Quantum Uncloneability Games and Applications to Cryptography

Eric Culf

Thesis submitted to the University of Ottawa
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

Many unique attributes of quantum cryptography arise from the no-cloning property of quantum information. We study this using two closely-related types of uncloneability game: no-cloning and monogamy-of-entanglement games. In a no-cloning game, a referee sends a quantum state encoding classical information to two cooperating players who split the state, then try simultaneously guessing the information, provided the key. In a monogamy-of-entanglement game, two cooperating players try to guess the referee's measurement result on a tripartite state the players prepared.

In this work, we prove winning probability bounds on no-cloning games based on coset states, which have the interesting property that the players guess two different strings. We also show a rigidity property for the original monogamy-of-entanglement game, letting it be used as a test of separability. Finally, we apply these properties to construct a variety of novel cryptographic protocols for uncloneable encryption, quantum key distribution, bit commitment, and randomness expansion.

Acknowledgements

First of all, I would like to thank my supervisor, Dr. Anne Broadbent, for her invaluable support, advice, and ideas. I could always count on her for new insight or directions.

I would also like to thank Dr. Arthur Mehta, Dr. Thomas Vidick, and Dr. Victor V. Albert, whom I had the good fortune of working closely with as well.

Finally, I would like to thank everyone in our research group: Christine, Martti, Peter, Pierre, Sébastien, Sherry, and Sohrab. It was always a pleasure to chat about far-fetched ideas, assignments, strange papers from the arXiv, and LaTeX formatting.

List of Publications

A list of publications from the author's MSc, both completed and in preparation, is included below. Those included in this thesis are highlighted with an asterisk.

- E. Culf and T. Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6: 791, 2022. DOI: 10.22331/q-2022-09-01-791.*
- A. Broadbent and E. Culf. Rigidity for monogamy-of-entanglement games. ArXiv preprint, 2021. To appear in ITCS 2023. DOI: 10.48550/ARXIV.2111.08081.*
- A. Broadbent and E. Culf. Uncloneable cryptographic primitives with interaction. Manuscript, 2022.*
- E. Culf, T. Vidick, and V. Albert. Group coset monogamy games and an application to device-independent continuous-variable QKD. ArXiv preprint, 2022. DOI: 10.48550/ARXIV.2212.03935.

Contents

List of Figures

List of Symbols

Acronyms

Symbols

Chapter 1

Introduction

An important feature that distinguishes quantum information from classical information is that an arbitrary quantum state cannot be perfectly copied, unlike a classical string. This is formalised via the *no-cloning theorem* [Par70, WZ82, Die82]. This theorem puts forward an important principle that has wide-ranging implications. In early discussions of entanglement, it was unknown whether there are any limitations on the strength of correlations permitted by quantum mechanics [EPR35]. For example, there exist maximally-entangled states on two systems with the property that a measurement in any basis on the first system may always be perfectly predicted by a corresponding measurement on the second system. This seemed to indicate that there is a way to use entanglement to achieve instantaneous communication, in violation of the well-established light-speed limit to information transmission [Her82, Per03]. However, such a communication scheme would require cloning of quantum states to be viable. As such, the no-cloning theorem provides a limitation on the strength of entanglement that allows it to avoid contradicting important predictions of classical physics. Interestingly, though the no-cloning theorem allows a condition of special relativity to be met, it requires no relativistic construction or argument to show, appealing only to the linear and probability-conserving nature of quantum operations.

The limitation on quantum operations given by no-cloning also relates to a limitation on multipartite entanglement. If quantum cloning channels existed, they would permit the creation of unphysical quantum states. This dual property to no-cloning is *monogamy-of-entanglement (MoE)*. Informally, the limitation of entanglement provided by MoE refers to the fact that a quantum system cannot be maximally entangled with two other systems at once. A state that violates this would arise by acting with a cloning operation on one system in a maximally-entangled state.

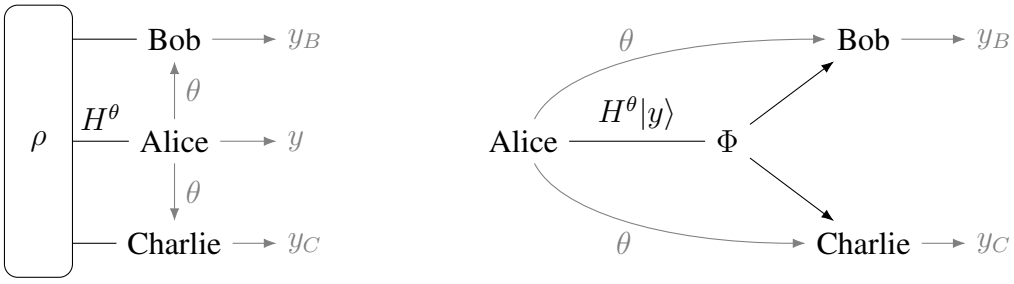
However, we might ask what happens in the cases where perfect copying would not be required: for example, where not all states are considered, or the states only need to be approximately cloned. Here, the no-cloning theorem does not directly imply any constraint. A drawback of the theorem arises due to this observation; it is rarely directly applicable to the study of quantum information and cryptography. In the same way as no-cloning, it is not straightforward to quantify the implications of MoE in particular scenarios.

