining conditions (1)–(3) for a morphism from $A(\mathbf{x}) \underset{F, I_G}{\times} \mathrm{Im}_G(\mathbf{z})$ to $\mathrm{Im}_{P_A}(\mathbf{x})$ in $\mathscr{C}(\mathbb{T})$. Note that defining conditions (2) and (3) for Q_A as a morphism from $A \underset{F, I_G}{\times} \mathrm{Im}_G$ to Im_{P_A} are the same as defining condition (2) and (3), respectively, for Q_A as a morphism from $A \underset{F, I_G}{\times} \mathrm{Im}_G$ to A, and hence are satisfied. It remains to consider defining condition (1). By ($\wedge$-E), we obtain

$$Q_A(\mathbf{x}, \mathbf{z}, \mathbf{u}) \vdash A(\mathbf{x}) \underset{F, I_G}{\times} \mathrm{Im}_G(\mathbf{z}). \tag{3.1.33}$$

It remains to show that $Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \vdash \mathrm{Im}_{P_A}(\mathbf{u})$. By (3.1.27), it suffices to show that

$$Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \vdash (\exists \mathbf{p})(A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{p})).$$

We first show that

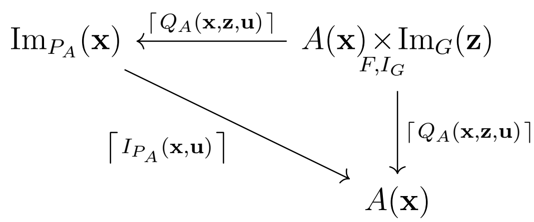
$$A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \vdash (\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p})) \tag{3.1.34}$$

via the following derivation in $\mathbb{T}$.

1	$A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z})$	
2	$A(\mathbf{x})$	($\wedge$-E), 1
3	$(\exists \mathbf{p})G(\mathbf{p},\mathbf{z})$	($\wedge$-E), Def. of Im_G, 1
4	$(\forall \mathbf{w})(F(\mathbf{x},\mathbf{w}) \Leftrightarrow (\mathrm{Im}_G(\mathbf{z}) \wedge \mathbf{z}=\mathbf{w}))$	($\wedge$-E), Def. of I_G, 1
5	$\mathbf{b}$ $G(\mathbf{b},\mathbf{z})$	
6	$B(\mathbf{b})$	Defining condition (1) for G, 5
7	$F(\mathbf{x},\mathbf{w})$	
8	$\mathrm{Im}_G(\mathbf{z}) \wedge \mathbf{z}=\mathbf{w}$	($\forall$-E), ($\Rightarrow$-E), 4, 7
9	$G(\mathbf{b},\mathbf{w})$	(=-E), 5, 8
10	$F(\mathbf{x},\mathbf{w}) \Rightarrow G(\mathbf{b},\mathbf{w})$	($\Rightarrow$-I), 7–9
11	$G(\mathbf{b},\mathbf{w})$	
12	$\mathbf{z}=\mathbf{w}$	Defining condition (3) for G, 5, 11
13	$\mathrm{Im}_G(\mathbf{z}) \wedge \mathbf{z}=\mathbf{w}$	($\exists$-I), ($\wedge$-I), 5, 12
14	$F(\mathbf{x},\mathbf{w})$	($\forall$-E), ($\Rightarrow$-E), 4, 13
15	$G(\mathbf{b},\mathbf{w}) \Rightarrow F(\mathbf{x},\mathbf{w})$	($\Rightarrow$-I), 11–14
16	$A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{b})$	($\wedge$-I), ($\forall$-I), 2, 6, 10, 15
17	$(\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p}))$	($\exists$-I), 16
18	$(\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p}))$	($\exists$-E), 3, 5–17

Therefore, by (3.1.33), we obtain $Q_A(\mathbf{x},\mathbf{y},\mathbf{u}) \vdash (\exists \mathbf{p})(A(\mathbf{x}) \underset{F,G}{\times} B(\mathbf{p}))$, from which it follows by the definition of Q_A and (=-E) that $Q_A(\mathbf{x},\mathbf{y},\mathbf{u}) \vdash (\exists \mathbf{p})(A(\mathbf{u}) \underset{F,G}{\times} B(\mathbf{p}))$. Defining condition (1) then follows by (3.1.27), ($\wedge$-I) and ($\Rightarrow$-I).

Therefore, $\ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \urcorner : A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \to \mathrm{Im}_{P_A}(\mathbf{x})$ is a morphism in $\mathscr{C}(\mathbb{T})$. We now show that $\ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}); I_{P_A}(\mathbf{x},\mathbf{u}) \urcorner = \ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \urcorner$, that is, that the diagram



commutes in $\mathscr{C}(\mathbb{T})$. By ($\wedge$-E) and (=-E), we obtain

$$\vdash (\exists \mathbf{q})(Q_A(\mathbf{x},\mathbf{z},\mathbf{q}) \wedge I_{P_A}(\mathbf{q},\mathbf{u})) \Rightarrow Q_A(\mathbf{x},\mathbf{z},\mathbf{u}).$$

Conversely, we have

$$Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \vdash Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \wedge (\mathrm{Im}_{P_A}(\mathbf{u}) \wedge \mathbf{u} = \mathbf{u})$$

by defining condition (1) for Q_A as a morphism from $A \underset{F,I_G}{\times} \mathrm{Im}_G$ to Im_{P_A}, (=-I), and ($\wedge$-I). We thus obtain

$$\vdash Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \Rightarrow (\exists \mathbf{q})(Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \wedge I_{P_A}(\mathbf{x},\mathbf{u}))$$

by ($\exists$-I), ($\Rightarrow$-I), and the definition of I_{P_A}. Hence, $\ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}); I_{P_A}(\mathbf{x},\mathbf{u}) \urcorner = \ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \urcorner$, and so in fact $\ulcorner Q_A(\mathbf{x},\mathbf{z},\mathbf{u}) \urcorner : A(\mathbf{x}) \underset{F,I_G}{\times} \mathrm{Im}_G(\mathbf{z}) \to A(\mathbf{x})$ and $\ulcorner I_{P_A}(\mathbf{x},\mathbf{u}) \urcorner : \mathrm{Im}_{P_A}(\mathbf{x}) \to A(\mathbf{x})$ are equivalent as monomorphisms into $A(\mathbf{x})$. Therefore, as noted above, $\ulcorner I_{P_A}(\mathbf{x},\mathbf{u}) \urcorner$ is indeed (up to isomorphism) the pullback of $\ulcorner I_G(\mathbf{z},\mathbf{w}) \urcorner$ along $\ulcorner F(\mathbf{x},\mathbf{w}) \urcorner$ and diagram (3.1.26) is a pullback square. Hence, images in $\mathscr{C}(\mathbb{T})$ are stable under pullback.

Consequently, $\mathscr{C}(\mathbb{T})$ is a regular category. ∎

Let $\mathbb{T}$ be a theory and let $\ulcorner F(\mathbf{x},\mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism in $\mathscr{C}(\mathbb{T})$. Note that, by the proof of Proposition 3.1.1.13, if $\ulcorner F \urcorner$ is a monomorphism in $\mathscr{C}(\mathbb{T})$, $A(\mathbf{x})$ is isomorphic in $\mathscr{C}(\mathbb{T})$ to the image $\mathrm{Im}_F(\mathbf{y})$ of $\ulcorner F \urcorner : A \to B$ via the isomorphism $\ulcorner F(\mathbf{x},\mathbf{v}) \urcorner : A(\mathbf{x}) \to \mathrm{Im}_F(\mathbf{y})$.

3.1.2 Syntactic partial map categories

Since we wish to consider results from recursion theory and eventually Turing categories in the context of syntactic categories, we need syntactic categories of arithmetical theories that have a notion of partial morphism. Hence, we define the syntactic partial map category associated to a theory and ensure that it is a restriction category.

3.1.2.1 Definition and basic results

Definition 3.1.2.1 Let $\mathbb{T}$ be a theory. We define the *syntactic partial map category* $\mathscr{P}(\mathbb{T})$ of $\mathbb{T}$ in the same way that we defined the syntactic category $\mathscr{C}(\mathbb{T})$ in Definition 3.1.1.2, except that we omit defining condition (2) for the morphisms. □

Lemma 3.1.2.2 *Let $\mathbb{T}$ be a theory. Then, $\mathscr{P}(\mathbb{T})$ is a category.*

Proof The same argument as in Proposition 3.1.1.5, omitting the part concerning defining condition (2), shows that composition in $\mathscr{P}(\mathbb{T})$ is well-defined. Moreover, since defining condition (2) is not used in order to show that $\mathscr{C}(\mathbb{T})$ is a category in the proof of Proposition 3.1.1.5, it follows that the same argument can be used to show that $\mathscr{P}(\mathbb{T})$ is a category. In particular, the characterisation of composition of any finite number of morphisms in $\mathscr{C}(\mathbb{T})$ is also valid in $\mathscr{P}(\mathbb{T})$. ■

Note that the objects of $\mathscr{P}(\mathbb{T})$ are exactly the objects of $\mathscr{C}(\mathbb{T})$ and that all morphisms of $\mathscr{C}(\mathbb{T})$ are morphisms of $\mathscr{P}(\mathbb{T})$. In particular, $\mathscr{C}(\mathbb{T})$ is a subcategory of $\mathscr{P}(\mathbb{T})$.

Note also that we may refer to the syntactic categories defined in Definition 3.1.1.2 as *syntactic total map categories* in order to better distinguish them from syntactic partial map categories if ambiguity may arise.

We wish to show that the syntactic partial map category $\mathscr{P}(\mathbb{T})$ of any theory $\mathbb{T}$ is a restriction category. For a presentation of restriction categories, see for example [4, 5]. A brief discussion is also included in Appendix B.

In order to show that $\mathscr{P}(\mathbb{T})$ is a restriction category, we must give a restriction combinator on $\mathscr{P}(\mathbb{T})$ sending each morphism $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ to its restriction

$$\overline{\lceil F(\mathbf{x},\mathbf{v})\rceil} := \lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil : A(\mathbf{x}) \to A(\mathbf{x}),$$

such that the following four conditions are satisfied:

(R1) $\lceil \overline{F}; F\rceil = \lceil F\rceil$;

(R2) $\lceil \overline{G}; \overline{F}\rceil = \lceil \overline{F}; \overline{G}\rceil$ whenever $\mathrm{dom}\,\lceil F\rceil = \mathrm{dom}\,\lceil G\rceil$;

(R3) $\left\lceil \overline{\overline{F}; G}\right\rceil = \lceil \overline{F}; \overline{G}\rceil$ whenever $\mathrm{dom}\,\lceil F\rceil = \mathrm{dom}\,\lceil G\rceil$;

(R4) $\lceil F; \overline{G}\rceil = \lceil \overline{F; G}; F\rceil$ whenever $\mathrm{cod}\,\lceil F\rceil = \mathrm{dom}\,\lceil G\rceil$.

Proposition 3.1.2.3 *Let $\mathscr{P}(\mathbb{T})$ be the syntactic partial map category of a theory $\mathbb{T}$. The combinator $\mathcal{R} = \overline{(\cdot)}$ associating to each morphism $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ of $\mathscr{P}(\mathbb{T})$ the morphism $\overline{\lceil F(\mathbf{x},\mathbf{v})\rceil} = \lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil : A(\mathbf{x}) \to A(\mathbf{x})$, where we define*

$$\overline{F}(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{q}) F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x} = \mathbf{u},$$

is a well-defined restriction combinator on $\mathscr{P}(\mathbb{T})$*. Note that if the list* $\mathbf{y}$ *is empty (i.e. if* B *has no free variables), we define* $\overline{F}(\mathbf{x},\mathbf{u})$ *to be the formula* $F(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$*, and if the list* $\mathbf{x}$ *is empty (i.e. if* A *has no free variables), we define* $\overline{F}$ *to be the formula* $(\exists \mathbf{q})F(\mathbf{q})$*.*

Proof We must show that (i) for each morphism $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{v})$ in $\mathscr{P}(\mathbb{T})$, $\lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil : A(\mathbf{x}) \to A(\mathbf{x})$ is a morphism in $\mathscr{P}(\mathbb{T})$, (ii) $\mathcal{R}$ is well-defined, and (iii) conditions (R1)–(R4) are satisfied.

(i) Let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be any morphism in $\mathscr{P}(\mathbb{T})$. Defining condition (1) for $\overline{F}(\mathbf{x},\mathbf{u})$ follows from defining condition (1) for F and (=-E), and defining condition (3) for $\overline{F}$ follows from (=-E). Hence, $\lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil$ is indeed a morphism on $A(\mathbf{x})$ in $\mathscr{P}(\mathbb{T})$.

(ii) Let $\lceil F(\mathbf{x},\mathbf{v})\rceil, \lceil G(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be two morphisms in $\mathscr{P}(\mathbb{T})$, and suppose that $\lceil F(\mathbf{x},\mathbf{v})\rceil = \lceil G(\mathbf{x},\mathbf{v})\rceil$. By the Equivalence Theorem and the rules for $\exists$, it follows that

$$\vdash (\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x} = \mathbf{u} \Leftrightarrow (\exists \mathbf{q})G(\mathbf{x},\mathbf{q}) \wedge \mathbf{x} = \mathbf{u},$$

and so $\lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil = \lceil \overline{G}(\mathbf{x},\mathbf{u})\rceil$. Hence, $\mathcal{R}$ is well-defined.

(iii) We show that conditions (R1)–(R4) are satisfied.

(R1) Let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be any morphism in $\mathscr{P}(\mathbb{T})$. We have

$$\overline{F}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{v}) \underset{\text{def}}{\equiv} (\exists \mathbf{p})(((\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x} = \mathbf{p}) \wedge F(\mathbf{p},\mathbf{v}))$$

by definition. Consequently, it follows by the rules for equality and $\exists$ in $\mathbb{T}$ that

$$\vdash \overline{F}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{v}) \Leftrightarrow F(\mathbf{x},\mathbf{v}).$$

Hence, we have

$$\lceil \overline{F}(\mathbf{x},\mathbf{u}); F(\mathbf{x},\mathbf{v})\rceil = \lceil F(\mathbf{x},\mathbf{v})\rceil,$$

and so condition (R1) holds.

(R2) Let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ and $\lceil G(\mathbf{x},\mathbf{w})\rceil : A(\mathbf{x}) \to C(\mathbf{z})$ be any two morphisms in $\mathscr{C}(\mathbb{T})$ with the same domain. We have

$$\overline{G}(\mathbf{x},\mathbf{u}); \overline{F}(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{p})(((\exists \mathbf{r})G(\mathbf{x},\mathbf{r}) \wedge \mathbf{x} = \mathbf{p}) \wedge ((\exists \mathbf{q})F(\mathbf{p},\mathbf{q}) \wedge \mathbf{p} = \mathbf{u}))$$

and similarly for $\overline{F}(\mathbf{x},\mathbf{u}); \overline{G}(\mathbf{x},\mathbf{u})$. We obtain

$$((\exists \mathbf{r})G(\mathbf{x},\mathbf{r}) \wedge \mathbf{x} = \mathbf{a}) \wedge ((\exists \mathbf{q})F(\mathbf{a},\mathbf{q}) \wedge \mathbf{a} = \mathbf{u}) \overset{\mathbf{a}}{\vdash} ((\exists \mathbf{q})F(\mathbf{a},\mathbf{q}) \wedge \mathbf{x} = \mathbf{a}) \wedge ((\exists \mathbf{r})G(\mathbf{x},\mathbf{r}) \wedge \mathbf{a} = \mathbf{u})$$

by the properties of conjunction in $\mathbb{T}$. It then follows by (=-E) and (∃-I) that

$$((\exists \mathbf{r})G(\mathbf{x},\mathbf{r})\wedge \mathbf{x}=\mathbf{a})\wedge((\exists \mathbf{q})F(\mathbf{a},\mathbf{q})\wedge \mathbf{a}=\mathbf{u}) \vdash^{\mathbf{a}} (\exists \mathbf{p})(((\exists \mathbf{q})F(\mathbf{x},\mathbf{q})\wedge \mathbf{x}=\mathbf{p})\wedge((\exists \mathbf{r})G(\mathbf{p},\mathbf{r})\wedge \mathbf{p}=\mathbf{u})).$$

By (∃-E) and (⇒-I), we then obtain

$$\vdash \overline{G}(\mathbf{x},\mathbf{u});\overline{F}(\mathbf{x},\mathbf{u}) \Rightarrow \overline{F}(\mathbf{x},\mathbf{u});\overline{G}(\mathbf{x},\mathbf{u}).$$

The converse implication is obtained in an analogous manner, and so

$$\lceil \overline{G}(\mathbf{x},\mathbf{u});\overline{F}(\mathbf{x},\mathbf{u}) \rceil = \lceil \overline{F}(\mathbf{x},\mathbf{u});\overline{G}(\mathbf{x},\mathbf{u}) \rceil .$$

Hence, condition (R2) holds.

(R3) Let $\lceil F(\mathbf{x},\mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ and $\lceil G(\mathbf{x},\mathbf{w}) \rceil : A(\mathbf{x}) \to C(\mathbf{z})$ be any two morphisms in $\mathscr{C}(\mathbb{T})$ with the same domain. By the rules for ∃ and for equality, similarly to the argument for condition (R2) above, it follows that

$$\begin{aligned}\vdash (\exists \mathbf{r})(\exists \mathbf{p})(((\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x}=\mathbf{p}) \wedge G(\mathbf{p},\mathbf{r})) \wedge \mathbf{x}=\mathbf{u}\\ \Leftrightarrow (\exists \mathbf{p})(((\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x}=\mathbf{p}) \wedge ((\exists \mathbf{r})G(\mathbf{p},\mathbf{r}) \wedge \mathbf{p}=\mathbf{u})),\end{aligned}$$

which is to say

$$\vdash \overline{\overline{F};G} \Leftrightarrow \overline{F};\overline{G}.$$

Hence, $\left\lceil \overline{\overline{F};G} \right\rceil = \lceil \overline{F};\overline{G} \rceil$, and so condition (R3) holds.

(R4) Let $\lceil F(\mathbf{x},\mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ and $\lceil G(\mathbf{y},\mathbf{w}) \rceil : B(\mathbf{y}) \to C(\mathbf{z})$ be any two morphisms in $\mathscr{C}(\mathbb{T})$ such that the codomain of $\lceil F \rceil$ is the domain of $\lceil G \rceil$. A straightforward argument using the rules for ∃ and equality shows that

$$\begin{aligned}\vdash (\exists \mathbf{p})(F(\mathbf{x},\mathbf{p}) \wedge ((\exists \mathbf{q})G(\mathbf{p},\mathbf{q}) \wedge \mathbf{p}=\mathbf{v}))\\ \Rightarrow (\exists \mathbf{r})(((\exists \mathbf{q})(\exists \mathbf{p})(F(\mathbf{x},\mathbf{p}) \wedge G(\mathbf{p},\mathbf{q})) \wedge \mathbf{x}=\mathbf{r}) \wedge F(\mathbf{r},\mathbf{v})),\end{aligned}$$

which is to say

$$\vdash F;\overline{G} \Rightarrow \overline{F;G};F.$$

In order to prove the converse implication in $\mathbb{T}$, we use the rules for ∃ and equality, as well as defining condition (3) for F in order to derive the $\mathbf{p}=\mathbf{v}$ subterm in the formula $F;\overline{G}$ from the formula $\overline{F;G};F$. Hence, we obtain $\lceil F;\overline{G} \rceil = \lceil \overline{F;G};F \rceil$, and so condition (R4) holds.

Therefore, $\mathcal{R}$ is indeed a well-defined restriction combinator on $\mathscr{P}(\mathbb{T})$, and so $\mathscr{P}(\mathbb{T})$ endowed with $\mathcal{R}$ is a restriction category. ∎

Proposition 3.1.2.4 *For any theory $\mathbb{T}$, $\mathscr{C}(\mathbb{T})$ is the subcategory of $\mathscr{P}(\mathbb{T})$ consisting of all the $\mathcal{R}$-total maps and is a restriction category when endowed with the restriction of $\mathcal{R}$ to $\mathscr{C}(\mathbb{T})$.*

Proof Let $\mathbb{T}$ be a theory. Since the objects of $\mathscr{C}(\mathbb{T})$ and $\mathscr{P}(\mathbb{T})$ are the same and all morphisms of $\mathscr{C}(\mathbb{T})$ are by definition morphisms of $\mathscr{P}(\mathbb{T})$, $\mathscr{C}(\mathbb{T})$ is a subcategory of $\mathscr{P}(\mathbb{T})$.

It remains to show that a morphism of $\mathscr{P}(\mathbb{T})$ is $\mathcal{R}$-total if and only if it is a morphism of $\mathscr{C}(\mathbb{T})$. Let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism of $\mathscr{P}(\mathbb{T})$. Suppose first that $\lceil F\rceil$ is in fact a morphism of $\mathscr{C}(\mathbb{T})$, that is, suppose that $\lceil F\rceil$ satisfies defining condition (2). Recall that

$$\overline{F}(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x} = \mathbf{u}$$

and that

$$\mathrm{id}_A(\mathbf{x},\mathbf{u}) \underset{\text{def}}{\equiv} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}.$$

We show that $\lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil = \lceil \mathrm{id}_A(\mathbf{x},\mathbf{u})\rceil$. We obtain

$$\overline{F}(\mathbf{x},\mathbf{u}), F(\mathbf{x},\mathbf{b}) \vdash^{\mathbf{b}} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$$

by defining condition (1) for $\lceil F\rceil$ and the rules for conjunction, from which it follows that

$$\overline{F}(\mathbf{x},\mathbf{u}) \vdash \mathrm{id}_A(\mathbf{x},\mathbf{u})$$

by ($\exists$-E). Furthermore,

$$A(\mathbf{x}) \vdash (\exists \mathbf{q})F(\mathbf{x},\mathbf{q})$$

by defining condition (2) for $\lceil F\rceil$, from which it follows that

$$\mathrm{id}_A(\mathbf{x},\mathbf{u}) \vdash \overline{F}(\mathbf{x},\mathbf{u}).$$

Hence, we obtain $\lceil \overline{F}(\mathbf{x},\mathbf{u})\rceil = \lceil \mathrm{id}_A(\mathbf{x},\mathbf{u})\rceil$, and so $\lceil F\rceil$ is $\mathcal{R}$-total.

Now suppose instead that $\lceil F\rceil$ is $\mathcal{R}$-total. Since $\lceil F\rceil$ is a morphism of $\mathscr{P}(\mathbb{T})$, F satisfies defining conditions (1) and (3). It remains to show that F satisfies defining condition (2) in order to show that $\lceil F\rceil$ is in fact a morphism of $\mathscr{C}(\mathbb{T})$. We obtain

$$A(\mathbf{x}) \vdash \mathrm{id}_A(\mathbf{x},\mathbf{x})$$

by (=-I) and ($\wedge$-I). Since $\lceil F\rceil$ is $\mathcal{R}$-total, we have

$$\mathrm{id}_A(\mathbf{x},\mathbf{u}) \vdash \overline{F}(\mathbf{x},\mathbf{u}).$$

We then obtain

$$\mathrm{id}_A(\mathbf{x},\mathbf{x}) \vdash (\exists \mathbf{q})F(\mathbf{x},\mathbf{q}) \wedge \mathbf{x}=\mathbf{x}$$

by the Substitution Theorem and the definition of $\overline{F}$. Hence, by ($\wedge$-E) and (Cut), we obtain

$$A(\mathbf{x}) \vdash (\exists \mathbf{q})F(\mathbf{x},\mathbf{q}),$$

and so F satisfies defining condition (2). Hence, $\lceil F \rceil$ is a morphism of $\mathscr{C}(\mathbb{T})$.

Therefore, $\mathscr{C}(\mathbb{T})$ is indeed the subcategory of $\mathscr{P}(\mathbb{T})$ consisting of all $\mathcal{R}$-total morphisms.

Furthermore, since applying $\mathcal{R}$ to a morphism in $\mathscr{C}(\mathbb{T})$ yields an identity morphism, and so a morphism of $\mathscr{C}(\mathbb{T})$, the restriction of $\mathcal{R}$ to $\mathscr{C}(\mathbb{T})$ is indeed a combinator on $\mathscr{C}(\mathbb{T})$ and conditions (R1)–(R4) still hold. Hence, the restriction of $\mathcal{R}$ to $\mathscr{C}(\mathbb{T})$ is indeed a well-defined restriction combinator on $\mathscr{C}(\mathbb{T})$, and so $\mathscr{C}(\mathbb{T})$ is a restriction category (albeit one with only total maps). ■

The next result follows immediately from the proof of Proposition 3.1.2.4.

Corollary 3.1.2.5 *Let $\mathbb{T}$ be a theory and let $\lceil F \rceil : A \to B$ be a morphism in $\mathscr{P}(\mathbb{T})$. Then, $\lceil F \rceil$ is $\mathcal{R}$-total if and only if F satisfies defining condition (2) for a morphism from A to B.*

Let $\mathbb{T}$ be any theory. Proposition 3.1.2.4 in fact shows that $\mathscr{C}(\mathbb{T})$ is precisely the subcategory $\mathbf{Tot}(\mathscr{P}(\mathbb{T}))$ of total morphisms of $\mathscr{P}(\mathbb{T})$, as defined in [3, 5]. We shall henceforth assume that, when considered as restriction categories, both $\mathscr{C}(\mathbb{T})$ and $\mathscr{P}(\mathbb{T})$ are endowed with the restriction combinator $\mathcal{R}$ defined in Proposition 3.1.2.3, although $\mathscr{C}(\mathbb{T})$ is, strictly speaking, endowed with the restriction of $\mathcal{R}$ to $\mathscr{C}(\mathbb{T})$. Since all morphisms of $\mathscr{C}(\mathbb{T})$ are $\mathcal{R}$-total, this restriction combinator on $\mathscr{C}(\mathbb{T})$ in fact corresponds to the *trivial restriction combinator* on $\mathscr{C}(\mathbb{T})$ given by $\lceil \overline{F} \rceil = \lceil \mathrm{id} \rceil$ for all morphisms $\lceil F \rceil$ in $\mathscr{C}(\mathbb{T})$.

Remark 3.1.2.6 As explained in Remark 3.1.1.6, $\mathscr{C}(\mathbb{T})$ is similar to the category **Set**. Similarly, $\mathscr{P}(\mathbb{T})$ is similar to the category **Par** of sets and partial functions, since we can again think of an object $A(\mathbf{x})$ in $\mathscr{P}(\mathbb{T})$ as the set $\{\mathbf{x} \mid \vdash A(\mathbf{x})\}$ and we can think of the $\mathbb{T}$-provably functional representative $F(\mathbf{x},\mathbf{v})$ of a morphism $\lceil F(\mathbf{x},\mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ as the graph of a partial function $f : \{\mathbf{x} \mid \vdash A(\mathbf{x})\} \to \{\mathbf{v} \mid \vdash B(\mathbf{v})\}$. Note that the restriction combinator $\mathcal{R}$ on $\mathscr{P}(\mathbb{T})$ corresponds to the usual restriction combinator on **Par** under this analogy (see [4] for a definition of the restriction combinator on **Par**). □

Since it is the presence of defining condition (2) that causes $\mathscr{C}(\mathbb{T})$ to only have total morphisms when endowed with this restriction combinator, we removed defining condition (2) in order to obtain a more interesting restriction category associated to $\mathbb{T}$, namely $\mathscr{P}(\mathbb{T})$, in which the obvious choice of restriction combinator does not necessarily correspond to the trivial restriction combinator. In particular, when $\mathbb{T}$ is an arithmetical theory, $\mathscr{P}(\mathbb{T})$ has non-total morphisms, as shown in Lemma 3.1.2.7.

Lemma 3.1.2.7 *Let $\mathbb{T}$ be an arithmetical theory. Then, $\mathscr{P}(\mathbb{T})$ has a non-total morphism, and hence the combinator $\mathcal{R}$ on $\mathscr{P}(\mathbb{T})$ is not the trivial restriction combinator.*

Proof Let

$$N(x) \underset{\text{def}}{\equiv} x = x$$

and let

$$F(x, u) \underset{\text{def}}{\equiv} x = 0 \wedge x = u.$$

We claim that $\lceil F(x,u) \rceil$ is a non-total morphism on $N(x)$ in $\mathscr{P}(\mathbb{T})$. We obtain

$$F(x, u) \vdash x = x \wedge u = u$$

by (=-I) and ($\wedge$-I) and we obtain

$$F(x, u) \wedge F(x, v) \vdash u = v$$

by (=-E). Hence, defining conditions (1) and (3) for $F(x, u)$ are satisfied, and so $\lceil F(x,u) \rceil : N(x) \to N(x)$ is a morphism in $\mathscr{P}(\mathbb{T})$.

It remains to show that $\lceil F(x,u) \rceil$ is not $\mathcal{R}$-total. By Corollary 3.1.2.5, it suffices to show that defining condition (2) for $F(x, u)$ as a morphism on $N(x)$ is not satisfied, that is, to show that

$$\nvdash x = x \Rightarrow (\exists u)F(x, u)$$

in $\mathbb{T}$. Since a formula is a theorem of $\mathbb{T}$ if and only if its closure is a theorem of $\mathbb{T}$, it in fact suffices to show that

$$\nvdash (\forall x)(x = x \Rightarrow (\exists u)F(x, u)). \tag{3.1.35}$$

We will show that

$$\vdash \neg(\forall x)(x = x \Rightarrow (\exists u)F(x, u)),$$

from which (3.1.35) will follow as $\mathbb{T}$ is consistent. We have the following derivation in $\mathbb{T}$.

1	$\quad (\forall x)(x = x \Rightarrow (\exists u)F(x,u))$	
2	$\quad \overline{1} = \overline{1} \Rightarrow (\exists u)F(\overline{1},u)$	(∀-E), 1
3	$\quad \overline{1} = \overline{1}$	(=-I)
4	$\quad (\exists u)F(\overline{1},u)$	(⇒-E), 2, 3
5	$\quad a \quad F(\overline{1},a)$	
6	$\quad\quad \overline{1} = 0$	Definition of F, (∧-E), 5
7	$\quad\quad \overline{1} \neq 0$	(M1)
8	$\quad\quad \bot$	(⊥-I), 6, 7
9	$\quad \bot$	(∃-E), 4, 5–8
10	$\neg(\forall x)(x = x \Rightarrow (\exists u)F(x,u))$	(¬-I), 1–9

We thus obtain (3.1.35) by the consistency of $\mathbb{T}$, and hence defining condition (2) for $F(x,u)$ is not satisfied. Hence, $\lceil F(x,u) \rceil : N(x) \to N(x)$ is a non-total morphism of $\mathscr{P}(\mathbb{T})$ by Corollary 3.1.2.5, and so $\lceil \overline{F} \rceil \neq \lceil \mathrm{id}_N \rceil$. Therefore, the combinator $\mathcal{R}$ on $\mathscr{P}(\mathbb{T})$ is not the trivial restriction combinator. ∎

3.1.2.2 Properties of morphisms in syntactic partial map categories

We present here some properties of morphisms and their restrictions in syntactic partial map categories.

Proposition 3.1.2.8 *Let $\mathbb{T}$ be a theory.*

(i) The isomorphisms of $\mathscr{P}(\mathbb{T})$ are precisely the isomorphisms of $\mathscr{C}(\mathbb{T})$.

(ii) The monomorphisms of $\mathscr{P}(\mathbb{T})$ are precisely the monomorphisms of $\mathscr{C}(\mathbb{T})$.

PROOF (i) Let $\lceil F \rceil : A \to B$ be an isomorphism of $\mathscr{P}(\mathbb{T})$. It has an inverse $\lceil G \rceil : B \to A$ in $\mathscr{P}(\mathbb{T})$. Since both $\lceil F \rceil$ and $\lceil G \rceil$ are isomorphisms of $\mathscr{P}(\mathbb{T})$, they are in particular monomorphisms of $\mathscr{P}(\mathbb{T})$, and so are in fact total morphisms by [5, Lemma 2.2]. Hence, $\lceil F \rceil$ and $\lceil G \rceil$ are in fact morphisms of $\mathscr{C}(\mathbb{T})$. Therefore, $\lceil F \rceil$ is a morphism of $\mathscr{C}(\mathbb{T})$ which has an inverse $\lceil G \rceil$ in $\mathscr{C}(\mathbb{T})$, and so $\lceil F \rceil$ is an isomorphism of $\mathscr{C}(\mathbb{T})$.

Now let $\lceil F \rceil : A \to B$ be an isomorphism of $\mathscr{C}(\mathbb{T})$. Then, $\lceil F \rceil : A \to B$ and its inverse are both morphisms of $\mathscr{P}(\mathbb{T})$ as $\mathscr{C}(\mathbb{T})$ is a subcategory of $\mathscr{P}(\mathbb{T})$. Hence $\lceil F \rceil$ has an inverse in $\mathscr{P}(\mathbb{T})$, and so is an isomorphism of $\mathscr{P}(\mathbb{T})$.

Therefore, the isomorphisms of $\mathscr{P}(\mathbb{T})$ are precisely the isomorphisms of $\mathscr{C}(\mathbb{T})$.

(ii) Let $\ulcorner F \urcorner : A \to B$ be a monomorphism of $\mathscr{P}(\mathbb{T})$. By [5, Lemma 2.2], $\ulcorner F \urcorner$ is $\mathcal{R}$-total, and hence is a morphism of $\mathscr{C}(\mathbb{T})$ by Proposition 3.1.2.4. Now let $\ulcorner G \urcorner, \ulcorner H \urcorner : C \to A$ be parallel morphisms of $\mathscr{C}(\mathbb{T})$ and suppose that $\ulcorner G; F \urcorner = \ulcorner G; H \urcorner$. Since $\ulcorner F \urcorner : A \to B$ is a monomorphism of $\mathscr{P}(\mathbb{T})$ and $\ulcorner G \urcorner, \ulcorner H \urcorner$ are also morphisms of $\mathscr{P}(\mathbb{T})$ as $\mathscr{C}(\mathbb{T}) = \mathbf{Tot}(\mathscr{P}(\mathbb{T}))$ is a subcategory of $\mathscr{P}(\mathbb{T})$, it follows that $\ulcorner G \urcorner = \ulcorner H \urcorner$. Hence, $\ulcorner F \urcorner$ is a monomorphism of $\mathscr{C}(\mathbb{T})$.

Conversely, let $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ be a monomorphism of $\mathscr{C}(\mathbb{T})$. Then by Proposition 3.1.1.13 and Definition 3.1.1.10, there exists a subobject $C(\mathbf{y})$ of $B(\mathbf{y})$, with associated monomorphism $\ulcorner C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \urcorner : C(\mathbf{y}) \to B(\mathbf{y})$, and an isomorphism $\ulcorner G(\mathbf{x}, \mathbf{v}) \urcorner : A(\mathbf{x}) \to C(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$ such that the diagram

$$\begin{array}{ccc} A(\mathbf{x}) & \xrightarrow{\ulcorner F(\mathbf{x},\mathbf{v}) \urcorner} & B(\mathbf{y}) \\ {\scriptstyle \ulcorner G(\mathbf{x},\mathbf{v}) \urcorner} \downarrow & \nearrow {\scriptstyle \ulcorner C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \urcorner} & \\ C(\mathbf{y}) & & \end{array} \tag{3.1.36}$$

commutes in $\mathscr{C}(\mathbb{T})$. Since $\mathscr{C}(\mathbb{T})$ is a subcategory of $\mathscr{P}(\mathbb{T})$, the above diagram is also a commutative diagram in $\mathscr{P}(\mathbb{T})$. By part (i), $\ulcorner G(\mathbf{x}, \mathbf{y}) \urcorner$ is an isomorphism in $\mathscr{P}(\mathbb{T})$, and so also a monomorphism in $\mathscr{P}(\mathbb{T})$. Moreover, $\ulcorner C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \urcorner$ is a monomorphism in $\mathscr{P}(\mathbb{T})$ by Lemma 3.1.1.11, which also holds in $\mathscr{P}(\mathbb{T})$ as defining condition (2) was never used in the proof. Thus, $\ulcorner G(\mathbf{x}, \mathbf{v}); (C(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}) \urcorner$ is a monomorphism in $\mathscr{P}(\mathbb{T})$ as it is the composite of two monomorphisms in $\mathscr{P}(\mathbb{T})$. Since diagram (3.1.36) commutes in $\mathscr{P}(\mathbb{T})$, it thus follows that $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner$ is a monomorphism in $\mathscr{P}(\mathbb{T})$.

Therefore, the monomorphisms of $\mathscr{P}(\mathbb{T})$ are precisely the monomorphisms of $\mathscr{C}(\mathbb{T})$. ■

Let $\mathbb{T}$ be a theory. By Proposition 3.1.2.8, the results in Sections 3.1.1.1 and 3.1.1.2 on isomorphisms, monomorphisms, and subobjects in $\mathscr{C}(\mathbb{T})$ also hold in $\mathscr{P}(\mathbb{T})$. Therefore, we may apply these results to $\mathscr{P}(\mathbb{T})$ instead of $\mathscr{C}(\mathbb{T})$ without further justification. Furthermore, we need not specify if a morphism $\ulcorner F \urcorner : A \to B$ is a monomorphism (isomorphism) in $\mathscr{C}(\mathbb{T})$ or a monomorphism (isomorphism, resp.) in $\mathscr{P}(\mathbb{T})$, as these conditions are equivalent.

In any syntactic partial map category, as in any restriction category, the morphisms are locally ordered (see also Appendix B, [4], or [5] for more information on local ordering of morphisms in restriction categories).

Definition 3.1.2.9 [4] Let $\mathscr{P}(\mathbb{T})$ be the syntactic partial map category of a theory $\mathbb{T}$. The morphisms of $\mathscr{P}(\mathbb{T})$ are locally ordered, that is to say, there is a partial order on the hom-sets of $\mathscr{P}(\mathbb{T})$ that is respected by composition. The order is defined as follows: given parallel morphisms $\lceil F \rceil, \lceil G \rceil : A \to B$ in $\mathscr{P}(\mathbb{T})$,

$$\lceil F \rceil \leq \lceil G \rceil \text{ if and only if } \lceil F \rceil = \lceil \overline{F}; G \rceil .$$

Lemma 3.1.2.10 *Let $\mathbb{T}$ be a theory and let*

$$A(\mathbf{x}) \xrightarrow{\lceil F(\mathbf{x},\mathbf{v}) \rceil} B(\mathbf{y}) \xrightarrow{\lceil G(\mathbf{y},\mathbf{w}) \rceil} C(\mathbf{z})$$

be morphisms in $\mathscr{P}(\mathbb{T})$. If $\lceil G \rceil$ is $\mathcal{R}$-total, then $\lceil \overline{F;G} \rceil = \lceil \overline{F} \rceil$.

Proof By definition,

$$\overline{F}(\mathbf{x}, \mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{p}) F(\mathbf{x}, \mathbf{p}) \wedge \mathbf{x} = \mathbf{u}$$

and

$$\overline{F;G}(\mathbf{x}, \mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{r}, \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge G(\mathbf{p}, \mathbf{r})) \wedge \mathbf{x} = \mathbf{u}.$$

Hence, we obtain

$$\vdash \overline{F;G}(\mathbf{x}, \mathbf{u}) \Rightarrow \overline{F}(\mathbf{x}, \mathbf{u})$$

by the rules for $\exists$ and conjunction.

Conversely, we obtain

$$\overline{F}(\mathbf{x}, \mathbf{u}), F(\mathbf{x}, \mathbf{b}) \mid\!\!\stackrel{\mathbf{b}}{-} B(\mathbf{b})$$

by defining condition (1) for F. Since $\lceil G \rceil$ is total, defining condition (2) holds for G by Corollary 3.1.2.5. Hence, we obtain

$$\overline{F}(\mathbf{x}, \mathbf{u}), F(\mathbf{x}, \mathbf{b}) \mid\!\!\stackrel{\mathbf{b}}{-} (\exists \mathbf{r}) G(\mathbf{b}, \mathbf{r})$$

by defining condition (2) for G. It then follows by the rules for $\exists$ and conjunction that

$$\overline{F}(\mathbf{x}, \mathbf{u}) \vdash (\exists \mathbf{r}, \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge G(\mathbf{p}, \mathbf{r})) \wedge \mathbf{x} = \mathbf{u},$$

from which

$$\vdash \overline{F}(\mathbf{x}, \mathbf{u}) \Rightarrow \overline{F;G}(\mathbf{x}, \mathbf{u})$$

follows by ($\Rightarrow$-I). Hence, $\lceil \overline{F;G} \rceil = \lceil \overline{F} \rceil$. ∎

We also make the following remark on split restriction idempotents in syntactic categories (see Appendix B for the definition of a restriction idempotent and of a split restriction category).

Remark 3.1.2.11 (Syntactic partial map categories are split) Let $\mathbb{T}$ be any theory. In order to show that $\mathscr{P}(\mathbb{T})$ is split, it suffices to show that, for each morphism $\lceil F(\mathbf{x}, \mathbf{v}) \rceil : A(\mathbf{x}) \to B(\mathbf{y})$ of $\mathscr{P}(\mathbb{T})$, the corresponding restriction $\lceil \overline{F}(\mathbf{x}, \mathbf{u}) \rceil$: $A(\mathbf{x}) \to A(\mathbf{x})$ splits in $\mathscr{P}(\mathbb{T})$. Define

$$D_F(\mathbf{x}) \underset{\text{def}}{\equiv} (\exists \mathbf{p}) F(\mathbf{x}, \mathbf{p}).$$

It is easy to show that the diagram

$$\begin{array}{ccc} A(\mathbf{x}) & \xrightarrow{\ulcorner \overline{F}(\mathbf{x},\mathbf{u}) \urcorner} & A(\mathbf{x}) \\ & {\scriptstyle \ulcorner \overline{F}(\mathbf{x},\mathbf{u}) \urcorner} \searrow \quad \nearrow {\scriptstyle \ulcorner \overline{F}(\mathbf{x},\mathbf{u}) \urcorner} & \\ & D_F(\mathbf{x}) & \end{array}$$

commutes in $\mathscr{P}(\mathbb{T})$. Since $\mathrm{id}_{D_F}(\mathbf{x},\mathbf{u}) \underset{\mathrm{def}}{\equiv} \overline{F}(\mathbf{x},\mathbf{u})$ by definition, it follows that the diagram

$$\begin{array}{ccc} D_F(\mathbf{x}) & \xrightarrow{\ulcorner \mathrm{id}_{D_F}(\mathbf{x},\mathbf{u}) \urcorner} & D_F(\mathbf{x}) \\ & {\scriptstyle \ulcorner \overline{F}(\mathbf{x},\mathbf{u}) \urcorner} \searrow \quad \nearrow {\scriptstyle \ulcorner \overline{F}(\mathbf{x},\mathbf{u}) \urcorner} & \\ & A(\mathbf{x}) & \end{array}$$

also commutes in $\mathscr{P}(\mathbb{T})$, and so $\ulcorner \overline{F} \urcorner$ indeed splits in $\mathscr{P}(\mathbb{T})$. It thus follows that both $\mathscr{P}(\mathbb{T})$ and $\mathscr{C}(\mathbb{T})$ are split. In particular, since $\mathscr{C}(\mathbb{T})$ is a trivial restriction category, the restriction idempotents of $\mathscr{C}(\mathbb{T})$ are precisely the identity morphisms of $\mathscr{C}(\mathbb{T})$. □

3.1.2.3 Cartesian restriction categories

As shown in Corollary 3.1.1.16, syntactic categories are finitely complete, and hence are in particular cartesian categories. We wish to show an analogous result for syntactic partial map categories. That is to say, we wish to show that syntactic partial map categories are cartesian restriction categories, which are the restriction category equivalent of cartesian categories (see for example [4]). In order to do so, we must show that syntactic partial map categories have a restriction terminal object and all binary partial products.