One way to approach these uncloneability properties, no-cloning and MoE, is by means of *quantum games*. They serve as thought experiments representing idealised versions of scenarios where quantum properties apply. Very generally, we consider games played cooperatively by multiple quantum players against a referee, which could always be won with certainty if the players had access to a quantum operation or state that violates no-cloning or MoE, respectively. Then, if the optimal winning probability of the game is strictly less than 1, the game provides a concrete manifestation of uncloneability. We study two families of *uncloneability games*. Both are played by two cooperating players, whom we refer to as Bob and Charlie, against a referee, Alice. The referee has fixed actions, but the players may undertake any actions within the constraints of the game.

The first family of uncloneability games are the *monogamy-of-entanglement games*. In an MoE game, the players are allowed to prepare a shared entangled state in their, and also the referee's, quantum systems. Then, Bob and Charlie are isolated and may no longer communicate. The referee makes a measurement sampled at random from some fixed set of options, and then informs the players of the measurement basis. By using their local quantum systems, the players each attempt to guess the referee's measurement result. Bob and Charlie win if both their results are equal to Alice's. If the game were played with only one player, for example Bob, he could share a maximally-entangled state with Alice, allowing him to always guess correctly. However, because MoE guarantees that there is no state where Alice is simultaneously maximally entangled with Bob and Charlie, the winning probability of an MoE game may be non-trivial. The MoE game model was first introduced by Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13], where they construct a game where the measurements are in the conjugate-coding bases, whose winning probability is exponentially small in the number of bits output. MoE games fit into the larger framework of extended nonlocal (XNL) games [JMRW16], which extend nonlocal games by allowing the referee's decision predicate to be based on a quantum measurement.

The second family of uncloneability games we study are the *no-cloning (NC) games*. In the simplest form of an NC game, Alice samples a question and an answer at random, and

prepares a state as a function of them. We usually assume that, for each question, the states for different answers are orthogonal — that is, they are distinguishable by a measurement. Then, Alice sends the state to Bob and Charlie, who may attempt to clone it by means of an arbitrary quantum operation. Afterwards, however, they are isolated. Alice communicates the question to Bob and Charlie, who try to guess the answer using their local quantum systems. They win if they both identify it correctly. As for an MoE game, either one of the players could always guess correctly by having the channel send the shared state directly to them. However, only the existence of a quantum cloning channel would allow the players to win all the time at any NC game. It is possible to represent an MoE game by an NC game by way of the duality between the two concepts. The NC form is often more useful for applications, as it relies only on the transmission of quantum states and not the generation of entanglement. For example, the transmitted state can be seen as a quantum encoding of a classical message represented by the answer of the underlying NC game. If the winning probability of the game is small, the NC game provides a way to encrypt a classical, easily clonable, message as an uncloneable quantum state [BL20]. On the other hand, the MoE form tends to be more amenable for analysis.



(a) TFKW MoE game.

(b) TFKW NC game

Figure 1.1: The MoE and NC game versions of the TFKW game. Quantum parties or information are indicated in black, while classical information is indicated in gray.

A simple but instructive example of an MoE game is the original game introduced in [TFKW13], which we refer to as the TFKW game after the authors. The structures of the TFKW game in the MoE game form, as well as an NC game form, are illustrated in Fig. 1.1. In its simplest form, Alice holds a one-qubit system and measures in one of two bases: either the computational or the Hadamard basis. They show that, for any shared state ρ_{ABC} and measurements Bob and Charlie may make, they can only guess correctly with probability $\cos^2\left(\frac{\pi}{8}\right) \approx 85\%$, even when Alice provides them with a bit θ indicating

her measurement basis. Alternately, this game may be represented as an NC game; in this version, Alice prepares a random state in either of the two bases rather than measuring. In this game, Bob and Charlie make use of a channel Φ to attempt to split the state and preserve the information, before they learn the preparation basis. The duality ensures that this version of the game satisfies the same winning probability bound.

We study two generalisations of the uncloneability property of the TFKW game. First, we study NC games where the states sent generalise the computational and Hadamard states of the TFKW game. These states are *subspace coset states*. A basis of subspace coset states is indicated by a linear subspace of the finite vector space of n bits, and the states are phased superpositions of the basis vectors of the corresponding n-qubit space indexed by the elements of a coset of this subspace. The computational and Hadamard bases are the trivial cases of the 0 subspace and the whole space, respectively. For an intermediate subspace, the basis is naturally indexed by two strings which indicate the coset representative and the phase. It was conjectured in [CLLZ21] that it is hard for Bob and Charlie to each simultaneously guess one of these two strings, in the NC game called the *strong coset state NC game* where Alice sends subspace coset states. We show this property by adapting the proof of [TFKW13] to this more involved context; and then generalise it by considering leaky and robust games where Bob's answer string leaks to Charlie, and there is some error tolerance. These end up providing a natural example of games highlighting uncloneability that exist beyond the purview of the extended nonlocal game model: when there is both leakage and error-robustness, Bob might use some fraction of his answer string to send information to Charlie.

The other generalisation we study is to demonstrate additional properties of the TFKW game. In [TFKW13], it was shown that this game may be won optimally with an unentangled strategy where the players simply send Alice a state and guess her result deterministically. That is, no entanglement is able to improve Bob and Charlie's winning probability. We strengthen this by showing that, if Bob and Charlie win the TFKW game optimally, they may not make use of any shared entanglement in their strategy. This provides the first rigidity result for a monogamy-of-entanglement game. To strengthen this basic observation, we generalise the result to be error-tolerant and hold in parallel repetition, so that the rigidity can be guaranteed from statistics observed when playing the game.

A natural way to see what is implied by uncloneability properties is to look for an application to cryptography. This gives a concrete realisation of the property to a scenario that is beyond the reach of the no-cloning theorem. To that end, we use the uncloneability

games that we study to inform the construction of cryptographic scenarios, and use our results to construct and prove properties of protocols therein. We apply the NC properties of the subspace coset state games to uncloneable encryption, quantum key distribution, and uncloneable bit commitment. On the other hand, we apply the rigidity of the TFKW game to bit commitment from weak string erasure and to randomness expansion.

1.1 Outline

We now outline the structure of the remainder of the thesis. We attempt to make each chapter as self-contained as possible, noting whenever we appeal to results in previous sections.

First, in Chapter 2, we provide a high-level summary of the contributions of this thesis. The general structure of this thesis follows the order therein.

In Chapter 3, we introduce the mathematical preliminaries and notations needed, drawn largely from algebra, representation theory, probability theory, and the theory of error-correcting codes. As much as reasonable — and probably in a few places where it is unreasonable — we provide proofs of the major results.

Next, in Chapter 4, we give background on quantum theory to introduce the postulates of quantum mechanics. Then, we discuss entanglement and its consequences, such as the no-cloning theorem; that provides a springboard to subsequently introduce the theory and notation of quantum information, that we make use of throughout the work.

In the next chapter, Chapter 5, we discuss how to interpret the monogamy-of-entanglement and no-cloning properties as games, and formally introduce the structures of the quantum games we study: MoE games and NC games. We discuss the parallel repetition of games, and study the relationship between MoE and NC games in a general context.

In Chapter 6, we formally introduce and analyse the strong, leaky, and robust leaky coset state games. The NC properties that come from the winning probability bounds are given as Theorem 6.2, Theorem 6.8, and Theorem 6.11. The expressions of these properties as entropic uncertainty relations, which is the form used in applications, are given as Corollary 6.15 and Corollary 6.17.

Our next theory contribution, rigidity of the TFKW game, is studied in Chapter 7. This provides the first example of rigidity for an MoE game. First we discuss the exact rigidity, which is the most intuitive, and then build up step by step to get to the form of the rigidity that is useful for applications. Our most general rigidity results are given by Theorem 7.11 and Theorem 7.14.

Finally, in Chapter 8 we provide some applications of these results to cryptography. We apply the coset state game bounds to uncloneable encryption, quantum key distribution, and bit commitment; and we apply the rigidity of TFKW to bit commitment from weak string erasure and to randomness expansion.

Chapter 2

Summary of Contributions

In this chapter, we summarise our contributions and the proof techniques we use to show them, at a high level. The order here follows the structure of the thesis. First, in Sections 2.1 and 2.2, we introduce the theory contributions, *i.e.* winning probabilities of new families of no-cloning games and the first rigidity result for a monogamy-of-entanglement game, respectively. Then, we introduce applications of these results to cryptography in Section 2.3.

2.1 Coset state games

We study a family of no-cloning games based on *subspace coset states*. These states generalise subspace states [AC12], which are uniform superpositions of the basis vectors indexed by a linear subspace $a \subseteq \mathbb{Z}_2^n$,

$$|a\rangle = \frac{1}{\sqrt{|a|}} \sum_{u \in a} |u\rangle. \tag{2.1.1}$$

The generalisation is attained by encrypting the subspace state with a quantum one-time pad $|a_{t,t'}\rangle = X^t Z^{t'} |a\rangle$ [CLLZ21, VZ21]. Alternately, this can be seen as a uniform superposition over a coset $t + a$, with phases provided by the coset of the orthogonal complement $t' + a^\perp$. Changing the coset representatives only affects the global phase of the coset state; and, for a fixed subspace, the subspace coset states ranging over a set of coset representatives form an orthonormal basis.

To construct a first example of a no-cloning game from coset states, we consider the

game called the *weak coset state NC game*, where Alice sends a subspace coset state $|a_{t,t'}\rangle$, and Bob and Charlie have to guess both cosets $(t + a, t' + a^{\perp})$. This game was introduced in [CLLZ21], wherein they show that its winning probability is subexponentially small in n. They also introduced a more powerful game, the *strong coset state NC game*, that makes full use of the two-index structure. In this game, Alice sends the same state, but Bob needs only guess $t + a$ and Charlie needs only guess $t' + a^{\perp}$. This breaks with the original structure of a no-cloning game, as, to win this game, Bob and Charlie need to guess two *independent* pieces of information. Also, we see that this game must be easier to win than the weak coset state NC game, as any strategy the players use in the weak game can be adapted to one for the strong game that succeeds with equal or higher probability. It was conjectured in [CLLZ21] that the value of the winning probability of the strong coset state NC game is also subexponentially small in n, which they show has applications to uncloneable decryption and copy-protection of pseudorandom functions. We provide the first proof of this conjecture by finding an exponentially small upper bound on the winning probability of this game.