Let $\mathbb{T}$ be a theory and recall that $\mathscr{C}(\mathbb{T})$ has a terminal object and all binary products, as shown in Proposition 3.1.1.15. We wish to show that the terminal object and products of $\mathscr{C}(\mathbb{T})$ are a restriction terminal object and partial products of $\mathscr{P}(\mathbb{T})$, respectively. Recall from Proposition 3.1.1.15 that $\mathscr{C}(\mathbb{T})$ has terminal object τ, where $\tau \underset{\mathrm{def}}{\equiv} \top \underset{\mathrm{def}}{\equiv} 0 = 0$ if $\mathbb{T}$ is an arithmetical theory and $\tau \underset{\mathrm{def}}{\equiv} (\forall x)(x = x)$ otherwise. For any object $A(\mathbf{x})$, the terminating morphism

$$\ulcorner !_A(\mathbf{x}) \urcorner := \ulcorner A(\mathbf{x}) \urcorner : A(\mathbf{x}) \to \tau$$

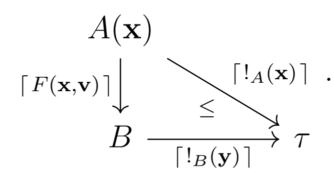
associated to A is the unique morphism from $A(\mathbf{x}) \to \tau$ in $\mathscr{C}(\mathbb{T})$, and hence is the unique $\mathcal{R}$-total morphism from $A(\mathbf{x})$ to τ in $\mathscr{P}(\mathbb{T})$ by Proposition 3.1.2.4. In order for τ to be a restriction terminal object in $\mathscr{P}(\mathbb{T})$, it remains to show that

(i) $\ulcorner !_\tau \urcorner = \ulcorner \mathrm{id}_\tau \urcorner$; and

(ii) for any morphism $\ulcorner F(\mathbf{x},\mathbf{y})\urcorner : A(\mathbf{x}) \to B(\mathbf{y})$,

$$\ulcorner F(\mathbf{x},\mathbf{v}); !_B(\mathbf{x})\urcorner \leq \ulcorner !_A(\mathbf{x})\urcorner,$$

as in the diagram



Given two objects $A(\mathbf{x})$ and $B(\mathbf{y})$, their (genuine) binary product in $\mathscr{C}(\mathbb{T})$ is given by the object $A(\mathbf{x}) \wedge B(\mathbf{y})$, together with the two projections

$$\ulcorner \pi_A(\mathbf{x},\mathbf{y},\mathbf{u})\urcorner := \ulcorner A(\mathbf{x}) \wedge B(\mathbf{y}) \wedge \mathbf{x} = \mathbf{u}\urcorner : A(\mathbf{x}) \wedge B(\mathbf{y}) \to A(\mathbf{x})$$

and

$$\ulcorner \pi_B(\mathbf{x},\mathbf{y},\mathbf{v})\urcorner := \ulcorner A(\mathbf{x}) \wedge B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}\urcorner : A(\mathbf{x}) \wedge B(\mathbf{y}) \to B(\mathbf{y}).$$

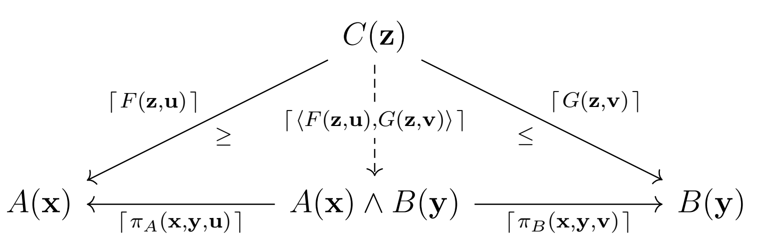
As noted in the proof of Proposition 3.1.1.15 (ii), we assume without loss of generality that the lists $\mathbf{x}$ and $\mathbf{y}$ are disjoint. By Proposition 3.1.2.4, $\ulcorner \pi_A\urcorner$ and $\ulcorner \pi_B\urcorner$ are $\mathcal{R}$-total maps in $\mathscr{P}(\mathbb{T})$. In order to show that $A(\mathbf{x}) \wedge B(\mathbf{y})$, together with the two total projections $\ulcorner \pi_A\urcorner$ and $\ulcorner \pi_B\urcorner$, is the binary partial product of $A(\mathbf{x})$ and $B(\mathbf{y})$ in $\mathscr{P}(\mathbb{T})$, it remains to show that for any object $C(\mathbf{z})$ and any morphisms $\ulcorner F(\mathbf{z},\mathbf{u})\urcorner : C(\mathbf{z}) \to A(\mathbf{x})$ and $\ulcorner G(\mathbf{z},\mathbf{v})\urcorner : C(\mathbf{z}) \to B(\mathbf{y})$ in $\mathscr{P}(\mathbb{T})$, there exists a unique morphism $\ulcorner \langle F(\mathbf{z},\mathbf{u}), G(\mathbf{z},\mathbf{v})\rangle\urcorner : C(\mathbf{z}) \to A(\mathbf{x}) \wedge B(\mathbf{y})$ in $\mathscr{P}(\mathbb{T})$ such that

(i) $\ulcorner \langle F, G\rangle; \pi_A\urcorner \leq \ulcorner F\urcorner$;

(ii) $\ulcorner \langle F, G\rangle; \pi_B\urcorner \leq \ulcorner G\urcorner$; and

(iii) $\left\ulcorner \overline{\langle F, G\rangle} \right\urcorner = \ulcorner \overline{F}; \overline{G}\urcorner$

as in the diagram



Proposition 3.1.2.12 *Let $\mathbb{T}$ be any theory. Then, $\mathscr{P}(\mathbb{T})$ is a cartesian restriction category.*

Proof We first show that τ, together with the terminating morphisms $\ulcorner !_A(\mathbf{x}) \urcorner := \ulcorner A(\mathbf{x}) \urcorner : A(\mathbf{x}) \to \tau$ for each object $A(\mathbf{x})$ in $\mathscr{P}(\mathbb{T})$, is a restriction terminal object of $\mathscr{P}(\mathbb{T})$. It remains to verify the two conditions stated above.

(i) Since τ has no free variables, $!_\tau$ and id_τ are both defined to be the formula τ. Therefore, $\ulcorner !_\tau \urcorner = \ulcorner \mathrm{id}_\tau \urcorner$ in $\mathscr{P}(\mathbb{T})$.

(ii) Let $\ulcorner F(\mathbf{x}, \mathbf{v}) \urcorner : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism of $\mathscr{P}(\mathbb{T})$. We must show that $\ulcorner F; !_B \urcorner \leq \ulcorner !_A \urcorner$, that is, that $\ulcorner F; B \urcorner \leq \ulcorner A \urcorner$. By the definition of the local order on morphisms of $\mathscr{P}(\mathbb{T})$ given in Definition 3.1.2.9, we must show that $\ulcorner F; B \urcorner = \ulcorner \overline{F; B}; A \urcorner$, that is, that

$$\vdash (\exists \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge B(\mathbf{p})) \Leftrightarrow (\exists \mathbf{q})[((\exists \mathbf{p})(F(\mathbf{x}, \mathbf{p}) \wedge B(\mathbf{p})) \wedge \mathbf{x} = \mathbf{q}) \wedge A(\mathbf{q})]. \quad (3.1.37)$$

By defining condition (1) for F, we obtain

$$F(\mathbf{x}, \mathbf{a}) \models^{\mathbf{a}} A(\mathbf{x}).$$

This fact, together with a straightforward argument using the rules for $\exists$ and equality, shows that (3.1.37) holds in $\mathbb{T}$. Hence, $\ulcorner F; B \urcorner \leq \ulcorner A \urcorner$ in $\mathscr{P}(\mathbb{T})$.

Hence, τ is a restriction terminal object of $\mathscr{P}(\mathbb{T})$.

Let $A(\mathbf{x})$ and $B(\mathbf{y})$ be two objects of $\mathscr{P}(\mathbb{T})$. As noted in the proof of Proposition 3.1.1.15 (ii), we can assume without loss of generality that the lists $\mathbf{x}$ and $\mathbf{y}$ are disjoint. In order to show that $A(\mathbf{x}) \wedge B(\mathbf{y})$, together with the $\mathcal{R}$-total projections $\ulcorner \pi_A(\mathbf{x}, \mathbf{y}, \mathbf{u}) \urcorner$ and $\ulcorner \pi_B(\mathbf{x}, \mathbf{y}, \mathbf{v}) \urcorner$, is a partial product in $\mathscr{P}(\mathbb{T})$, it remains to verify the conditions stated above. Let $C(\mathbf{z})$ be any object and let $\ulcorner F(\mathbf{z}, \mathbf{u}) \urcorner : C(\mathbf{z}) \to A(\mathbf{x})$ and $\ulcorner G(\mathbf{z}, \mathbf{v}) \urcorner : C(\mathbf{z}) \to B(\mathbf{y})$ be any morphisms of $\mathscr{P}(\mathbb{T})$. As in the case of genuine products in $\mathscr{C}(\mathbb{T})$, we define

$$\langle F(\mathbf{z}, \mathbf{u}), G(\mathbf{z}, \mathbf{v}) \rangle \underset{\text{def}}{\equiv} F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}).$$

As shown in the proof of Proposition 3.1.1.15, defining conditions (1) and (3) for $F \wedge G$ follow from defining conditions (1) and (3), respectively, for F and G. Hence, $\ulcorner F \wedge G \urcorner$ is indeed a morphism in $\mathscr{P}(\mathbb{T})$ from $C(\mathbf{z})$ to $A(\mathbf{x}) \wedge B(\mathbf{y})$. We now show that $\ulcorner F \wedge G \urcorner$ satisfies conditions (i)–(iii) for partial products stated above.

(i) In order to show that $\ulcorner (F \wedge G); \pi_A \urcorner \leq \ulcorner F \urcorner$, we must show that $\ulcorner (F \wedge G); \pi_A \urcorner = \ulcorner \overline{(F \wedge G); \pi_A}; F \urcorner$, that is, that

$$\vdash (\exists \mathbf{q}, \mathbf{p})((F(\mathbf{z}, \mathbf{q}) \wedge G(\mathbf{z}, \mathbf{p})) \wedge (A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q} = \mathbf{u})) \Leftrightarrow$$
$$(\exists \mathbf{w})[((\exists \mathbf{r}, \mathbf{q}, \mathbf{p})((F(\mathbf{z}, \mathbf{q}) \wedge G(\mathbf{z}, \mathbf{p})) \wedge (A(\mathbf{q}) \wedge B(\mathbf{p}) \wedge \mathbf{q} = \mathbf{r})) \wedge \mathbf{z} = \mathbf{w}) \wedge F(\mathbf{w}, \mathbf{u})]. \quad (3.1.38)$$

It follows from the rules for $\exists$ and equality, as well as defining condition (3) for F, that (3.1.38) holds in $\mathbb{T}$. Hence, $\ulcorner (F \wedge G); \pi_A \urcorner \leq \ulcorner F \urcorner$ in $\mathscr{P}(\mathbb{T})$.

(ii) An analogous argument to the one above shows that $\lceil (F \wedge G); \pi_B \rceil \leq \lceil G \rceil$ in $\mathscr{P}(\mathbb{T})$.

(iii) We obtain

$$\vdash (\exists \mathbf{q}, \mathbf{p})(F(\mathbf{z}, \mathbf{q}) \wedge G(\mathbf{z}, \mathbf{p})) \wedge \mathbf{z} = \mathbf{w} \Leftrightarrow (\exists \mathbf{r})[((\exists \mathbf{q}) F(\mathbf{z}, \mathbf{q}) \wedge \mathbf{z} = \mathbf{r}) \wedge ((\exists \mathbf{p}) G(\mathbf{r}, \mathbf{p}) \wedge \mathbf{r} = \mathbf{w})]$$

by the rules for $\exists$ and equality, and so $\lceil \overline{F \wedge G} \rceil = \lceil \overline{F}; \overline{G} \rceil$ in $\mathscr{P}(\mathbb{T})$.

It remains to show that $\lceil F \wedge G \rceil$ is the unique morphism from C to $A \wedge B$ in $\mathscr{P}(\mathbb{T})$ satisfying these conditions. Suppose that $\lceil H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \rceil : C(\mathbf{z}) \to A(\mathbf{x}) \wedge B(\mathbf{y})$ is some other morphism in $\mathscr{P}(\mathbb{T})$ satisfying conditions (i)–(iii) for partial products.

Since condition (iii) holds for both $\lceil H \rceil$ and $\lceil F \wedge G \rceil$, we obtain

$$\lceil \overline{H} \rceil = \lceil \overline{F \wedge G} \rceil . \tag{3.1.39}$$

Moreover, since $\lceil \pi_A \rceil$ and $\lceil \pi_B \rceil$ are total morphisms, we obtain

$$\left\lceil \overline{(F \wedge G); \pi_A} \right\rceil = \lceil \overline{F \wedge G} \rceil = \lceil \overline{H} \rceil = \lceil \overline{H; \pi_A} \rceil$$

and

$$\left\lceil \overline{(F \wedge G); \pi_B} \right\rceil = \lceil \overline{F \wedge G} \rceil = \lceil \overline{H} \rceil = \lceil \overline{H; \pi_B} \rceil$$

by Lemma 3.1.2.10. It thus follows by conditions (i)–(ii) for $\lceil H \rceil$ and $\lceil F \wedge G \rceil$ that

$$\lceil (F \wedge G); \pi_A \rceil = \left\lceil \overline{(F \wedge G)}; F \right\rceil = \lceil H; \pi_A \rceil \tag{3.1.40}$$

and

$$\lceil (F \wedge G); \pi_B \rceil = \left\lceil \overline{(F \wedge G)}; G \right\rceil = \lceil H; \pi_B \rceil . \tag{3.1.41}$$

We now show that $\vdash H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \Leftrightarrow F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v})$. We obtain

$$H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \vdash A(\mathbf{u}) \wedge B(\mathbf{v}) \wedge \mathbf{u} = \mathbf{u}$$

by defining condition (1) for H, (=-I), and ($\wedge$-I). We then obtain

$$H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \vdash (H; \pi_A)(\mathbf{z}, \mathbf{u})$$

by the definition of π_A, ($\wedge$-I), and ($\exists$-I). Thus,

$$H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \vdash (\overline{F \wedge G}; F)(\mathbf{z}, \mathbf{u})$$

follows by (3.1.40). By definition,

$$(\overline{F \wedge G}; F)(\mathbf{z}, \mathbf{u}) \underset{\text{def}}{\equiv} (\exists \mathbf{r})([(\exists \mathbf{q}, \mathbf{p})(F(\mathbf{z}, \mathbf{q}) \wedge G(\mathbf{z}, \mathbf{p})) \wedge \mathbf{z} = \mathbf{r}] \wedge F(\mathbf{r}, \mathbf{u})),$$

and so we obtain

$$(\overline{F \wedge G}; F)(\mathbf{z}, \mathbf{u}) \vdash F(\mathbf{z}, \mathbf{u}) \tag{3.1.42}$$

by (∃-E) and (=-E). Hence, we obtain

$$H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \vdash F(\mathbf{z}, \mathbf{u})$$

by (Cut). An analogous argument, using (3.1.41) instead of (3.1.40), shows that

$$H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \vdash G(\mathbf{z}, \mathbf{v}).$$

Thus, we obtain

$$\vdash H(\mathbf{z}, \mathbf{u}, \mathbf{v}) \Rightarrow F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v})$$

by (∧-I) and (⇒-I).

Conversely, by (∃-I) and (⇒-I), we obtain

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}) \vdash \overline{(F \wedge G)}(\mathbf{z}, \mathbf{z}),$$

from which

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}) \vdash \overline{H}(\mathbf{z}, \mathbf{z}),$$

and so also

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}) \vdash (\exists \mathbf{q}, \mathbf{p}) H(\mathbf{z}, \mathbf{q}, \mathbf{p}),$$

follows by (3.1.39) and (∧-E). We obtain

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} A(\mathbf{a}) \wedge B(\mathbf{b}) \wedge \mathbf{a} = \mathbf{a}$$

by defining condition (1) for H, (=-I), and (∧-I). It follows that

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} (H; \pi_A)(\mathbf{z}, \mathbf{a})$$

by (∧-I) and (∃-I). We thus obtain

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} (\overline{F \wedge G}; F)(\mathbf{z}, \mathbf{a})$$

by (3.1.40). By (3.1.42) and (Cut), we thus obtain

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} F(\mathbf{z}, \mathbf{a}),$$

from which it follows that

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} \mathbf{a} = \mathbf{u}$$

by defining condition (3) for F. A similar argument shows that

$$F(\mathbf{z}, \mathbf{u}) \wedge G(\mathbf{z}, \mathbf{v}), H(\mathbf{z}, \mathbf{a}, \mathbf{b}) \vdash^{\mathbf{a},\mathbf{b}} \mathbf{b} = \mathbf{v},$$

and so

$$\vdash F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v}) \Rightarrow H(\mathbf{z},\mathbf{u},\mathbf{v})$$

follows by (=-E), (∃-E), and (⇒-I).

Therefore, $\lceil H(\mathbf{z},\mathbf{u},\mathbf{v})\rceil = \lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v})\rceil$, and so $\lceil F(\mathbf{z},\mathbf{u}) \wedge G(\mathbf{z},\mathbf{v})\rceil$ is indeed the unique morphism from $C(\mathbf{z})$ to $A(\mathbf{x}) \wedge B(\mathbf{y})$ satisfying conditions (i)–(iii) for partial products. Thus, $A(\mathbf{x}) \wedge B(\mathbf{y})$ is indeed the partial product of $A(\mathbf{x})$ and $B(\mathbf{y})$ in $\mathscr{P}(\mathbb{T})$.

Hence, $\mathscr{P}(\mathbb{T})$ has a restriction terminal object and all binary partial products, and so is a cartesian restriction category. ■

It follows from Proposition 3.1.2.12 that, for any theory $\mathbb{T}$, the terminal object and products of $\mathscr{C}(\mathbb{T})$ coincide with the restriction terminal object and partial products of $\mathscr{P}(\mathbb{T})$. Hence, we may refer to the restriction terminal object and partial products of $\mathscr{P}(\mathbb{T})$ as the terminal object and products, respectively, of $\mathscr{P}(\mathbb{T})$.

3.2 Natural numbers objects in syntactic categories of arithmetical theories

Recall from Remark 3.1.1.6 that we make an analogy between the category **Set** and the syntactic category of a theory $\mathbb{T}$. Note further that $\mathbb{N}$ is a natural numbers object of **Set** (see for example [12]). Thus, when $\mathbb{T}$ is an arithmetical theory, we wish to formalise the argument showing that $\mathbb{N}$ is a natural numbers object in $\mathbb{T}$ in order to construct a natural numbers object in the syntactic category $\mathscr{C}(\mathbb{T})$.

By Corollary 3.1.1.16, the syntactic category $\mathscr{C}(\mathbb{T})$ of any arithmetical theory $\mathbb{T}$ is finitely complete and hence a cartesian category. However, we have not shown that $\mathscr{C}(\mathbb{T})$ is in general cartesian closed. Since genuine natural numbers objects (which we may refer to as a *non-parameterised* natural numbers objects) are only defined for a cartesian closed category [16, pp. 46, 68], we need to consider instead *parameterised* natural numbers objects in the context of syntactic categories.

In a general category, a parameterised natural numbers object can be defined in several equivalent ways [16, 28]. Adapting the definition from [16] to the context of syntactic categories yields the following definition, where we recall from Proposition 3.1.1.15 that we take $\top \underset{\text{def}}{\equiv} 0 = 0$ to be the terminal object of $\mathscr{C}(\mathbb{T})$.

Definition 3.2.0.1 Let $\mathscr{C}(\mathbb{T})$ be a syntactic category of an arithmetical theory $\mathbb{T}$. A *strong parameterised natural numbers object* in $\mathscr{C}(\mathbb{T})$ is given by an object N together with a pair of morphisms $\lceil \underline{0}\rceil : \top \to N$ and $\lceil \sigma\rceil : N \to N$ such that, for all morphisms $\lceil G\rceil : A \to B$ and $\lceil H\rceil : B \to B$ in $\mathscr{C}(\mathbb{T})$, there exists a unique morphism $\lceil K\rceil : N \wedge A \to B$, called the *parameterised iterator for* $\lceil G\rceil$ *and* $\lceil H\rceil$, making the diagram

$$\begin{array}{ccccc} A & \xrightarrow{\langle \ulcorner !_A;\underline{0} \urcorner, \ulcorner \mathrm{id}_A \urcorner \rangle} & N \wedge A & \xrightarrow{\ulcorner \sigma \urcorner \times \ulcorner \mathrm{id}_A \urcorner} & N \wedge A \\ & \searrow^{\ulcorner G \urcorner} & \Big\downarrow{\scriptstyle \ulcorner K \urcorner} & & \Big\downarrow{\scriptstyle \ulcorner K \urcorner} \\ & & B & \xrightarrow[\ulcorner H \urcorner]{} & B \end{array}$$

commute in $\mathscr{C}(\mathbb{T})$. If the uniqueness condition is omitted, N is a *weak parameterised natural numbers object*. □

Just as we can consider numerals in cartesian closed categories with a weak or strong natural numbers object, we can also consider numerals in cartesian categories with a weak or strong parameterised natural numbers object following the treatment in [16]. In the context of syntactic categories, we obtain the following definition.

Definition 3.2.0.2 Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$, let N be a weak or strong parameterised natural numbers object in $\mathscr{C}(\mathbb{T})$ with associated morphisms $\ulcorner \underline{0} \urcorner : \top \to N$ and $\ulcorner \sigma \urcorner : N \to N$. The *numerals* of $\mathscr{C}(\mathbb{T})$ are defined inductively as follows:

(i) $\ulcorner \underline{0} \urcorner : \top \to N$ is the 0^{th} numeral of $\mathscr{C}(\mathbb{T})$.

(ii) If $\ulcorner F \urcorner : \top \to N$ is the n^{th} numeral of $\mathscr{C}(\mathbb{T})$ $(n \geq 0)$, then $\ulcorner F; \sigma \urcorner : \top \to N$ is the $(n+1)^{\text{th}}$ numeral of $\mathscr{C}(\mathbb{T})$.

Numerals are said to be *standard* in $\mathscr{C}(\mathbb{T})$ if the only morphisms from $\top$ to N in $\mathscr{C}(\mathbb{T})$ are the numerals. □

Since we shall only consider parameterised natural numbers objects in the context of syntactic categories, we shall allow ourselves to omit the qualifier "parameterised". Therefore, we shall henceforth say "natural numbers object" instead of "parameterised natural numbers object" and "iterator" instead of "parameterised iterator" in the context of syntactic categories.

We claim that $N(x) \underset{\text{def}}{\equiv} x = x$ is a strong natural numbers object in the syntactic category $\mathscr{C}(\mathbb{T})$ of any arithmetical theory $\mathbb{T}$ with induction.

Lemma 3.2.0.3 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ and define*

$$N(x) \underset{\text{def}}{\equiv} x = x,$$

$$\underline{0}(u) \underset{\text{def}}{\equiv} 0 = u,$$

and

$$\sigma(x, u) \underset{\text{def}}{\equiv} S(x) = u.$$

Then, $\ulcorner \underline{0}(u) \urcorner$ is a morphism from $\top$ to $N(x)$ in $\mathscr{C}(\mathbb{T})$ and $\ulcorner \sigma(x,u) \urcorner$ is a morphism on $N(x)$ in $\mathscr{C}(\mathbb{T})$.

Let $A(\mathbf{y})$ be an object of $\mathscr{C}(\mathbb{T})$. Define

$$\underline{0}_A(\mathbf{y},u,\mathbf{v}) \underset{\text{def}}{\equiv} \underline{0}(u) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v})$$

and

$$\sigma_A(x,\mathbf{y},u,\mathbf{v}) \underset{\text{def}}{\equiv} \sigma(x,u) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v}).$$

Then,

$$\langle \ulcorner !_A(\mathbf{y}); \underline{0}(u) \urcorner, \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner \rangle = \ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}) \urcorner$$

as morphisms from $A(\mathbf{y})$ to $N(x) \wedge A(\mathbf{y})$ and

$$\ulcorner \sigma(x,u) \urcorner \times \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner = \ulcorner \sigma_A(x,\mathbf{y},u,\mathbf{v}) \urcorner$$

as morphisms on $N(x) \wedge A(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$.

Proof It follows from the rules for equality in $\mathbb{T}$ that $\ulcorner \underline{0}(u) \urcorner$ and $\ulcorner \sigma(x,u) \urcorner$ are indeed morphisms of $\mathscr{C}(\mathbb{T})$. Furthermore, by the definition of the product of two morphisms of $\mathscr{C}(\mathbb{T})$ given in Lemma 3.1.1.17, $\ulcorner \sigma(x,u) \urcorner \times \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner = \ulcorner \sigma_A(x,\mathbf{y},u,\mathbf{v}) \urcorner$ as morphisms on $N(x) \wedge A(\mathbf{y})$.

It remains to show that $\langle \ulcorner !_A(\mathbf{y}); \underline{0}(u) \urcorner, \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner \rangle = \ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}) \urcorner$ as morphisms from $A(\mathbf{y})$ to $N(x) \wedge A(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$. By the definition of the pairing of two morphisms in $\mathscr{C}(\mathbb{T})$ and the fact that $!_A(\mathbf{y}) \underset{\text{def}}{\equiv} A(\mathbf{y})$,

$$\langle \ulcorner !_A(\mathbf{y}); \underline{0}(u) \urcorner, \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner \rangle = \ulcorner (A(\mathbf{y}) \wedge \underline{0}(u)) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner.$$

Since $\underline{0}_A(\mathbf{y},u,\mathbf{v}) \underset{\text{def}}{\equiv} \underline{0}(u) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v})$, it suffices to show that

$$\vdash (A(\mathbf{y}) \wedge \underline{0}(u)) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v}) \Leftrightarrow \underline{0}(u) \wedge \mathrm{id}_A(\mathbf{y},\mathbf{v}) \tag{3.2.1}$$

holds in $\mathbb{T}$. Since $\mathrm{id}_A(\mathbf{y},\mathbf{v}) \underset{\text{def}}{\equiv} A(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}$, we obtain (3.2.1) by a straightforward application of the rules for conjunction in $\mathbb{T}$. Therefore, $\langle \ulcorner !_A(\mathbf{y}); \underline{0}(u) \urcorner, \ulcorner \mathrm{id}_A(\mathbf{y},\mathbf{v}) \urcorner \rangle = \ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}) \urcorner$ as morphisms from $A(\mathbf{y})$ to $N(x) \wedge A(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$. ∎

Hence, in order to show that $N(x) \underset{\text{def}}{\equiv} x = x$, together with the morphisms $\ulcorner \underline{0}(u) \urcorner$ and $\ulcorner \sigma(x,u) \urcorner$ from Lemma 3.2.0.3, is a strong natural numbers object in a syntactic category $\mathscr{C}(\mathbb{T})$ of an arithmetical theory $\mathbb{T}$ with induction, it suffices to show that for all morphisms $\ulcorner G(\mathbf{y},\mathbf{w}) \urcorner : A(\mathbf{y}) \to B(\mathbf{z})$ and $\ulcorner H(\mathbf{z},\mathbf{w}) \urcorner : B(\mathbf{z}) \to B(\mathbf{z})$ in $\mathscr{C}(\mathbb{T})$, there exists a unique morphism $\ulcorner K(x,\mathbf{y},\mathbf{w}) \urcorner : N(x) \wedge A(\mathbf{y}) \to B(\mathbf{z})$ making the diagram

$$\begin{array}{ccccc} A(\mathbf{y}) & \xrightarrow{\ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}) \urcorner} & N(x) \wedge A(\mathbf{y}) & \xrightarrow{\ulcorner \sigma_A(x,\mathbf{y},u,\mathbf{v}) \urcorner} & N(x) \wedge A(\mathbf{y}) \\ & \searrow^{\ulcorner G(\mathbf{y},\mathbf{w}) \urcorner} & \downarrow{\scriptstyle \ulcorner K(x,\mathbf{y},\mathbf{w}) \urcorner} & & \downarrow{\scriptstyle \ulcorner K(x,\mathbf{y},\mathbf{w}) \urcorner} \\ & & B(\mathbf{z}) & \xrightarrow[\ulcorner H(\mathbf{z},\mathbf{w}) \urcorner]{} & B(\mathbf{z}) \end{array} \tag{3.2.2}$$

commute in $\mathscr{C}(\mathbb{T})$, where $\underline{0}_A(\mathbf{y}, u, \mathbf{v}) \underset{\text{def}}{\equiv} \underline{0}(u) \wedge \mathrm{id}_A(\mathbf{y}, \mathbf{v})$ and $\sigma_A(x, \mathbf{y}, u, \mathbf{v}) \underset{\text{def}}{\equiv} \sigma(x, u) \wedge \mathrm{id}_A(\mathbf{y}, \mathbf{v})$ as in Lemma 3.2.0.3.

Note that we construct the iterator $\ulcorner K \urcorner$ for given morphisms $\ulcorner G \urcorner$ and $\ulcorner H \urcorner$ in $\mathscr{C}(\mathbb{T})$ by formalising the construction of the iterators associated to $\mathbb{N}$ as a strong (parameterised) natural numbers object of **Set**. Indeed, consider two functions $g : A \to B$ and $h : B \to B$ in **Set**. Then, the (parameterised) iterator $I_{g,h} : \mathbb{N} \times A \to B$ associated to g and h is the unique function in **Set** from $\mathbb{N} \times A$ to B satisfying

$$\begin{aligned} I_{g,h}(0, a) &= g(a) \\ I_{g,h}(n+1, a) &= h(I_{g,h}(n, a)) \end{aligned}$$

for all $n \in \mathbb{N}$ and $a \in A$. Thus, for each pair $(n, a) \in \mathbb{N} \times A$, we can determine the value $I_{g,h}(n, a)$ by taking the last element in the sequence

$$b_0 = g(a), b_1 = h(b_0), \dots, b_n = h(b_{n-1})$$

of length $n + 1$ of elements of B.

We can therefore formalise this construction in the syntactic category $\mathscr{C}(\mathbb{T})$ of an arithmetical theory with induction using the representing formula Λ of the β function (see Lemma 2.4.1.12), similarly to the construction we used in order to strongly represent functions obtained by primitive recursion in arithmetical theories with induction (see Sections 2.4.1.3 and 2.4.1.4). We first consider the case when the object B in diagram (3.2.2) has a single free variable. Given two morphisms $\ulcorner G(\mathbf{y}, w) \urcorner : A(\mathbf{y}) \to B(z)$ and $\ulcorner H(z, w) \urcorner : B(z) \to B(z)$ in $\mathscr{C}(\mathbb{T})$, we need to define a formula $K(x, \mathbf{y}, w)$ which is a provably functional relation from $N(x) \wedge A(\mathbf{y})$ to $B(z)$ and is such that for each $n \in \mathbb{N}$, $K(\overline{n}, \mathbf{y}, w)$ encodes in $\mathbb{T}$ a sequence $w_0, \dots, w_n$ such that

$$A(\mathbf{y}) \vdash G(\mathbf{y}, w_0) \wedge \left(\bigwedge_{j=0}^{n-1} H(w_j, w_{j+1}) \right) \tag{3.2.3}$$

and w_n is w. Since Λ strongly represents β in $\mathbb{T}$, we can give the above construction for sequences with length specified by a variable x instead of a numeral $\overline{n}$.

Lemma 3.2.0.4 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ with induction, let $A(\mathbf{y})$ and $B(z)$ be any objects of $\mathscr{C}(\mathbb{T})$ such that B has exactly one free variable, and let $\lceil G(\mathbf{y}, w)\rceil : A(\mathbf{y}) \to B(z)$ and $\lceil H(z, w)\rceil : B(z) \to B(z)$ be morphisms of $\mathscr{C}(\mathbb{T})$. Let Λ be the formula strongly representing β in $\mathbb{T}$ as defined in Lemma 2.4.1.12. Define*

$$K'(x, \mathbf{y}, w, q_0, q_1) \underset{\text{def}}{\equiv} (\exists w_0)(\Lambda(q_0, q_1, 0, w_0) \wedge G(\mathbf{y}, w_0)) \wedge \Lambda(q_0, q_1, x, w) \\ \wedge (\forall z)(z < x \Rightarrow (\exists p, p')(\Lambda(q_0, q_1, z, p) \wedge \Lambda(q_0, q_1, S(z), p') \wedge H(p, p')))$$

and

$$K(x, \mathbf{y}, w) \underset{\text{def}}{\equiv} (\exists q_0, q_1) K'(x, \mathbf{y}, w, q_0, q_1).$$

Then, $\lceil K(x, \mathbf{y}, w)\rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(z)$ and does not depend on the choice of representatives of the morphisms $\lceil G\rceil$ and $\lceil H\rceil$.

Proof We only present the main ideas of the proof. For the full details, see Appendix C.

As explained above, $K(x, \mathbf{y}, w)$ was constructed in order to encode a specific sequence $\mathbf{w}$ with last index x determined by the initial parameters $\mathbf{y}$ and the functional relations $G(\mathbf{y}, w)$ and $H(z, w)$. $K'(x, \mathbf{y}, w, q_0, q_1)$ expresses the fact that q_0, q_1 give an encoding of the sequence $\mathbf{w}$. It is a conjunction of three subformulas. The first of these subformulas, namely $(\exists w_0)(\Lambda(q_0, q_1, 0, w_0) \wedge G(\mathbf{y}, w_0))$, expresses the fact that the first element in the sequence $\mathbf{w}$ is the unique w_0 such that

$$A(\mathbf{y}) \vdash G(\mathbf{y}, w_0),$$

that is to say, w_0 is obtained by applying the provably functional relation G to $\mathbf{y}$. The second subformula, namely $\Lambda(q_0, q_1, x, w)$, sets w to be the element of the sequence $\mathbf{w}$ with index x, that is to say, the last element of the sequence $\mathbf{w}$. The third subformula, namely $(\forall z)(z < x \Rightarrow (\exists p, p')(\Lambda(q_0, q_1, z, p) \wedge \Lambda(q_0, q_1, S(z), p') \wedge H(p, p')))$, expresses the fact that, given an element p in the sequence with index $z < x$, the next element p' in the sequence is obtained by applying the provably functional relation H to the element p of index z.

We must show that K satisfies defining conditions (1)–(3) for a morphism from $N \wedge A$ to B in $\mathscr{C}(\mathbb{T})$.

(1) Note that $N(x) \underset{\text{def}}{\equiv} x = x$ is provably true in $\mathbb{T}$ by (=-I). Hence, it remains to show that $K(x, \mathbf{y}, w) \vdash A(\mathbf{y}) \wedge B(w)$. We have

$$K(x, \mathbf{y}, w) \vdash^{a_0, a_1} K'(x, \mathbf{y}, w, a_0, a_1),$$

for some a_0, a_1 encoding the required sequence $\mathbf{w}$. Since the first element in the sequence $\mathbf{w}$ is obtained by applying G to $\mathbf{y}$, we obtain

$$K'(x, \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1} A(\mathbf{y})$$

using the first subformula of K' and defining condition (1) for G. In order to show that

$$K'(x, \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1} B(w), \tag{3.2.4}$$

note first that we have

$$\vdash x = 0 \vee (\exists u)(x = S(u))$$

by axiom (M7), and so we can reason by cases. If we suppose that $x = 0$, then the first element of the sequence $\mathbf{w}$ is also the last. We thus obtain

$$K'(0, \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1} G(\mathbf{y}, w)$$

using the first two subformulas of K' and condition (P3) for Λ, and so

$$K'(0, \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1} B(w)$$

follows by defining condition (1) for G. If we suppose instead that $(\exists u)(x = S(u))$, then $x = S(d)$ for some d. We can therefore use the second and third subformulas of K' and condition (P3) for Λ to obtain

$$K'(S(d), \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1,d,e} \Lambda(a_0, a_1, d, e) \wedge \Lambda(a_0, a_1, S(d), w) \wedge H(e, w),$$

where we note that e is the element in the sequence $\mathbf{w}$ with index d and w, the element with index $S(d)$, is obtained by applying H to e. We then obtain

$$K'(S(d), \mathbf{y}, w, a_0, a_1) \vdash^{a_0,a_1,d} B(w)$$

by defining condition (1) for H. We thus obtain (3.2.4) by ($\vee$-E), and so defining condition (1) for K follows by ($\exists$-E).

(2) Since $N(x)$ is a theorem of $\mathbb{T}$, it suffices to prove

$$\vdash A(\mathbf{y}) \Rightarrow (\exists w)K(x, \mathbf{y}, w)$$

in order to show that defining condition (2) for K holds. We proceed by induction on x in $\mathbb{T}$. It suffices to prove

$$A(\mathbf{y}) \vdash (\exists w)K(0, \mathbf{y}, w) \tag{3.2.5}$$

and

$$A(\mathbf{y}) \vdash (\exists w)K(x, \mathbf{y}, w) \Rightarrow (\exists w)K(S(x), \mathbf{y}, w). \tag{3.2.6}$$

For (3.2.5), note first that $A(\mathbf{y}) \mathrel{\vert\!\overset{a}{-}} G(\mathbf{y}, a)$ for some a by defining condition (2) for G. Since $x = 0$ in this case, we merely need to give an encoding in $\mathbb{T}$ of the sequence of length one with unique element a. By Lemma 2.4.1.14, we can encode sequences of length one in $\mathbb{T}$ using (2.4.9), and so we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a) \mathrel{\vert\!\overset{a}{-}} (\exists q_0, q_1)\Lambda(q_0, q_1, 0, a).$$

It then follows that

$$A(\mathbf{y}), G(\mathbf{y}, a), \Lambda(b_0, b_1, 0, a) \mathrel{\vert\!\overset{a,b_0,b_1}{\longrightarrow}} K'(0, \mathbf{y}, a, b_0, b_1),$$

from which we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a) \mathrel{\vert\!\overset{a}{-}} K(0, \mathbf{y}, a),$$

and so also

$$A(\mathbf{y}) \vdash (\exists w)K(0, \mathbf{y}, w).$$

Thus, (3.2.5) holds in $\mathbb{T}$.

For (3.2.6), we first suppose that

$$\mathrel{\vert\!\overset{a}{-}} K(x, \mathbf{y}, a)$$

for some a. We thus obtain

$$\mathrel{\vert\!\overset{a,a',b_0,b_1}{\longrightarrow}} K'(x, \mathbf{y}, a, b_0, b_1) \wedge H(a, a')$$

using defining condition (1) for K and defining condition (2) for H. Note that b_0, b_1 encode in $\mathbb{T}$ the sequence $\mathbf{w}$ with last index x and last element a determined by $\mathbf{y}$, G, and H. Since a' is obtained by applying H to a, the sequence with last index $S(x)$ determined by $\mathbf{y}$, G, and H consists of the sequence $\mathbf{w}$ followed by a'. Using (2.4.12), we can encode in $\mathbb{T}$ the sequence obtained by appending a' to the sequence encoded by b_0, b_1. Indeed, we obtain

$$\mathrel{\vert\!\overset{a,a',b_0,b_1,c_0,c_1}{\longrightarrow}} (\forall w, z_0)(w \leq x \wedge \Lambda(b_0, b_1, w, z_0) \Rightarrow \Lambda(c_0, c_1, w, z_0)) \wedge \Lambda(c_0, c_1, S(x), a')$$

for some c_0, c_1. We can then show that

$$\mathrel{\vert\!\overset{a,a',b_0,b_1,c_0,c_1}{\longrightarrow}} K'(S(x), \mathbf{y}, a', c_0, c_1),$$

and so c_0, c_1 indeed encode the required sequence in $\mathbb{T}$. (3.2.6) then follows by the rules for $\exists$ and ($\Rightarrow$-I).

Therefore, we obtain

$$\vdash A(\mathbf{y}) \Rightarrow (\exists w)K(x, \mathbf{y}, w).$$

by induction on x in $\mathbb{T}$, and so defining condition (2) for K is satisfied.

(3) In order to show that K satisfies defining condition (3), it suffices to show that any two sequences with last index x determined by the same parameters $\mathbf{y}$ and functional relations G and H must contain exactly the same elements, regardless of their respective encodings in $\mathbb{T}$. Thus, we show

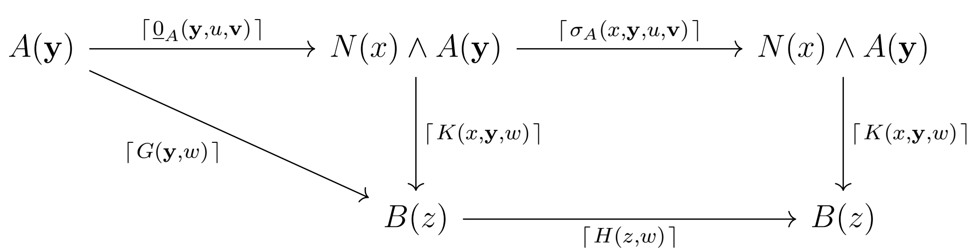
$$K'(x, \mathbf{y}, w, q_0, q_1), K'(x, \mathbf{y}, w', q_0', q_1') \vdash (\forall v)(\forall u)(v \leq x \wedge \Lambda(q_0, q_1, v, u) \Rightarrow \Lambda(q_0', q_1', v, u)) \tag{3.2.7}$$

by induction on v in $\mathbb{T}$. We use defining condition (3) for G and condition (P3) for Λ to establish the base case and we use defining condition (3) for H and condition (P3) for Λ to prove the induction step. Defining condition (3) for K then follows from (3.2.7) by condition (P3) for Λ.

Hence, $\lceil K(x, \mathbf{y}, w) \rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(z)$. Furthermore, note that since different representatives of the same morphism are provably equivalent in $\mathbb{T}$, it follows from the Equivalence Theorem that $\lceil K \rceil$ does not depend on the choice of representatives of the morphisms $\lceil G \rceil$ and $\lceil H \rceil$. ■

Note that $\mathbb{T}$ must have induction for the proof of Lemma 3.2.0.4 to hold since we use condition (P3) for Λ, which we have only established for arithmetical theories with induction, and induction on variables in $\mathbb{T}$.

Lemma 3.2.0.5 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ with induction, let $A(\mathbf{y})$ and $B(z)$ be any objects of $\mathscr{C}(\mathbb{T})$ such that B has exactly one free variable, let $\lceil G(\mathbf{y}, w) \rceil : A(\mathbf{y}) \to B(z)$ and $\lceil H(z, w) \rceil : B(z) \to B(z)$ be morphisms of $\mathscr{C}(\mathbb{T})$, and let $K(x, \mathbf{y}, w)$ be the formula defined in Lemma 3.2.0.4. Then, $\lceil K(x, \mathbf{y}, w) \rceil : N(x) \wedge A(\mathbf{y}) \to B(z)$ is the unique morphism of $\mathscr{C}(\mathbb{T})$ making the diagram*



commute in $\mathscr{C}(\mathbb{T})$.