Next, we introduce a version of the strong coset state NC game that is even easier to win, which we call the *leaky coset state NC game*. This game proceeds in the same way as the strong coset state NC game, but before Charlie makes his guess of t', Bob's guess of t leaks to him. In this way, we are able to see the information that Charlie gets as messages sent during an interaction between Alice and Bob, on which he eavesdrops. Also, we make this game robust by allowing Bob and/or Charlie's answers to have some small number of error bits. We show that the winning probabilities of these games are also exponentially small in n.

Major Theorem (informal version of Theorems 6.2, 6.8 and 6.11)**.** The optimal winning probabilities of the strong, leaky, and robust leaky subspace coset no-cloning games are exponentially small in the number of qubits Alice sends.

To formalise these games, we work with a very general form of the no-cloning game model. In this model, Bob and Charlie may receive different questions, and rather than requiring that they both guess the question that Alice has encoded, they come up with answers that satisfy some arbitrary decision predicate. This is a natural generalisation, as it corresponds to a generalised version of the MoE games which still fits into the XNL game model. However, even though the robust leaky game is only a slight variant of the leaky game, it does not fit into this model. In this game, the leaked answer from Bob to Charlie is allowed to be in some small neighbourhood of the string that Alice prepared. Hence,

Bob may freely choose a small fraction of the bits of his answer. As such, the question that is sent to Charlie is in part chosen by Bob. As the questions cannot be seen as being simply sampled by Alice, this cannot fit into the no-cloning game model, and in fact its entanglement-based version cannot fit in the XNL game model either. This provides an example of a useful quantum game beyond the XNL game model.

Proof techniques. To bound the winning probabilities of the subspace coset no-cloning games, we adapt the technique of [TFKW13]. Our approach for each game proceeds in a few steps. First, we transform the game into an MoE-like entanglement-based variant by making the splitting channel into a shared state with the Choi representation, so that we might consider the winning probability as the norm of an operator, as in [BL20]. Then, by purifying the strategy, the winning probability is the operator norm of a sum of projectors over the questions. By using the overlap lemma of [TFKW13], we bound this norm of a sum of operators as the sum of the *overlaps* — norms of products — of these operators. Making use of a couple simple operator inequalities, we can reduce the overlaps into overlaps of only Alice's operators. As the structure of Alice's operators are given by the definition of the game, we can work out a sufficient upper bound for this overlap. Putting this together provides an upper bound on the winning probability of the original game.

To take the no-cloning game winning probability bounds to a form more intuitively usable in applications, we express them as entropic uncertainty relations. Entropic uncertainty relations, and earlier uncertainty relations beginning with [Hei27], have played a foundational role in quantum information [WW10]. Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13] show an entropic uncertainty relation in the same scenario as their MoE game. We provide an entropic uncertainty relation that arises naturally from the scenario of the leaky subspace coset NC game, allowing us to work with the full strength of the no-cloning property in an entropy setting.

To show our relation, we generalise the min-entropy of guessing $H_{\min}(X|A)_\rho$ to what we refer to as the *sequential min-entropy*, $H_{\min}(X|A,Y|B)_\rho$ which represents the uncertainty of guessing X knowing A, followed by guessing Y knowing B, on the same state. To the best of our knowledge, this is a novel concept.

For any measurement M on A used to guess X, this decomposes as the entropic uncertainty relation

$$H_{\min}(X|M(A))_\rho + H_{\min}(Y|B)_{\rho_{|(M(A)=X)}} \geq H_{\min}(X|A,Y|B)_\rho, \tag{2.1.2}$$

where $\rho_{|(M(A)=X)}$ is the state conditioned on the guess of X being correct. A notable distinction between such an entropic uncertainty and a more standard relation is that the states on the two terms are different, although closely related. The winning probability of the leaky NC game can directly be expressed as $\exp(-H_{\min}(T|AB, T'|ATC)_\rho)$ using a sequential entropy, where $\rho_{ATT'BC}$ is the state such that A holds the subspace a, T and T' hold the coset representatives t, t', and B and C hold Bob and Charlie's quantum systems once they are isolated. Hence, the leaky NC property provides the entropic uncertainty relation

$$H_{\min}(T|M(AB))_\rho + H_{\min}(T'|ATC)_{\rho_{|(M(AB)=T)}} \in \Omega(n). \tag{2.1.3}$$

This may be compared to the MoE game-based entropic uncertainty relation that was studied in [TFKW13], $H_{\min}(X|\Theta B)_\rho + H_{\min}(X|\Theta C)_\rho \geq -2\lg\left[(1+2^{-n/2})/2\right] \in O(1)$, where ρ_{ABC} is any quantum state with $A = \mathbb{Z}_2^n$, X is the result of measuring A in a uniformly random Wiesner basis of states $|x^\theta\rangle = H^{\theta_1}|x_1\rangle \otimes \cdots H^{\theta_n}|x_n\rangle$, and Θ is the description of the basis. The relation is found in the same way as their bound on the winning probability of their MoE game, but is strictly weaker than that bound, since it only considers entropies with respect to the same state. This makes it too weak to provide security of related cryptographic primitives. In fact, even in the case of the subspace coset NC game, we similarly have

$$H_{\min}(T|M(AB))_\rho + H_{\min}(T'|ATC)_\rho \in O(1), \tag{2.1.4}$$

using the same simple attack: half the time, Bob takes the whole state, and the other half of the time, Charlie takes the whole state.

We can also handle the probability of approximate guessing in the robust leaky NC game as an entropic uncertainty relation, by representing the "entropy of approximate guessing" as an entropy of exact guessing on a modified state. Explicitly, the relation takes the now-familiar form

$$H_{\min}(T|M(AB))_\sigma + H_{\min}(T'|ATC)_{\sigma_{|(M(AB)=T)}} \in \Omega(n), \tag{2.1.5}$$

where σ is the state modified to account for the error bit flips $\sigma = \mathbb{E}_{|u|\leq\gamma n/2} X_T^u \rho X_T^u$.

2.2 Rigidity for monogamy-of-entanglement games

We study the MoE game of [TFKW13], where Alice measures either in the computational or the Hadamard basis. As shown there, Bob and Charlie can win with probability at most $\cos^2 \frac{\pi}{8} \approx 0.85$. The TFKW game has a particularly simple optimal strategy: Bob and Charlie share no entanglement; they just send Alice a Breidbart state $|\beta\rangle \propto |0\rangle + |+\rangle$, that sits directly between the computational zero $|0\rangle$ and the Hadamard zero $|+\rangle$, and always guess 0 for the measurement outcome. It is straightforward to see that, due to the symmetries of Alice's measurement bases under the action of the Pauli operators, there are at least 4 optimal unentangled strategies: the Wiesner-Breidbart states $|\beta\rangle$, $X|\beta\rangle$, $Z|\beta\rangle$, $XZ|\beta\rangle$. But the question remains: are these all the possible optimal strategies? Particularly, are there optimal strategies where the players use entanglement? This question is tantamount to asking about the *rigidity* of the TFKW game.

The idea of rigidity, first formally introduced by Mayers and Yao [MY04], is that certain games can be used to "self-test" quantum states: if such a game is won with high enough probability, then the self-test property tells us that the players must hold some quantum state, up to local isometry. More general are robust self-tests, where even a near-optimal winning probability gives a guarantee that the state is near to this optimal one. Up until now, the study of rigidity has been limited to *nonlocal games*. This area of study grew around the CHSH game. This game, introduced by Clauser, Horne, Shimony, and Holt [CHSH69] as a discrete-variable analogue of a Bell inequality [Bel64], was known, even before rigidity was formalised, to self-test a maximally-entangled state on two qubits [Tsi93]. This result was later extended to be robust [MYS12] and to hold under parallel repetition [Col17].

The rigidity of the CHSH game has found many applications: for example it was used to construct a protocol for quantum delegated computation [RUV13]. Other examples of nonlocal games include the Mermin-Peres magic square game — which can always be won and self-tests two copies of the maximally entangled state, and was used to show $\mathsf{MIP}^* = \mathsf{RE}$ [JNV+21] — and more generally linear constraint games [CMMN20].

Our main contribution in this part is to prove the first rigidity result for a monogamy-of-entanglement game:

Major Theorem (informal version of Theorem 7.5)**.** The state of any optimal strategy for the TFKW game is given as a convex combination of the unentangled optimal states $|\beta\rangle$, $X|\beta\rangle$, $Z|\beta\rangle$, $XZ|\beta\rangle$. This is robust and extends to multiple rounds played in parallel.

By convex combination, we mean a superposition of tensor product states where the components on Alice's register are the optimal Wiesner-Breidbart states and the components on Bob and Charlie's register have orthogonal supports. That is, Bob and Charlie can simultaneously distinguish which unentangled optimal state Alice receives. Note that a similar notion of rigidity holds for some nonlocal games: for example, Mančinska, Nielsen, and Prakash [MNP21] show that the glued magic square game self-tests a convex combination of inequivalent optimal strategies. This requirement on optimal strategies of the TFKW game forces Bob and Charlie to *not* use any of their shared entanglement while playing.

For applications, it is often necessary to extend the rigidity result to be robust and to the scenario where games are played in parallel. This is because playing the game only once gives essentially no information on the winning probability of the strategy used. What Alice can do to remedy this is to get Bob and Charlie to play many games at the same time and use that information to build up statistics about how often they win. As such, she needs the result to be robust — a guarantee that the state is near-optimal if the winning probability is near-optimal — as the sampling cannot quite show that the strategy is optimal. Also, she needs the result to hold for games played in parallel, to ensure that there is nothing different and more exotic they may do using their entanglement to win multiple games optimally. We show that the rigidity of the TFKW game holds in this general case.