Proof Since $\mathbb{T}$ has induction, $\lceil K(x, \mathbf{y}, w) \rceil : N(x) \wedge A(\mathbf{y}) \to B(z)$ is indeed a morphism of $\mathscr{C}(\mathbb{T})$ by Lemma 3.2.0.4. Moreover, we assume that K is defined using the formula Λ from Lemma 2.4.1.12, which strongly represents β in $\mathbb{T}$. We first show that diagram

$$\begin{array}{ccc} A(\mathbf{y}) & \xrightarrow{\ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v})\urcorner} & N(x)\wedge A(\mathbf{y}) \\ & {\scriptstyle \ulcorner G(\mathbf{y},w)\urcorner}\searrow & \Big\downarrow{\scriptstyle \ulcorner K(x,\mathbf{y},w)\urcorner} \\ & & B(z) \end{array} \tag{3.2.8}$$

commutes in $\mathscr{C}(\mathbb{T})$.

First note that, since $\underline{0}_A(\mathbf{y},u,\mathbf{v}) \underset{\text{def}}{\equiv} 0 = u \wedge (A(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v})$ by Lemma 3.2.0.3, we obtain

$$\vdash (\exists u,\mathbf{v})(\underline{0}_A(\mathbf{y},u,\mathbf{v}) \wedge K(u,\mathbf{v},w)) \Leftrightarrow (A(\mathbf{y}) \wedge K(0,\mathbf{y},w)).$$

Furthermore, by ($\wedge$-E) and defining condition (1) for K, we obtain

$$\vdash A(\mathbf{y}) \wedge K(0,\mathbf{y},w) \Leftrightarrow K(0,\mathbf{y},w)$$

It thus follows that

$$\ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}); K(x,\mathbf{y},w)\urcorner = \ulcorner K(0,\mathbf{y},w)\urcorner$$

as morphisms in $\mathscr{C}(\mathbb{T})$. Therefore, in order to show that diagram (3.2.8) commutes, it suffices to show that

$$\vdash K(0,\mathbf{y},w) \Leftrightarrow G(\mathbf{y},w) \tag{3.2.9}$$

holds in $\mathbb{T}$. By defining condition (1) for G, we have that $G(\mathbf{y},w) \vdash A(\mathbf{y})$. The same argument as in the proof of defining condition (2) for K in Lemma 3.2.0.4 shows that $A(\mathbf{y}), G(\mathbf{y},w) \vdash K(0,\mathbf{y},w)$. Hence, it follows that $G(\mathbf{y},w) \vdash K(0,\mathbf{y},w)$. Furthermore, using ($\exists$-E) and condition (P3) for Λ, we obtain that $K(0,\mathbf{y},w) \vdash G(\mathbf{y},w)$, and so (3.2.9) holds in $\mathbb{T}$. Therefore, diagram (3.2.8) commutes in $\mathscr{C}(\mathbb{T})$.

Next, we show that the diagram

$$\begin{array}{ccc} N(x)\wedge A(\mathbf{y}) & \xrightarrow{\ulcorner \sigma_A(x,\mathbf{y},u,\mathbf{v})\urcorner} & N(x)\wedge A(\mathbf{y}) \\ {\scriptstyle \ulcorner K(x,\mathbf{y},w)\urcorner}\Big\downarrow & & \Big\downarrow{\scriptstyle \ulcorner K(x,\mathbf{y},w)\urcorner} \\ B(z) & \xrightarrow[\ulcorner H(z,w)\urcorner]{} & B(z) \end{array}, \tag{3.2.10}$$

commutes in $\mathscr{C}(\mathbb{T})$. Note that, since $\sigma_A(x,\mathbf{y},u,\mathbf{v}) \underset{\text{def}}{\equiv} S(x) = u \wedge (A(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v})$ by Lemma 3.2.0.3, we have that

$$\vdash (\exists u,\mathbf{v})(\sigma_A(x,\mathbf{y},u,\mathbf{v}) \wedge K(u,\mathbf{v},w)) \Leftrightarrow A(\mathbf{y}) \wedge K(S(x),\mathbf{y},w).$$

Furthermore, we obtain

$$\vdash A(\mathbf{y}) \wedge K(S(x), \mathbf{y}, w) \Leftrightarrow K(S(x), \mathbf{y}, w)$$

by the same argument as above. Hence,

$$\lceil \sigma_A(x, \mathbf{y}, u, \mathbf{v}); K(x, \mathbf{y}, w) \rceil = \lceil K(S(x), \mathbf{y}, w) \rceil$$

as morphisms in $\mathscr{C}(\mathbb{T})$. Therefore, in order to show that (3.2.10) commutes, it suffices to show that

$$\vdash K(S(x), \mathbf{y}, w) \Leftrightarrow (\exists r)(K(x, \mathbf{y}, r) \wedge H(r, w)), \tag{3.2.11}$$

holds in $\mathbb{T}$.

In order to prove the forward implication of (3.2.11), note first that if $b, c \in \mathbb{N}$ encode some sequence $m_0, \ldots, m_n$ of natural numbers via β, then b, c also encode any shorter sequence of the form $m_0, \ldots, m_k$ for $k \leq n$. A similar situation is true for encodings via Λ in $\mathbb{T}$. We have

$$K(S(x), \mathbf{y}, w) \mid\!\overset{a_0, a_1}{\overline{}}\; K'(S(x), \mathbf{y}, w, a_0, a_1)$$

for some a_0, a_1 encoding the sequence $\mathbf{w}$ determined by $\mathbf{y}$, G, and H and ending with the element w of index $S(x)$. Since $\vdash x < S(x)$ by Proposition 2.2.2.8, it follows from the third subformula of K' and condition (P3) for Λ that

$$K(S(x), \mathbf{y}, w) \mid\!\overset{a_0, a_1, b}{\overline{}}\; \Lambda(a_0, a_1, x, b) \wedge H(b, w),$$

where b is the element of the sequence $\mathbf{w}$ with index x. Since a_0, a_1 also encode in $\mathbb{T}$ the sequence obtained from $\mathbf{w}$ by removing all elements with index greater than x, we obtain

$$K(S(x), \mathbf{y}, w) \mid\!\overset{a_0, a_1, b}{\overline{}}\; K'(x, \mathbf{y}, b, a_0, a_1).$$

It then follows that

$$K(S(x), \mathbf{y}, w) \mid\!\overset{a_0, a_1, b}{\overline{}}\; K(x, \mathbf{y}, b) \wedge H(b, w),$$

and so also

$$\vdash K(S(x), \mathbf{y}, w) \Rightarrow (\exists r)(K(x, \mathbf{y}, r) \wedge H(r, w)),$$

using the rules for $\exists$ in $\mathbb{T}$.

In order to show the converse implication, first note that

$$(\exists r)(K(x, \mathbf{y}, r) \wedge H(r, w)) \mid\!\overset{a, b_0, b_1}{\overline{}}\; K'(x, \mathbf{y}, a, b_0, b_1) \wedge H(a, w),$$

where b_0, b_1 encode the relevant sequence $\mathbf{v}$ ending with the element a of index x. We then use (2.4.12) from Lemma 2.4.1.15 in order to obtain an encoding c_0, c_1 of the sequence obtained by appending w to the end of the sequence $\mathbf{v}$. We can thus show

$$(\exists r)(K(x, \mathbf{y}, r) \wedge H(r, w)) \mid\!\overset{a, b_0, b_1, c_0, c_1}{\overline{}}\; K'(S(x), \mathbf{y}, w, c_0, c_1),$$

from which

$$\vdash (\exists r)(K(x,\mathbf{y},r) \wedge H(r,w)) \Rightarrow K(S(x),\mathbf{y},w)$$

follows. Hence, (3.2.11) holds, and so diagram (3.2.10) commutes in $\mathscr{C}(\mathbb{T})$.

It remains to show that $\ulcorner K(x,\mathbf{y},w)\urcorner : N(x) \wedge A(\mathbf{y}) \to B(z)$ is the unique morphism of $\mathscr{C}(\mathbb{T})$ making diagrams (3.2.8) and (3.2.10) commute. Suppose that $\ulcorner L(x,\mathbf{y},w)\urcorner : N(x) \wedge A(\mathbf{y}) \to B(z)$ is another morphism making diagrams (3.2.8) and (3.2.10) commute. Hence, (3.2.9) and (3.2.11) hold for L as well. That is to say,

$$\vdash L(0,\mathbf{y},w) \Leftrightarrow G(\mathbf{y},w) \tag{3.2.12}$$

and

$$\vdash L(S(x),\mathbf{y},w) \Leftrightarrow (\exists r)(L(x,\mathbf{y},r) \wedge H(r,w)) \tag{3.2.13}$$

hold in $\mathbb{T}$. We show $\vdash K(x,\mathbf{y},w) \Leftrightarrow L(x,\mathbf{y},w)$ by induction on x in $\mathbb{T}$. It follows from (3.2.9), (3.2.12), and ($\forall$-I) that

$$\vdash (\forall w)(K(0,\mathbf{y},w) \Leftrightarrow L(0,\mathbf{y},w))$$

holds in $\mathbb{T}$. Using (3.2.11) and (3.2.13) we obtain

$$\vdash (\forall w)(K(x,\mathbf{y},w) \Leftrightarrow L(x,\mathbf{y},w)) \Rightarrow (\forall w)(K(S(x),\mathbf{y},w) \Leftrightarrow L(S(x),\mathbf{y},w)).$$

By induction on x in $\mathbb{T}$, we thus obtain

$$\vdash (\forall w)(K(x,\mathbf{y},w) \Leftrightarrow L(x,\mathbf{y},w)),$$

from which it follows by ($\forall$-E) that

$$\vdash K(x,\mathbf{y},w) \Leftrightarrow L(x,\mathbf{y},w)$$

holds in $\mathbb{T}$. Hence, $\ulcorner K(x,\mathbf{y},w)\urcorner = \ulcorner L(x,\mathbf{y},w)\urcorner$, and so $\ulcorner K(x,\mathbf{y},w)\urcorner$ is indeed the unique morphism of $\mathscr{C}(\mathbb{T})$ making diagrams (3.2.8) and (3.2.10) commute. ∎

We have thus far only considered the commutativity of diagram (3.2.2) in the syntactic category $\mathscr{C}(\mathbb{T})$ of an arithmetical theory $\mathbb{T}$ with induction in the case when $B(z)$ has a single free variable. In order to show that $N(x)$ is indeed a strong natural numbers object of $\mathscr{C}(\mathbb{T})$, we also need to consider objects $B(\mathbf{z})$ with any finite number k of free variables. Similarly to the case $k = 1$ considered in Lemmas 3.2.0.4 and 3.2.0.5 above, given morphisms $\ulcorner G(\mathbf{y},\mathbf{w})\urcorner : A(\mathbf{y}) \to B(\mathbf{z})$ and $\ulcorner H(\mathbf{z},\mathbf{w})\urcorner : B(\mathbf{z}) \to B(\mathbf{z})$ (where $|\mathbf{z}| = k \geq 1$) in $\mathscr{C}(\mathbb{T})$, we need to define a formula $K_k(x,\mathbf{y},\mathbf{w})$ which is a provably functional relation from $N(x) \wedge A(\mathbf{y})$ to $B(\mathbf{z})$ and is such that for each $n \in \mathbb{N}$, $K_k(\overline{n},\mathbf{y},\mathbf{w})$ encodes in $\mathbb{T}$ a sequence

$$w_0^0, \ldots, w_{k-1}^0, w_0^1, \ldots, w_{k-1}^1, \ldots, w_0^n, \ldots, w_{k-1}^n,$$

i.e. a sequence $\mathbf{w^0}, \ldots, \mathbf{w^n}$, such that

$$A(\mathbf{y}) \vdash G(\mathbf{y}, \mathbf{w^0}) \wedge \left(\bigwedge_{j=0}^{n-1} H(\mathbf{w^j}, \mathbf{w^{j+1}}) \right)$$

and $\mathbf{w^n}$ is $\mathbf{w}$. The case $k = 0$ is dealt with separately since there is no sequence to encode.

In order to generalise Lemmas 3.2.0.4 and 3.2.0.5 to the case when $B(\mathbf{z})$ has any finite number of free variables, we first need to give generalised versions of (2.4.9) and (2.4.12).

Lemma 3.2.0.6 *Let $\mathbb{T}$ be an arithmetical theory with induction. Let $k \geq 1$ and let $\mathbf{y}$ denote the list $y_0, \ldots, y_{k-1}$ of k distinct variables. Then,*

$$\vdash (\forall \mathbf{y})(\exists u, v) \left(\bigwedge_{j=0}^{k-1} \Lambda(u, v, \overline{j}, y_j) \right) \tag{3.2.14}$$

and

$$\vdash (\forall x, u, v, \mathbf{y})(\exists u', v') \left[(\forall w, z)(w \leq x \wedge \Lambda(u, v, w, z) \Rightarrow \Lambda(u', v', w, z)) \wedge \bigwedge_{j=0}^{k-1} \Lambda(u', v', S(x) + \overline{j}, y_j) \right] \tag{3.2.15}$$

hold in $\mathbb{T}$.

Proof (3.2.14) and (3.2.15) follow from (2.4.9) and (2.4.12) by induction on k. The proof is straightforward and thus omitted. ∎

We can now generalise Lemma 3.2.0.4 by constructing K_k for each $k \geq 0$.

Lemma 3.2.0.7 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ with induction, let $A(\mathbf{y})$ and $B(\mathbf{z})$ be any objects of $\mathscr{C}(\mathbb{T})$, and let $\lceil G(\mathbf{y}, \mathbf{w}) \rceil : A(\mathbf{y}) \to B(\mathbf{z})$ and $\lceil H(\mathbf{z}, \mathbf{w}) \rceil : B(\mathbf{z}) \to B(\mathbf{z})$ be morphisms of $\mathscr{C}(\mathbb{T})$.*

(i) Suppose first that B has no free variables. Then, we have morphisms $\lceil G(\mathbf{y}) \rceil : A(\mathbf{y}) \to B$ and $\lceil H \rceil : B \to B$. Define

$$K_0(x, \mathbf{y}) \underset{\text{def}}{\equiv} G(\mathbf{y}) \wedge ((\exists x_0)(x = S(x_0)) \Rightarrow H).$$

Then, $\lceil K_0(x, \mathbf{y}) \rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to B.

(ii) Suppose that B has exactly $k \geq 1$ free variables, namely $z_0, \ldots, z_{k-1}$. Let Λ be the formula strongly representing β in $\mathbb{T}$, as defined in Lemma 2.4.1.12. Define

$$K'_k(x, \mathbf{y}, \mathbf{w}, q_0, q_1) \underset{\text{def}}{\equiv} (\exists \tilde{\mathbf{w}}) \left(\bigwedge_{j=0}^{k-1} \Lambda(q_0, q_1, \overline{j}, \tilde{w}_j) \wedge G(\mathbf{y}, \tilde{\mathbf{w}}) \right) \wedge \bigwedge_{j=0}^{k-1} \Lambda(q_0, q_1, (x \cdot \overline{k}) + \overline{j}, w_j)$$

$$\wedge(\forall z)\left(z < x \Rightarrow (\exists \mathbf{p}, \mathbf{p}')\left(\bigwedge_{j=0}^{k-1} \Lambda(q_0, q_1, (z \cdot \overline{k}) + \overline{j}, p_j) \wedge \bigwedge_{j=0}^{k-1} \Lambda(q_0, q_1, (S(z) \cdot \overline{k}) + \overline{j}, p'_j) \wedge H(\mathbf{p}, \mathbf{p}')\right)\right)$$

and

$$K_k(x, \mathbf{y}, \mathbf{w}) \underset{\text{def}}{\equiv} (\exists q_0, q_1) K'(x, \mathbf{y}, \mathbf{w}, q_0, q_1).$$

Then, $\lceil K_k(x, \mathbf{y}, \mathbf{w}) \rceil$ *is a morphism in* $\mathscr{C}(\mathbb{T})$ *from* $N(x) \wedge A(\mathbf{y})$ *to* $B(\mathbf{z})$*. In particular, we have that* $\lceil K_1(x, \mathbf{y}, w) \rceil = \lceil K(x, \mathbf{y}, w) \rceil$*, where* $K(x, \mathbf{y}, w)$ *is defined as in Lemma 3.2.0.4.*

Proof (i) We show that $K_0(x, \mathbf{y})$ satisfies defining conditions (1) and (2) for a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to B (recall that defining condition (3) is simply omitted as B has no free variables).

(1) Since $N(x) \underset{\text{def}}{\equiv} x = x$ is provably true in $\mathbb{T}$ by (=-I), we obtain $K_0(x, \mathbf{y}) \vdash N(x)$. Moreover, since $K_0(x, \mathbf{y}) \vdash G(\mathbf{y})$ by ($\wedge$-E) and $G(\mathbf{y}) \vdash A(\mathbf{y}) \wedge B$ by defining condition (1) for G, it follows that $K_0(x, \mathbf{y}) \vdash (N(x) \wedge A(\mathbf{y})) \wedge B$. Hence, defining condition (1) for $K_0(x, \mathbf{y})$ is satisfied.

(2) Since $N(x)$ is provably true in $\mathbb{T}$ by (=-I) and B has no free variables, it suffices to show that $A(\mathbf{y}) \vdash K_0(x, \mathbf{y})$. We obtain

$$A(\mathbf{y}) \vdash G(\mathbf{y})$$

by defining condition (2) for G, we obtain

$$G(\mathbf{y}) \vdash B$$

by defining condition (1) for G, and we obtain

$$B \vdash H$$

by defining condition (2) for H. Hence, we obtain

$$A(\mathbf{y}) \vdash H$$

by (Cut), from which it follows that

$$A(\mathbf{y}) \vdash (\exists x_0)(x = S(x_0)) \Rightarrow H$$

by ($\Rightarrow$-I). Hence, we obtain

$$A(\mathbf{y}) \vdash K_0(x, \mathbf{y})$$

by ($\wedge$-I), and so defining condition (2) for K_0 is satisfied.

Hence, $\ulcorner K_0(x, \mathbf{y}) \urcorner$ is indeed a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to B.

(ii) Suppose first that $k = 1$. Let z denote the unique free variable of B and note that

$$K_1'(x, \mathbf{y}, w, q_0, q_1) \underset{\text{def}}{\equiv} (\exists \tilde{w})(\Lambda(q_0, q_1, 0, \tilde{w}) \wedge G(\mathbf{y}, \tilde{w})) \wedge \Lambda(q_0, q_1, (x \cdot \overline{1}) + 0, w)$$
$$\wedge (\forall z)(z < x \Rightarrow (\exists p, p')(\Lambda(q_0, q_1, (z \cdot \overline{1}) + 0, p) \wedge \Lambda(q_0, q_1, (S(z) \cdot \overline{1}) + 0, p') \wedge H(p, p'))).$$

Since $\vdash (x \cdot \overline{1}) + 0 = x$ holds in any arithmetical theory $\mathbb{T}$ by Lemma 2.2.2.7 and (M3), we have that

$$\vdash K_1'(x, \mathbf{y}, w, q_0, q_1) \Leftrightarrow K'(x, \mathbf{y}, w, q_0, q_1),$$

from which it follows that

$$\vdash K_1(x, \mathbf{y}, w) \Leftrightarrow K(x, \mathbf{y}, w).$$

Hence, $\ulcorner K_1(x, \mathbf{y}, w) \urcorner = \ulcorner K(x, \mathbf{y}, w) \urcorner$, and so it follows from Lemma 3.2.0.4 that $\ulcorner K_1(x, \mathbf{y}, w) \urcorner$ is also a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(z)$.

Now suppose that $k \geq 2$. We must show that $K_k(x, \mathbf{y}, \mathbf{w})$ satisfies defining conditions (1)–(3) for a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(\mathbf{z})$. It is straightforward to adapt the proof of defining conditions (1)–(3) for $K(x, \mathbf{y}, w)$ in Lemma 3.2.0.4 to show that $K_k(x, \mathbf{y}, \mathbf{w})$ also satisfies defining conditions (1)–(3). For defining condition (1), since the definition of K_k is a generalisation of the definition of K, it suffices to consider, whenever appropriate, sequences of variables of length k instead of single variables and finite conjunctions of the form $\bigwedge_{j=0}^{k-1}(t_0, t_1, t_2^j, t_3^j)$ instead of single terms of the form $\Lambda(t_0, t_1, t_2, t_3)$. For defining condition (2), in addition to the differences noted for defining condition (1), we merely need to use (3.2.14) and (3.2.15) from Lemma 3.2.0.6 instead of (2.4.9) and (2.4.12), respectively. For defining condition (3), we use a generalisation of (3.2.7), namely

$$K_k'(x, \mathbf{y}, \mathbf{w}, q_0, q_1), K_k'(x, \mathbf{y}, \mathbf{w}', q_0', q_1')$$
$$\vdash (\forall v, u)(v \leq (x \cdot \overline{k}) + \overline{k-1} \wedge \Lambda(q_0, q_1, v, u) \Rightarrow \Lambda(q_0', q_1', v, u)),$$

instead of (3.2.7), but otherwise adapt the proof of defining condition (3) from Lemma 3.2.0.4 in the same way as for defining conditions (1) and (2).

Hence, $K_k(x, \mathbf{y}, \mathbf{w})$ satisfies defining conditions (1)–(3), and so $\ulcorner K(x, \mathbf{y}, \mathbf{w}) \urcorner$ is indeed a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(\mathbf{z})$. ∎

We can now generalise Lemma 3.2.0.5 to objects B with any finite number of free variables, thereby showing that $N(x)$ is indeed a strong natural numbers object of the syntactic category $\mathscr{C}(\mathbb{T})$ of any arithmetical theory $\mathbb{T}$ with induction.

Theorem 3.2.0.8 *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ with induction, let $A(\mathbf{y})$ and $B(\mathbf{z})$ be objects of $\mathscr{C}(\mathbb{T})$, and let $\ulcorner G(\mathbf{y},\mathbf{w})\urcorner : A(\mathbf{y}) \to B(\mathbf{z})$ and $\ulcorner H(\mathbf{z},\mathbf{w})\urcorner : B(\mathbf{z}) \to B(\mathbf{z})$ be be morphisms of $\mathscr{C}(\mathbb{T})$. Let k be the number of free variables of B (i.e. $k = |\mathbf{z}|$ and $\mathbf{z}$ denotes the list $z_0, \ldots, z_{k-1}$) and let $K_k(x,\mathbf{y},\mathbf{w})$ be the corresponding formula defined in Lemma 3.2.0.7. Then, $\ulcorner K_k(x,\mathbf{y},\mathbf{w})\urcorner : N(x) \wedge A(\mathbf{y}) \to B(\mathbf{z})$ is the unique morphism in $\mathscr{C}(\mathbb{T})$ making the diagram*

$$\begin{array}{ccccc} A(\mathbf{y}) & \xrightarrow{\ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v})\urcorner} & N(x)\wedge A(\mathbf{y}) & \xrightarrow{\ulcorner\sigma_A(x,\mathbf{y},u,\mathbf{v})\urcorner} & N(x)\wedge A(\mathbf{y}) \\ & \searrow^{\ulcorner G(\mathbf{y},\mathbf{w})\urcorner} & \downarrow{\scriptstyle \ulcorner K_k(x,\mathbf{y},\mathbf{w})\urcorner} & & \downarrow{\scriptstyle \ulcorner K_k(x,\mathbf{y},\mathbf{w})\urcorner} \\ & & B(\mathbf{z}) & \xrightarrow[\ulcorner H(\mathbf{z},\mathbf{w})\urcorner]{} & B(\mathbf{z}) \end{array} \tag{3.2.16}$$

commute in $\mathscr{C}(\mathbb{T})$.

Hence, $N(x)$, together with the morphisms $\ulcorner \underline{0}(u)\urcorner : \top \to N(x)$ and $\ulcorner \sigma(x,u)\urcorner : N(x) \to N(x)$, is a strong natural numbers object of $\mathscr{C}(\mathbb{T})$.

Proof Note first that, by the same argument as in the proof of Lemma 3.2.0.5, for any morphism $\ulcorner L(x,\mathbf{y},\mathbf{w})\urcorner : N(x) \wedge A(\mathbf{y}) \to B(\mathbf{z})$ in $\mathscr{C}(\mathbb{T})$,

$$\ulcorner \underline{0}_A(\mathbf{y},u,\mathbf{v}); L(x,\mathbf{y},\mathbf{w})\urcorner = \ulcorner L(0,\mathbf{y},\mathbf{w})\urcorner$$

and

$$\ulcorner \sigma_A(x,\mathbf{y},u,\mathbf{v}); L(S(x),\mathbf{y},\mathbf{w})\urcorner = \ulcorner L(S(x),\mathbf{y},\mathbf{w})\urcorner .$$

Hence, $\ulcorner L(x,\mathbf{y},\mathbf{w})\urcorner$ makes diagram (3.2.16) commute if and only if $L(x,\mathbf{y},\mathbf{w})$ satisfies

$$\vdash L(0,\mathbf{y},\mathbf{w}) \Leftrightarrow G(\mathbf{y},\mathbf{w}) \tag{3.2.17}$$

and

$$\vdash L(S(x),\mathbf{y},\mathbf{w}) \Leftrightarrow (\exists \mathbf{r})(L(x,\mathbf{y},\mathbf{r}) \wedge H(\mathbf{r},\mathbf{w})). \tag{3.2.18}$$

Therefore, it suffices to show that $K_k(x,\mathbf{y},\mathbf{w})$ satisfies (3.2.17) and (3.2.18) and that, if $\ulcorner L(x,\mathbf{y},\mathbf{w})\urcorner : N(x) \wedge A(\mathbf{y}) \to B(\mathbf{z})$ is a morphism of $\mathscr{C}(\mathbb{T})$ such that $L(x,\mathbf{y},\mathbf{w})$ satisfies (3.2.17) and (3.2.18), then

$$\vdash K_k(x,\mathbf{y},\mathbf{w}) \Leftrightarrow L(x,\mathbf{y},\mathbf{z})$$

holds in $\mathbb{T}$.

We first show that, for all $k \geq 0$, $K_k(x, \mathbf{y}, \mathbf{w})$ satisfies (3.2.17) and (3.2.18). Suppose first that $k = 0$. We begin by showing that $K_0(x, \mathbf{y})$ satisfies (3.2.17). By ($\wedge$-E), we obtain

$$K_0(0, \mathbf{y}) \vdash G(\mathbf{y}).$$

Moreover, since $\vdash 0 \neq S(x_0)$ by (M1), it follows that $\vdash (\exists x_0)(0 = S(x_0)) \Rightarrow H$ holds in $\mathbb{T}$ by (Con). Hence, we obtain

$$G(\mathbf{y}) \vdash K_0(0, \mathbf{y}),$$

and so

$$\vdash K_0(0, \mathbf{y}) \Leftrightarrow G(\mathbf{y})$$

follows. Thus, $K_0(x, \mathbf{y})$ indeed satisfies (3.2.17). We next show that $K_0(x, \mathbf{y})$ satisfies (3.2.18). That is to say, we show

$$\vdash K_0(S(x), \mathbf{y}) \Leftrightarrow K_0(x, \mathbf{y}) \wedge H.$$

Recall from Lemma 3.2.0.7 that

$$K_0(S(x), \mathbf{y}) \underset{\text{def}}{\equiv} G(\mathbf{y}) \wedge (\exists x_0)(S(x) = S(x_0)) \Rightarrow H.$$

Hence, we obtain

$$K_0(x, \mathbf{y}) \wedge H \vdash K_0(S(x), \mathbf{y})$$

by ($\wedge$-E), ($\Rightarrow$-I), and ($\wedge$-I). Conversely, we obtain $\vdash (\exists x_0)(S(x) = S(x_0))$ by (=-I) and ($\exists$-I). Hence, we obtain $K_0(S(x), \mathbf{y}) \vdash H$ by ($\wedge$-E) and ($\Rightarrow$-E), and so it follows that

$$K_0(S(x), \mathbf{y}) \vdash G(\mathbf{y}) \wedge (\exists x_0)(x = S(x_0)) \Rightarrow H$$

by ($\Rightarrow$-I), ($\wedge$-E), and ($\wedge$-I). Hence, we obtain

$$K_0(S(x), \mathbf{y}) \vdash K_0(x, \mathbf{y}) \wedge H$$

by ($\wedge$-I) and the definition of $K_0(x, \mathbf{y})$, and so

$$\vdash K_0(S(x), \mathbf{y}) \Leftrightarrow K_0(x, \mathbf{y}) \wedge H$$

follows. Hence, $\lceil K_0(x, \mathbf{y}) \rceil$ indeed makes diagram (3.2.16) commute in $\mathbb{T}$ when $k = 0$.

Suppose that $k = 1$. Since $\lceil K_1(x, \mathbf{y}, w) \rceil = \lceil K(x, \mathbf{y}, w) \rceil$ by Lemma 3.2.0.7, Lemma 3.2.0.5 holds with $\lceil K_1(x, \mathbf{y}, w) \rceil$ instead of $\lceil K(x, \mathbf{y}, w) \rceil$. Hence, $\lceil K_1(x, \mathbf{y}, w) \rceil$ indeed makes diagram (3.2.16) commute and, in particular, $K_1(x, \mathbf{y}, w)$ satisfies (3.2.17) and (3.2.18).

Suppose that $k \geq 2$. We can generalise the argument in the proof of Lemma 3.2.0.5 to show that $K_k(x, \mathbf{y}, \mathbf{w})$ satisfies (3.2.17) and (3.2.18) in the same way that we generalised the argument from the proof of Lemma 3.2.0.4 in order to prove Lemma 3.2.0.7

(ii). In particular, we again use (3.2.15) from Lemma 3.2.0.6 instead of (2.4.12) from Lemma 2.4.1.15.

So, for all $k \geq 0$, $K_k(x, \mathbf{y}, \mathbf{w})$ satisfies (3.2.17) and (3.2.18), and so $\lceil K_k(x, \mathbf{y}, \mathbf{w}) \rceil$ makes diagram (3.2.16) commute in $\mathscr{C}(\mathbb{T})$ for all $k \geq 0$. Now let $k \geq 0$ and suppose that $\lceil L(x, \mathbf{y}, \mathbf{w}) \rceil : N(x) \wedge A(\mathbf{y}) \to B(\mathbf{z})$ is a morphism of $\mathscr{C}(\mathbb{T})$ such that $L(x, \mathbf{y}, \mathbf{w})$ satisfies (3.2.17) and (3.2.18), that is, $\lceil L(x, \mathbf{y}, \mathbf{w}) \rceil$ makes diagram (3.2.16) commute. The same argument by induction on x in $\mathbb{T}$ as in the proof of Lemma 3.2.0.5 shows that

$$\vdash K_k(x, \mathbf{y}, \mathbf{w}) \Leftrightarrow L(x, \mathbf{y}, \mathbf{z})$$

holds in $\mathbb{T}$. Hence, $\lceil K_k(x, \mathbf{x}, \mathbf{w}) \rceil$ is indeed the unique morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(\mathbf{z})$ making diagram (3.2.16) commute.

Therefore, $N(x)$ is a strong natural numbers object of $\mathscr{C}(\mathbb{T})$. ■

Let $\mathbb{T}$ be an arithmetic theory with induction. Now that we have shown that $N(x) \underset{\text{def}}{\equiv} x = x$, together with the morphisms $\lceil \underline{0}(u) \rceil : \top \to N(x)$ and $\lceil \sigma(x, u) \rceil : N(x) \to N(x)$ from Lemma 3.2.0.3, is a strong natural numbers object of $\mathscr{C}(\mathbb{T})$, we can consider the associated numerals in $\mathscr{C}(\mathbb{T})$, as defined in Definition 3.2.0.2.

Lemma 3.2.0.9 *Let $\mathbb{T}$ be an arithmetical theory with induction. Recall from Theorem 3.2.0.8 that $N(x) \underset{\text{def}}{\equiv} x = x$, together with the morphisms $\lceil \underline{0}(u) \rceil : \top \to N(x)$ and $\lceil \sigma(x, u) \rceil : N(x) \to N(x)$ from Lemma 3.2.0.3, is a strong natural numbers object of $\mathscr{C}(\mathbb{T})$. For each $n \in \mathbb{N}$, let*

$$\underline{n}(u) \underset{\text{def}}{\equiv} \overline{n} = u.$$

Then, for each $n \in \mathbb{N}$, the n^{th} numeral of $\mathscr{C}(\mathbb{T})$ is the morphism

$$\lceil \underline{n}(u) \rceil : \top \to N(x).$$

Proof Note first that it easily follows from the rules for equality in $\mathbb{T}$ that $\lceil \underline{n}(u) \rceil$ is a morphism from $\top$ to $N(x)$ in $\mathscr{C}(\mathbb{T})$ for all $n \in \mathbb{N}$ (in fact, this is true even when $\mathbb{T}$ does not have induction).

We proceed by induction on $n \in \mathbb{N}$. By Definition 3.2.0.2, the 0^{th} numeral of $\mathscr{C}(\mathbb{T})$ is the morphism

$$\lceil \underline{0}(u) \rceil : \top \to N(x),$$

where $\underline{0}(u) \underset{\text{def}}{\equiv} 0 = u$ as defined in Lemma 3.2.0.3. Now let $n \in \mathbb{N}$ and suppose that the n^{th} numeral of $\mathscr{C}(\mathbb{T})$ is equal to the morphism

$$\lceil \underline{n}(u) \rceil : \top \to N(x).$$

By Definition 3.2.0.2, the $(n+1)^{\text{th}}$ numeral of $\mathscr{C}(\mathbb{T})$ is then the morphism

$$\lceil \underline{n}(u); \sigma(x, u) \rceil : \top \to N(x),$$

where $\sigma(x,u) \underset{\text{def}}{\equiv} S(x) = u$ as defined in Lemma 3.2.0.3. Note that

$$\vdash (\exists q)(\overline{n} = q \wedge S(q) = u) \Leftrightarrow \overline{n+1} = u$$

by the definition of numerals in $\mathbb{T}$ (see Definition 2.2.2.5) and the rules for equality and $\exists$. Hence, $\lceil \underline{n}(u); \sigma(x,u) \rceil = \lceil \underline{n+1}(u) \rceil$, and so the $(n+1)^{\text{th}}$ numeral of $\mathscr{C}(\mathbb{T})$ is in fact the morphism

$$\lceil \underline{n+1}(u) \rceil : \top \to N(x).$$

Hence, it follows that the n^{th} numeral of $\mathscr{C}(\mathbb{T})$ is the morphism

$$\lceil \underline{n}(u) \rceil : \top \to N(x)$$

for all $n \in \mathbb{N}$. ■

In fact, if $\mathbb{T}$ is an intuitionistic arithmetical theory with induction, we can show that the numerals of $\mathscr{C}(\mathbb{T})$ are standard.

Theorem 3.2.0.10 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory. Then, the morphisms $\top$ to $N(x)$ are precisely the morphisms $\lceil \underline{n}(u) \rceil : \top \to N(x)$ for $n \in \mathbb{N}$. Hence, if $\mathbb{T}$ has induction, the numerals of $\mathscr{C}(\mathbb{T})$ are standard.*

Proof Let $\lceil F(u) \rceil : \top \to N(x)$ be a morphism in $\mathscr{C}(\mathbb{T})$. We wish to show that there exists an $n \in \mathbb{N}$ such that $\lceil F(u) \rceil = \lceil \underline{n}(u) \rceil$ as morphisms in $\mathscr{C}(\mathbb{T})$ from $\top$ to $N(x)$. Since $\lceil F(u) \rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$, defining condition (2) holds for F in $\mathbb{T}$. Since $\top$ is a closed theorem of $\mathbb{T}$, it follows that $\vdash (\exists u)F(u)$ holds in $\mathbb{T}$. Since the existence property holds in $\mathbb{T}$ as $\mathbb{T}$ is an intuitionistic theory (see Section 2.3.3), there exists an $n \in \mathbb{N}$ such that $\vdash F(\overline{n})$ holds in $\mathbb{T}$. We wish to show that

$$\vdash F(u) \Leftrightarrow \overline{n} = u.$$

Since $\vdash F(\overline{n})$ holds in $\mathbb{T}$, we it follows that $\vdash \overline{n} = u \Rightarrow F(u)$. Moreover, we obtain

$$F(u) \vdash F(\overline{n}) \wedge F(u)$$

by ($\wedge$-I), from which

$$\vdash F(u) \Rightarrow \overline{n} = u$$

follows by defining condition (3) for F and ($\Rightarrow$-I). Hence, $\vdash F(u) \Leftrightarrow \overline{n} = u$ holds in $\mathbb{T}$, and so $\lceil F(u) \rceil = \lceil \underline{n}(u) \rceil$ in $\mathscr{C}(\mathbb{T})$.

Since $\lceil \underline{n}(u) \rceil$ is a morphism from $\top$ to $N(x)$ for each $n \in \mathbb{N}$ by Lemma 3.2.0.9, it thus follows that the morphisms from $\top$ to $N(x)$ in $\mathscr{C}(\mathbb{T})$ are precisely the morphisms of the form $\lceil \underline{n}(u) \rceil$ for $n \in \mathbb{N}$.

If $\mathbb{T}$ has induction, then by Lemma 3.2.0.9, the morphisms $\lceil \underline{n}(u) \rceil : \top \to N(x)$ are precisely the numerals of $\mathscr{C}(\mathbb{T})$. Hence, the only morphisms from $\top$ to $N(x)$ in $\mathscr{C}(\mathbb{T})$ are the numerals, and so the numerals in $\mathscr{C}(\mathbb{T})$ are standard. ■

As mentioned in the proof of Lemma 3.2.0.9, the syntactic category $\mathscr{C}(\mathbb{T})$ of any arithmetical theory $\mathbb{T}$ (with or without induction) contains the morphisms $\lceil \underline{n}(u) \rceil : \top \to N(x)$ for all $n \in \mathbb{N}$. We thus allow ourselves to call the morphisms $\lceil \underline{n}(u) \rceil : \top \to N(x)$ for all $n \in \mathbb{N}$ the numerals of $\mathscr{C}(\mathbb{T})$, even when $N(x)$ was not shown to be a strong natural numbers object of $\mathbb{T}$ and $\mathscr{C}(\mathbb{T})$ does not technically have numerals as defined in Definition 3.2.0.2.

3.3 Turing categories

We refer to Appendix B for the definition of a Turing category and of any other notions related to (cartesian) restriction categories and Turing categories mentioned here. We also recall the following results from recursion theory.

Theorem 3.3.0.1 (Enumeration Theorem) [11, 4] *For each $k \geq 1$, there exists a partial recursive function $\Phi^{(k)} : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$, called a* universal (enumerating) function*, satisfying the following property: for each partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$, there exists a number $e \in \mathbb{N}$, called a* code *for f, such that*

$$f(\mathbf{m}) \simeq \Phi^k(e, \mathbf{m})$$

for all $\mathbf{m} \in \mathbb{N}^k$.

Note that Theorem 3.3.0.1 is a direct consequence of the Kleene Normal Form Theorem (Theorem 2.4.2.1). Indeed, given $k \geq 1$, we define $\Phi^{(k)} : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ by setting

$$\Phi^{(k)}(e, \mathbf{m}) \simeq U(\mu_n T_k(e, \mathbf{m}, n)) \tag{3.3.1}$$

for all $e \in \mathbb{N}$ and $\mathbf{m} \in \mathbb{N}^k$, where T_k is the k-ary Kleene T-predicate and U is the output function from Theorem 2.4.2.1. It then follows from Theorem 2.4.2.1 that $\Phi^{(k)}$ has the desired property stated in Theorem 3.3.0.1 for each $k \geq 1$.

We henceforth assume that the universal functions are defined according to (3.3.1) for each $k \geq 1$. We thus obtain the following standard enumeration of all partial recursive functions. For each $e, k \in \mathbb{N}$, we define the e^{th} partial recursive function of k variables to be the partial recursive function $\phi_e^{(k)} : \mathbb{N}^k \dashrightarrow \mathbb{N}$ defined as follows:

(i) when $k \geq 1$, we let

$$\phi_e^{(k)}(\mathbf{m}) \simeq \Phi^{(k)}(e, \mathbf{m}) \simeq U(\mu_n T_k(e, \mathbf{m}, n))$$

for all $\mathbf{m} \in \mathbb{N}^k$;

(ii) when $k = 0$, we let $\phi_0^{(0)} : \mathbb{N}^0 \dashrightarrow \mathbb{N}$ be the completely undefined function from $\mathbb{N}^0$ to $\mathbb{N}$ and we let

$$\phi_e^{(0)}(*) = \underline{e-1}(*) = e - 1$$

whenever $e \geq 1$.

Then, it follows from Theorem 3.3.0.1 and Lemma 2.1.2.9 that, for each $k \geq 0$, the list

$$\phi_0^{(k)}, \phi_1^{(k)}, \phi_2^{(k)}, \ldots$$

is an enumeration of all partial recursive functions of k variables, called the *standard enumeration.*

We also define the following simplified notation. For all $k \geq 1$, $e \in \mathbb{N}$ and $m \in \mathbb{N}^k$, we define

$$e \bullet_k \mathbf{m} \simeq \phi_e^{(k)}(\mathbf{m}) \simeq \Phi^{(k)}(e, \mathbf{m}).$$

Note that we may drop the subscripts if no ambiguity arises. Furthermore, when $k = 1$, we obtain a partial binary operation $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ on $\mathbb{N}$ called *Kleene application.* Generalising this terminology, we may call the partial operation $\bullet_k : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ *Kleene application of index* k for all $k \geq 1$.

The standard enumeration of partial recursive functions also satisfies the following property.

Theorem 3.3.0.2 (S-m-n Theorem) [11, 4] *For every $n, m > 0$, there exists a primitive recursive function $S_m^n : \mathbb{N}^{n+1} \to \mathbb{N}$ such that for all $e \in \mathbb{N}$, $\mathbf{k} \in \mathbb{N}^n$, and $\mathbf{p} \in \mathbb{N}^m$,*

$$S_m^n(e, \mathbf{k}) \bullet_m \mathbf{p} \simeq e \bullet_{n+m} (\mathbf{k}, \mathbf{p}). \tag{3.3.2}$$

A standard example of a Turing category is the restriction category $\mathbf{Comp}(\mathbb{N})$, also called *Kleene's First Model* in [10]. The objects of $\mathbf{Comp}(\mathbb{N})$ are the finite powers of $\mathbb{N}$ and morphisms $\mathbb{N}^k \to \mathbb{N}^j$ in $\mathbf{Comp}(\mathbb{N})$ are j-tuples of partial recursive functions in k variables. It follows from Theorems 3.3.0.1 and 3.3.0.2 that $\mathbf{Comp}(\mathbb{N})$ is a Turing category with Turing object $\mathbb{N}$ and Turing morphism given by Kleene application $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$.

Note that $\mathbf{Comp}(\mathbb{N})$ is in some sense the canonical example of a Turing category in the context of sets. We wish to construct and analogous Turing category in the context of syntactic categories. More precisely, given an arithmetical theory $\mathbb{T}$, we wish to construct a Turing category that is to the syntactic category $\mathscr{C}(\mathbb{T})$ of $\mathbb{T}$ as $\mathbf{Comp}(\mathbb{N})$ is to $\mathbf{Set}$. Note that $\mathbf{Comp}(\mathbb{N})$ is a sub restriction category of $\mathbf{Par}$, the objects of which are the finite powers of $\mathbb{N}$, which is a natural numbers object of $\mathbf{Set} = \mathbf{Tot}(\mathbf{Par})$ (see for example [12]). Furthermore, the morphisms of $\mathbf{Comp}(\mathbb{N})$ are tuples of partial recursive functions, which form a subset of the morphisms between powers of $\mathbb{N}$ in $\mathbf{Par}$ with additional properties. As explained in Remarks 3.1.1.6 and 3.1.1.6, there is an analogy between $\mathscr{C}(\mathbb{T})$ and $\mathbf{Set}$ and between $\mathscr{P}(\mathbb{T})$ and $\mathbf{Par}$. Furthermore, as shown in Theorem 3.2.0.8, $N(x) \underset{\text{def}}{\equiv} x = x$ is a strong (parameterised) natural numbers object of $\mathscr{C}(\mathbb{T}) = \mathbf{Tot}(\mathscr{P}(\mathbb{T}))$. Hence, by analogy with $\mathbf{Comp}(\mathbb{N})$ in the context of sets, we wish to consider sub restriction categories of $\mathscr{P}(\mathbb{T})$ having as objects the finite powers of $N(x)$ and determine what conditions the set of morphisms must satisfy in order for such a subcategory to be a Turing category.

In order to extend the analogy between the context of sets and the context of syntactic (partial map) categories of an arithmetical theory $\mathbb{T}$ to the Turing category $\mathbf{Comp}(\mathbb{N})$, we will need to formalise Theorems 3.3.0.1 and 3.3.0.2 in $\mathbb{T}$. We can then formalise the argument showing that $\mathbf{Comp}(\mathbb{N})$ is a Turing category in order to determine necessary and sufficient conditions for a sub restriction category of $\mathscr{P}(\mathbb{T})$ on the powers of $N(x)$ to be a Turing category.

3.3.1 Computational subcategories

We first consider the sub restriction categories of the syntactic partial map category $\mathscr{P}(\mathbb{T})$ of an arithmetical theory $\mathbb{T}$ having as objects the finite powers of $N(x)$ in more detail.

Definition 3.3.1.1 Let $\mathbb{T}$ be an arithmetical theory. For each $k \geq 0$ let $\mathbf{x}^{(k)}$ denote the list $x_1, \ldots, x_k$ of the first k variables in the standard enumeration of variables of $\mathbb{T}$ and define

$$N_k(\mathbf{x}^{(k)}) \underset{\text{def}}{\equiv} \mathbf{x}^{(k)} = \mathbf{x}^{(k)}.$$

If $k = 0$, we consider $\mathbf{x}^{(0)}$ to be the empty list and so omitted. We thus have

$$N_0 \underset{\text{def}}{\equiv} \top.$$

We let $\mathbf{P}(N)$ be the set containing precisely the objects $N_k(\mathbf{x}^{(k)})$ for all $k \geq 0$.

We henceforth assume that, unless specified otherwise, N_k is defined as above with the free variables $\mathbf{x}^{(k)}$, although we usually denote $\mathbf{x}^{(k)}$ by $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$, etc. Note also that when we consider $N_k(\mathbf{x}^{(k)})$ for $k \in \{1, 2, 3\}$, we shall generally denote x_1, x_2, x_3 by x, y, z, respectively. Furthermore, we usually drop the subscript 1, and so we denote $N_1(x_1)$ by $N(x)$. It follows that, unless explicitly specified otherwise, whenever we refer to $N_k(\mathbf{x})$ in what follows, we assume that $\mathbf{x}$ is in fact the list $\mathbf{x}^{(k)}$. □

Remark 3.3.1.2 Let $\mathbb{T}$ be an arithmetical theory. As noted in the proof of Proposition 3.1.1.15 (ii), for any object $A(\mathbf{y})$ in $\mathscr{C}(\mathbb{T})$, the product of $A(\mathbf{y})$ with itself in $\mathscr{C}(\mathbb{T})$ is of the form $A(\mathbf{y}) \wedge A(\mathbf{z})$, where $\mathbf{z}$ is a list of distinct new variables not occurring in $A(\mathbf{y})$ and of the same length as $\mathbf{y}$.

Consider the object $N(x)$ of $\mathscr{C}(\mathbb{T})$. Note that, as remarked in Definition 3.3.1.1, we assume that $N(x)$ is in fact $N_1(x_1)$. The product of zero copies of $N(x)$ is by definition a terminal object of $\mathscr{C}(\mathbb{T})$, and hence is up to isomorphism the object $N_0 \underset{\text{def}}{\equiv} \top$ of $\mathscr{C}(\mathbb{T})$. Moreover, since formulas that are equivalent in $\mathbb{T}$ and contain exactly the same number of free variables are isomorphic as objects in $\mathscr{C}(\mathbb{T})$ by Lemma 3.1.1.7 and since changing the variables of an object A yields an object A' isomorphic to A in $\mathscr{C}(\mathbb{T})$ by Remark 3.1.1.8, the product in $\mathscr{C}(\mathbb{T})$ of $k \geq 1$ copies of $N(x)$ is isomorphic to the object $N_k(\mathbf{x})$ of $\mathscr{C}(\mathbb{T})$ (where $\mathbf{x}$ is in fact the list $\mathbf{x}^{(k)}$ as remarked in Definition 3.3.1.1). Therefore, since products in categories are unique up to isomorphism, it follows that for all $k \geq 0$, the product in $\mathscr{C}(\mathbb{T})$ of k copies of $N(x)$ is in fact $N_k(\mathbf{x})$. Note that the corresponding projections are the morphisms $\lceil \pi_i(\mathbf{x}, u) \rceil : N_k(\mathbf{x}) \to N(x)$ for $1 \leq i \leq k$, where

$$\pi_i(\mathbf{x}, u) \underset{\text{def}}{\equiv} \mathbf{x} = \mathbf{x} \wedge x_i = u.$$

By an analogous argument, it is clear that for any $k, j \geq 0$, the product of $N_k(\mathbf{x}^{(k)})$ and $N_j(\mathbf{x}^{(j)})$ in $\mathscr{C}(\mathbb{T})$ is, up to isomorphism, given by the object $N_{k+j}(\mathbf{x}^{(k+j)})$, together with the obvious associated projections.

Since the products and terminal object of $\mathscr{C}(\mathbb{T})$ correspond to the partial products and restriction terminal object of $\mathscr{P}(\mathbb{T})$ and objects are isomorphic in $\mathscr{C}(\mathbb{T})$ if and only if they are isomorphic in $\mathscr{P}(\mathbb{T})$ by Proposition 3.1.2.8, this entire remark also applies to $\mathscr{P}(\mathbb{T})$.

Note also that, for all $j \geq 0$ and $k \geq 2$, given a morphism $\lceil \varphi_i(\mathbf{y}, u) \rceil : N_j(\mathbf{y}) \to N(x)$ in $\mathscr{C}(\mathbb{T})$ for each $i \in \{1, \ldots, k\}$, we have that

$$\left\lceil \bigwedge_{i=1}^{k} \varphi_i(\mathbf{y}, u_i) \right\rceil : N_j(\mathbf{y}) \to N_k(\mathbf{x})$$

is the unique morphism in $\mathscr{C}(\mathbb{T})$ such that

$$\left\lceil \left(\bigwedge_{\ell=1}^{k} \varphi_i(\mathbf{y}, u_\ell) \right) ; \pi_i(\mathbf{x}, u) \right\rceil = \lceil \varphi_i(\mathbf{y}, u) \rceil$$

for all $i \in \{1, \ldots, k\}$. In the case of $\mathscr{P}(\mathbb{T})$, we obtain a similar result, but $\left\lceil \bigwedge_{i=1}^{k} \varphi_i(\mathbf{y}, u_i) \right\rceil$ satisfies the conditions for the weaker notion of pairing in the case of partial products instead. □

Remark 3.3.1.3 Let $\mathbb{T}$ be an arithmetical theory. Note that for any $k, j \geq 0$ and lists $\mathbf{x}, \mathbf{v}$ of variables of lengths k, j, respectively, we obtain

$$\vdash N_k(\mathbf{x}) \wedge N_j(\mathbf{v})$$

by (=-I). Hence, any formula $F(\mathbf{x}, \mathbf{v})$ satisfies defining condition (1) for a morphism from $N_k(\mathbf{x})$ to $N_j(\mathbf{y})$ in $\mathscr{P}(\mathbb{T})$. Thus, in order to show that $\lceil F \rceil$ is a morphism from N_k to N_j in $\mathscr{P}(\mathbb{T})$ ($\mathscr{C}(\mathbb{T})$, respectively), it suffices to show that F satisfies defining condition (3) (defining conditions (2) and (3), respectively) for a morphism from N_k to N_j. Furthermore, since $\vdash N_k(\mathbf{x})$ holds in $\mathbb{T}$, defining condition (2) for F is equivalent to condition (P4) for F, namely $\vdash (\exists \mathbf{v}) F(\mathbf{x}, \mathbf{v})$. Since defining condition (3) for F coincides with condition (P3) for F, it follows that $\lceil F(\mathbf{x}, \mathbf{v}) \rceil$ is a morphism in $\mathscr{P}(\mathbb{T})$ ($\mathscr{C}(\mathbb{T})$, respectively) from $N_k(\mathbf{x})$ to $N_j(\mathbf{y})$ if and only if $F(\mathbf{x}, \mathbf{v})$ satisfies condition (P3) (conditions (P3) and (P4), respectively).

Furthermore, if $j = 0$, defining condition (3) is undefined and so considered omitted. Hence, if $F(\mathbf{x})$ is any formula of $\mathbb{T}$ containing exactly the variables in the list $\mathbf{x}$ free, then $\lceil F \rceil : N_k \to N_0$ is immediately a morphism in $\mathscr{P}(\mathbb{T})$. Moreover, $\lceil F \rceil : N_k \to N_0$ is total (that is, is a morphism in $\mathscr{C}(\mathbb{T})$) if and only if $F(\mathbf{x})$ satisfies condition (P4), which in this case is simply $\vdash F(\mathbf{x})$. □

Note that, since we have shown in Theorem 2.4.4.2 that any partial function that is representable in an arithmetical theory is partial recursive, it follows that we can, without loss of generality, consider only partial recursive functions in the following result.

Proposition 3.3.1.4 *Let $\mathbb{T}$ be an arithmetical theory and let $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ be a partial recursive function. If f is type-one representable in $\mathbb{T}$ by $\varphi_f(\mathbf{y}, u)$, then $\lceil \varphi_f(\mathbf{y}, u) \rceil$ is a morphism from $N_k(\mathbf{y})$ to $N(x)$ in $\mathscr{P}(\mathbb{T})$. If f is in fact strongly representable in $\mathbb{T}$ by $\varphi_f(\mathbf{y}, u)$, then $\lceil \varphi_f(\mathbf{y}, u) \rceil$ is total.*

Proof Suppose first that f is type-one representable in $\mathbb{T}$ by $\varphi_f(\mathbf{y}, u)$. Then, $\varphi_f(\mathbf{y}, u)$ satisfies condition (P3), and hence $\lceil \varphi_f(\mathbf{y}, u) \rceil$ is a morphism from $N_k(\mathbf{y})$ to $N(x)$ in $\mathscr{P}(\mathbb{T})$ as noted in Remark 3.3.1.3.

Now suppose that f is strongly representable in $\mathbb{T}$ by $\varphi_f(\mathbf{x}, v)$. Then, $\varphi_f(\mathbf{y}, u)$ satisfies conditions (P3) and (P4), and hence $\lceil \varphi_f(\mathbf{y}, u) \rceil$ is a morphism from $N_k(\mathbf{y})$ to $N(x)$ in $\mathscr{C}(\mathbb{T})$ as noted in Remark 3.3.1.3. ■

Proposition 3.3.1.5 *Let $\mathbb{T}$ be an arithmetical theory. Let $\mathscr{N}_F(\mathbb{T})$ be the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$ from Definition 3.3.1.1. Then, $\mathscr{N}_F(\mathbb{T})$ is a cartesian restriction category and a sub restriction category of $\mathscr{P}(\mathbb{T})$.*

Proof Since $\mathscr{N}_F(\mathbb{T})$ is the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$, the set of morphisms of $\mathscr{N}_F(\mathbb{T})$ is closed under the restriction operator of $\mathscr{P}(\mathbb{T})$. Moreover, conditions (R1)–(R4) are satisfied in $\mathscr{N}_F(\mathbb{T})$ by the same argument as in the proof of Proposition 3.1.2.3. Hence, $\mathscr{N}_F(\mathbb{T})$ is a restriction category. Since the restriction operator on $\mathscr{N}_F(\mathbb{T})$ is obtained by restricting the restriction operator on $\mathscr{P}(\mathbb{T})$ to the object set $\mathbf{P}(N)$, it follows immediately that the inclusion functor $\mathscr{N}_F(\mathbb{T}) \to \mathscr{P}(\mathbb{T})$ is a restriction functor, and hence $\mathscr{N}_F(\mathbb{T})$ is a sub restriction category of $\mathscr{P}(\mathbb{T})$.

Since $\mathscr{N}_F(\mathbb{T})$ is the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$ and $\mathscr{N}_F(\mathbb{T})$ is a sub restriction category of $\mathscr{P}(\mathbb{T})$, $N_0 \underset{\text{def}}{\equiv} \top$ is a restriction terminal object of $\mathscr{N}_F(\mathbb{T})$ by the same argument as in the proof of Proposition 3.1.2.12. For the same reasons, the arguments in Remark 3.3.1.2 also imply that, for each $k, j \geq 0$, N_{j+k} is a partial product of N_j and N_k in $\mathscr{N}_F(\mathbb{T})$. Hence, $\mathscr{N}_F(\mathbb{T})$ is a cartesian restriction category. ■

For any arithmetical theory $\mathbb{T}$, note that we will henceforth assume that the cartesian restriction structure of $\mathscr{N}_F(\mathbb{T})$ is specified to be the structure appearing in the proof of Proposition 3.3.1.5 and it not just defined up to isomorphism as it was in the case of $\mathscr{P}(\mathbb{T})$. The same will be true for any subcategories of $\mathscr{N}_F(\mathbb{T})$ that we will investigate in the interest of determining which ones are Turing categories.

Since we are attempting to determine which subcategories of $\mathscr{N}_F(\mathbb{T})$ are Turing categories by formalising the argument showing that $\mathbf{Comp}(\mathbb{N})$ is a Turing category, we can restrict our search to a class of subcategories of $\mathscr{N}_F(\mathbb{T})$ satisfying certain reasonable conditions, as detailed in the following definition.

Definition 3.3.1.6 Let $\mathbb{T}$ be an arithmetical theory. We say that a subcategory $\mathscr{N}(\mathbb{T})$ of $\mathscr{N}_F(\mathbb{T})$ is a *computational subcategory associated to* $\mathbb{T}$ if it satisfies the following conditions:

(i) The objects of $\mathscr{N}(\mathbb{T})$ are precisely those in the set $\mathbf{P}(N)$ given in Definition 3.3.1.1.

(ii) $\mathscr{N}(\mathbb{T})$ is a sub cartesian restriction category of $\mathscr{N}_F(\mathbb{T})$. That is to say, the inclusion functor $\mathscr{N}(\mathbb{T}) \to \mathscr{P}(\mathbb{T})$ is a cartesian restriction functor. Note in particular that the cartesian restriction structure on $\mathscr{N}(\mathbb{T})$ is hence also specified and in fact the same as the structure on $\mathscr{N}_F(\mathbb{T})$.

(iii) $\mathscr{N}(\mathbb{T})$ contains the total morphisms $\lceil \underline{0}(u) \rceil : \top \to N(x)$ and $\lceil \sigma(x,u) \rceil : N(x) \to N(x)$ defined in Lemma 3.2.0.3.

(iv) $N_k \lhd N$ in $\mathscr{N}(\mathbb{T})$ for all $k \geq 1$. □

Let $\mathscr{N}(\mathbb{T})$ be any computational subcategory associated to $\mathbb{T}$. Conditions (i) and (ii) of Definition 3.3.1.6 ensure that $\mathscr{N}(\mathbb{T})$ is a sub-cartesian restriction category of $\mathscr{P}(\mathbb{T})$ whose objects are precisely the finite powers of N, analogously to $\mathbf{Comp}(\mathbb{N})$. As shown in 3.3.1.7, condition (iii) of Definition 3.3.1.6 ensures that $\mathscr{N}(\mathbb{T})$ contains numerals, which are necessary in order to formalise the necessary basic notions and results from number theory in $\mathscr{N}(\mathbb{T})$.

Lemma 3.3.1.7 *Let $\mathbb{T}$ be an arithmetical theory and let $n \in \mathbb{N}$. As noted after Theorem 3.2.0.10, $\lceil \underline{n}(u) \rceil : \top \to N(x)$, where $\underline{n}(u) \underset{\text{def}}{\equiv} \overline{n} = u$, is a total morphism of $\mathscr{C}(\mathbb{T})$, which we call the n^{th} numeral of $\mathscr{C}(\mathbb{T})$. If $\mathscr{N}(\mathbb{T})$ is any computational subcategory associated to $\mathbb{T}$, then $\lceil \underline{n}(u) \rceil : \top \to N(x)$ is a total morphism in $\mathscr{N}(\mathbb{T})$.*

Proof This result follows from condition (iii) of Definition 3.3.1.6 via a simple argument using induction on $n \in \mathbb{N}$. ■

Furthermore, as shown in Lemma 3.3.1.8, condition (iv) of Definition 3.3.1.6 ensures that N is a universal object of $\mathscr{N}(\mathbb{T})$, which is a necessary condition that N must satisfy in order to be a Turing object of $\mathscr{N}(\mathbb{T})$.

Lemma 3.3.1.8 *Let $\mathbb{T}$ be an arithmetical theory with induction and let $\mathscr{N}(\mathbb{T})$ be any computational subcategory associated to $\mathbb{T}$. Then, $N(x)$ is a universal object of $\mathscr{N}(\mathbb{T})$.*

Proof Note that it follows from Definition 3.3.1.6 that N is a universal object of $\mathscr{N}(\mathbb{T})$ if and only if N_k is a retract of N in $\mathscr{N}(\mathbb{T})$ for all $k \geq 0$.

Let $k = 0$ and recall from Definition 3.3.1.1 that $N_0 \underset{\text{def}}{\equiv} \top$. We wish to show that $\top \lhd N(x)$. By condition (iii) of Definition 3.3.1.6, $\ulcorner \underline{0}(u) \urcorner : \top \to N(x)$, where $\underline{0}(u) \underset{\text{def}}{\equiv} 0 = u$, is a morphism of $\mathscr{N}(\mathbb{T})$. Moreover, by Proposition 3.1.1.15, the terminating morphism $\ulcorner !_N(x) \urcorner := \ulcorner N(x) \urcorner : N(x) \to \top$ is the unique total morphism from $N(x)$ to $\top$ in $\mathscr{P}(\mathbb{T})$, and hence is a morphism of $\mathscr{N}(\mathbb{T})$ by condition (ii) of Definition 3.3.1.6. Furthermore,

$$\underline{0}; !_N \underset{\text{def}}{\equiv} \underline{0}; N \underset{\text{def}}{\equiv} (\exists q)(0 = q \wedge q = q),$$

and

$$\mathrm{id}_\top \underset{\text{def}}{\equiv} \top.$$

It clearly follows that $\ulcorner \underline{0}; !_N \urcorner = \ulcorner \mathrm{id}_\top \urcorner$, and so $(\ulcorner \underline{0} \urcorner, \ulcorner !_N \urcorner) : \top \lhd N$ in $\mathscr{N}(\mathbb{T})$.

Now let $k \geq 1$. By condition (iv) of Definition 3.3.1.6, we have that $N_k \lhd N$ in $\mathscr{N}(\mathbb{T})$.

Therefore, N_k is a retract of N in $\mathscr{N}(\mathbb{T})$ for all $k \geq 0$, and so N is a universal object of $\mathscr{N}(\mathbb{T})$. ∎

Note that any computational subcategory $\mathscr{N}(\mathbb{T})$ associated to $\mathbb{T}$ is determined entirely by its set of morphisms. In fact, it follows from Definition 3.3.1.6 and the definition of a sub cartesian restriction category (see Appendix B) that a subset M of the set of morphisms of $\mathscr{N}_F(\mathbb{T})$ is the set of morphisms of a computational subcategory $\mathscr{N}(\mathbb{T})$ if and only if M contains an embedding-retraction pair $(m, r) : N_k \lhd N$ for all $k \geq 1$, the morphisms $\ulcorner \underline{0}(u) \urcorner$ and $\ulcorner \sigma(x, u) \urcorner$ and all of the identity morphisms, projections, and terminating morphisms (i.e. total maps into $N_0 \underset{\text{def}}{\equiv} \top$) of $\mathscr{N}_F(\mathbb{T})$, and is closed under composition, pairing, and the restriction operator of $\mathscr{N}_F(\mathbb{T})$.

Now let $\mathbb{T}$ be an arithmetical theory with induction. We wish to show that $\mathscr{N}_F(\mathbb{T})$ is itself a computational subcategory associated to $\mathbb{T}$. By Proposition 3.3.1.5, $\mathscr{N}_F(\mathbb{T})$ satisfies conditions (i) and (ii) of Definition 3.3.1.6. $\mathscr{N}_F(\mathbb{T})$ also satisfies condition (iii) of Definition 3.3.1.6 by virtue of being the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$. Hence, it only remains to show that $N_k \lhd N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$. In fact, since $\mathbb{T}$ has induction, we will show a stronger result, namely that $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$.

An analogous result is true in $\mathbf{Comp}(\mathbb{N})$. Indeed, recall from Lemma 2.4.4.1 that the Cantor pairing function $J : \mathbb{N}^2 \to \mathbb{N}$ is a primitive recursive bijection. Hence, J lies in $\mathbf{Comp}(\mathbb{N})$ and can thus be used to show that $\mathbb{N}^2 \cong \mathbb{N}$ in $\mathbf{Comp}(\mathbb{N})$. Induction on k can then be used in order to show that $\mathbb{N}_k \cong \mathbb{N}$ in $\mathbf{Comp}(\mathbb{N})$ for all $k \geq 1$.

We aim to formalise this argument in $\mathscr{N}_F(\mathbb{T})$. Note first that since $\mathscr{N}_F(\mathbb{T})$ is the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$, it follows that Proposition 3.3.1.4 holds with $\mathscr{P}(\mathbb{T})$ replaced by $\mathscr{N}_F(\mathbb{T})$, and so the representing formulas of functions representable in $\mathbb{T}$ are morphisms in $\mathscr{N}_F(\mathbb{T})$. Note also that, as shown in

Lemma 3.3.1.10 below, provably bijective morphisms are in fact isomorphisms in syntactic categories. Hence, it suffices to find a provably bijective representing formula of J in $\mathbb{T}$ in order to show that $N_2 \cong N$ in $\mathscr{N}_F(\mathbb{T})$.

Definition 3.3.1.9 Let $\mathbb{T}$ be a theory and let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be a morphism in $\mathscr{P}(\mathbb{T})$.

(i) $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is said to be *provably injective* in $\mathbb{T}$ if

$$\vdash F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v}) \Rightarrow \mathbf{x} = \mathbf{x}'$$

holds in $\mathbb{T}$.

(ii) $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is said to be *provably surjective* in $\mathbb{T}$ if

$$\vdash B(\mathbf{y}) \Rightarrow (\exists \mathbf{p})F(\mathbf{p},\mathbf{y}))$$

holds in $\mathbb{T}$.

Note that if $B(\mathbf{y})$ is provably true in $\mathbb{T}$, $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is provably surjective in $\mathbb{T}$ if and only if

$$\vdash (\exists \mathbf{p})F(\mathbf{p},\mathbf{y})$$

holds in $\mathbb{T}$.

(iii) $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is said to be *provably bijective* in $\mathbb{T}$ if it is both provably injective and provably surjective in $\mathbb{T}$. □

Lemma 3.3.1.10 *Let $\mathbb{T}$ be a theory and let $\lceil F(\mathbf{x},\mathbf{v})\rceil : A(\mathbf{x}) \to B(\mathbf{y})$ be a total morphism in $\mathscr{P}(\mathbb{T})$. If $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is provably bijective in $\mathbb{T}$, then $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is an isomorphism in $\mathscr{P}(\mathbb{T})$ with inverse $\lceil F^{-1}(\mathbf{y},\mathbf{u})\rceil : B(\mathbf{y}) \to A(\mathbf{x})$, where $F^{-1}(\mathbf{y},\mathbf{u}) \underset{\text{def}}{\equiv} F(\mathbf{u},\mathbf{y})$.*

Proof Since $\lceil F(\mathbf{x},\mathbf{v})\rceil$ is provably bijective in $\mathbb{T}$, it follows from Definition 3.3.1.9 that

$$\vdash F(\mathbf{x},\mathbf{v}) \wedge F(\mathbf{x}',\mathbf{v}) \Rightarrow \mathbf{x} = \mathbf{x}' \tag{3.3.3}$$

and

$$\vdash B(\mathbf{y}) \Rightarrow (\exists \mathbf{p})F(\mathbf{p},\mathbf{y}) \tag{3.3.4}$$

hold in $\mathbb{T}$. Define

$$F^{-1}(\mathbf{y},\mathbf{u}) \underset{\text{def}}{\equiv} F(\mathbf{u},\mathbf{y}).$$

We first show that $\lceil F^{-1}(\mathbf{y},\mathbf{u})\rceil$ is a morphism in $\mathscr{P}(\mathbb{T})$ from $B(\mathbf{y})$ to $A(\mathbf{x})$. Defining condition (1) for F^{-1} follows immediately from defining condition (1) for F, defining condition (2) for F^{-1} corresponds to (3.3.4), and defining condition (3) for F^{-1} corresponds to (3.3.3). Thus, $\lceil F^{-1}(\mathbf{y},\mathbf{u})\rceil$ is in fact a total morphism in $\mathscr{P}(\mathbb{T})$ from $B(\mathbf{y})$ to $A(\mathbf{x})$.

We claim that $\lceil F^{-1}(\mathbf{y},\mathbf{u})\rceil$ is the inverse of $\lceil F(\mathbf{x},\mathbf{v})\rceil$ in $\mathscr{P}(\mathbb{T})$. We first show that

$$\left\lceil F(\mathbf{x},\mathbf{v}); F^{-1}(\mathbf{y},\mathbf{u})\right\rceil = \lceil \mathrm{id}_A(\mathbf{x},\mathbf{u})\rceil,$$

that is, that

$$\vdash (\exists \mathbf{q})(F(\mathbf{x},\mathbf{q}) \wedge F(\mathbf{u},\mathbf{q})) \Leftrightarrow A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$$

holds in $\mathbb{T}$. We obtain

$$F(\mathbf{x},\mathbf{b}) \wedge F(\mathbf{u},\mathbf{b}) \mathrel{|\!\!\!\overset{\mathbf{b}}{-}} A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$$

by defining condition (1) for F and (3.3.3). Hence,

$$\vdash (\exists \mathbf{q})(F(\mathbf{x},\mathbf{q}) \wedge F(\mathbf{u},\mathbf{q})) \Rightarrow A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}$$

follows by (∃-E) and (⇒-I). Conversely, we obtain

$$A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \vdash (\exists \mathbf{q}) F(\mathbf{x},\mathbf{q})$$

by defining condition (2) for F, from which

$$A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u}, F(\mathbf{x},\mathbf{b}) \mathrel{|\!\!\!\overset{\mathbf{b}}{-}} F(\mathbf{x},\mathbf{b}) \wedge F(\mathbf{u},\mathbf{b})$$

follows by (=-E) and (∧-I). Hence, we obtain

$$\vdash A(\mathbf{x}) \wedge \mathbf{x} = \mathbf{u} \Rightarrow (\exists \mathbf{q})(F(\mathbf{x},\mathbf{q}) \wedge F(\mathbf{u},\mathbf{q}))$$

by (∃-I), (∃-E), and (⇒-I). Thus, we indeed obtain

$$\left\lceil F(\mathbf{x},\mathbf{v}); F^{-1}(\mathbf{y},\mathbf{u})\right\rceil = \lceil \mathrm{id}_A(\mathbf{x},\mathbf{u})\rceil.$$

We now show that

$$\left\lceil F^{-1}(\mathbf{y},\mathbf{u}); F(\mathbf{x},\mathbf{v})\right\rceil = \lceil \mathrm{id}_B(\mathbf{y},\mathbf{v})\rceil,$$

that is, that

$$\vdash (\exists \mathbf{p})(F(\mathbf{p},\mathbf{y}) \wedge F(\mathbf{p},\mathbf{v})) \Leftrightarrow B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}$$

holds in $\mathbb{T}$. We obtain

$$F(\mathbf{a},\mathbf{y}) \wedge F(\mathbf{a},\mathbf{v}) \mathrel{|\!\!\!\overset{\mathbf{a}}{-}} B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}$$

by defining conditions (1) and (3) for F. Hence,

$$\vdash (\exists \mathbf{p})(F(\mathbf{p},\mathbf{y}) \wedge F(\mathbf{p},\mathbf{v})) \Rightarrow B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v}$$

follows by (∃-E) and (⇒-I). Conversely, we obtain

$$B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \vdash (\exists \mathbf{p}) F(\mathbf{p}, \mathbf{y})$$

by (3.3.4), from which

$$\vdash B(\mathbf{y}) \wedge \mathbf{y} = \mathbf{v} \Rightarrow (\exists \mathbf{p})(F(\mathbf{p}, \mathbf{y}) \wedge F(\mathbf{p}, \mathbf{v}))$$

follows, similarly to the case above. Thus, we indeed obtain

$$\lceil F^{-1}(\mathbf{y}, \mathbf{u}); F(\mathbf{x}, \mathbf{v}) \rceil = \lceil \mathrm{id}_B(\mathbf{y}, \mathbf{v}) \rceil,$$

and so $\lceil F^{-1}(\mathbf{y}, \mathbf{u}) \rceil$ is the inverse of $\lceil F(\mathbf{x}, \mathbf{v}) \rceil$ in $\mathscr{P}(\mathbb{T})$. Therefore, $\lceil F(\mathbf{x}, \mathbf{v}) \rceil$ is indeed an isomorphism in $\mathscr{P}(\mathbb{T})$. ■

We now construct a provably bijective representing formula for the Cantor pairing function $J : \mathbb{N}^2 \to \mathbb{N}$. Note that the construction we give only satisfies the desired conditions when $\mathbb{T}$ has induction.

Lemma 3.3.1.11 *Let $\mathbb{T}$ be an arithmetical theory with induction, let $J : \mathbb{N}^2 \to \mathbb{N}$ be the Cantor pairing function from Lemma 2.4.4.1, and define $p_J(v_1, v_2)$ to be the polynomial expression*

$$(v_1 + v_2)^2 + (v_1 + v_2) + 2v_1.$$

Note that J is in fact given by

$$J(m, n) = \frac{(m+n)^2 + (m+n) + 2m}{2} = \frac{p_J(m, n)}{2}$$

for all $m, n \in \mathbb{N}$.

(i) Let $\hat{p}_J(x, y)$ denote the term

$$(x + y)^2 + (x + y) + x \cdot \overline{2},$$

i.e. the term

$$(x + y) \cdot (x + y) + (x + y) + x \cdot \overline{2}.$$

Then,

$$\vdash \hat{p}_J(x, y) = \hat{p}_J(u, v) \Rightarrow (x = u \wedge y = v) \tag{3.3.5}$$

holds in $\mathbb{T}$.

(ii) Define

$$\varphi_J(x, y, z) \underset{\mathrm{def}}{\equiv} \hat{p}_J(x, y) = z \cdot \overline{2} \underset{\mathrm{def}}{\equiv} (x + y)^2 + (x + y) + x \cdot \overline{2} = z \cdot \overline{2}.$$

Then, $\varphi_J(x, y, z)$ strongly represents J in $\mathbb{T}$.

(iii) *By Proposition 3.3.1.4, $\ulcorner \varphi_J(x, y, u) \urcorner : N_2(x, y) \to N(x)$ is a total morphism in $\mathscr{P}(\mathbb{T})$, and hence also in $\mathscr{N}_F(\mathbb{T})$. Furthermore, $\ulcorner \varphi_J(x, y, u) \urcorner$ is provably bijective in $\mathbb{T}$, and hence an isomorphism by Lemma 3.3.1.10.*

Proof (i) Let $L : \mathbb{N}^2 \to \mathbb{N}$ be defined by

$$L(m, n) = 2 \cdot J(m, n) = p_J(m, n) = (m + n)^2 + (m + n) + 2m$$

for all $m, n \in \mathbb{N}$.

In order to show that (3.3.5) holds in $\mathbb{T}$, we will first give a simple arithmetical proof that L is injective and then formalise this proof in $\mathbb{T}$. Let $m, n, a, b \in \mathbb{N}$ and suppose that $L(m, n) = L(a, b)$. We with to show that $m = a$ and $n = b$. Suppose first that $m + n < a + b$. Then, there exists a $k \in \mathbb{N}$ such that $m + n + s(k) = a + b$, where we recall that $s : \mathbb{N} \to \mathbb{N}$ is the successor function given in Definition 2.1.2.1. It thus follows that

$$\begin{aligned} L(a, b) &= (a + b)^2 + (a + b) + 2a \\ &= ((m + n) + s(k))^2 + ((m + n) + s(k)) + 2a \\ &= (m + n)^2 + (m + n) + 2m + 2km + 2s(k)n + s(k)^2 + s(k) + 2a \\ &= L(m, n) + u \qquad \text{where } u \neq 0, \end{aligned}$$

and hence $L(m, n) < L(a, b)$. This is a contradiction since $L(m, n) = L(a, b)$, and so $m + n \not< a + b$. Similarly, $a + b \not< m + n$, and so it follows that

$$m + n = a + b.$$

Thus, we obtain

$$(m + n)^2 + (m + n) = (a + b)^2 + (a + b).$$

Hence, since

$$(m + n)^2 + (m + n) + 2m = L(m, n) = L(a, b) = (a + b)^2 + (a + b) + 2a$$

holds, it follows by the cancellation law for addition that

$$2m = 2a.$$

Since $2 \neq 0$, it thus follows by the cancellation law for multiplication that

$$m = a.$$

It remains to show that $n = b$. Suppose to the contrary that $n < b$. Then,

$$m + n < m + b = a + b,$$

a contradiction. Hence, $n \not< b$ and we obtain that $b \not< n$ by an analogous argument. Therefore, it must be true that $n = b$.

Now note that since $\mathbb{T}$ has induction and the above proof uses only the properties and laws of arithmetic and ordering that hold for variables in $\mathbb{T}$ by Proposition 2.2.2.12 and [14, Ch. VIII, §38–39], it follows that

$$\vdash [(x+y)^2 + (x+y) + x \cdot \overline{2} = (u+v)^2 + (u+v) + u \cdot \overline{2}] \Rightarrow (x = u \wedge y = v),$$

that is, (3.3.5), holds in $\mathbb{T}$.

(ii) Note first that, since $L(m,n) = p_J(m,n)$ for all $m,n \in \mathbb{N}$, it follows by Proposition 2.4.1.7 that the formula

$$\varphi_L(x,y,z) \underset{\text{def}}{\equiv} \hat{p}_J(x,y) = z$$

strongly represents L in $\mathbb{T}$. Note also that

$$\varphi_J(x,y,z) \underset{\text{def}}{\equiv} \varphi_L(x,y,z \cdot \overline{2})$$

by definition of $\varphi_J(x,y,z)$. We now show that φ_J strongly represents J in $\mathbb{T}$.

(P1') Let $m,n \in \mathbb{N}$. Since φ_L strongly represents L in $\mathbb{T}$, we obtain

$$\vdash \hat{p}_J(\overline{m},\overline{n}) = \overline{L(m,n)}$$

by condition (P1') for L. Recall that $L(m,n) = J(m,n) \cdot 2$, and hence it follows by Lemma 2.2.2.6 that $\vdash \overline{L(m,n)} = \overline{J(m,n)} \cdot \overline{2}$ holds in $\mathbb{T}$. Hence, we obtain

$$\vdash \hat{p}_J(\overline{m},\overline{n}) = \overline{J(m,n)} \cdot \overline{2},$$

and so condition (P1') for φ_J is satisfied.

(P3) We obtain

$$\varphi_J(x,y,z) \wedge \varphi_J(x,y,z') \vdash z \cdot \overline{2} = z' \cdot \overline{2}$$

by (=-E). Condition (P3) for φ_J thus follows by Proposition 2.2.2.12 (iii) and ($\Rightarrow$-I).

(P4) As in [14, §40, pp. 191–194], we can introduce the following notion of divisibility in all arithmetical theories: we let $x|y$ (read "x divides y") abbreviate the formula $(\exists z)(x \cdot z = y)$. In [9, pp. 33–35], the same notion of divisibility is introduced for classical arithmetical theories with a restricted induction schema for open formulas and is used to show that

$$\vdash (\forall x, y)(\exists z)((x + y) \cdot (x + y + \overline{1}) + \overline{2} \cdot x = \overline{2} \cdot z) \tag{3.3.6}$$

holds in these theories. Since the properties of divisibility used to show (3.3.6) in [9] hold in all arithmetical theories with induction (be they classical or intuitionistic), as shown in [14, §40, pp. 191–194], it follows that (3.3.6) holds in all arithmetical theories with induction, and so in particular in $\mathbb{T}$. Now note that we obtain

$$\vdash (x + y) \cdot (x + y + \overline{1}) + \overline{2} \cdot x = \hat{p}_J(x, y)$$

and

$$\vdash \overline{2} \cdot z = z \cdot \overline{2}$$

in $\mathbb{T}$ by Proposition 2.2.2.12 and Lemma 2.2.2.7, and hence it follows that

$$\vdash (\exists z)(\hat{p}_J(x, y) = z \cdot \overline{2}),$$

that is,

$$\vdash (\exists z)\varphi_J(x, y, z)$$

holds in $\mathbb{T}$. Thus, condition (P4) for φ_J is satisfied.

Hence, the formula $\varphi_J(x, y, z)$ indeed strongly represents the Cantor pairing function J in $\mathbb{T}$.

(iii) We first show that $\lceil \varphi_J(x, y, u) \rceil$ is provably injective in $\mathbb{T}$, that is, that

$$\vdash (\varphi_J(x, y, z) \wedge \varphi_J(u, v, z)) \Rightarrow (x = u \wedge y = v) \tag{3.3.7}$$

holds in $\mathbb{T}$. By (=-E), we obtain

$$\varphi_J(x, y, z) \wedge \varphi_J(u, v, z) \vdash \hat{p}_J(x, y) = \hat{p}_J(u, v).$$

By (3.3.5), which is shown to hold in $\mathbb{T}$ in part (i) of this proof, it follows that

$$\varphi_J(x, y, z) \wedge \varphi_J(u, v, z) \vdash x = u \wedge y = v$$

holds in $\mathbb{T}$, from which (3.3.7) follows by ($\Rightarrow$-I).

As noted in Definition 3.3.1.9, since $N(x)$ is provably true in $\mathbb{T}$, $\lceil \varphi_J(x, y, u) \rceil$ is provably surjective in $\mathbb{T}$ if and only if

$$\vdash (\exists x, y)\varphi_J(x, y, z) \tag{3.3.8}$$

holds in $\mathbb{T}$. In [9, Thm 1.18, pp. 34–35], it is shown that

$$\vdash (\forall z)(\exists x, y)((x + y) \cdot (x + y + \overline{1}) + \overline{2} \cdot x = \overline{2} \cdot z) \tag{3.3.9}$$

holds in all classical arithmetical theories with a restricted induction schema for open formulas. Note that by Proposition 2.2.2.12, the induction schema (IND), and the properties of divisibility in all arithmetical theories with induction given in [14, §40, pp. 191–194], the argument from [9, Thm 1.18, pp. 34–35] in fact applies to all arithmetical theories with induction, and so in particular (3.3.9) holds in $\mathbb{T}$. Thus, by the same argument as in the proof of condition (P4) for φ_J, it follows that (3.3.8) holds in $\mathbb{T}$, and so $\lceil \varphi_J(x, y, u) \rceil$ is in fact provably surjective in $\mathbb{T}$.

Hence, $\lceil \varphi_J(x, y, u) \rceil : N_2(x, y) \to N(x)$ is in fact provably bijective in $\mathbb{T}$, and hence an isomorphism in $\mathscr{P}(\mathbb{T})$ by Lemma 3.3.1.10. As $\mathscr{N}_F(\mathbb{T})$ is the full subcategory of $\mathscr{P}(\mathbb{T})$ on the object set $\mathbf{P}(N)$, $\lceil \varphi_J(x, y, u) \rceil : N_2(x, y) \to N(x)$ is in fact also an isomorphism in $\mathscr{N}_F(\mathbb{T})$. ∎

We can now show that, for any arithmetical theory $\mathbb{T}$ with induction, $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$. We first recall a useful result.

Remark 3.3.1.12 Let $\mathcal{C}$ be a cartesian or cartesian restriction category, and let A, A', B, B' be objects of $\mathcal{C}$. If $A \cong A'$ and $B \cong B'$ in $\mathcal{C}$, then $A \times B \cong A' \times B'$ in $\mathcal{C}$. Indeed, if $A \cong A'$ and $B \cong B'$ via isomorphisms $\varphi : A \to A'$ and $\psi : B \to B'$, then it is easily shown that $\varphi \times \psi : A \times B \to A' \times B'$ is an isomorphism in $\mathcal{C}$ with inverse $\varphi^{-1} \times \psi^{-1} : A' \times B' \to A \times B$. □

Proposition 3.3.1.13 *Let $\mathbb{T}$ be an arithmetical theory with induction. Then, $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$.*

Proof We proceed by induction on $k \geq 1$. Suppose first that $k = 1$. Since $N_1 \underset{\text{def}}{\equiv} N$ by definition, it follows immediately that $N_1 \cong N$ in $\mathscr{N}_F(\mathbb{T})$.

Now suppose that $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for some $k \geq 1$. As remarked after Proposition 3.3.1.5, $\mathscr{N}_F(\mathbb{T})$ has specified (partial) products. In particular, we have that $N_{k+1} = N_k \times N$ and $N_2 = N \times N$ in $\mathscr{N}_F(\mathbb{T})$. By Remark 3.3.1.12 and the induction hypothesis, we thus obtain

$$N_{k+1} = N_k \times N \cong N \times N = N_2$$

in $\mathscr{N}_F(\mathbb{T})$. By Lemma 3.3.1.11 (iii), $N_2 \cong N$ in $\mathscr{N}_F(\mathbb{T})$ via the isomorphism $\lceil \varphi_J(x, y, u) \rceil$. It thus follows that

$$N_{k+1} \cong N$$

in $\mathscr{N}_F(\mathbb{T})$.

Therefore, it follows by induction on $k \geq 1$ that $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$. ∎

Proposition 3.3.1.14 *Let $\mathbb{T}$ be an arithmetical theory with induction. Then, $\mathscr{N}_F(\mathbb{T})$ is a computational subcategory associated to $\mathbb{T}$ (as defined in Definition 3.3.1.6).*

Proof As remarked following Definition 3.3.1.6, it follows from Proposition 3.3.1.5 and the definition of $\mathscr{N}_F(\mathbb{T})$ that $\mathscr{N}_F(\mathbb{T})$ satisfies conditions (i)–(iii) of Definition 3.3.1.6. Moreover, by Proposition 3.3.1.13, we have that $N_k \cong N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$, and so it follows that $N_k \triangleleft N$ in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 1$. Thus, $\mathscr{N}_F(\mathbb{T})$ also satisfies condition (iv) of Definition 3.3.1.6. Therefore, $\mathscr{N}_F(\mathbb{T})$ is indeed a computational subcategory associated to $\mathbb{T}$. ■

Note that a subcategory of $\mathscr{N}_F(\mathbb{T})$ does not need to contain non-total morphisms in order to be a computational subcategory associated to $\mathbb{T}$. In fact, when $\mathbb{T}$ is an intuitionistic arithmetical theory with induction, the subcategory of $\mathscr{N}_F(\mathbb{T})$ containing exactly the total morphisms of $\mathscr{N}_F(\mathbb{T})$, namely $\mathscr{N}_{Tot}(\mathbb{T}) := \mathbf{Tot}(\mathscr{N}_F(\mathbb{T}))$, is also a computational subcategory associated to $\mathbb{T}$.