Proof techniques. We present a sum-of-squares (SOS) decomposition of the game polynomial for the TFKW game. The state $|\psi\rangle$ of any optimal strategy is in an eigenspace of the game polynomial in terms of the observables of that strategy, which provides a selection of relations for the observables. There are two types of relations that come out: one allows to exchange Bob and Charlie's observables and the other gives that $|\psi\rangle$ is an eigenvector of a particular sum of observables. In particular, these imply that each of the players' observables must commute with respect to the state, generating a $|\psi\rangle$-representation of $\mathbb{Z}_2^2$. As such, we invoke the Gowers-Hatami theorem as in [Vid18] to locally dilate the players' space isometrically and transform this into a bona fide representation. These observables are simultaneously diagonalisable, so the dilated shared space can be decomposed as a direct sum of orthogonal subspaces on which they act as scalars. Returning to the relations from the SOS decomposition using the dilated observables allows us to constrain where the shared state lives in this orthogonal sum and show that the components on Alice's space must take the form $X^{s_0}Z^{s_1}|\beta\rangle$.

We then build on this technique to show the rigidity in the robust case. Here, however, since the winning probability is assumed to be some $\varepsilon > 0$ smaller than optimal, the value of each of the terms in the SOS decomposition are not zero when acting on the state, but rather in $O(\varepsilon)$. Nevertheless, we can use the relations to get an approximate representation, which we dilate similarly with Gowers-Hatami. Of course, this cannot give that the state is exactly a convex combination as above, but rather that its projection onto the unwanted subspaces is small, giving that this is $O(\sqrt{\varepsilon})$ close to an optimal state.

We show the exact rigidity for a parallel repetition of n TFKW games by extracting many optimal strategies for a single game, assuming Bob and Charlie can guess each of the answer bits for the repeated games with optimal probability. We show first that the observables related to each copy of the TFKW game must act in the same way on $|\psi\rangle$ by using the rigidity decomposition, and then use this as tool to show that all of the observables commute. This induces, again with Gowers-Hatami, a representation of $(\mathbb{Z}_2^2)^n$ and lets us conclude in a similar way as for the single-game case that the state must be a convex combination of tensor products of states of the form $X^{s_0}Z^{s_1}|\beta\rangle$.

The most general rigidity result we prove is the robust case of the parallel repetition of TFKW games. To generalise the exact-case method, we use a technique of [Col17] to extract sufficiently many strategies for TFKW that win near-optimally. Proceeding similarly as before, we get that the state is $O(n^3\sqrt{\varepsilon})$ away from an optimal state.

Finally, we adapt a technique of [RUV13] to be able to pass from winning statistics Alice may observe when playing TFKW games in parallel to a guarantee on the winning probability of a large subset of the games. Knowing upper bounds on the winning probability of each of the games, we can use Hoeffding's inequality to show that there is but a low probability that the players win most games while the winning probability for too many of them is more than ε away from optimal.

2.3 Applications

Quantum uncloneability has powerful implications for cryptographic scenarios by providing properties that are classically impossible. Through the study of uncloneability games, we are able to quantitatively exhibit uncloneability properties, such as no-cloning and monogamy-of-entanglement. As such, if we construct cryptographic protocols around the structures of these games, the uncloneability properties serve as resources we may use to show security of concrete instantiations.

We present a variety of applications of the above results on uncloneability games to cryptographic scenarios.

2.3.1 Uncloneable encryption

Uncloneable encryption as is currently understood was introduced in [BL20], building on earlier concepts such as the tamper-evident encryption of [Got03] and the MoE games of [TFKW13]. In its most general form, an uncloneable encryption scheme provides a way to encrypt messages in such a way that they cannot be simultaneously read by two malicious parties, Bob and Charlie, under the assumption that they are isolated once the encryption key is released. To the best of our knowledge, it is unknown whether this is achievable in the plain model, even if we allow computational assumptions. Uncloneable encryption schemes in the quantum random oracle model (QROM) have been studied [BL20] and provide nearly optimal security; nevertheless, security in the random oracle model, even classically, does not imply security in the plain model [CGH04], though this relies on a contrived counterexample. Computational assumptions have been considered: under the assumption of post-quantum one-way functions, [AK21] show that it is possible to turn an uncloneable encryption scheme into one with semantic security; and under the assumption of a post-quantum public key encryption scheme, they show how to turn the scheme into a public-key uncloneable encryption scheme. Since all these rely on the existence of uncloneable encryption, a key open question remains concerning the existence of an "uncloneable bit" — an optimal uncloneable encryption scheme in the plain model that encrypts one-bit message. This is a fundamental object as any uncloneable encryption scheme implies an uncloneable bit [BL20, Theorem 9].

We construct and show information-theoretic security of an uncloneable encryption scheme in a model that is slightly different from the one in which it was originally defined. Originally, the encryption was represented by a quantum encryption of classical messages (QECM), a protocol that encrypts classical messages as quantum ciphertexts, which can be decrypted using only the classical encryption key [BL20]. We extend this by replacing the decryption algorithm by an interaction between the sender and the receiver, what we call a quantum encryption of classical messages with interactive decryption (QECM-ID).

A QECM scheme is uncloneable if two receivers, Bob and Charlie, receive a ciphertext, split it arbitrarily, and only get the key once they are isolated, then they can simultaneously learn the message with at best near-trivial probability. To adapt this to a QECM-ID scheme, we again have two receivers, whom we call Bob and Eve, who split a ciphertext.