Corollary 3.3.1.15 *Let $\mathbb{T}$ be an arithmetical theory with induction. Then, $\mathscr{N}_{Tot}(\mathbb{T}) := \mathbf{Tot}(\mathscr{N}_F(\mathbb{T}))$, the subcategory of $\mathscr{N}_F(\mathbb{T})$ containing exactly the total morphisms of $\mathscr{N}_F(\mathbb{T})$, is a computational subcategory associated to $\mathbb{T}$.*

Proof Note that $\mathscr{N}_{Tot}(\mathbb{T})$ is also the full subcategory of $\mathscr{C}(\mathbb{T})$ on the object set $\mathbf{P}(N)$. Hence, it immediately follows that $\mathscr{N}_{Tot}(\mathbb{T})$ satisfies conditions (i) and (iii) of Definition 3.3.1.6. Moreover, similar arguments to the ones in Proposition 3.1.2.4 and Proposition 3.3.1.5 show that $\mathscr{N}_{Tot}(\mathbb{T})$ satisfies condition (ii) of Definition 3.3.1.6. Finally, the isomorphism $\lceil \varphi_J(x,y,u) \rceil : N_2(x,y) \to N(x)$ from Lemma 3.3.1.11 is a total morphism of $\mathscr{N}_F(\mathbb{T})$, and hence lies in $\mathscr{N}_{Tot}(\mathbb{T})$. Thus, Proposition 3.3.1.13 holds for $\mathscr{N}_{Tot}(\mathbb{T})$, and so the argument in the proof of Proposition 3.3.1.14 shows that $\mathscr{N}_{Tot}(\mathbb{T})$ is a computational subcategory associated to $\mathbb{T}$. ■

3.3.2 Necessary and sufficient conditions for a computational subcategory to be a Turing category

For any arithmetical theory $\mathbb{T}$ with induction and any computational subcategory $\mathscr{N}(\mathbb{T})$ associated to $\mathbb{T}$, we can simplify the condition for $\mathscr{N}(\mathbb{T})$ to be a Turing category with Turing object $N(x)$ as follows, although we will only consider intuitionistic arithmetical theories with induction.

Lemma 3.3.2.1 *Let $\mathbb{T}$ be an arithmetical theory with induction and let $\mathscr{N}(\mathbb{T})$ be any computational subcategory associated to $\mathbb{T}$. Then, $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ if and only if there exists a morphism $\lceil \Theta(x,y,u) \rceil : N_2(x,y) \to N(x)$ in $\mathscr{N}(\mathbb{T})$ satisfying the following property for all $k \geq 0$:*

(TM) for each morphism $\lceil F(\mathbf{z},z',u) \rceil : N_{k+1}(\mathbf{z},z') \to N(x)$ in $\mathscr{N}(\mathbb{T})$, there exists a

total morphism $\ulcorner H(\mathbf{z},u)\urcorner : N_k(\mathbf{z}) \to N(x)$ *in* $\mathscr{N}(\mathbb{T})$ *such that the diagram*

$$\begin{array}{ccc} N_2(x,y) & \xrightarrow{\ulcorner \Theta(x,y,u)\urcorner} & N(x) \\ {\scriptstyle \ulcorner H(\mathbf{z},u)\wedge z'=v\urcorner}\uparrow & \nearrow {\scriptstyle \ulcorner F(\mathbf{z},z',u)\urcorner} & \\ N_{k+1}(\mathbf{z},z') & & \end{array}$$

commutes in $\mathscr{N}(\mathbb{T})$.

In this case, $\ulcorner \Theta(x,y,u)\urcorner$ *is a Turing morphism on* $N(x)$ *in* $\mathscr{N}(\mathbb{T})$.

Note that in the special case when $k=0$*, property (TM) for* $\ulcorner \Theta(x,y,u)\urcorner$ *becomes:*

for each morphism $\ulcorner F(x,u)\urcorner : N(x) \to N(x)$ *in* $\mathscr{N}(\mathbb{T})$*, there exists a total morphism* $\ulcorner H(u)\urcorner : \top \to N(x)$ *in* $\mathscr{N}(\mathbb{T})$*, that is, a formula* $H(u)$ *in* $\mathbb{T}$ *with exactly one free variable satisfying*

$$\vdash (\exists! u) H(u),$$

such that the diagram

$$\begin{array}{ccc} N_2(x,y) & \xrightarrow{\ulcorner \Theta(x,y,u)\urcorner} & N(x) \\ {\scriptstyle \ulcorner H(u)\wedge x=v\urcorner}\uparrow & \nearrow {\scriptstyle \ulcorner F(x,u)\urcorner} & \\ N(x) & & \end{array} \tag{3.3.10}$$

commutes in $\mathscr{N}(\mathbb{T})$.

Proof By Lemma 3.3.1.8, $N(x)$ is a universal object of $\mathscr{N}(\mathbb{T})$. Thus, $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ if and only if there exists a Turing morphism on $N(x)$ in $\mathscr{N}(\mathbb{T})$ (see Theorem B.1.1.4 and Definition B.1.1.3 in Appendix B for the definition of a Turing category and a Turing morphism, respectively). Note that $N_2(x,y)$ is the specified partial product of $N(x)$ with itself in $\mathscr{N}(\mathbb{T})$ as remarked following Proposition 3.3.1.5. Note also that all objects of $\mathscr{N}(\mathbb{T})$ are of the form N_k for some $k \geq 0$ and the specified partial product of N_k and N in $\mathscr{N}(\mathbb{T})$ is the object N_{k+1}. Note further that for any morphism $\ulcorner H(\mathbf{z},u)\urcorner : N_k(\mathbf{z}) \to N(x)$ in $\mathscr{N}(\mathbb{T})$, we have that

$$\ulcorner H(\mathbf{z},u)\urcorner \times \ulcorner \mathrm{id}_N(z',v)\urcorner = \ulcorner H(\mathbf{z},u) \wedge z' = v\urcorner$$

as morphisms from $N_{k+1}(\mathbf{z},z')$ to $N_2(x,y)$ in $\mathscr{N}(\mathbb{T})$. Hence, it follows that a Turing morphism on $N(x)$ in $\mathscr{N}(\mathbb{T})$ is given by a morphism $\ulcorner \Theta(x,y,u)\urcorner : N_2(x,y) \to N(x)$ in $\mathscr{N}(\mathbb{T})$ satisfying following property (TM).

The special case when $k=0$ clearly follows. ∎

3.3.2.1 Formalising results from recursion theory in arithmetical theories with induction

As explained above, we wish to formalise Theorems 3.3.0.1 and 3.3.0.2 in $\mathbb{T}$. Since the Kleene Normal Form Theorem (Theorem 2.4.2.1) is used to prove Theorem 3.3.0.1 and to construct the standard enumeration of the partial recursive functions, we begin by considering a formalisation of this theorem.

Recall first that for a formula $\psi(\mathbf{x}, y)$ of an arithmetical theory $\mathbb{T}$ containing exactly $k+1$ free variables ($k \geq 0$), condition (P3), namely

$$\vdash \psi(\mathbf{x}, y) \wedge \psi(\mathbf{x}, y') \Rightarrow y = y', \tag{3.3.11}$$

is the same as defining condition (3) for the representative of a morphism from N_k to N in $\mathscr{N}_F(\mathbb{T})$. We also say that $\psi(\mathbf{x}, y)$ is *provably functional in y (in $\mathbb{T}$)* if (3.3.11) is satisfied. Furthermore, condition (P4) for $\psi(\mathbf{x}, y)$, namely

$$\vdash (\exists y)\psi(\mathbf{x}, y), \tag{3.3.12}$$

is equivalent to defining condition (2) for the representative of a morphism from N_k to N in $\mathscr{N}_F(\mathbb{T})$ as noted in Remark 3.3.1.3. We say that $\psi(\mathbf{x}, y)$ is *provably total in y (in $\mathbb{T}$)* if (3.3.12) is satisfied.

Now suppose that $\mathbb{T}$ is an intuitionistic arithmetical theory with induction. Let $U : \mathbb{N} \to \mathbb{N}$ be the primitive recursive output function and $T_k \subseteq \mathbb{N}^{k+2}$ (for each $k \geq 1$) be the primitive recursive T-predicates from Theorem 2.4.2.1. As noted in [14, §57] and [15, Appendix 1], we can take the T-predicates to be functional in the last argument. Indeed, since we have assigned Gödel numbers to proofs (see Section 2.2.1), we immediately obtain an ordering of proofs. Thus, given $k \geq 1$, $e, n \in \mathbb{N}$, and $\mathbf{m} \in \mathbb{N}^k$, we can take $T_k(e, \mathbf{m}, n)$ to mean that n is the Gödel number of the least proof showing that $e \bullet_k \mathbf{m}$ is defined. Hence, for each $k \geq 1$, $e \in \mathbb{N}$, and $\mathbf{m} \in \mathbb{N}^k$, there is at most one $n \in \mathbb{N}$ such that $T_k(e, \mathbf{m}, n)$ holds, and so T_k is functional in the last argument.

By Theorem 2.4.1.23 and Corollary 2.4.1.24, there exist formulas $\varphi_U(u, v)$ and $\tau_k(z, \mathbf{x}, y)$ that strongly represent U and T_k in $\mathbb{T}$ for all $k \geq 1$. We may refer to the formulas τ_k for $k \geq 1$ as the *formal T-predicates (in $\mathbb{T}$)*. Since φ_U satisfies conditions (P3) and (P4), we can form a conservative extension $\mathbb{T}'$ of $\mathbb{T}$ by adding the well-defined unary function symbol U to $\mathbb{T}$ with the defining axiom

$$\varphi_U(x, u) \Leftrightarrow U(x) = u. \tag{3.3.13}$$

Since $\mathbb{T}'$ is a conservative extension of $\mathbb{T}$ we can simply assume without loss of generality that $\mathbb{T}$ itself is equipped with this unary function symbol U with defining axiom (3.3.13). In fact, we assume without loss of generality that any intuitionistic arithmetical theory with induction mentioned hereafter is equipped with such a unary function symbol U. As explained in [15, Appendix 1] and [35, §1.3.10, 3.7], we can assume that U and the τ_k for all $k \geq 1$ satisfy certain additional properties. First, we can assume without loss of generality that for all $k \geq 1$ the formal T-predicate $\tau_k(z, \mathbf{x}, y)$ is provably functional in y in $\mathbb{T}$, that is, that

$$\vdash \tau_k(z, \mathbf{x}, y) \wedge \tau_k(z, \mathbf{x}, y') \Rightarrow y = y' \tag{3.3.14}$$

holds in $\mathbb{T}$. Second, the following property, called *Church's Rule*, is satisfied for all formulas $F(\mathbf{x}, u)$ of $\mathbb{T}$ with exactly $k+1$ free variables ($k \geq 1$) [20, 35]:

(CR) if $F(\mathbf{x}, u)$ is provably total in u in $\mathbb{T}$, that is, if

$$\vdash (\exists u) F(\mathbf{x}, u)$$

holds in $\mathbb{T}$, then

$$\vdash (\exists z)(\forall \mathbf{x})(\exists v)(\tau_k(z, \mathbf{x}, v) \wedge F(\mathbf{x}, U(v))) \tag{3.3.15}$$

holds in $\mathbb{T}$ and hence there exists an $e \in \mathbb{N}$ such that

$$\vdash (\forall \mathbf{x})(\exists v)(\tau_k(\overline{e}, \mathbf{x}, v) \wedge F(\mathbf{x}, U(v))) \tag{3.3.16}$$

holds in $\mathbb{T}$.

Note that the last part of (CR) is obtained by (EP), which holds for $\mathbb{T}$ since $\mathbb{T}$ is intuitionistic.

Note that although (CR) is in some way a formalisation of the Kleene Normal Form Theorem, it only applies to provably total formulas $F(\mathbf{x}, u)$, which is not sufficient for our purposes as we need to consider representatives of arbitrary morphisms from N_k to N in computational subcategories $\mathscr{N}(\mathbb{T})$ associated to $\mathbb{T}$ that are not necessarily total. Thus, we consider instead the *Partial Church's Rule* for a formula $F(\mathbf{x}, u)$ of $\mathbb{T}$ containing exactly $k+1$ free variables ($k \geq 1$), namely

(PCR) if $F(\mathbf{x}, u)$ is provably functional in u in $\mathbb{T}$, that is, if

$$\vdash F(\mathbf{x}, u) \wedge F(\mathbf{x}, u') \Rightarrow u = u' \tag{3.3.17}$$

holds in $\mathbb{T}$, then

$$\vdash (\exists z)(\forall \mathbf{x})[((\exists u) F(\mathbf{x}, u) \Leftrightarrow (\exists y)\tau_k(z, \mathbf{x}, y)) \wedge (\forall v)(\tau_k(z, \mathbf{x}, v) \Rightarrow F(\mathbf{x}, U(v)))] \tag{3.3.18}$$

holds in $\mathbb{T}$, and so by (EP) there exists an $e \in \mathbb{N}$ such that

$$\vdash (\forall \mathbf{x})[((\exists u) F(\mathbf{x}, u) \Leftrightarrow (\exists y)\tau_k(\overline{e}, \mathbf{x}, y)) \wedge (\forall v)(\tau_k(\overline{e}, \mathbf{x}, v) \Rightarrow F(\mathbf{x}, U(v)))] \tag{3.3.19}$$

holds in $\mathbb{T}$.

The property (PCR) provides a formalisation in $\mathbb{T}$ of the Kleene Normal Form Theorem (Theorem 2.4.2.1), even in the non-total case. Indeed, Theorem 2.4.2.1 states that given a partial recursive function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ ($k \geq 1$), there exists an $e \in \mathbb{N}$ such that, for all $\mathbf{m} \in \mathbb{N}^k$,

(i) there exists an $p \in \mathbb{N}$ such that $f(\mathbf{m}) \simeq p$ if and only if there exists an $n \in \mathbb{N}$ such that $T_k(e, \mathbf{m}, n)$;

(ii) if there exists a $n \in \mathbb{N}$ such that $T_k(e, \mathbf{m}, n)$, then $f(\mathbf{m}) = U(n)$.

We note that (3.3.19) directly formalises statements (i) and (ii) in $\mathbb{T}$ with the provably functional formula $F(\mathbf{x}, u)$ instead of the partial recursive function f, the numeral $\overline{e}$ instead of the number $e \in \mathbb{N}$, the formula $\tau_k(z, \mathbf{x}, y)$ instead of the T-predicate T_k, and the unary function symbol U instead of the output function.

However, it is important to note that, unlike the case with (CR), (PCR) does not necessarily hold for all provably functional formulas of $\mathbb{T}$. Indeed, (PCR) is similar to the *Extended Church's Rule* mentioned in [35, §3.7.1], which only holds for a restricted class of formulas, and so it is reasonable to suppose that the same is true for (PCR).

Similarly to how the T-predicates allow us to encode the partial recursive functions (see the discussion following Theorem 3.3.0.1), we can use the formal T-predicates τ_k and the unary function symbol U in order to encode the subclass of provably functional formulas in $\mathbb{T}$ for which (PCR) does hold and thus obtain a formalisation of Theorem 3.3.0.1 in an intuitionistic arithmetical theory $\mathbb{T}$.

Definition 3.3.2.2 Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction and let $F(\mathbf{x}, u)$ be a formula in $\mathbb{T}$ with exactly $k+1$ free variables ($k \geq 1$) that is provably functional in u in $\mathbb{T}$. We say that $F(\mathbf{x}, u)$ is *encodable* in $\mathbb{T}$ if

$$\vdash (\exists z)[(\exists q)(\tau_k(z, \mathbf{x}, q) \wedge U(q) = u) \Leftrightarrow F(\mathbf{x}, u)] \tag{3.3.20}$$

holds in $\mathbb{T}$. Since $\mathbb{T}$ is intuitionistic, if (3.3.20) holds in $\mathbb{T}$, it follows by (EP) and ($\exists$-I) that $F(\mathbf{x}, u)$ is encodable in $\mathbb{T}$ if and only if there exists an $e \in \mathbb{N}$ such that

$$\vdash (\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = u) \Leftrightarrow F(\mathbf{x}, u) \tag{3.3.21}$$

holds in $\mathbb{T}$, in which case we say that e *encodes* (or *is a code for*) $F(\mathbf{x}, u)$ in $\mathbb{T}$. □

Note in particular that, if $\lceil F(\mathbf{y}, u) \rceil : N_k(\mathbf{y}) \to N(x)$ is a morphism in a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to an intuitionistic arithmetical theory with induction, then $F(\mathbf{y}, u)$ is in particular provably functional in u in $\mathbb{T}$, and so Definition 3.3.2.2 applies to representatives of morphisms from N_k to N in $\mathscr{N}(\mathbb{T})$ for all $k \geq 1$.

Lemma 3.3.2.3 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction and let $F(\mathbf{x}, u)$ be a formula in $\mathbb{T}$ with exactly $k+1$ free variables ($k \geq 1$) that is provably functional in u in $\mathbb{T}$ (i.e. that satisfies condition (P3)). Then, $F(\mathbf{x}, u)$ is encodable in $\mathbb{T}$ if and only if (PCR) is satisfied for $F(\mathbf{x}, u)$.*

Proof Suppose first that $F(\mathbf{x}, u)$ is encodable in $\mathbb{T}$. Therefore, there exists an $e \in \mathbb{N}$ that encodes F in $\mathbb{T}$. We wish to show that (3.3.19) holds for F and this code e. A straightforward proof using (3.3.21) for F and e shows that

$$\vdash (\exists u)F(\mathbf{x}, u) \Leftrightarrow (\exists y)\tau_k(\overline{e}, \mathbf{x}, y) \tag{3.3.22}$$

holds in $\mathbb{T}$.

We next show that

$$\vdash (\forall v)(\tau_k(\overline{e}, \mathbf{x}, v) \Rightarrow F(\mathbf{x}, U(v))) \tag{3.3.23}$$

holds in $\mathbb{T}$. We have the following derivation in $\mathbb{T}$.

1	$\tau_k(\overline{e}, \mathbf{x}, v)$	
2	$(\exists y)\tau_k(\overline{e}, \mathbf{x}, y)$	($\exists$-I), 1
3	$(\exists u)F(\mathbf{x}, u)$	(3.3.22), 2
4	a $F(\mathbf{x}, a)$	
5	$(\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = a)$	(3.3.21) for F and e, 4
6	b $\tau_k(\overline{e}, \mathbf{x}, b) \wedge U(b) = a$	
7	$v = b$	τ_k provably functional in $\mathbb{T}$, 1, 6
8	$U(v) = a$	(=-E), 6, 7
9	$F(\mathbf{x}, U(v))$	(=-E), 4, 8
10	$F(\mathbf{x}, U(v))$	($\exists$-E), 5, 6–9
11	$F(\mathbf{x}, U(v))$	($\exists$-E), 3, 4–10
12	$(\forall v)(\tau_k(\overline{e}, \mathbf{x}, v) \Rightarrow F(\mathbf{x}, U(v)))$	($\Rightarrow$-I), ($\forall$-I), 1–11

We then obtain (3.3.19) for F and e from (3.3.22) and (3.3.23) by ($\wedge$-I) and ($\forall$-I). Furthermore, (3.3.18) for F follows from (3.3.19) by ($\exists$-I). Hence, (PCR) holds for $F(\mathbf{x}, u)$ as F is provably functional in u by hypothesis.

Conversely, suppose that (PCR) is satisfied for $F(\mathbf{x}, u)$. Then, there exists an $e \in \mathbb{N}$ such that (3.3.19) holds for F and e in $\mathbb{T}$. We wish to show that (3.3.21) holds for F and e in $\mathbb{T}$. From (3.3.19) for F and e, we obtain

$$\vdash (\exists u)F(\mathbf{x}, u) \Leftrightarrow (\exists y)\tau_k(\overline{e}, \mathbf{x}, y) \tag{3.3.24}$$

and

$$\vdash (\forall v)(\tau_k(\overline{e}, \mathbf{x}, v) \Rightarrow F(\mathbf{x}, U(v))). \tag{3.3.25}$$

From (3.3.24), we obtain

$$F(\mathbf{x}, u) \stackrel{a}{\vdash} \tau_k(\overline{e}, \mathbf{x}, a)$$

for some a. We then obtain

$$F(\mathbf{x}, u) \stackrel{a}{\vdash} F(\mathbf{x}, U(a))$$

by (3.3.25), and so it follows that

$$F(\mathbf{x}, u) \stackrel{a}{\vdash} \tau_k(\overline{e}, \mathbf{x}, a) \wedge U(a) = u$$

as $F(\mathbf{x}, u)$ is provably functional in u in $\mathbb{T}$. We then obtain

$$F(\mathbf{x}, u) \vdash (\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = u)$$

by the rules for $\exists$ in $\mathbb{T}$.

Conversely, we obtain

$$\tau_k(\overline{e}, \mathbf{x}, b) \wedge U(b) = u \stackrel{b}{\vdash} F(\mathbf{x}, U(b))$$

by (3.3.25), from which

$$(\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = u) \vdash F(\mathbf{x}, u)$$

follows by (=-E) and ($\exists$-E).

Thus, we obtain

$$\vdash (\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = u) \Leftrightarrow F(\mathbf{x}, u),$$

and so (3.3.21) holds for F and e in $\mathbb{T}$. Hence, $F(\mathbf{x}, u)$ is encodable in $\mathbb{T}$. ∎

Recall from above that, in an intuitionistic arithmetical theory $\mathbb{T}$ with induction, Church's Rule (CR) holds for any formula $F(\mathbf{x}, u)$ with exactly $k+1$ free variables ($k \geq 1$) that is provably total in u in $\mathbb{T}$. Hence, we can encode any such formula $F(\mathbf{x}, u)$ that is both provably functional and provably total in u in $\mathbb{T}$ without the additional assumption that (PCR) holds for $F(\mathbf{x}, u)$.

Lemma 3.3.2.4 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction and let $F(\mathbf{x}, u)$ be a formula in $\mathbb{T}$ with exactly $k+1$ free variables ($k \geq 1$) that is both provably functional and provably total in u in $\mathbb{T}$ (i.e. that satisfies conditions (P3) and (P4)). Then, $F(\mathbf{x}, u)$ is encodable in $\mathbb{T}$.*

Proof Since $F(\mathbf{x}, u)$ is provably total in u in $\mathbb{T}$, it follows from (CR) that there exists an $e \in \mathbb{N}$ such that (3.3.16), that is to say

$$\vdash (\forall \mathbf{x})(\exists v)(\tau_k(\overline{e}, \mathbf{x}, v) \wedge F(\mathbf{x}, U(v))),$$

holds in $\mathbb{T}$. It then follows by condition (P3) for τ_k, conditions (P3) and (P4) for F, and the rules for $\exists$ and equality in $\mathbb{T}$ that (3.3.21), that is to say

$$\vdash (\exists q)(\tau_k(\overline{e}, \mathbf{x}, q) \wedge U(q) = u) \Leftrightarrow F(\mathbf{x}, u),$$

holds in $\mathbb{T}$. Therefore, $F(\mathbf{x}, u)$ is indeed encodable in $\mathbb{T}$. ∎

We now formalise Theorem 3.3.0.2 in an intuitionistic arithmetical theory $\mathbb{T}$ with induction.

Theorem 3.3.2.5 (Formal S-m-n Theorem) *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction. For all $m, n \geq 1$, there exists a formula $\mathbf{S}^n_m(z, \mathbf{x}, w)$ in $\mathbb{T}$ containing exactly $n+2$ free variables that strongly represents the primitive recursive function $S^n_m : \mathbb{N}^{n+1} \to \mathbb{N}$ from Theorem 3.3.0.2 in $\mathbb{T}$ and is such that*

$$\vdash (\exists p, q)(\mathbf{S}^n_m(z, \mathbf{x}, q) \wedge \tau_m(q, \mathbf{y}, p) \wedge U(p) = v) \Leftrightarrow (\exists r)(\tau_{n+m}(z, \mathbf{x}, \mathbf{y}, r) \wedge U(r) = v) \tag{3.3.26}$$

holds in $\mathbb{T}$, where $|\mathbf{x}| = n$ and $|\mathbf{y}| = m$.

Proof A description of the formalisation of elementary recursion theory (including a version of the S-m-n Theorem) in Heyting arithmetic is given in [36, Ch. 3, §7, pp. 152–155]. Since $\mathbb{T}$ is a consistent r.e. extension of the theory H for Heyting arithmetic, we can conclude that the formalisation of the S-m-n Theorem given above, which is a reformulation of the result in [36] in our setting, holds in $\mathbb{T}$. ■

Note that we will only require Theorem 3.3.2.5 when $m = 1$ in order to show that a certain computational subcategory $\mathscr{N}(\mathbb{T})$ satisfies property (TM) from Lemma 3.3.2.1. Moreover, note that for all $n \geq 1$, $\mathbf{S}^n_1(z, \mathbf{x}, w)$ strongly represents S^n_1 in $\mathbb{T}$ and so satisfies conditions (P3) and (P4). Hence, we can form a conservative extension of $\mathbb{T}$ by adjoining to $\mathbb{T}$ a new $(n+1)$-ary function symbol σ^n_1 with the defining axiom

$$\mathbf{S}^n_1(z, \mathbf{x}, w) \Leftrightarrow \sigma^n_1(z, \mathbf{x}) = w \tag{3.3.27}$$

for each $n \geq 1$. Therefore, we can henceforth suppose without loss of generality that any intuitionistic arithmetical theory $\mathbb{T}$ with induction contains not only the unary function symbol U with defining axiom (3.3.13) but also the $(n+1)$-ary function symbol σ^n_1 with defining axiom (3.3.27) for each $n \geq 1$. Consequently, any intuitionistic arithmetical theory $\mathbb{T}$ with induction satisfies the following property:

(SMN) for each $n \geq 1$, the $(n+1)$-ary function symbol σ^n_1 of $\mathbb{T}$ given by defining axiom (3.3.27) is such that

$$\vdash (\exists p)(\tau_1(\sigma^n_1(z, \mathbf{x}), y, p) \wedge U(p) = v) \Leftrightarrow (\exists r)(\tau_{n+1}(z, \mathbf{x}, y, r) \wedge U(r) = v) \tag{3.3.28}$$

holds in $\mathbb{T}$.

Note that (SMN) is indeed a formalisation in $\mathbb{T}$ of the S-m-n Theorem (Theorem 3.3.0.2) in the case when $m = 1$. Indeed, let each $n \geq 1$, $e, p \in \mathbb{N}$, and $\mathbf{k} \in \mathbb{N}^n$. Then, the primitive recursive function $S^n_1 : \mathbb{N}^{n+1} \to \mathbb{N}$ given in Theorem 3.3.0.2 is such that

$$S^n_1(e, \mathbf{k}) \bullet_1 p \simeq e \bullet_{n+1} (\mathbf{k}, p). \tag{3.3.29}$$

By the definition of Kleene application, we can rewrite (3.3.29) as

$$U(\mu_m T_1(S^n_1(e, \mathbf{k}), p, m)) \simeq U(\mu_{m'}(T_{n+1}(e, \mathbf{k}, p, m'))). \tag{3.3.30}$$

Since we assume without loss of generality that the T-predicates are functional in the last variable, there exists at most one $m \in \mathbb{N}$ for which $T_1(S_1^n(e, \mathbf{k}), p, m)$ holds and at most one $m' \in \mathbb{N}$ for which $T_{n+1}(e, \mathbf{k}, p, m')$ holds. Hence, (3.3.30) is in fact equivalent to the following statement:

> There exists $m \in \mathbb{N}$ such that $T_1(S_1^n(e, \mathbf{k}), p, m)$ holds if and only if there exists $m' \in \mathbb{N}$ such that $T_{n+1}(e, \mathbf{k}, p, m')$ holds. Moreover, if such m, m' do exist, then $U(m) = U(m')$. (3.3.31)

(SMN) is then a direct formalisation of (3.3.31) in $\mathbb{T}$ with the function symbol σ_1^n representing the primitive recursive function S_1^n and the formal T-predicates τ_1 and τ_{n+1} representing the T-predicates T_1 and T_{n+1}.

3.3.2.2 Sufficient condition

Throughout this section, we assume that $\mathbb{T}$ is an intuitionistic arithmetical theory with induction. We wish to give a sufficient condition for a computational subcategory associated to $\mathbb{T}$ to be a Turing category with Turing object $N(x)$. We first construct a candidate for a Turing morphism.

Proposition 3.3.2.6 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction.*

(i) Define

$$\Psi(x, y, u) \underset{\text{def}}{\equiv} (\exists q)(\tau_1(x, y, q) \wedge U(q) = u). \tag{3.3.32}$$

Then, $\lceil \Psi(x, y, u) \rceil$ is a morphism from $N_2(x, y)$ to $N(x)$ in $\mathscr{N}_F(\mathbb{T})$.

(ii) For all $n \geq 1$, $\lceil \mathbf{S}_1^n(x, \mathbf{z}, u) \rceil = \lceil \sigma_1^n(x, \mathbf{z}) = u \rceil$ is a total morphism from $N_{n+1}(x, \mathbf{z})$ to $N(x)$ in $\mathscr{N}_F(\mathbb{T})$, where $\mathbf{S}_1^n$ is as defined in Theorem 3.3.2.5 and σ_1^n is the $(n+1)$-ary function symbol of $\mathbb{T}$ given by defining axiom (3.3.27).

Proof (i) Defining condition (3) for $\Psi(x, y, u)$ follows directly from the fact that τ_1 is provably functional in $\mathbb{T}$ in the last variable. Hence, as noted in Remark 3.3.1.3, it immediately follows that $\lceil \Psi(x, y, u) \rceil$ is a morphism from $N_2(x, y)$ to $N(x)$ in $\mathscr{P}(\mathbb{T})$, and so also in $\mathscr{N}_F(\mathbb{T})$.

(ii) Since $\mathbf{S}_1^n(x, \mathbf{z}, u)$ strongly represents the primitive recursive function $S_1^n : \mathbb{N}^{n+1} \to \mathbb{N}$ from Theorem 3.3.0.2 in $\mathbb{T}$, it satisfies conditions (P3) and (P4). As noted in Remark 3.3.1.3, it immediately follows that $\lceil \mathbf{S}_1^n(x, \mathbf{z}, u) \rceil$ is a total morphism from $N_{n+1}(x, \mathbf{z})$ to $N(x)$ in $\mathscr{P}(\mathbb{T})$, and so also in $\mathscr{N}_F(\mathbb{T})$. Moreover, it follows from the defining axiom (3.3.27) that $\lceil \mathbf{S}_1^n(x, \mathbf{z}, u) \rceil = \lceil \sigma_1^n(x, \mathbf{z}) = u \rceil$. ∎

Note that the morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ corresponds to the Kleene application operation $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ (which is equal to the universal function $\Phi^{(1)} : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ constructed after Theorem 3.3.0.1) since $\Psi(x, y, u)$ is constructed from the formal T-predicate τ_1 and the unary function symbol U in the same way that $\bullet$ is defined in terms of the T-predicate T_1 and the output function U, although we do not need to take partial minimisation into account as we assume without loss of generality that both T_1 and τ_1 are provably functional in the last argument. In fact, $\Psi(x, y, u)$ type-one represents $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ in any intuitionistic arithmetical theory with induction.

Lemma 3.3.2.7 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction and let $\Psi(x, y, u)$ be defined as in Proposition 3.3.2.6. Then, $\Psi(x, y, u)$ type-one represents the Kleene application operation $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ in $\mathbb{T}$.*

Proof By Proposition 3.3.2.6, $\Psi(x, y, u)$ satisfies defining condition (3), which is the same as condition (P3). It remains to show condition (P1). Let $e, m, p \in \mathbb{N}$ and suppose first that $e \bullet m \simeq p$. Recall that

$$e \bullet m \simeq U(\mu_n T_1(e, m, n))$$

and that T_1 is assumed to be functional in the last argument. Hence, there exists a (unique) $n \in \mathbb{N}$ such that $T_1(e, m, n)$ holds and $U(n) = p$. Since τ_1 and φ_U strongly represents T_1 and U in $\mathbb{T}$, it follows from condition (B) for τ_1, condition (P1) for φ_U, and defining axiom (3.3.13) that

$$\vdash \tau_1(\overline{e}, \overline{m}, \overline{n}) \wedge U(\overline{n}) = \overline{p}$$

holds in $\mathbb{T}$. We thus obtain

$$\vdash \Psi(\overline{e}, \overline{m}, \overline{p})$$

by ($\exists$-I).

Now suppose instead that $\vdash \Psi(\overline{e}, \overline{m}, \overline{p})$ holds in $\mathbb{T}$. Since $\mathbb{T}$ is intuitionistic, it follows from the Existence Property (EP) that there exists a $k \in \mathbb{N}$ such that

$$\vdash \tau_1(\overline{e}, \overline{m}, \overline{k}) \wedge U(\overline{k}) = \overline{p}$$

holds in $\mathbb{T}$. It thus follows from condition (B) for τ_1 and condition (P1) for φ_U that $T_1(e, m, k)$ holds and $U(k) = p$. Since T_1 is assumed to be functional in the last argument, $k = \mu_n T_1(e, m, n)$, and so $e \bullet m \simeq p$.

Thus, condition (P1) for $\Psi(x, y, u)$ is satisfied, and so $\Psi(x, y, u)$ indeed type-one represents $\bullet = \Phi^{(1)} : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ in $\mathbb{T}$. ∎

Theorem 3.3.2.8 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction. Let $\mathscr{N}(\mathbb{T})$ be a computational subcategory associated to $\mathbb{T}$ containing the morphisms $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ and $\lceil \mathbf{S}^n_1(x, \mathbf{z}, u) \rceil : N_{n+1}(x, \mathbf{z}) \to N(x)$ (for all $n \geq 1$) from Proposition 3.3.2.6. If all representatives of morphisms from N_m to N in $\mathscr{N}(\mathbb{T})$ (for all $m \geq 1$) are encodable in $\mathbb{T}$, then $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$.*

PROOF Suppose that all representatives of morphisms from N_m to N in $\mathscr{N}(\mathbb{T})$ (for all $m \geq 1$) are encodable in $\mathbb{T}$. By Lemma 3.3.2.1, in order to show that $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$, it suffices to show that $\lceil \Psi(x, y, u) \rceil$ satisfies condition (TM) for all $k \geq 0$.

Suppose first that $k \geq 1$ and let $\lceil F(\mathbf{z}, z', u) \rceil : N_{k+1}(\mathbf{z}, z') \to N(x)$ be any morphism in $\mathscr{N}(\mathbb{T})$. By hypothesis, there exists an $e \in \mathbb{N}$ that encodes $F(\mathbf{z}, z', u)$ in $\mathbb{T}$, and so

$$\vdash (\exists q)(\tau_{k+1}(\overline{e}, \mathbf{z}, z', q) \wedge U(q) = u) \Leftrightarrow F(\mathbf{z}, z', u) \tag{3.3.33}$$

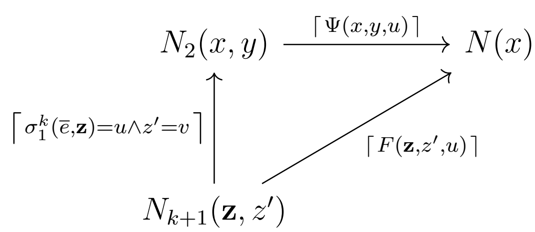
holds in $\mathbb{T}$. By Lemma 3.3.1.7,

$$\lceil \underline{e}(u) \rceil := \lceil \overline{e} = u \rceil : \top \to N(x)$$

is a total morphism in $\mathscr{N}(\mathbb{T})$. Furthermore, the morphism $\lceil \mathbf{S}_1^k \rceil : N_{k+1} \to N$ lies in $\mathscr{N}(\mathbb{T})$ by hypothesis and is total by Proposition 3.3.2.6. Hence, the morphism

$$\lceil \mathbf{S}_1^k(\overline{e}, \mathbf{z}, u) \rceil = \lceil \sigma_1^k(\overline{e}, \mathbf{z}) = u \rceil : N_k(\mathbf{z}) \to N(x)$$

is also a total morphism in $\mathscr{N}(\mathbb{T})$ as it is obtained from the total morphisms $\lceil \underline{e} \rceil$, $\lceil \mathrm{id}_{N_k} \rceil$, and $\lceil \mathbf{S}_1^k \rceil$ of $\mathscr{N}(\mathbb{T})$ by product and composition of morphisms. We wish to show that the diagram



(3.3.34)

commutes in $\mathscr{N}(\mathbb{T})$. By the rules for $\exists$ and equality in $\mathbb{T}$, we obtain

$$\lceil \sigma_1^k(\overline{e}, \mathbf{z}) = u \wedge z' = v \rceil ; \lceil \Psi(x, y, u) \rceil = \lceil \Psi(\sigma_1^k(\overline{e}, \mathbf{z}), z', u) \rceil .$$

Furthermore, note that

$$\Psi(\sigma_1^k(\overline{e}, \mathbf{z}), z', u) \underset{\text{def}}{\equiv} (\exists q)(\tau_1(\sigma_1^k(\overline{e}, \mathbf{z}), z', q) \wedge U(q) = u)$$

by definition. Since (SMN) holds in $\mathbb{T}$, it thus follows by (3.3.28) that

$$\vdash \Psi(\sigma_1^k(\overline{e}, \mathbf{z}), z', u) \Leftrightarrow (\exists q)(\tau_{k+1}(\overline{e}, \mathbf{z}, z', q) \wedge U(q) = u)$$

holds in $\mathbb{T}$. By (3.3.33), it then follows that

$$\vdash \Psi(\sigma_1^k(\overline{e}, \mathbf{z}), z', u) \Leftrightarrow F(\mathbf{z}, z', u)$$

holds in $\mathbb{T}$, and so diagram (3.3.34) indeed commutes in $\mathscr{N}(\mathbb{T})$. Therefore, $\lceil \Psi(x, y, u) \rceil$ indeed satisfies property (TM) in $\mathscr{N}(\mathbb{T})$ in the case when $k \geq 1$.

Now suppose that $k = 0$. Let $\lceil F(x, u) \rceil : N(x) \to N(x)$ be any morphism on $N(x)$ in $\mathscr{N}(\mathbb{T})$. By hypothesis there exists an $e \in \mathbb{N}$ that encodes $F(x, u)$ in $\mathbb{T}$, and so

$$\vdash (\exists q)(\tau_1(\overline{e}, x, q) \wedge U(q) = u) \Leftrightarrow F(x, u)$$

holds in $\mathbb{T}$. By definition of Ψ, we in fact obtain that

$$\vdash \Psi(\overline{e}, x, u) \Leftrightarrow F(x, u) \tag{3.3.35}$$

holds in $\mathbb{T}$. Consider again the total morphism $\lceil \underline{e}(u) \rceil := \lceil \overline{e} = u \rceil : \top \to N(x)$ of $\mathscr{N}(\mathbb{T})$. We wish to show that the diagram

$$\begin{array}{ccc} N_2(x, y) & \xrightarrow{\lceil \Psi(x,y,u) \rceil} & N(x) \\ {\scriptstyle \lceil \underline{e}(u) \wedge x = v \rceil} \uparrow & \nearrow {\scriptstyle \lceil F(x,u) \rceil} & \\ N(x) & & \end{array} \tag{3.3.36}$$

commutes in $\mathscr{N}(\mathbb{T})$. As in the previous case where $k \geq 1$, we have that

$$\lceil \underline{e}(u) \wedge x = v \rceil \, ; \lceil \Psi(x, y, u) \rceil = \lceil \Psi(\overline{e}, x, u) \rceil \, ,$$

and so it follows immediately from (3.3.35) that diagram (3.3.36) commutes in $\mathscr{N}(\mathbb{T})$. Thus, $\lceil \Psi(x, y, u) \rceil$ also satisfies property (TM) in $\mathscr{N}(\mathbb{T})$ in the case when $k = 0$.

Therefore, $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ satisfies property (TM) in $\mathscr{N}(\mathbb{T})$ for all $k \geq 0$, and so $\mathscr{N}(\mathbb{T})$ is indeed a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$. ∎

As noted previously, since the objects of all computational subcategories associated to $\mathbb{T}$ are the same, a computational subcategory is determined entirely by the choice of subset of the morphisms of $\mathscr{N}_F(\mathbb{T})$. If we can find such a subset of morphisms that satisfies the conditions in Theorem 3.3.2.8, we will obtain a concrete example of a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to $\mathbb{T}$ that is a Turing category. We conjecture that such a subset may be found by considering the morphisms of $\mathscr{N}_F(\mathbb{T})$ which are the equivalence classes of formulas $F(\mathbf{y}, u)$ such that $(\exists u)F(\mathbf{y}, u)$ is almost negative (the almost negative formulas are constructed from the Σ_1 formulas using $\forall$, $\wedge$ and $\Rightarrow$ [35, §3.2.9]). Indeed, the Extended Church's Rule given in [35] is shown to hold for such formulas, and so it seems reasonable to suppose that the same is true for our Partial Church's Rule (PCR), as these two rules are quite similar.

3.3.2.3 The special case of total morphisms

Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction. If $k \geq 1$ and $\lceil F(\mathbf{y}, u) \rceil : N_k(\mathbf{y}) \to N(x)$ is any total morphism in $\mathscr{N}_F(\mathbb{T})$, then $F(\mathbf{y}, u)$ satisfies conditions (P3) and (P4) as noted in Remark 3.3.1.3. Hence, (CR) holds for $F(\mathbf{y}, u)$ and, as shown in Lemma 3.3.2.4, no additional assumptions are necessary for $F(\mathbf{y}, u)$ to be encodable in $\mathbb{T}$. We thus obtain the following result, which is similar to Theorem 3.3.2.8 in the case of total morphisms, but requires fewer hypotheses.

Proposition 3.3.2.9 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction and let $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ be the morphism of $\mathscr{N}_F(\mathbb{T})$ defined in Proposition 3.3.2.6. Then, $\lceil \Psi(x, y, u) \rceil$ satisfies the special case of property (TM) from Lemma 3.3.2.1 for total morphisms from N_{k+1} to N in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 0$.*

Proof $\mathscr{N}_F(\mathbb{T})$ contains the morphisms $\lceil \mathbf{S}_1^n(x, \mathbf{z}, u) \rceil : N_{n+1}(x, \mathbf{z}) \to N(x)$ for all $n \geq 1$ by Proposition 3.3.2.6. Moreover, the representatives of all total morphisms from N_m to N in $\mathscr{N}_F(\mathbb{T})$ for all $m \geq 1$ satisfy conditions (P3) and (P4) and hence are encodable in $\mathbb{T}$ by Lemma 3.3.2.4. It thus follows from the proof of Theorem 3.3.2.8 that $\lceil \Psi(x, y, u) \rceil$ satisfies the special case of property (TM) for total morphisms from N_{k+1} to N in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 0$. ■

Recall from Corollary 3.3.1.15 that $\mathscr{N}_{Tot}(\mathbb{T})$, the subcategory of $\mathscr{N}_F(\mathbb{T})$ containing exactly the total morphisms of $\mathscr{N}_F(\mathbb{T})$, is a computational subcategory associated to the intuitionistic arithmetical theory $\mathbb{T}$ with induction. However, although we have shown that $\lceil \Psi(x, y, u) \rceil$ satisfies property (TM) for all total morphisms from N_{k+1} to N in $\mathscr{N}_F(\mathbb{T})$ for all $k \geq 0$, it does not follow from Proposition 3.3.2.9 that $\mathscr{N}_{Tot}(\mathbb{T})$ is a Turing category. Indeed, as shown in Lemma 3.3.2.7, $\Psi(x, y, u)$ type-one represents the Kleene application operation $\bullet : \mathbb{N}^2 \dashrightarrow \mathbb{N}$ in $\mathbb{T}$. Since $\bullet = \Phi^{(1)}$, the universal enumerating function for the partial recursive functions of one variable defined after Theorem 3.3.0.1, it is a non-total function and so cannot be strongly represented in the intuitionistic theory $\mathbb{T}$ by Theorem 2.3.3.3. Hence, $\Psi(x, y, u)$ cannot satisfy condition (P4), and so $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ is a non-total morphism of $\mathscr{N}_F(\mathbb{T})$. Hence, $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ does not lie in $\mathscr{N}_{Tot}(\mathbb{T})$, and so cannot be a Turing morphism of $\mathscr{N}_{Tot}(\mathbb{T})$ even though it satisfies property (TM) for all morphisms from N_{k+1} to N in $\mathscr{N}_{Tot}(\mathbb{T})$ for all $k \geq 0$.

It follows from Corollary 2.4.4.3 that every morphism from N_k to N in $\mathscr{N}_{Tot}(\mathbb{T})$ for all $k \geq 0$ is the equivalence class of a formula strongly representing a total recursive function in $\mathbb{T}$. If we could find total recursive enumerating functions (analogous to the ones in Theorem 3.3.0.1) for the class of total recursive functions, we could use similar constructions and arguments to the ones leading to Theorem 3.3.2.8 in order to show that the representing formula of the enumerating function for the total recursive functions yields a Turing morphism on N in $\mathscr{N}_{Tot}(\mathbb{T})$. However, a standard diagonal argument shows that there do not exist enumerating functions for any given subset of the class of total recursive functions that lie within this subset. Hence, if $\mathscr{N}(\mathbb{T})$ is any computational subcategory associated to $\mathbb{T}$ that contains only total morphisms, $\mathscr{N}(\mathbb{T})$ cannot be a Turing category with Turing object $N(x)$, as otherwise we would obtain enumerating functions for the subset of total recursive functions strongly represented in $\mathbb{T}$ by representatives of morphisms in $\mathscr{N}(\mathbb{T})$ that lie within this subset.

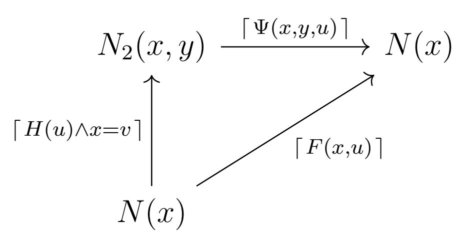
3.3.2.4 Necessary and sufficient condition

We also wish to give necessary conditions for a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to an intuitionistic arithmetical theory $\mathbb{T}$ with induction to be a Turing category with Turing object $N(x)$. Ideally, we would like to show that the converse of Theorem 3.3.2.8 is true.

If $\mathscr{N}(\mathbb{T})$ is a computational subcategory satisfying the hypotheses of Theorem 3.3.2.8 and containing $N(x)$ as a Turing object and $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$ as a Turing morphism, then we can certainly show that every representative of a morphism on $N(x)$ in $\mathscr{N}(\mathbb{T})$ is encodable in $\mathbb{T}$ (see Lemma 3.3.2.10 below). However, showing that morphisms from N_m to N in $\mathscr{N}(\mathbb{T})$ are encodable for all $m \geq 1$ is not so simple.

Lemma 3.3.2.10 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction. Let $\mathscr{N}(\mathbb{T})$ be a computational subcategory associated to $\mathbb{T}$ containing the morphism $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$ from Proposition 3.3.2.6. Suppose that $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$. Then, all representatives of morphisms on $N(x)$ in $\mathscr{N}(\mathbb{T})$ are encodable in $\mathbb{T}$.*

Proof Suppose that $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$. Let $F(x,u)$ be the representative of some morphism on $N(x)$ in $\mathscr{N}(\mathbb{T})$. We wish to show that $F(x,u)$ is encodable in $\mathbb{T}$. Since $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$ is a Turing morphism on $\mathscr{N}(\mathbb{T})$, there exists a total morphism $\lceil H(u) \rceil : \top \to N(x)$ in $\mathscr{N}(\mathbb{T})$ such that the diagram



(3.3.37)

commutes in $\mathscr{N}(\mathbb{T})$ by Lemma 3.3.2.1. Note that since $\lceil H(u) \rceil : \top \to N(x)$ is a total morphism in $\mathscr{N}(\mathbb{T})$, it is in fact a morphism of $\mathscr{C}(\mathbb{T})$. Since $\mathbb{T}$ is an intuitionistic arithmetical theory with induction, it follows from Theorem 3.2.0.10 that the numerals are standard in $\mathscr{C}(\mathbb{T})$. Moreover, by Lemma 3.3.1.7, all numerals are contained in $\mathscr{N}(\mathbb{T})$. Hence, there exists an $e \in \mathbb{N}$ such that

$$\lceil H(u) \rceil = \lceil \underline{e}(u) \rceil : \top \to N(x)$$

as morphism of $\mathscr{N}(\mathbb{T})$, where

$$\underline{e}(u) \underset{\text{def}}{\equiv} \overline{e} = u$$

as in Lemma 3.2.0.9. Therefore, it follows from the commutativity of diagram (3.3.37) that

$$\vdash \Psi(\overline{e}, x, u) \Leftrightarrow F(x, u)$$

holds in $\mathbb{T}$, as in the proof of Theorem 3.3.2.8. By definition of Ψ, this means that

$$\vdash (\exists q)(\tau_1(\overline{e}, x, q) \wedge U(q) = u) \Leftrightarrow F(x, u)$$

holds in $\mathbb{T}$, and hence $F(x, u)$ is encodable in $\mathbb{T}$. ■

We now wish to consider the full converse of Theorem 3.3.2.8 rather than the special case in Lemma 3.3.2.10. Under the hypotheses of Lemma 3.3.2.10 we would like to show that all representatives of morphisms from N_k to N in $\mathscr{N}(\mathbb{T})$ (for all $k \geq 1$) are encodable in $\mathbb{T}$. The case $k = 1$ was dealt with in Lemma 3.3.2.10. Note that in order to prove Theorem 3.3.2.8, we used a formalisation of the S-m-n Theorem (Theorem 3.3.0.2) in $\mathbb{T}$. It thus makes sense to consider a formalisation in $\mathbb{T}$ of a result that in some sense does the opposite of Theorem 3.3.0.2 in order to deal with the case $k > 1$.

In the context of sets, we have the following situation. Let $k \geq 1$ and $e \in \mathbb{N}$ and consider the e^{th} partial recursive function on k variables, namely $\phi_e^{(k)} = e \bullet_k (\cdot) : \mathbb{N}^k \dashrightarrow \mathbb{N}$. We can then construct a partial recursive function $f : \mathbb{N}^{k+1} \dashrightarrow \mathbb{N}$ by setting

$$f(\mathbf{m}, n) \simeq (e \bullet_k \mathbf{m}) \bullet n$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$. Since f is also a partial recursive function, it follows by Theorem 3.3.0.1 that there exists a code $e' \in \mathbb{N}$ such that $\phi_{e'}^{(k+1)} = f$, that is, such that

$$e' \bullet_{k+1} (\mathbf{m}, n) \simeq (e \bullet_k \mathbf{m}) \bullet n$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$. Proceeding in this manner for each $e \in \mathbb{N}$, we obtain a function $C^k : \mathbb{N} \to \mathbb{N}$ such that

$$C^k(e) \bullet_{k+1} (\mathbf{m}, n) \simeq (e \bullet_k \mathbf{m}) \bullet n$$

for all $(\mathbf{m}, n) \in \mathbb{N}^{k+1}$. Note that C^k has, in some sense, the opposite effect of the function S_1^k from Theorem 3.3.0.2. Indeed, S_1^k allows us to rewrite an expression using Kleene application of index $k + 1$ in terms of Kleene application of index 1, whereas C^k allows us to rewrite an expression in terms of Kleene application of indices k and 1 in terms of Kleene application of $k + 1$. Hence, S_1^k rewrites expressions in terms of Kleene application of a lower index and C^k rewrites expressions in terms of Kleene application of a higher index.

Note that the functions $C^k : \mathbb{N} \to \mathbb{N}$ constructed above for all $k \geq 1$ are neither unique nor necessarily primitive recursive. However, a similar argument to the one in the proof of the S-m-n Theorem (see for example [14, §65, Thm XXIII]) should yield, for each $k \geq 1$, a primitive recursive function $C^k : \mathbb{N} \to \mathbb{N}$ such that, for all $e, n \in \mathbb{N}$ and $\mathbf{m} \in \mathbb{N}^k$,

$$C^k(e) \bullet_{k+1} (\mathbf{m}, n) \simeq (e \bullet_k \mathbf{m}) \bullet n.$$

Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction. Assuming that our encoding of the partial recursive functions via the $\mathbb{T}$-predicates satisfies the existence of such primitive recursive functions $C^k : \mathbb{N} \to \mathbb{N}$ for each $k \geq 1$, we can seek to formalise the above result in $\mathbb{T}$ similarly to the way that we formalised the S-m-n Theorem. By formalising, we obtain the following property that $\mathbb{T}$ may or may not satisfy:

For each $k \geq 1$, there exists a formula $\varphi_{C^k}(x, y)$ satisfying conditions (P3) and (P4) in $\mathbb{T}$ such that

$$\vdash (\exists w, p)(\varphi_{C^k}(z, w) \wedge \tau_{k+1}(w, \mathbf{x}, y, p) \wedge U(p) = u) \\ \Leftrightarrow (\exists q, r)(\tau_k(z, \mathbf{x}, q) \wedge \tau_1(U(q), y, r) \wedge U(r) = u) \quad (3.3.38)$$

holds in $\mathbb{T}$.

Note that if $\mathbb{T}$ satisfies the above property, we can form a conservative extension of $\mathbb{T}$ by introducing, for each $k \geq 1$, a new unary function symbol C^k with defining axiom

$$\varphi_{C^k}(x, y) \Leftrightarrow C^k(x) = y, \quad (3.3.39)$$

and so assume without loss of generality that $\mathbb{T}$ itself contains these unary function symbols. Hence, we can replace the above property by the following equivalent property:

($\star$) For each $k \geq 1$, there exists a unary function symbol C^k in $\mathbb{T}$ such that

$$\vdash (\exists p)(\tau_{k+1}(C^k(z), \mathbf{x}, y, p) \wedge U(p) = u) \\ \Leftrightarrow (\exists q, r)(\tau_k(z, \mathbf{x}, q) \wedge \tau_1(U(q), y, r) \wedge U(r) = u) \quad (3.3.40)$$

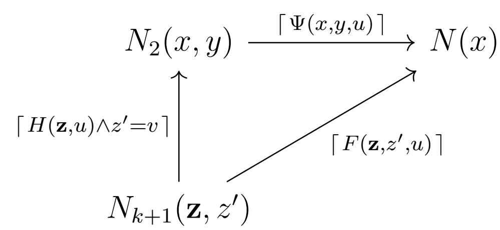
holds in $\mathbb{T}$.

Then, provided that $\mathbb{T}$ satisfies the property ($\star$), we can use Lemma 3.3.2.10 and induction on k in order to prove the converse of Theorem 3.3.2.8 as desired.

Proposition 3.3.2.11 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction satisfying property ($\star$). Let $\mathscr{N}(\mathbb{T})$ be a computational subcategory associated to $\mathbb{T}$ containing the morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$ from Proposition 3.3.2.6. Suppose that $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x, y, u) \rceil : N_2(x, y) \to N(x)$. Then, each representative $F(\mathbf{z}, u)$ of a morphism from $N_k(\mathbf{z})$ to $N(x)$ (for $k \geq 1$) is encodable in $\mathbb{T}$.*

Proof We show by induction on $k \geq 1$ that each representative of a morphism from N_k to N in $\mathscr{N}(\mathbb{T})$ is encodable in $\mathbb{T}$. The case $k = 1$ is shown in Lemma 3.3.2.10.

Now let $k \geq 1$ and suppose that each representative of a morphism from $N_k(\mathbf{z})$ to $N(x)$ in $\mathscr{N}(\mathbb{T})$ is encodable in $\mathbb{T}$. Consider a representative $F(\mathbf{z}, z', u)$ of a morphism from $N_{k+1}(\mathbf{z}, z')$ to $N(x)$ in $\mathscr{N}(\mathbb{T})$. Since $\lceil \Psi(x, y, u) \rceil$ is a Turing morphism in $\mathscr{N}(\mathbb{T})$, there exists a total morphism $\lceil H(\mathbf{z}, u) \rceil : N_k(\mathbf{z}) \to N(x)$ in $\mathscr{N}(\mathbb{T})$ such that the diagram



(3.3.41)

commutes in $\mathscr{N}(\mathbb{T})$. It follows that

$$\vdash (\exists p)(H(\mathbf{z}, p) \wedge \Psi(p, z', u)) \Leftrightarrow F(\mathbf{z}, z', u) \tag{3.3.42}$$

holds in $\mathbb{T}$. Since $H(\mathbf{z}, u)$ is a representative of a morphism from N_k to N in $\mathscr{N}(\mathbb{T})$, it follows by the induction hypothesis that $H(\mathbf{z}, u)$ is encodable in $\mathbb{T}$. Hence, by Definition 3.3.2.2, there exists an $e \in \mathbb{N}$ such that

$$\vdash (\exists q)(\tau_k(\overline{e}, \mathbf{z}, q) \wedge U(q) = u) \Leftrightarrow H(\mathbf{z}, u) \tag{3.3.43}$$

holds in $\mathbb{T}$. It then follows from (3.3.42) and (3.3.43) that

$$\vdash (\exists p)[(\exists q)(\tau_k(\overline{e}, \mathbf{z}, q) \wedge U(q) = p) \wedge \Psi(p, z', u)] \Leftrightarrow F(\mathbf{z}, z', u)$$

holds in $\mathbb{T}$. By the definition of Ψ and the rules for $\exists$ and equality in $\mathbb{T}$, we thus obtain

$$\vdash (\exists q, r)[\tau_k(\overline{e}, \mathbf{z}, q) \wedge \tau_1(U(q), z', r) \wedge U(r) = u] \Leftrightarrow F(\mathbf{z}, z', u).$$

It then follows from the property $(\star)$ that

$$\vdash (\exists p)(\tau_{k+1}(C^k(\overline{e}), \mathbf{z}, z', p) \wedge U(p) = u) \Leftrightarrow F(\mathbf{z}, z', u)$$

holds in $\mathbb{T}$, from which it follows by ($\exists$-I) that

$$\vdash (\exists w)[(\exists p)(\tau_{k+1}(w, \mathbf{z}, z', p) \wedge U(p) = u) \Leftrightarrow F(\mathbf{z}, z', u)]$$

holds in $\mathbb{T}$. Hence, $F(\mathbf{z}, z', u)$ is encodable in $\mathbb{T}$.

It thus follows by induction on $k \geq 1$ that all representatives of a morphism from N_k to N in $\mathscr{N}(\mathbb{T})$ for all $k \geq 1$ are encodable in $\mathbb{T}$. ∎

We then obtain the following necessary and sufficient condition for a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to an intuitionistic arithmetical theory $\mathbb{T}$ with induction satisfying the property $(\star)$ to be a Turing category.

Theorem 3.3.2.12 *Let $\mathbb{T}$ be an intuitionistic arithmetical theory with induction satisfying property $(\star)$. Let $\mathscr{N}(\mathbb{T})$ be a computational subcategory associated to $\mathbb{T}$ containing the morphisms $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$ and $\lceil \mathbf{S}_1^n(x,\mathbf{z},u) \rceil : N_{n+1}(x,\mathbf{z}) \to N(x)$ (for all $n \geq 1$) from Proposition 3.3.2.6. Then, $\mathscr{N}(\mathbb{T})$ is a Turing category with Turing object $N(x)$ and Turing morphism $\lceil \Psi(x,y,u) \rceil : N_2(x,y) \to N(x)$ if and only if the representatives of all morphisms from N_k to N in $\mathscr{N}(\mathbb{T})$ (for all $k \geq 1$) are encodable in $\mathbb{T}$.*

Proof This result follows directly from Theorem 3.3.2.8 and Proposition 3.3.2.11. ∎

3.4 Conclusion

In this chapter, we have considered certain aspects of recursion theory in the setting of syntactic and syntactic partial map categories of arithmetical theories. We constructed a strong natural numbers object $N(x)$ in the syntactic category of an arithmetical theory $\mathbb{T}$ with induction using the encoding of sequences in $\mathbb{T}$ via a strong representing formula of Gödel's β-function. This construction is similar to that used to strongly represent functions obtained by primitive recursion (see Section 2.4.1.4). We then considered computational subcategories associated to an intuitionistic arithmetical theory $\mathbb{T}$ with induction. These are sub cartesian restriction categories of the syntactic partial map category $\mathscr{P}(\mathbb{T})$ on the powers of $N(x)$ that are candidates for being a Turing category with Turing object $N(x)$. We define a partial version of Church's Rule and a formalisation of the S-m-n Theorem in $\mathbb{T}$ in order to give some necessary and sufficient conditions for such a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to $\mathbb{T}$ to be a Turing category.

We make a few final observations. First, as discussed in Section 3.3.2.3, if we consider computational subcategories associated to an intuitionistic arithmetical theory $\mathbb{T}$ with induction that contain only total morphisms, we cannot obtain a Turing category. Indeed, such a computational subcategory $\mathscr{N}(\mathbb{T})$ of total morphisms corresponds to a subclass of the total recursive functions, and a Turing morphism in $\mathscr{N}(\mathbb{T})$ would correspond to an enumerating function of this subclass. Since it can be shown by the usual diagonal argument that any subclass of total recursive functions cannot contain an enumerating function for this subclass, $\mathscr{N}(\mathbb{T})$ cannot be a Turing category.

Second, we cannot use the constructions and arguments in Section 3.3.2 to consider Turing categories associated to classical arithmetical theories with induction. Indeed, in order to obtain a Turing category associated to an intuitionistic arithmetical theory with induction, we consider morphisms with representatives satisfying (PCR), the partial version of Church's Rule. Thus, the representatives of all total morphisms must also satisfy (CR), the usual version of Church's Rule. However, Church's Rule is incompatible with classical logic and does not hold in general in classical arithmetical theories with induction. Furthermore, in order to prove the necessary and sufficient condition in Section 3.3.2.4, we need the numerals in $\mathscr{C}(\mathbb{T})$ to be standard, which is not the case when $\mathbb{T}$ is classical. Therefore, we cannot apply the results and constructions from Section 3.3.2 to classical arithmetical theories with induction, only to intuitionistic ones.

Third, we remarked at the end of Section 3.3.2.2 that we might be able to find a concrete example of a computational subcategory $\mathscr{N}(\mathbb{T})$ associated to an intuitionistic arithmetical theory $\mathbb{T}$ that is a Turing category by considering the morphisms of $\mathscr{N}_F(\mathbb{T})$ that are equivalence classes of formulas $F(\mathbf{y}, u)$ such that $(\exists u)F(\mathbf{y}, u)$ is almost negative. Indeed, it is shown in [35] that a similar property to (PCR) holds for such formulas. Another possibility would be to consider morphisms of $\mathscr{N}_F(\mathbb{T})$ that are equivalence classes of Σ_1-formulas. We should be able to show that the class of representing formulas of partial recursive functions that are Σ_1-formulas is closed under composition, thus obtaining a computational subcategory with equivalence classes of Σ_1-formulas as morphisms. However, we would still need to determine if the other conditions from Theorem 3.3.2.8, such as (PCR), are satisfied.

Chapter 4

Future perspectives

Considering the material in Chapter 2 from a category-theoretic perspective leads us to consider the representability of computable functions in categories with a natural numbers object. The total numerical functions representable in the free cartesian category with weak parameterised natural numbers object are precisely the primitive recursive functions [28]. The total numerical functions representable in the free cartesian closed category with weak natural numbers object are a proper subset of the total recursive functions, namely the ϵ_0-recursive functions [16, 31]. The representability of partial numerical functions is also considered, albeit in different categories. In [16], it is shown that the partial numerical functions representable in the free topos and in the free C-monoid are precisely the partial recursive functions. In [23], the representability of partial recursive functions in monoidal categories with binary sums and weak left (or right) natural numbers object is considered.

We would like to expand on the work of Lambek, Scott, and Román [16, 28] on the representability of total recursive functions in cartesian and cartesian closed categories with natural numbers objects, in particular by adding equalisers and considering the representability of all partial recursive functions in this setting. Note that a cartesian category with equalisers is a lex category (also called a finitely complete category), and hence a cartesian closed category with equalisers may be called a cartesian closed lex category. We would like to do the following:

(i) Give a construction of $\mathcal{L}_N$, the free lex category with weak parameterised natural numbers object, and of $\mathcal{C}_N$, the free cartesian closed lex category with weak natural numbers object.

(ii) Give a notion of representability of a partial numerical function in $\mathcal{L}_N$ and $\mathcal{C}_N$ that generalises the notion of representability of a total numerical function in such categories given in [16, p. 257].

(iii) Determine the subclass of total recursive functions that are representable in $\mathcal{L}_N$ and $\mathcal{C}_N$.

(iv) Determine the subclass of partial recursive functions that are representable in $\mathcal{L}_N$ and $\mathcal{C}_N$.

Román conjectured that a partial numerical function is representable in $\mathcal{C}_N$ if and only if it is partial recursive. Although this claim seems reasonable, Román never gave a satisfactory proof of his conjecture. Indeed, he never gave a concrete definition or construction of $\mathcal{C}_N$, nor did he give an adequate definition of the representability of a partial numerical function in $\mathcal{C}_N$ [27].

We propose to use the notions of Partial Horn Logic and quasi-equational theories presented by Palmgren and Vickers [22] in order to construct $\mathcal{L}_N$ and $\mathcal{C}_N$. Palmgren and Vickers construct a quasi-equational theory for a lex category, which we call $\mathbb{T}_{lex}$ (although it is called $\mathbb{T}_{cart}$ in [22]). Since a lex category $\mathscr{C}$ is cartesian closed if and only if the slice category $\mathscr{C}/1$ over the terminal object 1 is cartesian closed, we can adapt the construction of the quasi-equational theory $\mathbb{T}_{lccc}$ for a locally cartesian closed lex category in [22] in order to obtain a quasi-equational theory $\mathbb{T}_{cclex}$ for a cartesian closed lex category. We can then extend the theories $\mathbb{T}_{lex}$ and $\mathbb{T}_{cclex}$ to obtain a quasi-equational theory $\mathbb{T}^N_{lex}$ for a lex category with weak parameterised natural numbers object and a quasi-equational theory $\mathbb{T}^N_{cclex}$ for a cartesian closed lex category with weak natural numbers object, respectively, using the discussion in [22, p. 329] on how to express categorical structure quasi-equationally and the presentation of natural numbers objects in [16, §I.9–I.11].

For any quasi-equational theory $\mathbb{T}$, we can construct the closed term model $Ter(\mathbb{T})$, which consists of the sets of closed provably defined terms of each sort modulo provable equality and interprets each closed provably defined term as itself. $Ter(\mathbb{T})$ is the initial set-theoretic model of $\mathbb{T}$, and hence $Ter(\mathbb{T})$ is initial in $\mathbb{T}-\mathbf{PMod}$, the category of all set-theoretic models of $\mathbb{T}$ [22, §3–4.1]. It is shown in [22] that the set-theoretic models of $\mathbb{T}_{lex}$ correspond exactly to the small lex categories. We can show an analogous result, namely that set-theoretic models of $\mathbb{T}^N_{lex}$ and $\mathbb{T}^N_{cclex}$ are exactly the categories in $\mathbf{lex_N}$ (the category of all small lex categories with weak parameterised natural numbers object) and in $\mathbf{cclex_N}$ (the category of all small cartesian closed lex categories with weak natural numbers object), respectively. More precisely, we can construct the following isomorphisms of categories:

$$\mathbb{T}^N_{lex}-\mathbf{PMod} \underset{\underset{\mathbf{M}}{\cong}}{\overset{\overset{\mathbf{C}}{\cong}}{\rightleftarrows}} \mathbf{lex_N}$$

and

$$\mathbb{T}^N_{cclex}-\mathbf{PMod} \underset{\underset{\mathbf{M}}{\cong}}{\overset{\overset{\mathbf{C}}{\cong}}{\rightleftarrows}} \mathbf{cclex_N} \ .$$

We therefore obtain concrete constructions of the free categories $\mathcal{L}_N$ and $\mathcal{C}_N$ by constructing the closed term models $Ter(\mathbb{T}^N_{lex})$ and $Ter(\mathbb{T}^N_{cclex})$ and applying the appropriate isomorphism $\mathbf{C}$ from above.

We can then consider the representability of both total and partial numerical functions in the free categories $\mathcal{L}_N$ and $\mathcal{C}_N$. For the representability of total numerical functions, we simply use the following definition from [16, p. 257].

Definition 4.0.0.1 [16, p. 257] Let $\mathscr{C}$ be a cartesian category with weak parameterised natural numbers object $1 \xrightarrow{0} N \xrightarrow{S} N$. For all $n \geq 0$, we denote the n^{th} standard numeral S^n0 of $\mathscr{C}$ by $\overline{n} : 1 \to N$. A total function $f : \mathbb{N}^k \to \mathbb{N}$ is said to be *representable* in $\mathscr{C}$ if there exists a morphism $F : N^k \to N$ in $\mathscr{C}$ such that, for all $(m_1, \ldots, m_k) \in \mathbb{N}^k$,

$$F \circ \langle \overline{m_1}, \ldots, \overline{m_k} \rangle = \overline{f(m_1, \ldots, m_k)}. \tag{4.0.1}$$

□

It is then a straightforward matter to adapt the proofs in [16, 28] to show that all primitive recursive functions are representable in $\mathcal{L}_N$ and $\mathcal{C}_N$. More generally, we wish to determine exactly which subclasses of total recursive functions are representable in $\mathcal{L}_N$ and in $\mathcal{C}_N$. We conjecture that the presence of all finite limits will allow us to represent more total recursive functions than in the free cartesian category with weak parameterised natural numbers object and in the free cartesian closed category with weak natural numbers object. In fact, we claim that all total recursive functions are representable in $\mathcal{C}_N$. In order to prove this result, we need to determine how to represent functions obtained by total minimisation using equalisers or other finite limits.

To be able to consider the representability of partial numerical functions in $\mathcal{L}_N$ and $\mathcal{C}_N$, we first need to find an appropriate definition of this notion. We want the definition of representability of a partial numerical function to be equivalent to the definition in [16, p. 257] in the case of total functions and to adequately express the inherent partial nature of non-total functions. That is to say, if $f : \mathbb{N}^k \to \mathbb{N}$ is a total function and $g : \mathbb{N}^k \dashrightarrow \mathbb{N}$ is a partial function that is a restriction of f to a strictly smaller domain of definition, we do not want to allow f and g to be representable by the same morphism in a category. A possible definition of representability of a partial numerical function in $\mathcal{L}_N$ and $\mathcal{C}_N$ that we might consider is obtained from Definition 4.0.0.1 by allowing $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ to be partial and replacing (4.0.1) by

$$f(m_1, \ldots, m_k) \simeq n \text{ if and only if } F \circ \langle \overline{m_1}, \ldots, \overline{m_k} \rangle = \overline{n}. \tag{4.0.2}$$

This definition is similar to the definition of strong representability of a partial function in a monoidal category from [23, §5]. However, this definition, although it would generalise Definition 4.0.0.1 to partial functions, does not seem adequate. Indeed, if $F : N^k \to N$ represents some partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ in $\mathcal{L}_N$ (or $\mathcal{C}_N$) according to this definition and $f(m_1, \ldots, m_k)$ is not defined for some $(m_1, \ldots, m_k) \in \mathbb{N}^k$, then

$F \circ \langle \overline{m_1}, \ldots, \overline{m_k} \rangle : 1 \to N$ is a morphism from 1 to N in $\mathcal{L}_N$ ($\mathcal{C}_N$, respectively) that cannot be equal to any standard numeral $\overline{n} : 1 \to N$. Since it seems likely that the numerals of $\mathcal{L}_N$ and $\mathcal{C}_N$ are standard, it would then be impossible to represent any non-total function in these categories.

A possible solution would be to use the notion of partial morphism in a lex category defined in [22, §7]. Such a partial morphism $f : A \rightharpoondown B$ in a lex category $\mathscr{C}$ is a pair (d_f, m_f), where $d_f : D_f \to A$ is a monomorphism in $\mathscr{C}$ called the *domain of definition* of f and $m_f : D_f \to B$ is any morphism in $\mathscr{C}$. We shall therefore refer to such partial morphisms as *spans*. Equality of spans is defined by the following equivalence relation: two spans $f, f' : A \rightharpoondown B$ are equal if and only if there exists an isomorphism $h : D_{f'} \to D_f$ such that

$$d_f \circ h = d_{f'}.$$

The (partial) composition of spans $f : A \rightharpoondown B$ and $g : B \rightharpoondown C$, denoted $g \odot f$, is obtained by taking the pullback of m_f and d_g. Note that any morphism $f : A \to B$ of $\mathscr{C}$ can be viewed as the span $\widehat{f} = (1_A, f) : A \rightharpoondown B$ [22].

We could then attempt to represent a partial function $f : \mathbb{N}^k \dashrightarrow \mathbb{N}$ in $\mathcal{L}_N$ or $\mathcal{C}_N$ by a span $F = (m_F, d_F) : N^k \rightharpoondown N$. Since morphisms of $\mathcal{L}_N$ and $\mathcal{C}_N$ can be viewed as spans, this notion of representability of partial functions would generalise the notion of representability in Definition 4.0.0.1 in the case of total functions.

Once we have determined a satisfactory definition for the representability of partial numerical functions in $\mathcal{L}_N$ and $\mathcal{C}_N$, we can then consider which subclass of the partial recursive functions are representable in these categories. We would hope to be able to show that all partial recursive functions are representable in $\mathcal{C}_N$, thus proving Román's conjecture.

Appendix A

First-order languages and theories

We assume that the reader is familiar with the notions of first-order languages and theories. For reference, see for example [33], [19], and [14]. Since the presentation of first-order languages and theories varies from author to author, we present here the terminology and notation we chose to use.

A.1 First-order languages

Since we wish to consider both intuitionistic and classical theories, we need to define all logical connectives and quantifiers separately, as the usual relationships between the connectives and quantifiers that are valid in classical logic and are used in order to define certain quantifiers and connectives in terms of others are not valid intuitionistically in general.

Definition A.1.0.1 A first-order language $\mathscr{L}$ is a formal language with *signature* $\Sigma_{\mathscr{L}}$ consisting of the following symbols:

(i) A countably infinite set of *variables*, generally denoted by $x, y, z, w, x', y', z', w', x_1, x_2, \ldots$ Since there are countably many variables, we choose a fixed enumeration of the variables, called the *standard enumeration*, which will be the same for all first-order languages.

(ii) The *logical connectives* $\neg$, $\wedge$, $\vee$, $\Rightarrow$, the *existential quantifier* $\exists$, and the *universal quantifier* $\forall$.

(iii) A finite or countably infinite set of *predicate symbols*, each having an *arity* $k \geq 0$. Among the predicate symbols must necessarily be the binary predicate $=$ for equality.

(iv) A finite or countably infinite (possibly empty) set of *function symbols*, each having an *arity* $k \geq 0$. A function symbol of arity 0 is called a *(formal) constant.*

The function symbols and the predicate symbols other than = are called *nonlogical symbols*; all other symbols are called *logical symbols*. The set of nonlogical symbols of $\mathscr{L}$ is denoted by $\Sigma^N_{\mathscr{L}}$.

We then define the *terms* of $\mathscr{L}$ via the following generalised inductive definition:

(i) A variable is a term.

(ii) If f is a k-ary function symbol and $t_1, \ldots, t_k$ are terms, then $f(t_1, \ldots, t_k)$ is a term. Note that if we consider the case $k = 0$, we obtain that formal constants are terms.

The set of terms of $\mathscr{L}$ is denoted $TERM_{\mathscr{L}}$. The *formulas* of $\mathscr{L}$ are then given by the following generalised inductive definition:

(i) If P is a k-ary function symbol and $t_1, \ldots, t_k$ are terms of $\mathscr{L}$, then $P(t_1, \ldots, t_k)$ is called an *atomic formula*. Every atomic formula is a formula.

(ii) If A is a formula, then $\neg A$ is a formula.

(iii) If A, B are formulas, then $A \wedge B$, $A \vee B$, and $A \Rightarrow B$ are formulas.

(iv) If A is a formula and x is a variable, then $(\exists x)A$ and $(\forall x)A$ are formulas.

The set of formulas of $\mathscr{L}$ is denoted $FOR_{\mathscr{L}}$. An *expression* of $\mathscr{L}$ is either a term or a formula of $\mathscr{L}$.

A first-order language is completely determined by its nonlogical symbols. These symbols may be any symbols which are not already assigned to another purpose. However, we follow Shoenfield's convention and agree that, if a symbol is used as an n-ary function symbol in one first-order language, then it will not be used in any other first-order language except as an n-ary function symbol (for the same n); and similarly for predicate symbols. Hence, if two first-order languages have the same nonlogical symbols, they are identical [33, p. 15]. □

Given two first-order languages $\mathscr{L}_1$ and $\mathscr{L}_2$, we call $\mathscr{L}_1$ a *sublanguage* of $\mathscr{L}_2$ and, equivalently, we call $\mathscr{L}_2$ an *extension* of $\mathscr{L}_1$ if each symbol of $\mathscr{L}_1$ is a symbol of $\mathscr{L}_2$, i.e. if $\Sigma^N_{\mathscr{L}_1} \subseteq \Sigma^N_{\mathscr{L}_2}$. If $\mathscr{L}_1$ and $\mathscr{L}_2$ are both extensions of each other, then they have the same set of nonlogical symbols and so are in fact the same language.

We introduce the following additional definitions, terminology, notations and conventions:

(i) We generally use the following letters to denote the following mathematical objects or symbols, although some overlap may occur in practice, but this will be clear from context:

(a) $i, j, k, m, n, \ldots$ for natural numbers and indices,

(b) Roman capitals such as $E, F, P, Q, \ldots$ for relations on $\mathbb{N}$,

(c) $t, s, r, \ldots$ for terms,

(d) Roman capitals such as $A, B, C, D, \ldots$ or greek letters such as $\varphi, \psi, \gamma, \theta, \ldots$ for formulas,

(e) Roman capitals such as $P, Q, \ldots$ for predicate symbols,

(f) $x, y, z, u, v, w, \ldots$ for variables,

(g) $f, g, h, \ldots$ for function symbols and for functions in the usual sense (e.g. over $\mathbb{N}$),

(h) $a, b, c, d, e, \ldots$ for (formal) constants and for arbitrary variables used in derivations.

(ii) We use bold letters such as $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}, \ldots$ to denote lists of (distinct) variables, and we denote the length of a list $\mathbf{x}$ of variables by $|\mathbf{x}|$. We say that two lists $\mathbf{x}$ and $\mathbf{y}$ are *disjoint* if there is no variable that appears in both $\mathbf{x}$ and $\mathbf{y}$. Note that this is not the same as $\mathbf{x}$ and $\mathbf{y}$ being *distinct*. Indeed, the lists x_1, x_2 and x_1, x_2, x_3 are distinct but not disjoint.

(iii) We mostly follow [14, §18, 33, pp. 16–17] for the notions of free and bound variables and substitution. An occurrence of a variable x in a formula A may be either bound or free. An occurrence of x in A is *bound* if it occurs in a subformula of A of the form $(\exists x)B$ or $(\forall x)B$ for some formula B; otherwise it is a *free* occurrence. The variable x is said to be *bound (free) in* A if some occurrence of x is bound (respectively, free) in A. Note that x may be both bound and free in A. A is said to be *open* if it contains no bound variables (i.e. if it contains no quantifiers) and *closed* if it contains no free variables.

A term t is said to be *free* or *substitutable for* x in A if replacing all free occurrences of x in A by the term t does not cause any of the variables in t to become bound in the new formula thus obtained, i.e. if for each variable y in t, no subformula of A of the form $(\exists y)B$ or $(\forall y)B$ contains an occurrence of x that is free in A. If t is free for x in A, we may form the formula $A\left[\frac{t}{x}\right]$ by replacing each free occurrence of x in A by the term t. This can be extended to the several variable case $A\left[\frac{t_1}{x_1}, \ldots, \frac{t_k}{x_k}\right]$, where it is agreed that $x_1, \ldots, x_k$ are distinct variables and each t_i is free for x_i in A. Moreover, we may sometimes write $A(x)$ to emphasize the fact that the variable x may (or may not as the case may be) occur free in A and that no other variable occurs free in A. Similarly, writing $A(x_1, \ldots, x_n)$ means that the free variables of A are among $x_1, \ldots, x_n$. Then, $A\left[\frac{t}{x}\right]$ may be written as $A(t)$ and $A\left[\frac{t_1}{x_1}, \ldots, \frac{t_n}{x_n}\right]$ may be written as $A(t_1, \ldots, t_n)$ if it is clear from the context which terms are being substituted for which variables.

(iv) We adopt the following conventions regarding the use of parentheses in formulas:

(a) The logical connectives and quantifiers in decreasing order of binding strength are: $\neg$, $\forall$ and $\exists$, $\wedge$ and $\vee$, $\Rightarrow$ and $\Leftrightarrow$. Hence, $\neg A \Rightarrow \neg B$ means $(\neg A) \Rightarrow (\neg B)$, $A \Leftrightarrow B \vee C$ means $A \Leftrightarrow (B \vee C)$, and $(\forall x)A \wedge B \Rightarrow (\exists y)C$ means $(((\forall x)A) \wedge B) \Rightarrow ((\exists y)C)$. Furthermore, no further parentheses may be omitted from $(\neg(A \vee B) \Rightarrow C) \wedge D$ and $(\exists x)(A \Rightarrow B \vee C)$ without changing the formulas.

(b) Repeated logical connectives and quantifiers of the same strength are by default associated to the right. Hence, $A \Rightarrow B \Rightarrow C$ means $A \Rightarrow (B \Rightarrow C)$, $\neg\neg A$ means $\neg(\neg A)$, $(\forall x)(\exists y)A$ means $(\forall x)((\exists y)A)$, $A \vee B \vee C$ means $A \vee (B \vee C)$, and $A \wedge B \wedge C$ means $A \wedge (B \wedge C)$.

Note that while repeated $\wedge$ and $\vee$ connectives are by default associated to the right, $\wedge$ and $\vee$ are provably associative in all of the theories we consider, and so the exact placement of parentheses will become irrelevant in this situation.

(v) We define the following abbreviations of formulas, where $\mathbf{x}$ and $\mathbf{y}$ denote the lists $x_1, \ldots, x_k$ and $y_1, \ldots, y_k$ of (distinct) variables:

- If $\bigcirc$ is a binary function or predicate symbol, then $t \bigcirc s$ abbreviates $\bigcirc(t, s)$
- If $\bigcirc$ is a binary predicate symbol, then $t \not\bigcirc s$ abbreviates $\neg(t \bigcirc s)$
- $(\forall x_1, \ldots, x_k)A$ or $(\forall \mathbf{x})A$ abbreviates $(\forall x_1)(\forall x_2) \cdots (\forall x_k)A$
- $(\exists x_1, \ldots, x_k)A$ or $(\exists \mathbf{x})A$ abbreviates $(\exists x_1)(\exists x_2) \cdots (\exists x_k)A$
- $\bigvee_{i=1}^{k} A_i$ abbreviates $A_i \vee \ldots \vee A_k$
- $\bigwedge_{i=1}^{k} A_i$ abbreviates $A_i \wedge \ldots \wedge A_k$
- $\mathbf{x} = \mathbf{y}$ abbreviates $x_1 = y_1 \wedge \ldots \wedge x_k = y_k$

A.2 First-order theories

Formally, an intuitionistic (classical) first-order theory $\mathbb{T}$ with equality over a first-order language $\mathscr{L}$ is a formal theory defined using the logical axioms and rules of inference for intuitionistic (classical, respectively) predicate calculus in [14, §19 pp. 81–83, §23 p. 101] together with the following logical axioms for equality

(i) $x = y \vee x \neq y$

(ii) $x = x$

(iii) $x = y \Rightarrow y = x$

(iv) $x = y \wedge y = z \Rightarrow x = z$

and possibly some nonlogical axioms, which vary from theory to theory. A formal deduction of a formula A from a finite set of formulas Γ is then defined to be a finite list of formulas such that the last formula is A and each formula in the list is either an axiom of $\mathbb{T}$ or an immediate consequence of preceding formulas in the list via one of the inference rules. We write $\Gamma \vdash_{\mathbb{T}} A$ to say that such a list exists [14, §20].

However, for our purposes, it is simpler to use the equivalent presentation of first-order theories in Definition A.2.0.1, where we specify deduction rules for the provability relation $\vdash_{\mathbb{T}}$ directly (see also [14, §20–23] and [19, §2.3–2.6]). This yields an equivalent and more easily usable presentation of a first-order theory. In particular, we allow ourselves the abuse of notation stating that $\Gamma \vdash A$ *is* a formal deduction, although it in fact merely indicates the existence of one.

Definition A.2.0.1 (First-order theory) Let $\mathscr{L}$ be a first-order language. A *first-order theory* $\mathbb{T}$ (with equality) in the language $\mathscr{L}$ is a formal theory given by the following elements:

(i) The language of $\mathbb{T}$ is $\mathscr{L}$.

(ii) The axioms of $\mathbb{T}$ consist of certain specified formulas of $\mathbb{T}$ and are divided into two different types. There is a set $NLA_{\mathbb{T}}$ of formulas called the *nonlogical axioms*. This set may be empty, finite or countably infinite and varies from theory to theory. The only *logical axiom* present in all first-order theories is the axiom for the decidability of equality, namely

(DE) $x = y \vee x \neq y$

(iii) A provability relation $\vdash_{\mathbb{T}}$ satisfying the general properties and deduction rules given below. Note that we may omit the subscript if no ambiguity arises. If Γ is a finite set of formulas of $\mathbb{T}$ and A is a formula of $\mathbb{T}$, we write

$$\Gamma \vdash A$$

and say that "Γ proves A (in $\mathbb{T}$)" if A can be deduced from Γ using a finite number of the deduction rules and general properties of $\vdash$. As noted above, we call both the statement $\Gamma \vdash A$ and its proof a *formal deduction of A from Γ (in $\mathbb{T}$)* although, strictly speaking, the statement $\Gamma \vdash A$ indicates the *existence* of such a formal deduction. The formulas in the set Γ are called the *premisses* and A is called the *conclusion* of the formal deduction $\Gamma \vdash A$. By convention, sets of premisses are always finite.

If $\Gamma = \varnothing$, we write $\vdash A$, if $\Gamma = \{A_1, \ldots, A_k\}$, we write $A_1, \ldots, A_k \vdash A$, and if $\Gamma = \Delta_1 \cup \Delta_2$ or $\Gamma = \Delta \cup \{B\}$, we write $\Delta_1, \Delta_2 \vdash A$ or $\Delta, B \vdash A$, respectively.

The general properties of the provability relation are as follows:

(a) $\Gamma \vdash A$ for all $A \in \Gamma$.