To decrypt, Bob initiates an interaction with Alice. Only after this point does Bob need to be seen as the intended recipient of the message. To avoid the trivial attack where Bob simply gives the decrypted message to Eve, they may not communicate directly during the interaction step — nevertheless, Eve may eavesdrop on the communication between Alice and Bob. We therefore say that the encryption is uncloneable if, for any actions Bob and Eve take, the probability that Eve guesses the message correctly once the interaction finishes and the decryption protocol does not abort is near-trivial.

Finally, we also adapt uncloneable-indistinguishable security, which is meant to represent an uncloneablility version of chosen-plaintext attack (CPA) security. We say that a QECM-ID is uncloneable-indistinguishable secure if, after the decryption interaction, the probability that, simultaneously, Alice accepts the decryption and Eve distinguishes a chosen message distribution from a fixed message is near trivial, *i.e.* half the probability of accepting. This adapts the uncloneable-indistinguishable security of QECMs defined in [BL20]. For a QECM, this is the property that Bob and Eve cannot simultaneously distinguish the encryption of a chosen message distribution from a fixed message. Intuitively, the condition that Bob guesses correctly is replaced with the condition that Alice accepts the decryption in order to adapt the definition to a QECM-ID. We show there is an equivalence between these two definitions up to scalar multiple, which extends the property shown in [BL20] that uncloneable security implies uncloneable-indistinguishable security for QECMs. We also show that our construction satisfies both of these definitions separately.

Proof techniques. To instantiate an uncloneable QECM-ID, we make use of the leaky no-cloning property. Note that this bound implies that, if Bob is able to provide t to Alice, then with high probability Eve is unable to guess t' correctly even if she learns t. Hence, Alice can use the interaction to check whether Bob knows t. If he does, she is sure with high probability that t' has not been cloned, so she can share the message, encrypted classically using a key that is a function of t'.

2.3.2 Quantum key distribution

Quantum key distribution (QKD), introduced by Bennett and Brassard [BB84], is a foundationally important quantum cryptographic primitive. In its most basic form, it allows an honest sender, Alice, to share a secret key with an honest receiver, Bob, over a public channel without an eavesdropper Eve learning the key. Many variants of QKD that require

only weaker assumptions on the honest parties have been proposed. In particular, device-independent protocols, initiated by Ekert [Eke91], seek to allow QKD with few, if any, assumptions on the behaviour of Alice and Bob's devices. One-sided device-independent QKD, shown in [TFKW13], allows Bob's quantum device to be fully untrusted, relying on a monogamy-of-entanglement game winning probability bound for security; and fully device-independent QKD, shown by Vazirani and Vidick [VV14], allows both Alice and Bob's quantum devices to be untrusted, with security coming from the rigidity of a nonlocal game. These varying assumptions allow implementations of QKD to balance practicality and security, depending on available resources.

We show security of QKD in a model extending the one-sided device-independent model, which we call *receiver-independent QKD*. In this model, Alice's quantum device remains fully trusted, but neither Bob's quantum nor his *classical* device is trusted. However, we require that Bob's communication be trusted: if Bob's communication were not trusted, any QKD scheme would be susceptible to the trivial attack where Bob sends his final key to Eve. In this way, this model can be seen as the minimal assumption on the receiver, hence warranting the name "receiver-independent".

Receiver-independent QKD schemes are distinct in a number of ways. First, since any computation Bob might want to make is inherently untrusted, he cannot be trusted to check any property of the shared state. As such, only Alice may be given the power to abort the protocol. In this way, the interactions between Alice and Bob take the form of a sequence of challenges and responses. Also, the idea of correctness must be altered to account for the fact that Bob's classical computations are untrusted. This is because it is not possible to be certain that Bob has access to the final key, but it is possible to be sure that his device can compute it.

Proof techniques. We construct a receiver-independent QKD scheme using coset states, and show its security using an error-robust generalisation of the leaky NC property. Alice sends a coset state $|a_{t,t'}\rangle$ to Bob. To verify that Eve does not have t', Alice asks Bob to provide t, acting as the parameter estimation step. If he is able to, with only small error, then Alice issues challenges to Bob that allow her to correct her t' to match the guess $\hat{t}'$ Bob's device claims to have, and then verify this match, which act as the error correction and information reconciliation steps, respectively. Finally, for privacy amplification, Alice acts on her corrected raw key with a quantum-proof strong extractor and instructs Bob to do the same. It is worth noting that our use of an entropic uncertainty relation brings the

security proof intuitively closer to the original proofs of QKD security than the proof of [TFKW13], which works directly with an MoE game.

2.3.3 Bit commitment

Bit commitment is a fundamental cryptographic primitive with a variety of applications, *e.g.* to zero-knowledge proofs, and to two-party computation via its association to oblivious transfer. In commitment, a sender Alice commits to a string that a receiver Bob can only access when Alice chooses. Ideally, the commitment should be *hiding*, in the sense that Bob cannot learn the string Alice has committed until she chooses to reveal, and *binding*, in the sense that Alice must reveal the same string to which she had committed. The problem is that, without additional assumptions, bit commitment is impossible [May96, LC97, BS16], but there are a variety of models in which it was shown to exist. For example, under classical computational assumptions [Cha87, Nao91] (see also [Cré11]) or in the noisy quantum storage model [KWW12]. We study two different ways to apply uncloneability games to the problem of commitment.