(b) If $\Gamma \vdash A$, then $\Delta, \Gamma \vdash A$ for any set Δ of premisses. In particular, if A is a theorem of $\mathbb{T}$, then $\Gamma \vdash A$ for any set Γ of premisses.

(c) If $\Gamma \vdash A$, then $\Delta \vdash A$, where Δ is obtained from Γ by omitting any of the formulas of Γ which are provable in $\mathbb{T}$ or deducible from the remaining formulas.

The deduction rules consist of introduction rules, denoted ($\bigcirc$-I), and elimination rules, denoted ($\bigcirc$-E), for the logical connectives, quantifiers, and equality. Note that in the presentation of the rules below, Γ is a set of premisses, A, B, C are formulas, t, s are terms and x, u are variables.

($\exists$-I) If $\Gamma \vdash A\left[\frac{t}{x}\right]$, then $\Gamma \vdash (\exists x)A$.

($\exists$-E) If $\Gamma \vdash (\exists x)A$ and $\Gamma, A\left[\frac{b}{x}\right] \overset{b}{\vdash} B$, then $\Gamma \vdash B$, where b is some arbitrary variable that does not occur free in B or in any formula of Γ.

($\forall$-I) If $\Gamma \vdash A\left[\frac{u}{x}\right]$, then $\Gamma \vdash (\forall x)A$, provided that u does not occur free in $(\forall x)A$ or in any formula of Γ.

($\forall$-E) If $\Gamma \vdash (\forall x)A$, then $\Gamma \vdash A\left[\frac{t}{x}\right]$, where t is free for x in A.

($\wedge$-I) If $\Gamma \vdash A$ and $\Gamma \vdash B$, then $\Gamma \vdash A \wedge B$.

($\wedge$-E) If $\Gamma \vdash A \wedge B$, then $\Gamma \vdash A$ and $\Gamma \vdash B$.

($\Rightarrow$-I) If $\Gamma, A \vdash B$, then $\Gamma \vdash A \Rightarrow B$.

($\Rightarrow$-E) If $\Gamma \vdash A$ and $\Gamma \vdash A \Rightarrow B$, then $\Gamma \vdash B$.

($\vee$-I) If $\Gamma \vdash A$, then $\Gamma \vdash A \vee B$ and $\Gamma \vdash B \vee A$.

($\vee$-E) If $\Gamma \vdash A \vee B$, $\Gamma, A \vdash C$, and $\Gamma, B \vdash C$, then $\Gamma \vdash C$.

($\neg$-I) If $\Gamma, A \vdash B$ and $\Gamma, A \vdash \neg B$, then $\Gamma \vdash \neg A$.

(Con) If $\Gamma \vdash A$ and $\Gamma \vdash \neg A$, then $\Gamma \vdash B$.

Note that "Con" stands for "Contradiction". This rule is also sometimes known as (*weak*) ($\neg$-E).

(=-I) $\Gamma \vdash t = t$, where t is any term.

(=-E) If $\Gamma \vdash t = s$ and $\Gamma \vdash A\left[\frac{t}{x}\right]$, then $\Gamma \vdash A\left[\frac{s}{x}\right]$, where t, s are terms free for x in A.

The set $\mathit{THM}_{\mathbb{T}}$ of *theorems* of $\mathbb{T}$ is the set of all formulas A such that $\vdash_{\mathbb{T}} A$ holds. □

If $\vdash_{\mathbb{T}} A$, we say that "A is a theorem of $\mathbb{T}$", "A is provable in $\mathbb{T}$", or "A is provably true in $\mathbb{T}$". If $\nvdash_{\mathbb{T}} A$ we say that "A is not a theorem of $\mathbb{T}$", that "A is not provable in $\mathbb{T}$", or that "A is not provably true in $\mathbb{T}$". It is only when we have $\vdash_{\mathbb{T}} \neg A$ that we say that "A is *(provably) false* in $\mathbb{T}$" or that "A is or *refutable* in $\mathbb{T}$".

Note also that we shall henceforth generally use the term *theory* to mean "first-order theory with equality" as defined in Definition A.2.0.1.

Let $\mathbb{T}$ be a theory and let A be a formula of $\mathbb{T}$. A *variant* of A is a formula A' obtained from A by renaming any number of bound variables of A in such a way that no variable-capture occurs. Since all variants of A are provably equivalent to A in $\mathbb{T}$ [33, Ch. 4], we may freely change bound variables in formulas of $\mathbb{T}$. Moreover, we may henceforth assume that no variable-capture occurs during substitution, as we may always use variants of formulas in which the bound variables are distinct from all other variables in play.

We can also introduce a new defined symbol for unique existence as follows.

Definition A.2.0.2 Let $\mathbb{T}$ be a theory and let A be a formula of $\mathbb{T}$. Then, we can define $(\exists! x)A$ as an abbreviation for the formula

$$(\exists x)A \wedge (\forall x)(\forall y)\left(A \wedge A\left[\frac{y}{x}\right] \Rightarrow x = y\right),$$

where, due to the equivalence of variants in $\mathbb{T}$, we only need to require that y be distinct from x and free for x in A.

Note that if we wish to specify the formula abbreviated by $(\exists! x)A$ exactly (including the specific choice of bound variables), we can require y to be the first variable in the standard enumeration of the variables that does not occur in A and is distinct from x. □

Definition A.2.0.3 (Extensions and subtheories) [33, pp. 41–42, 19, p. 79]

(i) The theory $\mathbb{T}'$ is an *extension* of the theory $\mathbb{T}$ (equivalently, $\mathbb{T}$ is a *subtheory* of $\mathbb{T}'$) if $\mathscr{L}(\mathbb{T}')$ is an extension of $\mathscr{L}(\mathbb{T})$ and every theorem of $\mathbb{T}$ is a theorem of $\mathbb{T}'$. Equivalently, $\mathbb{T}'$ is an extension of $\mathbb{T}$ if $\mathscr{L}(\mathbb{T}')$ is an extension of $\mathscr{L}(\mathbb{T})$ and every axiom (logical and nonlogical) of $\mathbb{T}$ is a theorem of $\mathbb{T}'$.

(ii) The theories $\mathbb{T}$ and $\mathbb{T}'$ are *equivalent* if each is an extension of the other, that is, if they have the same language and the same theorems. Note that if $\mathbb{T}'$ is an extension of $\mathbb{T}$, then any theory equivalent to $\mathbb{T}'$ is an extension of any theory equivalent to $\mathbb{T}$.

(iii) $\mathbb{T}'$ is a *conservative extension* of $\mathbb{T}$ if $\mathbb{T}'$ is an extension of $\mathbb{T}$ such that every formula of $\mathbb{T}$ which is a theorem of $\mathbb{T}'$ is also a theorem of $\mathbb{T}$. Note that if $\mathbb{T}'$ is a conservative extension of $\mathbb{T}$, then a formula of $\mathbb{T}$ is a theorem of $\mathbb{T}$ if and only if it is a theorem of $\mathbb{T}'$. □

Following the treatment in [33, pp. 57–61], we obtain a notion of extensions by definitions which will later prove useful.

Definition A.2.0.4 (Extensions by definitions) Let $\mathbb{T}$ a theory over a language $\mathscr{L}$. We present two ways of obtaining an extension of $\mathbb{T}$.

(i) Let D_P be a formula of $\mathbb{T}$ and let $x_1, \ldots, x_n$ be a list of variables of $\mathbb{T}$ containing the free variables of D_P. We obtain an extension of $\mathbb{T}$ by adjoining a new n-ary predicate symbol P to the language $\mathscr{L}$ and a new axiom

$$P(x_1, \ldots, x_n) \Leftrightarrow D_P,$$

called the *defining axiom* of P, to the set of nonlogical axioms of $\mathbb{T}$.

(ii) Let D_f be a formula of $\mathbb{T}$ and let $x_1, \ldots, x_n, y$ be a list of variables of $\mathbb{T}$ containing the free variables of D_f. We obtain an extension of $\mathbb{T}$ by adjoining a new n-ary function symbol f to the language $\mathscr{L}$ and a new axiom

$$f(x_1, \ldots, x_n) = y \Leftrightarrow D_f,$$

called the *defining axiom* of f, to the set of nonlogical axioms of $\mathbb{T}$.

Any extension $\mathbb{T}'$ of $\mathbb{T}$ obtained from $\mathbb{T}$ by a finite number of successive extensions described in (i)–(ii) above is said to be an *extension by definitions* of $\mathbb{T}$. □

Let $\mathbb{T}$ be a theory and let $\mathbb{T}'$ be an extension by definitions of $\mathbb{T}$. Then, $\mathbb{T}'$ is a conservative extension of $\mathbb{T}$ and $\mathbb{T}'$ is consistent if and only if $\mathbb{T}$ is consistent [33, pp. 57–61].

We make a similar distinction between intuitionistic and classical theories to the one in [14, §23].

Definition A.2.0.5 (Intuitionistic and classical theories) Let $\mathbb{T}$ be a theory over a language $\mathscr{L}$. If for every formula A in $\mathbb{T}$,

$$\vdash A \vee \neg A$$

holds in $\mathbb{T}$, $\mathbb{T}$ is said to be *classical*. Otherwise, $\mathbb{T}$ is said to be *intuitionistic*. □

If $\mathbb{T}$ is any theory, we define $\mathbb{T}_C$ to be the theory obtained from $\mathbb{T}$ by adding the following axiom scheme for the rule of the excluded middle:

(EM) $A \vee \neg A$, where A is any formula of $\mathscr{L}(\mathbb{T})$.

If $\mathbb{T}$ is a classical theory, then $\mathbb{T}$ is equivalent (as theories) to the theory $\mathbb{T}_C$ obtained from $\mathbb{T}$ by adding the axiom scheme (EM). Hence, we may assume without loss of generality that every classical theory $\mathbb{T}$ has (EM) as an explicit axiom scheme, as we may always work in $\mathbb{T}_C$ instead of $\mathbb{T}$ without changing the set of theorems in any way.

It follows from this assumption that, in order to fully specify a theory over a language $\mathscr{L}$, it suffices to specify whether it is intuitionistic or classical and which nonlogical axioms are chosen. Furthermore, the axiom scheme (EM) is considered to be a logical axiom scheme of any classical theory as we consider it to be present in each of them. In particular, a classical first-order theory with a finite number of nonlogical axioms is still finitely axiomatised (see Definition 2.2.1.2); the presence of the infinite axiom scheme (EM) does not change this.

A.3 Derived rules and further results

We summarise here some derived rules and other results in first-order theories. Most of the material in this section is taken or adapted from [14] or [33]. The proofs of the results given here are either very straightforward or adapted from [14] or [33], and hence generally omitted.

Unless clearly specified otherwise, we assume that we are working in an arbitrary theory $\mathbb{T}$ (which could be either intuitionistic or classical).

Proposition A.3.0.1 *Let $\mathbb{T}$ be a theory. If $\mathbb{T}$ contains the formal constant 0, we define $\top \underset{\text{def}}{\equiv} 0 = 0$. If $\mathbb{T}$ does not contain 0, we define $\top \underset{\text{def}}{\equiv} (\forall x)(x = x)$. We define $\bot$ to be the negation of $\top$, that is, we define $\bot \underset{\text{def}}{\equiv} \neg\top$. We consider $\top$ and $\bot \underset{\text{def}}{\equiv} \neg\top$ to be fixed for any theory $\mathbb{T}$. Note that $\top$ and $\bot$ are closed formulas of $\mathbb{T}$ such that $\top$ is provably true in $\mathbb{T}$ and $\bot$ is provably false in $\mathbb{T}$.*

Using $\bot$, we obtain the following derived rules, where A is any formula of $\mathbb{T}$:

($\bot$-I) If $\Gamma \vdash A$ and $\Gamma \vdash \neg A$, then $\Gamma \vdash \bot$.

($\bot$-E) If $\Gamma \vdash \bot$, then $\Gamma \vdash B$ for any formula B.

($\neg$-I) If $\Gamma, A \vdash \bot$, then $\Gamma \vdash \neg A$.

Note that this is a special case of the ($\neg$-I) rule in Definition A.2.0.1 and will also be referred to as ($\neg$-I).

Note that since a formula that is always false is a unit for disjunction, we consider the empty disjunction to be the formula $\bot$.

Proposition A.3.0.2 *The following versions of the* Cut Rule, *both denoted* (Cut), *hold for any theory $\mathbb{T}$.*

(i) If $\Gamma \vdash A$ and $\Delta, A \vdash B$, then $\Gamma, \Delta \vdash B$.

(ii) If $\Gamma \vdash A_i$ for $1 \leq i \leq n$ and $\Delta, A_1, \ldots, A_n \vdash B$, then $\Gamma, \Delta \vdash B$.

Proposition A.3.0.3 [14, §26–27] *Let $\mathbb{T}$ be a theory. $\wedge$ and $\vee$ are associative, commutative and distribute over one another. Moreover, if $n \geq 2$ and $A_1, \ldots, A_n$ are formulas of $\mathbb{T}$, we obtain*

(i) $\vdash (\neg A_1 \wedge \ldots \wedge \neg A_n) \Leftrightarrow \neg(A_1 \vee \ldots \vee A_n)$

(ii) $\vdash (\neg A_1 \vee \ldots \vee \neg A_n) \Rightarrow \neg(A_1 \wedge \ldots \wedge A_n)$

Note that the converse of (ii) is not provable in general if $\mathbb{T}$ is intuitionistic. However, if $\mathbb{T}$ is classical, then the converse of (ii) is provable, and hence both of the De Morgan laws hold, that is,

(ii)' $\vdash (\neg A_1 \vee \ldots \vee \neg A_n) \Leftrightarrow \neg(A_1 \wedge \ldots \wedge A_n)$

holds when $\mathbb{T}$ is classical.

In view of Proposition A.3.0.3 and the Equivalence Theorem (Theorem A.3.0.7) proved below, we can use the usual properties of $\wedge$ and $\vee$ at will in a theory $\mathbb{T}$. Moreover, we can consider repeated $\wedge$ or $\vee$ connectives to be associated either to the right (as they are by default) or to the left (since this is then a provably equivalent formula) as convenient. Indeed, we shall generally omit all parentheses in sequences of repeated $\wedge$ and $\vee$ connectives as Theorem A.3.0.7 allows us to consider provably equivalent formulas and subformulas as being effectively interchangeable.

Lemma A.3.0.4 *Let $\mathbb{T}$ be a theory. The following derived rules adapted from [14, §27, Theorem 7] give additional methods for eliminating a disjunction and may all be referred to as ($\vee$-E).*

(i) Let A, B be any formulas.

$$\text{If } \Gamma \vdash A \vee B \text{ and } \Gamma \vdash \neg A, \text{ then } \Gamma \vdash B.$$

$$\text{If } \Gamma \vdash A \vee B \text{ and } \Gamma \vdash \neg B, \text{ then } \Gamma \vdash A.$$

(ii) Let $n \geq 2$ and let $A_1, \ldots, A_n$ be any formulas.

$$\text{If } \Gamma \vdash A_1 \vee \ldots \vee A_n \text{ and } \Gamma, A_i \vdash B \text{ for all } 1 \leq i \leq n, \text{ then } \Gamma \vdash B.$$

(iii) Let $n \geq 2$ and let $A_1, \ldots, A_n$ be any formulas.

Let $j \in \{1, \ldots, n\}$. If $\Gamma \vdash A_1 \vee \ldots \vee A_n$ and $\Gamma \vdash \neg A_i$ for all $i \neq j$, then $\Gamma \vdash A_j$.

Adapting some of the results from [14, §32, Theorem 13], we obtain the following generalised introduction and elimination rules for the quantifiers $\forall$ and $\exists$.

Proposition A.3.0.5 *Let $\mathbb{T}$ be a theory. We can generalise the ($\exists$-E) rule to take several existential formulas or quantifications into account. We obtain the following derived rules, which we will also refer to as ($\exists$-E):*

(i) If $\Gamma \vdash (\exists x_1, \ldots, x_n)A$ and $\Gamma, A\left[\frac{a_1}{x_1}, \ldots, \frac{a_k}{x_k}\right] \vdash^{a_1,\ldots,a_n} B$, where none of the variables a_i occur free in B, then $\Gamma \vdash B$.

(ii) If $\Gamma \vdash (\exists x_i)A_i$ for $1 \leq i \leq n$ and $\Gamma, A_1\left[\frac{a_1}{x_1}\right], \ldots, A_k\left[\frac{a_n}{x_n}\right] \vdash^{a_1,\ldots,a_n} B$, where none of the variables a_i occur free in B, then $\Gamma \vdash B$.

(iii) If $\Gamma \vdash (\exists \mathbf{x}^{(\mathbf{i})})A_1(\mathbf{x}^{(\mathbf{i})})$ for all $i = 1, \ldots, n$ and $A_1(\mathbf{a}^{(\mathbf{1})}), \ldots, A_n(\mathbf{a}^{(\mathbf{n})}) \vdash^{\mathbf{a}^{(\mathbf{1})},\ldots,\mathbf{a}^{(\mathbf{n})}} B$ where none of the variables in the lists $\mathbf{a}^{(\mathbf{i})}$ occur free in B, then $\Gamma \vdash B$.

Theorem A.3.0.6 (Substitution Theorem) [33, pp. 31–32], [14, §32, Theorem 13, *66] *Let $\mathbb{T}$ be a theory, A a formula of $\mathbb{T}$, $x_1, \ldots, x_n$ distinct variables, and $t_1, \ldots, t_n$ terms such that t_i is free for x_i in A for all i.*

1. *If* $\vdash A$, *then* $\vdash A\left[\frac{t_1}{x_1},\ldots,\frac{t_n}{x_n}\right]$.
2. *If* Γ *is a set of formulas not containing any of the* x_i *free and* $\Gamma \vdash A$, *then* $\Gamma \vdash A\left[\frac{t_1}{x_1},\ldots,\frac{t_n}{x_n}\right]$.

Theorem A.3.0.7 (Equivalence Theorem) [33, pp. 34–35], [14, §26] *Let* A' *be obtained from* A *by replacing some occurrences of the subformulas* $B_1,\ldots,B_n$ *by* $B'_1,\ldots,B'_n$ *respectively. If* $\Gamma \vdash B_1 \Leftrightarrow B'_1$ *for all* $1 \le i \le n$, *then* $\Gamma \vdash A \Leftrightarrow A'$.

Remark A.3.0.8 Let $\mathbb{T}$ be a theory. By the equivalence of variants in $\mathbb{T}$ and Theorem A.3.0.6, if A is a theorem of $\mathbb{T}$, then the formula A' obtained by replacing some (or even all) of the variables occurring in A (either as bound or as free variables) with different variables, as long as no variable-capture occurs, is also a theorem of $\mathbb{T}$. Thus, by Theorem A.3.0.7, A and A' may be used interchangeably. □

Theorem A.3.0.9 (Equality theorem) [33, pp. 35–36], [14, §39, Theorem 24] *Let* $\mathbb{T}$ *be a theory, let* $n \ge 1$, *let* $s, t_1,\ldots,t_n, t'_1,\ldots,t'_n$ *be terms, and let* $A(x_1,\ldots,x_n)$ *be a formula such that* t_i, t'_i *are free for* x_i *in* A *for all* i. *Let* s' *be obtained from* s *by replacing all occurrences of* t_i *with* t'_i *for all* i. *Then,*

$$\vdash (t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n) \Rightarrow s = s'$$

and

$$\vdash (t_1 = t'_1 \wedge \cdots \wedge t_n = t'_n) \Rightarrow \left(A\left[\frac{t_1}{x_1},\ldots,\frac{t_n}{x_n}\right] \Leftrightarrow A\left[\frac{t'_1}{x_1},\ldots,\frac{t'_n}{x_n}\right]\right)$$

From this, we obtain the following derived rules:

(i) *If* $\Gamma \vdash t_i = t'_i$ *for all* $1 \le i \le k$, *then* $\Gamma \vdash s = s'$.

(ii) *If* $\Gamma \vdash t_i = t'_i$ *for all* $1 \le i \le k$ *and* $\Gamma \vdash A\left[\frac{t_1}{x_1},\ldots,\frac{t_n}{x_n}\right]$, *then* $\Gamma \vdash A\left[\frac{t'_1}{x_1},\ldots,\frac{t'_n}{x_n}\right]$.

Furthermore, equality between terms of $\mathbb{T}$ *is both symmetric and transitive. Hence, any number of the equalities above may appear reversed and the derived rules will still apply.*

Note that since derived rule (ii) in Theorem A.3.0.9 is essentially a generalised version of (=-E), we shall often simply refer to it as (=-E).

Appendix B

Category theory

We present here some basic concepts in category theory used in Chapter 2. For further background information about category theory, we refer to [17], [16], and [1].

Note that we use diagrammatic order for the composition of morphisms in categories (denoted using a semi-colon).

Definition B.0.0.1 Let $\mathcal{C}$ be a category and let $f : X \to Y$ be a morphism in $\mathcal{C}$.

(i) f is a *monomorphism* if, for any parallel morphisms $g, h : Z \to X$ in $\mathcal{C}$, if the diagram

$$Z \underset{h}{\overset{g}{\rightrightarrows}} X \xrightarrow{f} Y$$

commutes (that is, if $g; f = h; f$), then $g = h$.

(ii) f is an *epimorphism* if, for any parallel morphisms $g, h : Y \to Z$ in $\mathcal{C}$, if the diagram

$$X \xrightarrow{f} Y \underset{h}{\overset{g}{\rightrightarrows}} Z$$

commutes (that is, if $f; g = f; h$), then $g = h$. □

A category $\mathscr{C}$ is *finitely complete* or a *lex category* if it admits all limits of diagrams $F : \mathcal{J} \to \mathscr{C}$ where $\mathcal{J}$ is finite [17]. An equivalent and easier to verify condition for $\mathscr{C}$ to be finitely complete is given in Proposition B.0.0.2.

Proposition B.0.0.2 [17, 22] *The following are equivalent for a category $\mathscr{C}$:*

(i) $\mathscr{C}$ is finitely complete;

(ii) $\mathscr{C}$ has a terminal object and all binary products and equalizers;

(iii) $\mathscr{C}$ has a terminal object and all binary pullbacks.

Definition B.0.0.3 (Regular categories) [21, 29, 30] A category $\mathscr{C}$ is said to be *regular* if the following conditions hold.

(i) $\mathscr{C}$ is finitely complete.

(ii) For every morphism $f : A \to B$ in $\mathscr{C}$, there is a smallest subobject $\mathrm{Im}(f)$ of B, with associated morphism $\mathrm{Im}(f) \xrightarrow{I_f} B$, through which f factors, i.e. the diagram

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & \searrow \quad \nearrow_{I_f} & \\ & \mathrm{Im}(f) & \end{array}$$

commutes. $\mathrm{Im}(f)$ is called the *image* of f in $\mathscr{C}$.

Any category $\mathscr{C}$ satisfying this condition is said to *have images*.

(iii) Images are preserved under pullback in the following sense: Let

$$\begin{array}{ccc} A \times_C B & \xrightarrow{g'} & B \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[g]{} & C \end{array}$$

be a pullback square. Then, the pullback of $\mathrm{Im}_f \xrightarrow{I_f} C$ along g is $\mathrm{Im}_{f'} \xrightarrow{I_{f'}} A$, that is,

$$\begin{array}{ccc} \mathrm{Im}_{f'} & \longrightarrow & \mathrm{Im}_f \\ {\scriptstyle I_{f'}}\downarrow & & \downarrow{\scriptstyle I_f} \\ A & \xrightarrow[g]{} & C \end{array}$$

is also a pullback square.

Equivalently, a category $\mathscr{C}$ is said to be *regular* if the following conditions hold.

(a) $\mathscr{C}$ is finitely complete.

(b) The kernel pair

$$\begin{array}{ccc} D \times_C D & \xrightarrow{p_1} & D \\ {\scriptstyle p_2}\downarrow & & \downarrow{\scriptstyle f} \\ D & \xrightarrow[f]{} & C \end{array}$$

of any morphism $f : D \to C$ (i.e. the pullback of f along itself) admits a coequalizer

$$D \times_C D \underset{p_2}{\overset{p_1}{\rightrightarrows}} D \xrightarrow{c} \mathrm{coeq}(p_1, p_2) \ .$$

(c) Regular epimorphisms are stable under pullback in the following sense: the pullback of a regular epimorphism (that is, an epimorphism that is the coequaliser of a parallel pair of morphisms) along any morphism is again a regular epimorphism. More precisely, if $e : A \to B$ is a regular epimorphism, $g : C \to B$ is any morphism, and

$$\begin{array}{ccc} A \times_B C & \xrightarrow{p_1} & A \\ {\scriptstyle p_2}\downarrow & & \downarrow{\scriptstyle e} \\ C & \xrightarrow[g]{} & B \end{array}$$

is a pullback square, then $p_2 : A \times_B C \to C$ is also a regular epimorphism. □

B.1 Restriction categories

For a more detailed presentation of restriction categories, see [5].

Definition B.1.0.1 [4, 5] Let $\mathcal{C}$ be a category. A *restriction combinator* (or *restriction operator*) on $\mathcal{C}$ is a combinator $\overline{(\cdot)} : \mathcal{C}_1 \to \mathcal{C}_1$ (where $\mathcal{C}_1$ denotes the collection of morphisms of $\mathcal{C}$) sending each morphism $f : A \to B$ in $\mathcal{C}$ to a morphism $\overline{f} : A \to A$, called the *restriction* of f, such that the following four conditions are satisfied:

(R1) $\overline{f}; f = f$

(R2) $\overline{g}; \overline{f} = \overline{f}; \overline{g}$ whenever $\mathrm{dom}(f) = \mathrm{dom}(g)$

(R3) $\overline{\overline{f}; g} = \overline{f}; \overline{g}$ whenever $\mathrm{dom}(f) = \mathrm{dom}(g)$

(R4) $f; \overline{g} = \overline{f; g}; f$ whenever $\mathrm{cod}(f) = \mathrm{dom}(g)$

$\mathcal{C}$ is a *restriction category* when endowed with a restriction combinator. □

A morphism $f : A \to B$ in a restriction category $\mathcal{C}$ with restriction combinator $\overline{(\cdot)}$ is said to be $\overline{(\cdot)}$*-total*, or simply *total*, if $\overline{f} = \mathrm{id}_A : A \to A$. In any restriction category, identity morphisms are total and the composition of total morphisms yields a total morphism [4].

Note that every category can be seen as a restriction category when endowed with the *trivial restriction combinator* where the restriction of each morphism is simply the identity on the domain of the morphism. Therefore, a given category may have more than one restriction operator, which shows that a restriction operator is an additional structure on the category, and not a property of said category [5, p. 227, 3, p. 418].

A basic example of a restriction category is **Par**, the category of sets and partial functions. The usual restriction operator on **Par** associates to each partial function $f : X \to Y$, its restriction $\overline{f} : Y \to Y$ defined by

$$\overline{f}(x) = \begin{cases} x & \text{if } f(x)\downarrow \\ \uparrow & \text{otherwise} \end{cases}$$

for all $x \in X$. The restriction $\overline{f}$ represents the domain of definition $D_f \subseteq X$ of the morphism $f : X \to Y$.

In any restriction category $\mathcal{C}$, the morphisms are locally ordered. For two parallel morphisms, $f, g : X \to Y$ in $\mathcal{C}$, we have that

$$f \leq g \text{ if and only if } f = \overline{f}; g.$$

For example, in **Par**, the restriction $\overline{f}$ represents the domain of definition $D_f \subseteq X$ of a morphism f. Consequently, $f \leq g$ in **Par** if and only if f and g agree on the domain of definition of f [4].

A morphism $f : A \to B$ in a restriction category $\mathcal{C}$ is a *restriction idempotent* if it satisfies $f = \overline{f}$. In particular, each restriction idempotent is an endomorphism, an idempotent morphism in the usual sense, and is of the form $\overline{f}$ for some morphism f, since $\overline{f} = \overline{\overline{f}}$ for all morphisms f of $\mathcal{C}$ [5, Lemma 2.1]. As noted above, morphisms in $\mathcal{C}$ are locally ordered. In the particular case of restriction idempotents e, e' on the same object A, we have that $e \leq e'$ if and only if $e = e; e' = e'; e$ [5, §2.1.4].

A restriction idempotent $\overline{f}$ of $\mathcal{C}$ is *split* (or *splits*) if it can be written as $\overline{f} = r; m$ with $m; r = \text{id}$. If that is the case, the monic part m is called a *restriction monic*. The restriction category $\mathcal{C}$ is *split* if all of its restriction idempotents split.

The restriction category analogue of cartesian categories are called *cartesian restriction categories* and are restriction categories with a restriction terminal object and all binary partial products. For a full definition, see [4].

For the definition of restriction and cartesian restriction functors, see [4, §2.1–2.2] and [6, §4.1, p. 797]. Then, given two (cartesian) restriction categories $\mathcal{C}$ and $\mathcal{D}$, we say that $\mathcal{C}$ is a *sub (cartesian) restriction category* of $\mathcal{D}$ if $\mathcal{C}$ is a subcategory of $\mathcal{D}$ and the inclusion functor $\varphi : \mathcal{C} \to \mathcal{D}$ is a (cartesian) restriction functor. Note in particular that these definitions of a cartesian restriction functor and a sub cartesian restriction category only apply to cartesian restriction categories with specified structure.

B.1.1 Turing categories

For additional information on Turing categories, see [4].

Definition B.1.1.1 [4] Let $\mathcal{C}$ be a restriction category.

(i) Let $C, D \in \mathcal{C}$. We say that C is a *retract* of D if there exist morphisms $m : C \to D$ and $r : D \to C$ in $\mathcal{C}$ such that $m; r = \text{id}_C$. The *embedding* m is a monomorphism and so total, but the *retraction* r need not be total. If C is a retract of D, we write $C \lhd D$ or $(m, r) : C \lhd D$ if we wish to specify a particular embedding-retraction pair.

(ii) An object D of $\mathcal{C}$ is a *universal object* of $\mathcal{C}$ if every object $C \in \mathcal{C}$ is a retract of D, that is, if $C \lhd D$ for all $C \in \mathcal{C}$. □

Note that if C, D are two isomorphic objects of a restriction category $\mathcal{C}$, it follows immediately that both $C \triangleleft D$ and $D \triangleleft C$ in $\mathcal{C}$ and that any isomorphism $f : C \to D$ yields embedding-retraction pairs $(f, f^{-1}) : C \triangleleft D$ and $(f^{-1}, f) : D \triangleleft C$.

Definition B.1.1.2 [4, Definition 3.1] Let $\mathcal{C}$ be a cartesian restriction category.

(i) Let $\tau_{X,Y} : A \times X \to Y$ be a morphism of $\mathcal{C}$. A morphism $f : Z \times X \to Y$ *admits a* $\tau_{X,Y}$*-index* when there exists a total morphism $h : Z \to A$ such that the diagram

$$\begin{array}{ccc} A \times X & \xrightarrow{\tau_{X,Y}} & Y \\ {\scriptstyle h\times \mathrm{id}_X} \uparrow & \nearrow_{f} & \\ Z \times X & & \end{array}$$

commutes. h is then called a $\tau_{X,Y}$*-index* for f.

(ii) A morphism $\tau_{X,Y}$ is a *universal application* (or simply *universal*) when every morphism $f : Z \times X \to Y$ admits a $\tau_{X,Y}$-index.

(iii) A *Turing object* in $\mathcal{C}$ is an object A such that, for each $X, Y \in \mathcal{C}$, there exists a universal application $\tau_{X,Y} : A \times X \to Y$.

(iv) $\mathcal{C}$ is a *Turing category* if it possesses a Turing object. □

Definition B.1.1.3 [4] Let $\mathcal{C}$ be a cartesian restriction category and A and object of $\mathcal{C}$. A *Turing morphism* (*on* A) is a universal self-application map, that is, a morphism $A \times A \xrightarrow{\bullet} A$ such that, for every morphism $f : C \times A \to A$ in $\mathcal{C}$, there exists a total map $h : C \to A$ such that

$$\begin{array}{ccc} A \times A & \xrightarrow{\bullet} & A \\ {\scriptstyle h\times \mathrm{id}_A} \uparrow & \nearrow_{f} & \\ C \times A & & \end{array}$$

commutes. □

Theorem B.1.1.4 [4, Theorem 3.4] *For a cartesian restriction category* $\mathcal{C}$*, the following are equivalent:*

(i) $\mathcal{C}$ *is a Turing category;*

(ii) There exists a universal object A *and a Turing morphism* $A \times A \xrightarrow{\bullet} A$ *on* A *in* $\mathcal{C}$*. In this case,* A *is a Turing object on* $\mathcal{C}$*.*

Note that if a cartesian restriction category $\mathcal{C}$ admits a universal object A together with a Turing morphism $A \times A \xrightarrow{\bullet} A$, then A is a Turing object of $\mathcal{C}$. However, A is not necessarily the unique Turing object of A and there may be many ways of constructing the universal applications $\tau_{X,Y} : A \times X \to Y$ for each $X, Y \in \mathcal{C}$ from the universal self-application map $A \times A \xrightarrow{\bullet} A$ [4].

Appendix C

Technical/Detailed Proofs

Lemma (2.4.1.10) *Let* $\mathbb{T}$ *be an arithmetical theory and let* $\mathrm{rm} : \mathbb{N}^2 \to \mathbb{N}$ *be the remainder function as defined above. Define*

$$\delta(x, y, z) \underset{\text{def}}{\equiv} (\exists u)(u \leq x \wedge x = y \cdot u + z \wedge z < y) \vee (y = 0 \wedge z = x).$$

Then, rm *is numeralwise representable in* $\mathbb{T}$ *by* $\delta(x, y, z)$*. If* $\mathbb{T}$ *has induction, then* rm *is strongly representable in* $\mathbb{T}$ *by* $\delta(x, y, z)$*.*

Proof We first show condition (P1') for δ. Let $m, n \in \mathbb{N}$ and $p = \mathrm{rm}(m, n)$. There are two cases to consider.

Case 1: Suppose that $n = 0$. Then, $p = m$ by the definition of rm. Hence, we must show $\vdash \delta(\overline{m}, 0, \overline{m})$. We obtain $\vdash 0 = 0 \wedge \overline{m} = \overline{m}$ by (=-I), and so $\vdash \delta(\overline{m}, 0, \overline{m})$ follows by ($\vee$-I).

Case 2: Suppose that $n \neq 0$. Then, $p < n$ and there exists a $d \in \mathbb{N}$ such that $d \leq m$ and $m = nd + p$ by the definition of rm. It thus follows from Lemma 2.2.2.6 and Proposition 2.4.1.7 that $\vdash \overline{d} \leq \overline{m}$, $\vdash \overline{p} < \overline{n}$, and $\vdash \overline{m} = \overline{n} \cdot \overline{d} + \overline{p}$. Hence, we obtain $\vdash \delta(\overline{m}, \overline{n}, \overline{p})$ by ($\exists$-I) and ($\vee$-I).

Thus, we obtain $\vdash \delta(\overline{m}, \overline{n}, \overline{p})$ in both possible cases, whence condition (P1') holds for δ.

We now show condition (P2) for δ. Let $m, n \in \mathbb{N}$ and first consider the case when $n \neq 0$. We have the following derivation in $\mathbb{T}$.

1	$\delta(\overline{m},\overline{n},z) \land \delta(\overline{m},\overline{n},z')$	
2	$\overline{n} \neq 0$	Lemma 2.2.2.6 as $n \neq 0$
3	$(\exists u)(u \leq \overline{m} \land \overline{m} = \overline{n} \cdot u + z \land z < \overline{n})$	($\lor$-E), 1, 2
4	$(\exists u)(u \leq \overline{m} \land \overline{m} = \overline{n} \cdot u + z' \land z' < \overline{n})$	($\lor$-E), 1, 2
5	a, b $a \leq \overline{m} \land \overline{m} = \overline{n} \cdot a + z \land z < \overline{n}$	
6	$b \leq \overline{m} \land \overline{m} = \overline{n} \cdot b + z' \land z' < \overline{n}$	
7	$a = 0 \lor \ldots \lor a = \overline{m}$	Proposition 2.2.2.8, 5
8	$z = 0 \lor \ldots \lor z = \overline{n-1}$	Proposition 2.2.2.8 as $n \neq 0$, 5
9	$b = 0 \lor \ldots \lor b = \overline{m}$	Proposition 2.2.2.8, 6
10	$z' = 0 \lor \ldots \lor z' = \overline{n-1}$	Proposition 2.2.2.8 as $n \neq 0$, 6
11	$a = \overline{d}$	Some $0 \leq d \leq m$
12	$z = \overline{p}$	Some $0 \leq p < n$
13	$b = \overline{q}$	Some $0 \leq q \leq m$
14	$z' = \overline{r}$	Some $0 \leq r < n$
15	$\overline{m} = \overline{n \cdot d + p} \land \overline{p} < \overline{n}$	(=-E), Lemma 2.2.2.6, 5, 11, 12
16	$\overline{m} = \overline{n \cdot q + r} \land \overline{r} < \overline{n}$	(=-E), Lemma 2.2.2.6, 6, 13, 14

It thus follows by Lemma 2.2.2.6 and Proposition 2.4.1.7, that $nd + p = nq + r$ and $p, r < n$ in $\mathbb{N}$. Hence, it follows that $d = q$ and $p = r$ in $\mathbb{N}$ by the uniqueness of the quotient and remainder in the division algorithm as $n \neq 0$. Consequently, we obtain $\vdash \overline{p} = \overline{r}$ in $\mathbb{T}$. We can therefore continue the derivation as follows.

17	$\overline{p} = \overline{r}$	As remarked above, 15, 16
18	$z = z'$	(=-E), 12, 14, 17
19	$z = z'$	Simultaneous ($\lor$-E), 7, 8, 9, 10, 11–18
20	$z = z'$	($\exists$-E), 3, 4, 5–19
21	$\delta(\overline{m},\overline{n},z) \land \delta(\overline{m},\overline{n},z') \Rightarrow z = z'$	($\Rightarrow$-I), 1–20

Now suppose instead that $n = 0$. Then $\overline{n}$ is the term 0 and we have the following derivation in $\mathbb{T}$.

1	$\delta(\overline{m}, 0, z) \wedge \delta(\overline{m}, 0, z')$	
2	$z \nless 0$	Proposition 2.2.2.8
3	$\neg(\exists u)(u \leq \overline{m} \wedge \overline{m} = 0 \cdot u + z \wedge z < 0)$	(¬-I), 2
4	$0 = 0 \wedge z = \overline{m}$	(∨-E), 1, 3
5	$0 = 0 \wedge z' = \overline{m}$	Same argument with z' instead of z, 2–4
6	$z = z'$	(=-E), 4, 5
7	$\delta(\overline{m}, 0, z) \wedge \delta(\overline{m}, 0, z') \Rightarrow z = z'$	(⇒-I), 1–6

Therefore, we obtain $\vdash \delta(\overline{m}, \overline{n}, z) \wedge \delta(\overline{m}, \overline{n}, z') \Rightarrow z = z'$ in both cases, and so condition (P2) holds for δ. Hence, rm is numeralwise representable in $\mathbb{T}$ by $\delta(x, y, z)$.

Now suppose that $\mathbb{T}$ has induction. $\delta(x, y, z)$ satisfies condition (P1') as shown above. We first show that condition (P4) holds for δ, namely that $\vdash (\exists z)\delta(x, y, z)$ holds in $\mathbb{T}$. We use induction on x in $\mathbb{T}$ in the case when $y \neq 0$, similarly to [19, pp. 164–165].

1	$y = 0 \vee y \neq 0$	(DE)
2	$y = 0$	
3	$y = 0 \wedge x = x$	(=-I), (∧-I), 2
4	$(\exists z)\delta(x, y, z)$	(∨-I), (∃-I), 3
5	$y \neq 0$	
6	$0 \leq 0$	(=-I), (∨-I)
7	$0 = y \cdot 0 + 0$	(M5), (M3)
8	$0 < y$	Proposition 2.2.2.8, 5
9	$\delta(0, y, 0)$	(∧-I),(∃-I), (∨-I), 6, 7, 8
10	$(\exists z)\delta(0, y, z)$	(∃-I), 9

11	$(\exists z)\delta(x,y,z)$	
12	$a \mid \delta(x,y,a)$	
13	$\neg(y=0 \wedge a=x)$	($\neg$-I), 5
14	$(\exists u)(u \leq x \wedge x = y \cdot u + a \wedge a < y)$	($\vee$-E), 12, 13
15	$b \mid b \leq x \wedge x = y \cdot b + a \wedge a < y$	
16	$S(x) = S(y \cdot b + a)$	(=-I), (=-E), 15
17	$S(x) = (y \cdot b + a) + \overline{1}$	Lemma 2.2.2.7, 16
18	$S(x) = y \cdot b + S(a)$	Prop. 2.2.2.12, Lem. 2.2.2.7, 17
19	$S(a) = y \vee S(a) < y$	Proposition 2.2.2.12, 15
20	$S(a) = y$	
21	$S(x) = y \cdot b + y$	(=-E), 18, 20
22	$S(x) = y \cdot S(b) + 0$	(M6), (M3), 21
23	$S(b) \leq S(x)$	Proposition 2.2.2.8, 15
24	$S(b) \leq S(x) \wedge S(x) = y \cdot S(b) + 0 \wedge 0 < y$	($\wedge$-I), 23, 22, 8
25	$(\exists z)\delta(S(x),y,z)$	($\exists$-I), ($\vee$-I), 24
26	$S(a) < y$	
27	$b \leq S(x) \wedge S(x) = y \cdot b + S(a) \wedge S(a) < y$	Prop. 2.2.2.8, ($\wedge$-I), 15, 18, 26
28	$(\exists z)\delta(S(x),y,z)$	($\exists$-I), ($\vee$-I), 27
29	$(\exists z)\delta(S(x),y,z)$	($\vee$-E), 19, 20–25, 26–28
30	$(\exists z)\delta(S(x),y,z)$	($\exists$-E), 14, 15–29
31	$(\exists z)\delta(S(x),y,z)$	($\exists$-E), 11, 12–30
32	$(\exists z)\delta(x,y,z) \Rightarrow (\exists z)\delta(S(x),y,z)$	($\Rightarrow$-I), 11–31
33	$(\exists z)\delta(x,y,z)$	(IND), 10, 32
34	$(\exists z)\delta(x,y,z)$	($\vee$-E), 1, 2–4, 5–33

It remains to show condition (P3) for δ. We have the following derivation in $\mathbb{T}$, where we again use an argument similar to the one in [19, p. 165].

1	$\delta(x, y, z) \wedge \delta(x, y, z')$	
2	$y = 0 \vee y \neq 0$	(DE)
3	$y = 0$	
4	$\delta(x, 0, z) \wedge \delta(x, 0, z')$	(=-E), 1, 3
5	$z \not< 0$	Proposition 2.2.2.8
6	$\neg(\exists u)(u \leq x \wedge x = 0 \cdot u + z \wedge z < 0)$	(¬-I), 5
7	$y = 0 \wedge z = x$	(∨-E), 6, 4
8	$y = 0 \wedge z' = x$	Same argument with z' instead of z, 5–7
9	$z = z'$	(=-E), 7, 8

10	$y \neq 0$	
11	$\neg(y = 0 \land z = x)$	($\neg$-I), 10
12	$(\exists u)(u \leq x \land x = y \cdot u + z \land z < y)$	($\lor$-E), 1, 11
13	$(\exists u)(u \leq x \land x = y \cdot u + z' \land z' < y)$	Same argument with z' instead of z, 11–12
14	a, a' $\quad a \leq x \land x = y \cdot a + z \land z < y$	
15	$a' \leq x \land x = y \cdot a' + z' \land z' < y$	
16	$a < a' \lor a = a' \lor a' < a$	(M8)
17	$y \cdot a + z = y \cdot a' + z'$	(=-E), 14, 15
18	$a < a'$	
19	b $\quad a + S(b) = a'$	
20	$y \cdot a + z = y \cdot (a + S(b)) + z'$	(=-E), 17, 19
21	$y \cdot a + z = y \cdot a + (y \cdot S(b) + z')$	Proposition 2.2.2.12, 20
22	$z = y \cdot S(b) + z'$	Proposition 2.2.2.12 (cancellation), 21
23	$S(b) \neq 0$	(M1)
24	$y \leq y \cdot S(b) + z'$	Proposition 2.2.2.12, 23
25	$z < y \cdot S(b) + z'$	Proposition 2.2.2.8 (transitivity of $<$), 14, 24
26	$z \neq y \cdot S(b) + z'$	Proposition 2.2.2.12, 25
27	$\bot$	($\bot$-I), 22, 26
28	$\bot$	($\exists$-E), 18, 19–27
29	$\neg(a < a')$	($\neg$-I), 18–28
30	$\neg(a' < a)$	Same argument, swapping a, z for a', z', 18–29
31	$a = a'$	($\lor$-E), 16, 29, 30
32	$y \cdot a + z = y \cdot a + z'$	(=-E), 31, 17
33	$z = z'$	Proposition 2.2.2.12 (cancellation), 32
34	$z = z'$	($\exists$-E), 12, 13, 14–33
35	$z = z'$	($\lor$-E), 2, 3–9, 10–34
36	$\delta(x, y, z) \land \delta(x, y, z') \Rightarrow z = z'$	($\Rightarrow$-I), 1–35

Therefore, $\delta(x, y, z)$ satisfies condition (P4), and so strongly represents rm in $\mathbb{T}$. ■

Proposition (2.4.1.16) *Let $\mathbb{T}$ be an arithmetical theory with induction, let $k \geq 0$, and let $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^{k+2} \to \mathbb{N}$ be total functions that are strongly representable in $\mathbb{T}$ by the formulas $\varphi_g(\mathbf{x}, u)$ and $\varphi_h(\mathbf{x}, v_1, v_2, v_3)$, respectively. Let $f : \mathbb{N}^{k+1} \to \mathbb{N}$ be obtained from g, h by primitive recursion. As in Lemma 2.4.1.13, let $\Theta(\mathbf{x}, y, z, q_0, q_1)$ be the formula*

$$(\exists u)(\Lambda(q_0, q_1, 0, u) \wedge \varphi_g(\mathbf{x}, u)) \wedge \Lambda(q_0, q_1, y, z) \wedge \\ (\forall w)[w < y \Rightarrow (\exists v)(\exists v')(\Lambda(q_0, q_1, w, v) \wedge \Lambda(q_0, q_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))],$$

where Λ is the representing formula for β given in Lemma 2.4.1.12, and define

$$\rho(\mathbf{x}, y, z) \underset{\text{def}}{\equiv} (\exists q_0)(\exists q_1)\Theta(\mathbf{x}, y, z, q_0, q_1).$$

Then, $\rho(\mathbf{x}, y, z)$ strongly represents f in $\mathbb{T}$.

Proof By Lemma 2.4.1.13, condition (P1') holds for $\rho(\mathbf{x}, y, z)$ and f in $\mathbb{T}$. Note also that, since $\mathbb{T}$ has induction, Λ strongly represents β in $\mathbb{T}$ by Lemma 2.4.1.12.

In order to show that condition (P3) holds for ρ, we first show

$$\vdash \Theta(\mathbf{x}, y, z, u_0, v_0) \wedge \Theta(\mathbf{x}, y, z', u_0', v_0') \Rightarrow (\forall p)(\forall r)(\Lambda(u_0, v_0, p, r) \wedge p \leq y \Rightarrow \Lambda(u_0', v_0', p, r)) \tag{C.1}$$

by induction on the variable p in $\mathbb{T}$.

1	$\Theta(\mathbf{x}, y, z, u_0, v_0)$	
2	$\Theta(\mathbf{x}, y, z', u_0', v_0')$	
3	$\quad \Lambda(u_0, v_0, 0, r) \wedge 0 \leq y$	
4	$\quad e, e' \quad \Lambda(u_0, v_0, 0, e) \wedge \varphi_g(\mathbf{x}, e)$	
5	$\quad\quad \Lambda(u_0', v_0', 0, e') \wedge \varphi_g(\mathbf{x}, e')$	
6	$\quad\quad e = e'$	Condition (P3) for φ_g, 4, 5
7	$\quad\quad r = e$	Condition (P3) for Λ, 3, 4
8	$\quad\quad r = e'$	(=-E), 6, 7
9	$\quad\quad \Lambda(u_0', v_0', 0, r)$	(=-E), 5, 8
10	$\quad \Lambda(u_0', v_0', 0, r)$	($\exists$-E), 1, 2, 4–9
11	$(\forall r)(\Lambda(u_0, v_0, 0, r) \wedge 0 \leq y \Rightarrow \Lambda(u_0', v_0', 0, r))$	($\Rightarrow$-I), ($\forall$-I), 3–10

12	$(\forall r)(\Lambda(u_0, v_0, p, r) \wedge p \leq y \Rightarrow \Lambda(u_0', v_0', p, r))$	
13	$\Lambda(u_0, v_0, S(p), r) \wedge S(p) \leq y$	
14	$p < y$	Prop. 2.2.2.8, 13
15	$(\exists w)(\exists w')(\Lambda(u_0, v_0, p, w) \wedge \Lambda(u_0, v_0, S(p), w') \wedge \varphi_h(\mathbf{x}, p, w, w'))$	($\forall$-E), ($\Rightarrow$-E), 14, 1
16	$(\exists w)(\exists w')(\Lambda(u_0', v_0', p, w) \wedge \Lambda(u_0', v_0', S(p), w') \wedge \varphi_h(\mathbf{x}, p, w, w'))$	($\forall$-E), ($\Rightarrow$-E), 14, 2
17	a^*, b^* $\Lambda(u_0, v_0, p, a) \wedge \Lambda(u_0, v_0, S(p), b) \wedge \varphi_h(\mathbf{x}, p, a, b)$	
18	$\Lambda(u_0', v_0', p, a') \wedge \Lambda(u_0', v_0', S(p), b') \wedge \varphi_h(\mathbf{x}, p, a', b')$	
19	$\Lambda(u_0, v_0, p, a) \wedge p \leq y$	($\vee$-I), ($\wedge$-I), 14, 17
20	$\Lambda(u_0', v_0', p, a)$	($\forall$-E), ($\Rightarrow$-E), 12, 19
21	$a = a'$	(P3) for Λ, 18, 20
22	$\varphi_h(\mathbf{x}, p, a, b')$	(=-E), 18, 21
23	$b = b'$	(P3) for φ_h, 17, 22
24	$r = b$	(P3) for Λ, 13, 17
25	$r = b'$	(=-E), 23, 24
26	$\Lambda(u_0', v_0', S(p), r)$	(=-E), 25, 18
27	$\Lambda(u_0', v_0', S(p), r)$	($\exists$-E), 15, 16, 17–26
28	$(\forall r)(\Lambda(u_0, v_0, S(p), r) \wedge S(p) \leq y \Rightarrow \Lambda(u_0', v_0', S(p), r))$	($\Rightarrow$-I), ($\forall$-I), 13–27
29	$(\forall r)(\Lambda(u_0, v_0, p, r) \wedge p \leq y \Rightarrow \Lambda(u_0', v_0', p, r)) \Rightarrow$ $(\forall r)(\Lambda(u_0, v_0, S(p), r) \wedge S(p) \leq y \Rightarrow \Lambda(u_0', v_0', S(p), r))$	($\Rightarrow$-I), 12–28
30	$(\forall p)(\forall r)(\Lambda(u_0, v_0, p, r) \wedge p \leq y \Rightarrow \Lambda(u_0', v_0', p, r))$	Ind. on p, ($\forall$-I), 11, 29

It thus follows by ($\Rightarrow$-I) that (C.1) holds in $\mathbb{T}$. We then have the following derivation in $\mathbb{T}$ to show condition (P3) for ρ.

1		$\rho(\mathbf{x}, y, z) \wedge \rho(\mathbf{x}, y, z')$	
2	c^*, d^*	$\Theta(\mathbf{x}, y, z, c, d)$	
3		$\Theta(\mathbf{x}, y, z', c', d')$	
4		$(\forall p)(\forall r)(\Lambda(c, d, p, r) \wedge p \leq y \Rightarrow \Lambda(c', d', p, r))$	(C.1), 2, 3
5		$\Lambda(c, d, y, z) \wedge y \leq y$	($\wedge$-E), (=-I), ($\vee$-I), ($\wedge$-I), 2
6		$\Lambda(c', d', y, z)$	($\forall$-E), ($\Rightarrow$-E), 4
7		$\Lambda(c', d', y, z')$	($\wedge$-E), 3
8		$z = z'$	Condition (P3) for Λ, 6, 7
9	$z = z'$		($\exists$-E), 1, 2–8

Therefore, we obtain condition (P3) for ρ by ($\Rightarrow$-I).

In order to show condition (P4) for ρ, we proceed by induction on y in $\mathbb{T}$. We have the following derivation in $\mathbb{T}$, in which we use (2.4.9) and (2.4.10), as noted in the discussion preceding Lemma 2.4.1.14.

1	$(\exists u)\varphi_g(\mathbf{x}, u)$	Condition (P4) for φ_g
2	a $\varphi_g(\mathbf{x}, a)$	
3	$(\exists u)(\exists v)\Lambda(u, v, 0, a)$	(2.4.9), ($\forall$-E)
4	b_* $\Lambda(b_0, b_1, 0, a)$	
5	$\Theta(\mathbf{x}, 0, a, b_0, b_1)$	($\wedge, \exists, \Rightarrow, \forall$-I), Prop. 2.2.2.8, 2, 4
6	$(\exists z)\rho(\mathbf{x}, 0, z)$	($\exists$-I), 5
7	$(\exists z)\rho(\mathbf{x}, 0, z)$	($\exists$-E), 3, 4–6
8	$(\exists z)\rho(\mathbf{x}, 0, z)$	($\exists$-E), 1, 2–7
9	$(\exists z)\rho(\mathbf{x}, y, z)$	
10	c, d_* $\Theta(\mathbf{x}, y, c, d_0, d_1)$	
11	$(\exists v_3)\varphi_h(\mathbf{x}, y, c, v_3)$	Condition (P4) for φ_h
12	c' $\varphi_h(\mathbf{x}, y, c, c')$	
13	$(\exists u', v')[(\forall w)(w \leq y \Rightarrow (\exists z)(\Lambda(d_0, d_1, w, z) \wedge \Lambda(u', v', w, z)))$ $\wedge \Lambda(u', v', S(y), c')]$	(2.4.10), ($\forall$-E)
14	e_* $(\forall w)(w \leq y \Rightarrow (\exists z)(\Lambda(d_0, d_1, w, z) \wedge \Lambda(e_0, e_1, w, z)))$ $\wedge \Lambda(e_0, e_1, S(y), c')$	
15	$0 \leq y$	Proposition 2.2.2.8
16	$(\exists z)(\Lambda(d_0, d_1, 0, z) \wedge \Lambda(e_0, e_1, 0, z))$	($\forall$-E), ($\Rightarrow$-E), 14, 15
17	$(\exists u)(\Lambda(d_0, d_1, 0, u) \wedge \varphi_g(\mathbf{x}, u))$	($\wedge$-E), 10
18	b^* $\Lambda(d_0, d_1, 0, b) \wedge \Lambda(e_0, e_1, 0, b)$	
19	$\Lambda(d_0, d_1, 0, b') \wedge \varphi_g(\mathbf{x}, b')$	
20	$b = b'$	Condition (P3) for Λ, 18, 19
21	$\Lambda(e_0, e_1, 0, b') \wedge \varphi_g(\mathbf{x}, b')$	(=-E), ($\wedge$-I), 18, 19, 20
22	$(\exists u)(\Lambda(e_0, e_1, 0, u) \wedge \varphi_g(\mathbf{x}, u))$	($\exists$-I), 21
23	$(\exists u)(\Lambda(e_0, e_1, 0, u) \wedge \varphi_g(\mathbf{x}, u))$	($\exists$-E), 16, 17, 18–22

24	$w < S(y)$	
25	$w \leq y$	Prop. 2.2.2.8, 24
26	$(\exists z)(\Lambda(d_0, d_1, w, z) \wedge \Lambda(e_0, e_1, w, z))$	$(\forall$-E), ($\Rightarrow$-E), 14, 25
27	$w < y$	
28	$(\exists v)(\exists v')(\Lambda(d_0, d_1, w, v) \wedge \Lambda(d_0, d_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))$	($\wedge$-E), ($\forall$-E), ($\Rightarrow$-E), 27, 10
29	$S(w) \leq y$	Prop. 2.2.2.12, 27
30	$(\exists z)(\Lambda(d_0, d_1, S(w), z) \wedge \Lambda(e_0, e_1, S(w), z))$	($\forall$-E), ($\Rightarrow$-E), 14, 29
31	f_* $\Lambda(d_0, d_1, w, f_1) \wedge \Lambda(e_0, e_1, w, f_1)$	
32	$\Lambda(d_0, d_1, w, f_2) \wedge \Lambda(d_0, d_1, S(w), f_3) \wedge \varphi_h(\mathbf{x}, w, f_2, f_3)$	
33	$\Lambda(d_0, d_1, S(w), f_4) \wedge \Lambda(e_0, e_1, S(w), f_4)$	
34	$f_1 = f_2$	(P3) for Λ, 31, 32
35	$f_3 = f_4$	(P3) for Λ, 32, 33
36	$\Lambda(e_0, e_1, w, f_2) \wedge \Lambda(e_0, e_1, S(w), f_3) \wedge \varphi_h(\mathbf{x}, w, f_2, f_3)$	(=-E), ($\wedge$-E), ($\wedge$-I), 31–35
37	$(\exists v)(\exists v')(\Lambda(e_0, e_1, w, v) \wedge \Lambda(e_0, e_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))$	($\exists$-I), 36
38	$(\exists v)(\exists v')(\Lambda(e_0, e_1, w, v) \wedge \Lambda(e_0, e_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))$	($\exists$-E), 26, 28, 30, 31–37
39	$w = y$	
40	$(\exists z)(\Lambda(d_0, d_1, y, z) \wedge \Lambda(e_0, e_1, y, z))$	(=-E), 26, 39
41	$\Lambda(d_0, d_1, y, c)$	($\wedge$-E), 10
42	g $\Lambda(d_0, d_1, y, g) \wedge \Lambda(e_0, e_1, y, g)$	
43	$c = g$	(P3) for Λ, 41, 42
44	$\Lambda(e_0, e_1, y, c)$	(=-E), 42, 43
45	$\Lambda(e_0, e_1, y, c)$	($\exists$-E), 40, 42–44
46	$\Lambda(e_0, e_1, y, c) \wedge \Lambda(e_0, e_1, S(y), c') \wedge \varphi_h(\mathbf{x}, y, c, c')$	($\wedge$-I), 45, 14, 12
47	$(\exists v)(\exists v')(\Lambda(e_0, e_1, w, v) \wedge \Lambda(e_0, e_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))$	(=-E), ($\exists$-I), 39, 46
48	$(\exists v)(\exists v')(\Lambda(e_0, e_1, w, v) \wedge \Lambda(e_0, e_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v'))$	($\vee$-E), 25, 27–38, 39–47
49	$(\forall w)(w < S(y) \Rightarrow (\exists v)(\exists v')(\Lambda(e_0, e_1, w, v) \wedge \Lambda(e_0, e_1, S(w), v') \wedge \varphi_h(\mathbf{x}, w, v, v')))$	($\Rightarrow$-I), ($\forall$-I), 24–48
50	$\Theta(\mathbf{x}, S(y), c', e_0, e_1)$	($\wedge$-I), 23, 14, 49
51	$(\exists z)\rho(\mathbf{x}, S(y), z)$	($\exists$-I), 50
52	$(\exists z)\rho(\mathbf{x}, S(y), z)$	($\exists$-E), 13, 14–51
53	$(\exists z)\rho(\mathbf{x}, S(y), z)$	($\exists$-E), 11, 12–52
54	$(\exists z)\rho(\mathbf{x}, S(y), z)$	($\exists$-E), 9, 10–53
55	$(\exists z)\rho(\mathbf{x}, y, z) \Rightarrow (\exists z)\rho(\mathbf{x}, S(y), z)$	($\Rightarrow$-I), 9–54
56	$(\exists z)\rho(\mathbf{x}, y, z)$	Induction on y, 8, 55

Hence, we obtain $\vdash (\exists z)\rho(\mathbf{x}, y, z)$, and so condition (P4) for ρ is satisfied. Therefore, $\rho(\mathbf{x}, y, z)$ strongly represents $f : \mathbb{N}^{k+1} \to \mathbb{N}$ in $\mathbb{T}$. ∎

Lemma (3.2.0.4) *Let $\mathscr{C}(\mathbb{T})$ be the syntactic category of an arithmetical theory $\mathbb{T}$ with induction, let $A(\mathbf{y})$ and $B(z)$ be any objects of $\mathscr{C}(\mathbb{T})$ such that B has exactly* *one free variable, and let* $\ulcorner G(\mathbf{y}, w) \urcorner : A(\mathbf{y}) \to B(z)$ *and* $\ulcorner H(z, w) \urcorner : B(z) \to B(z)$ *be morphisms of* $\mathscr{C}(\mathbb{T})$*. Let* Λ *be the formula strongly representing* β *in* $\mathbb{T}$ *as defined in Lemma 2.4.1.12. Define*

$$K'(x, \mathbf{y}, w, q_0, q_1) \underset{\text{def}}{\equiv} (\exists w_0)(\Lambda(q_0, q_1, 0, w_0) \wedge G(\mathbf{y}, w_0)) \wedge \Lambda(q_0, q_1, x, w) \\ \wedge (\forall z)(z < x \Rightarrow (\exists p, p')(\Lambda(q_0, q_1, z, p) \wedge \Lambda(q_0, q_1, S(z), p') \wedge H(p, p')))$$

and

$$K(x, \mathbf{y}, w) \underset{\text{def}}{\equiv} (\exists q_0, q_1) K'(x, \mathbf{y}, w, q_0, q_1).$$

Then, $\ulcorner K(x, \mathbf{y}, w) \urcorner$ *is a morphism in* $\mathscr{C}(\mathbb{T})$ *from* $N(x) \wedge A(\mathbf{y})$ *to* $B(z)$ *and does not depend on the choice of representatives of the morphisms* $\ulcorner G \urcorner$ *and* $\ulcorner H \urcorner$*.*

Proof As explained preceding the original statement of Lemma 3.2.0.4, $K(x, \mathbf{y}, w)$ was constructed in order to encode a specific sequence $\mathbf{w}$ with last index x determined by the initial parameters $\mathbf{y}$ and the functional relations $G(\mathbf{y}, w)$ and $H(z, w)$. $K'(x, \mathbf{y}, w, q_0, q_1)$ expresses the fact that q_0, q_1 give an encoding of the sequence $\mathbf{w}$. It is a conjunction of three subformulas. The first of these subformulas, namely $(\exists w_0)(\Lambda(q_0, q_1, 0, w_0) \wedge G(\mathbf{y}, w_0))$, expresses the fact that the first element in the sequence $\mathbf{w}$ is the unique w_0 such that

$$A(\mathbf{y}) \vdash G(\mathbf{y}, w_0),$$

that is to say, w_0 is obtained by applying the provably functional relation G to $\mathbf{y}$. The second subformula, namely $\Lambda(q_0, q_1, x, w)$, sets w to be the element of the sequence $\mathbf{w}$ with index x, that is to say, the last element of the sequence $\mathbf{w}$. The third subformula, namely $(\forall z)(z < x \Rightarrow (\exists p, p')(\Lambda(q_0, q_1, z, p) \wedge \Lambda(q_0, q_1, S(z), p') \wedge H(p, p')))$, expresses the fact that, given an element p in the sequence with index $z < x$, the next element p' in the sequence is obtained by applying the provably functional relation H to the element p of index z.

We must show that K satisfies defining conditions (1)–(3) for a morphism from $N \wedge A$ to B in $\mathscr{C}(\mathbb{T})$.

(1) Note that $N(x) \underset{\text{def}}{\equiv} x = x$ is provably true in $\mathbb{T}$ by (=-I). We then have the following derivation in $\mathbb{T}$.

1	$K(x, \mathbf{y}, w)$	
2	a_* $K'(x, \mathbf{y}, w, a_0, a_1)$	
3	b $\Lambda(a_0, a_1, 0, b) \wedge G(\mathbf{y}, b)$	
4	$A(\mathbf{y})$	Defining cond. (1) for G, 3
5	$A(\mathbf{y})$	($\exists$-E), 2, 3–4
6	$x = 0 \vee (\exists u)(x = S(u))$	(M7)
7	$x = 0$	
8	$(\exists w_0)(\Lambda(a_0, a_1, 0, w_0) \wedge G(\mathbf{y}, w_0)) \wedge \Lambda(a_0, a_1, 0, w)$	($\wedge$-E), (=-E), 2, 7
9	c $\Lambda(a_0, a_1, 0, c) \wedge G(\mathbf{y}, c)$	
10	$w = c$	Condition (P3) for Λ, 8, 9
11	$G(\mathbf{y}, w)$	(=-E), 9, 10
12	$B(w)$	Defining cond. (1) for G, 11
13	$B(w)$	($\exists$-E), 8, 9–12
14	$(\exists u)(x = S(u))$	
15	d $x = S(d)$	
16	$\Lambda(a_0, a_1, S(d), w)$	($\wedge$-E), (=-E), 2, 15
17	$(\forall z)(z < S(d) \Rightarrow$ $(\exists p, p')(\Lambda(a_0, a_1, z, p) \wedge \Lambda(a_0, a_1, S(z), p') \wedge H(p, p')))$	($\wedge$-E), (=-E), 2, 15
18	$d < S(d)$	Proposition 2.2.2.8
19	$(\exists p, p')(\Lambda(a_0, a_1, d, p) \wedge \Lambda(a_0, a_1, S(d), p') \wedge H(p, p'))$	($\forall$-E), ($\Rightarrow$-E), 17, 18
20	e, e' $\Lambda(a_0, a_1, d, e) \wedge \Lambda(a_0, a_1, S(d), e') \wedge H(e, e')$	
21	$w = e'$	Condition (P3) for Λ, 16, 20
22	$H(e, w)$	(=-E), 20, 21
23	$B(w)$	Defining cond. (1) for H, 22
24	$B(w)$	($\exists$-E), 19, 20–23
25	$B(w)$	($\exists$-E), 14, 15–24
26	$B(w)$	($\vee$-E), 6, 7–13, 14–25
27	$(N(x) \wedge A(\mathbf{y})) \wedge B(w)$	(=-I), ($\wedge$-I), 5, 26
28	$(N(x) \wedge A(\mathbf{y})) \wedge B(w)$	($\exists$-E), 1, 2–27

We thus obtain $\vdash K(x, \mathbf{y}, w) \Rightarrow (N(x) \wedge A(\mathbf{y})) \wedge B(w)$ by ($\Rightarrow$-I), and so defining condition (1) for K is satisfied.

(2) Since $N(x)$ is a theorem of $\mathbb{T}$, it suffices to prove

$$\vdash A(\mathbf{y}) \Rightarrow (\exists w)K(x, \mathbf{y}, w)$$

in order to show that defining condition (2) for K holds. We proceed by induction on x in $\mathbb{T}$. It suffices to prove

$$A(\mathbf{y}) \vdash (\exists w)K(0, \mathbf{y}, w) \tag{C.2}$$

and

$$A(\mathbf{y}) \vdash (\exists w)K(x, \mathbf{y}, w) \Rightarrow (\exists w)K(S(x), \mathbf{y}, w). \tag{C.3}$$

For (C.2), note first that $A(\mathbf{y}) \vdash (\exists w)G(\mathbf{y}, w)$ by defining condition (2) for G. Furthermore, by Lemma 2.4.1.14, (2.4.9) holds in $\mathbb{T}$ and so we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a) \vdash^{a} (\exists q_0, q_1)\Lambda(q_0, q_1, 0, a)$$

by ($\forall$-E). Hence, we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a), \Lambda(b_0, b_1, 0, a) \vdash^{a,b_0,b_1} (\exists w_0)(\Lambda(b_0, b_1, 0, w_0) \wedge G(\mathbf{y}, w_0)) \wedge \Lambda(b_0, b_1, 0, a)$$

by ($\wedge$-I) and ($\exists$-I). Moreover, since $\vdash \neg(z < 0)$ holds in $\mathbb{T}$, we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a), \Lambda(b_0, b_1, 0, a) \vdash^{a,b_0,b_1}$$
$$(\forall z)(z < 0 \Rightarrow (\exists p, p')(\Lambda(b_0, b_1, z, p) \wedge \Lambda(b_0, b_1, S(z), p') \wedge H(p, p')))$$

by (Con). Hence, we obtain

$$A(\mathbf{y}), G(\mathbf{y}, a), \Lambda(b_0, b_1, 0, a) \vdash^{a,b_0,b_1} K'(0, \mathbf{y}, a, b_0, b_1)$$

by ($\wedge$-I), from which it follows that

$$A(\mathbf{y}), G(\mathbf{y}, a) \vdash^{a} K(0, \mathbf{y}, a),$$

and so also

$$A(\mathbf{y}) \vdash (\exists w)K(0, \mathbf{y}, w),$$

by ($\exists$-I) and ($\exists$-E). Thus, (C.2) holds.

For (C.3), we have the following derivation in $\mathbb{T}$.

1	$A(\mathbf{y})$	
2	$(\exists w)K(x,\mathbf{y},w)$	
3	a $K(x,\mathbf{y},a)$	
4	$B(a)$	Def. cond. (1) for K, ($\wedge$-E), 3
5	$(\exists w)H(a,w)$	Def. cond. (2) for H, 4
6	a', b_* $H(a,a')$	
7	$K'(x,\mathbf{y},a,b_0,b_1)$	
8	$(\exists u',v')[(\forall w,z_0)(w \leq x \wedge \Lambda(b_0,b_1,w,z_0) \Rightarrow \Lambda(u',v',w,z_0))$ $\wedge\Lambda(u',v',S(x),a')]$	(2.4.12), ($\forall$-E)
9	c_* $(\forall w,z_0)(w \leq x \wedge \Lambda(b_0,b_1,w,z_0) \Rightarrow \Lambda(c_0,c_1,w,z_0))$ $\wedge\Lambda(c_0,c_1,S(x),a')$	
10	$0 \leq x$	Prop. 2.2.2.8
11	$(\exists w_0)(\Lambda(b_0,b_1,0,w_0) \wedge G(\mathbf{y},w_0))$	($\wedge$-E), 7
12	d $\Lambda(b_0,b_1,0,d) \wedge G(\mathbf{y},d)$	
13	$0 \leq x \wedge \Lambda(b_0,b_1,0,d) \Rightarrow \Lambda(c_0,c_1,0,d)$	($\wedge$-E), ($\forall$-E), 9
14	$\Lambda(c_0,c_1,0,d) \wedge G(\mathbf{y},d)$	($\wedge$-E), ($\Rightarrow$-E), ($\wedge$-I), 10, 12, 13
15	$(\exists w_0)(\Lambda(c_0,c_1,0,w_0) \wedge G(\mathbf{y},w_0))$	($\exists$-I), 14
16	$(\exists w_0)(\Lambda(c_0,c_1,0,w_0) \wedge G(\mathbf{y},w_0))$	($\exists$-E), 11, 12–15
17	$z < S(x)$	
18	$z < x \vee z = x$	Prop. 2.2.2.8, 17
19	$z < x$	
20	$(\exists p,p')(\Lambda(b_0,b_1,z,p) \wedge \Lambda(b_0,b_1,S(z),p') \wedge H(p,p'))$	($\wedge$-E), ($\forall$-E), ($\Rightarrow$-E), 7, 19
21	e, e' $\Lambda(b_0,b_1,z,e) \wedge \Lambda(b_0,b_1,S(z),e') \wedge H(e,e')$	
22	$z \leq x$	($\vee$-I), 19
23	$S(z) \leq x$	Prop. 2.2.2.12, 19
24	$\Lambda(c_0,c_1,z,e) \wedge \Lambda(c_0,c_1,S(z),e') \wedge H(e,e')$	($\forall$-E), ($\Rightarrow$-E), ($\wedge$-E), ($\wedge$-I), 9, 21–23
25	$(\exists p,p')(\Lambda(c_0,c_1,z,p) \wedge \Lambda(c_0,c_1,S(z),p') \wedge H(p,p'))$	($\exists$-I), 24
26	$(\exists p,p')(\Lambda(c_0,c_1,z,p) \wedge \Lambda(c_0,c_1,S(z),p') \wedge H(p,p'))$	($\exists$-E), 20, 21–25

27	$z = x$	
28	$x \leq x$	(=-I), (∨-I)
29	$\Lambda(b_0, b_1, x, a)$	(∧-E), 7
30	$\Lambda(c_0, c_1, x, a)$	(∀-E), (⇒-E), 28, 29, 9
31	$\Lambda(c_0, c_1, x, a) \wedge \Lambda(c_0, c_1, S(x), a') \wedge H(a, a')$	(∧-E), (∧-I), 30, 9, 6
32	$(\exists p, p')(\Lambda(c_0, c_1, x, p) \wedge \Lambda(c_0, c_1, S(x), p') \wedge H(p, p'))$	(∃-I), 31
33	$(\exists p, p')(\Lambda(c_0, c_1, z, p) \wedge \Lambda(c_0, c_1, S(z), p') \wedge H(p, p'))$	(=-E), 32, 27
34	$(\exists p, p')(\Lambda(c_0, c_1, z, p) \wedge \Lambda(c_0, c_1, S(z), p') \wedge H(p, p'))$	(∨-E), 18, 19–26, 27–33
35	$(\forall z)(z < S(x) \Rightarrow$ $(\exists p, p')(\Lambda(c_0, c_1, z, p) \wedge \Lambda(c_0, c_1, S(z), p') \wedge H(p, p')))$	(⇒-I), (∀-I), 17–34
36	$K'(S(x), \mathbf{y}, a', c_0, c_1)$	(∧-E), (∧-I), 16, 9, 35
37	$(\exists w)K(S(x), \mathbf{y}, w)$	(∃-I), 36
38	$(\exists w)K(S(x), \mathbf{y}, w)$	(∃-E), 8, 9–37
39	$(\exists w)K(S(x), \mathbf{y}, w)$	(∃-E), 3, 5, 6–38
40	$(\exists w)K(S(x), \mathbf{y}, w)$	(∃-E), 2, 3–39
41	$(\exists w)K(x, \mathbf{y}, w) \Rightarrow (\exists w)K(S(x), \mathbf{y}, w)$	(⇒-I), 2–40

Hence, (C.3) holds in $\mathbb{T}$, and so we obtain

$$\vdash A(\mathbf{y}) \Rightarrow (\exists w)K(x, \mathbf{y}, w).$$

by induction on x in $\mathbb{T}$ and (⇒-I).

(3) We first show

$$K'(x, \mathbf{y}, w, q_0, q_1), K'(x, \mathbf{y}, w', q_0', q_1') \vdash (\forall v)(\forall u)(v \leq x \wedge \Lambda(q_0, q_1, v, u) \Rightarrow \Lambda(q_0', q_1', v, u)) \quad \text{(C.4)}$$

by induction on v in $\mathbb{T}$. For ease of reference, we shall define

$$I(x, q_0, q_1, q_0', q_1', v) \underset{\text{def}}{\equiv} (\forall u)(v \leq x \wedge \Lambda(q_0, q_1, v, u) \Rightarrow \Lambda(q_0', q_1', v, u)).$$

We have the following derivation in $\mathbb{T}$.

1	$K'(x, \mathbf{y}, w, q_0, q_1)$	
2	$K'(x, \mathbf{y}, w', q'_0, q'_1)$	
3	$0 \leq x \wedge \Lambda(q_0, q_1, 0, u)$	
4	$(\exists w_0)(\Lambda(q_0, q_1, 0, w_0) \wedge G(\mathbf{y}, w_0))$	$(\wedge$-E), 1
5	$(\exists w_0)(\Lambda(q'_0, q'_1, 0, w_0) \wedge G(\mathbf{y}, w_0))$	$(\wedge$-E), 2
6	a^* $\Lambda(q_0, q_1, 0, a) \wedge G(\mathbf{y}, a)$	
7	$\Lambda(q'_0, q'_1, 0, a') \wedge G(\mathbf{y}, a')$	
8	$a = a'$	Defining condition (3) for G, 6, 7
9	$u = a$	Condition (P3) for Λ, 3, 6
10	$u = a'$	(=-E), 8, 9
11	$\Lambda(q'_0, q'_1, 0, u)$	(=-E), 7, 10
12	$\Lambda(q'_0, q'_1, 0, u)$	$(\exists$-E), 4, 5, 6–11
13	$I(x, q_0, q_1, q'_0, q'_1, 0)$	$(\Rightarrow$-I), $(\forall$-I), 3–12

14	$I(x, q_0, q_1, q_0', q_1', v)$	
15	$S(v) \leq x \wedge \Lambda(q_0, q_1, S(v), u)$	
16	$v < x$	Proposition 2.2.2.8, 15
17	$(\exists p, p')(\Lambda(q_0, q_1, v, p) \wedge \Lambda(q_0, q_1, S(v), p') \wedge H(p, p'))$	($\wedge$-E), ($\forall$-E), ($\Rightarrow$-E), 1, 16
18	$(\exists p, p')(\Lambda(q_0', q_1', v, p) \wedge \Lambda(q_0', q_1', S(v), p') \wedge H(p, p'))$	($\wedge$-E), ($\forall$-E), ($\Rightarrow$-E), 2, 16
19	b^*, c^* $\Lambda(q_0, q_1, v, b) \wedge \Lambda(q_0, q_1, S(v), b') \wedge H(b, b')$	
20	$\Lambda(q_0', q_1', v, c) \wedge \Lambda(q_0', q_1', S(v), c') \wedge H(c, c')$	
21	$v \leq x \wedge \Lambda(q_0, q_1, v, b)$	($\vee$-I), ($\wedge$-E), ($\wedge$-I), 16, 19
22	$\Lambda(q_0', q_1', v, b)$	($\forall$-E), ($\Rightarrow$-E), 14, 21
23	$b = c$	Condition (P3) for Λ, 20, 22
24	$u = b'$	Condition (P3) for Λ, 15, 19
25	$H(b, u) \wedge H(b, c')$	($\wedge$-E), ($\wedge$-I), (=-E), 19, 20, 23, 24
26	$u = c'$	Defining condition (3) for H, 25
27	$\Lambda(q_0', q_1', S(v), u)$	($\wedge$-E), (=-E), 20, 26
28	$\Lambda(q_0', q_1', S(v), u)$	($\exists$-E), 17, 18, 19–27
29	$I(x, q_0, q_1, q_0', q_1', S(v))$	($\Rightarrow$-I), ($\forall$-I), 15–28
30	$I(x, q_0, q_1, q_0', q_1', v) \Rightarrow I(x, q_0, q_1, q_0', q_1', S(v))$	($\Rightarrow$-I), 14–29
31	$(\forall v) I(x, q_0, q_1, q_0', q_1', v)$	Induction on v in $\mathbb{T}$, ($\forall$-I), 13, 30

Hence, (C.4) holds in $\mathbb{T}$. We can now show that

$$\vdash K(x, \mathbf{y}, w) \wedge K(x, \mathbf{y}, w') \Rightarrow w = w'$$

holds in $\mathbb{T}$. We have the following derivation in $\mathbb{T}$.

1	$K(x, \mathbf{y}, w) \wedge K(x, \mathbf{y}, w')$	
2	a_*, b_* $K'(x, \mathbf{y}, w, a_0, a_1)$	
3	$K'(x, \mathbf{y}, w', b_0, b_1)$	
4	$x \leq x$	(=-I), (∨-I)
5	$\Lambda(a_0, a_1, x, w)$	(∧-E), 2
6	$\Lambda(b_0, b_1, x, w)$	(∀-E) and (⇒-E) applied to (C.4), 4, 5
7	$\Lambda(b_0, b_1, x, w')$	(∧-E), 3
8	$w = w'$	Condition (P3) for Λ, 6, 7
9	$w = w'$	(∃-E), 1, 2–8

We therefore obtain $\vdash K(x, \mathbf{y}, w) \wedge K(x, \mathbf{y}, w') \Rightarrow w = w'$ by (⇒-I), and so defining condition (3) for K is satisfied.

Hence, $\lceil K(x, \mathbf{y}, w) \rceil$ is a morphism in $\mathscr{C}(\mathbb{T})$ from $N(x) \wedge A(\mathbf{y})$ to $B(z)$. Furthermore, note that since different representatives of the same morphism are provably equivalent in $\mathbb{T}$, it follows from the Equivalence Theorem that $\lceil K \rceil$ does not depend on the choice of representatives of the morphisms $\lceil G \rceil$ and $\lceil H \rceil$. ∎

Bibliography

[1] S. Awodey. *Category Theory*. Oxford Logic Guides. Oxford University Press, 2006.

[2] G. S. Boolos and R. C. Jeffrey. *Computability and Logic*. Cambridge University Press, 1974.

[3] J. Cockett, X. Guo, and P. Hofstra. "Range categories I: General theory". In: *Theory and Applications of Categories* 26.17 (2012), pp. 412–452.

[4] J. Cockett and P. Hofstra. "Introduction to Turing categories". In: *Annals of Pure and Applied Logic* 156.2 (2008), pp. 183–209.

[5] J. Cockett and S. Lack. "Restriction categories I: categories of partial maps". In: *Theoretical Computer Science* 270.1 (2002), pp. 223–259. DOI: `https://doi.org/10.1016/S0304-3975(00)00382-0`.

[6] R. Cockett and S. Lack. "Restriction categories III: colimits, partial limits and extensivity". In: *Mathematical Structures in Computer Science* 17.4 (2007), pp. 775–817. DOI: `10.1017/S0960129507006056`.

[7] M.-F. Coste-Roy, M. Coste, and L. Mahé. "Contribution to the Study of the Natural Number Object in Elementary Topoi". In: *Journal of Pure and Applied Algebra* 17 (1980), pp. 35–68.

[8] W. Craig. "On Axiomatizability Within a System". In: *The Journal of Symbolic Logic* 18.1 (1953), pp. 30–32. DOI: `doi:10.2307/2266324`.

[9] P. Hájek and P. Pudlák. *Metamathematics of First-Order Arithmetic*. Perspectives in Logic. Cambridge University Press, 2017. DOI: `10.1017/9781316717271.001`.

[10] P. Hofstra and P. Scott. "Aspects of Categorical Recursion Theory". (Manuscript). 2019.

[11] P. J. W. Hofstra. *Recursion Theory*. Lecture Notes. Dec. 2007.

[12] N. Jacobson. *Basic Algebra I*. 2nd ed. W.H. Freeman, 1985.

[13] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium: Volume 2*. Oxford Logic Guides 44. Oxford University Press, 2002.

[14] S. C. Kleene. *Introduction to Metamathematics*. The University Series in Higher Mathematics. D. Van Nostrand Company, Inc., 1952.

[15] J. Lambek and P. Scott. "Intuitionistic Type Theory and the Free Topos". In: *Journal of Pure and Applied Algebra* 19 (1980), pp. 215–257.

[16] J. Lambek and P. Scott. *Introduction to higher order categorical logic*. Vol. 7. Cambridge studies in advanced mathematics. Cambridge University Press, 1986.

[17] S. Mac Lane. *Categories for the Working Mathematician*. 2nd ed. Vol. 5. Graduate Texts in Mathematics. Springer-Verlag New York, 1978.

[18] S. Mac Lane and I. Moerdijk. *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*. Universitext. Springer-Verlag, 1992.

[19] E. Mendelson. *Introduction to Mathematical Logic*. 5th ed. Discrete Mathematics and its Applications. Taylor & Francis Group, 2010.

[20] J. Moschovakis. "Intuitionistic Logic". In: *The Stanford Encyclopedia of Philosophy*. Ed. by E. N. Zalta. Winter 2018. `https://plato.stanford.edu/archives/win2018/entries/logic-intuitionistic/`. Metaphysics Research Lab, Stanford University, 2018.

[21] nLab authors. *regular category*. `https://ncatlab.org/nlab/show/regular+category`. Aug. 2019.

[22] E. Palmgren and S. Vickers. "Partial Horn logic and cartesian categories". In: *Annals of Pure and Applied Logic* 145.3 (2007), pp. 314–353. URL: `http://dx.doi.org/10.1016/j.apal.2006.10.001`.

[23] G. Plotkin. "Partial Recursive Functions and Finality". In: *Computation, Logic, Games, and Quantum Foundations. The Many Facets of Samson Abramsky: Essays Dedicated to Samson Abramsky on the Occasion of His 60th Birthday*. Ed. by B. Coecke, L. Ong, and P. Panangaden. Springer Berlin Heidelberg, 2013, pp. 311–326. DOI: `10.1007/978-3-642-38164-5_21`.

[24] H. Putnam and R. M. Smullyan. "Exact Separation of Recursively Enumerable Sets Within Theories". In: *Proceedings of the American Mathematical Society* 11.4 (1960), pp. 574–577.

[25] R. W. Ritchie and P. R. Young. "Strong Representability of Partial Functions in Arithmetic Theories". In: *Information Sciences* 1.2 (1969), pp. 189–204. DOI: `https://doi.org/10.1016/0020-0255(69)90016-4`.

[26] W. E. Ritter. "Representability of Partial Recursive Functions in Formal Theories". In: *Proceedings of the American Mathematical Society* 18.4 (Aug. 1967), pp. 647–651.

[27] L. Román. *Categories with finite limits and natural numbers object*. (Unpublished manuscript).

[28] L. Román. "Cartesian Categories with Natural Numbers Object". In: *Journal of Pure and Applied Algebra* 58 (1989), pp. 267–278.

[29] P. J. Scott. "Some Categorical Aspects of Intuitionistic Mathematics". Ph.D. Thesis. U. Waterloo, 1976.

[30] P. J. Scott. "The "Dialectica" Interpretation and Categories". In: *Zeitschr. f. math. Logik und Grundlagen d. Math.* 24 (1978), pp. 553–575.

[31] P. J. Scott. "Computable Functions in Categories". In: *Mathematical Logic and Theoretical Computer Science*. Ed. by D. Kueker, E. Lopez-Escobar, and C. H. Smith. Marcel Dekker, 1987.

[32] J. C. Shepherdson. "Representability of recursively enumerable sets in formal theories". In: *Archiv für mathematische Logik und Grundlagenforschung* 5.3 (Mar. 1961), pp. 119–127. DOI: 10.1007/BF01974157.

[33] J. R. Shoenfield. *Mathematical Logic*. Addison-Wesley Series in Logic. Addison-Wesley Publishing Company, 1967.

[34] C. Smoryński. *Logical Number Theory I: An Introduction*. Universitext. Springer-Verlag, 1991.

[35] A. S. Troelstra. *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*. Lecture Notes in Mathematics 344. Springer-Verlag, 1973.

[36] A. Troelstra and D. van Dalen, eds. *Constructivism in Mathematics*. Vol. 121. Studies in Logic and the Foundations of Mathematics. Elsevier, 1988, pp. 113–183.