First, we introduce a method to make a bit string commitment scheme uncloneable. A problem underlying many classically-defined cryptographic primitives is that they are inherently cloneable; if an eavesdropper Eve is able to eavesdrop on the communications between Alice and Bob, she may be able to produce a transcript of their interactions and hence learn the final string whenever it is revealed. This is the case for bit commitment: in fact, the reveal step is usually represented as a public broadcast with no indication of security against an eavesdropper. To remedy this, we define an *uncloneable bit string commitment scheme* as a commitment scheme with an additional check step in between the commit and reveal steps, where Alice verifies whether an eavesdropper has attempted to clone the commitment. If the commitment passes this check, then an honest Alice can be sure that only Bob will be able to open it during the reveal phase, despite a lack of prior agreement between them. Bob may even be malicious: the only restriction needed on him is that he does not communicate directly to Eve after the check. With this in mind, the point in time when Alice chooses to undertake the check allows it to be run under varying assumptions. In particular, Alice may check immediately after committing, which means that no honest party needs to store any quantum information, but Alice needs to be sure that Bob does not communicate privately with Eve at any point after committing. This is more feasible for near-term quantum devices, but requires that Bob not communicate information to Eve for a period of time between steps. On the other hand, if Alice waits

until immediately before revealing to do the check, she may assume that Bob and Eve have arbitrary communication after committing. The drawback is that Bob must store a quantum state even if he is honest.

Secondly, we consider an alternate model, with two colluding receivers, and show that that bit commitment is possible in this model. Two-prover bit commitment was studied before in the classical context [BGKW88], where it was shown that separating the *sender* into two isolated parties can be used to ensure the binding property (see also [CSST11]). In contrast, we introduce a third party Charlie who is initially in full collusion with Bob, but who is isolated from Bob once Alice measures. Under the assumption of a public broadcast from Alice to Bob and Charlie, we are able to achieve bit commitment. To the best of our knowledge, this is the first such scheme; furthermore, we show that, with classical communication only, our model reduces to the single-receiver model — where unconditionally secure bit commitment is impossible — meaning that we have identified a new qualitative advantage for quantum communication in cryptography.

Proof techniques We use the leaky NC property to provide a way to turn a commitment scheme into an uncloneable commitment of the above form, which works under the same assumptions as the original commitment. In order to commit to $e(t', r)$, where e is a quantum-proof strong extractor, Alice commits to r using the original commitment and sends a coset state $|a_{t,t'}\rangle$ to Bob. Because Bob does not know a, he has no information about t' and r has not been revealed, so the commitment is hiding. Next, to check for cloning, Alice sends a to Bob and verifies that he can measure t. Due to the leaky NC property, this implies that Eve is only able to guess t' with low probability. Finally, to reveal, Alice reveals r and Bob queries Alice for some information about t' to make sure that their values are consistent, making the scheme binding. With a good choice of strong extractor, this causes only a polynomial decrease in the length of the committed string and an exponentially small change in the binding parameter.

On the other hand, to give a construction of two-receiver commitment, we make use of the rigidity of the TFKW game. Using a reduction of König, Wehner, and Wullschleger [KWW12], we first show the security of *weak string erasure* (WSE), which implies both bit commitment and oblivious transfer, in this model. WSE is a cryptographic primitive that allows the sharing of partial information between mistrustful parties, a sender Alice and a receiver Bob. In WSE, Alice receives a random bit string x while Bob receives a substring; Bob knows which bits of x he holds but is unable to determine the remainder, while Alice

is unable to determine which substring Bob holds. We construct a WSE scheme whose security is based upon the rigidity of the TFKW game. The receiver Bob prepares a state ρ_{ABC} shared between Alice, Bob, and Charlie, where Alice holds $N \in \texttt{poly}(n)$ qubits. In the honest case, this has the form of an unentangled optimal strategy for the parallel-repeated TFKW game. Then, Alice verifies that the state must be near an optimal state for the TFKW game by playing the game with Bob and Charlie using $N-n$ of her qubits. This check fails with exponentially small probability in n. On the remaining n qubits, however, she measures in a random Wiesner-Breidbart basis, *i.e.* either the basis $|\beta\rangle, XZ|\beta\rangle$ or the basis $Z|\beta\rangle, X|\beta\rangle$. Giving Bob the information about which basis she chose for these n qubits, he may guess on average half of the bits and have no information about the rest. This provides security against a dishonest Bob. For security against a dishonest Alice, we note that the rigidity still gives Bob the freedom to choose the Wiesner-Breidbart state on the register he gives to Alice. These states constitute a pair of mutually-unbiased bases. Therefore, if Bob chooses the state randomly, this eliminates Alice's chance of guessing which bits he knows. The isolation requirement between Bob and Charlie is necessary to prevent an attack where they jointly share a maximally entangled state with Alice and then can always measure each bit in the correct basis. The requirement that Alice broadcast publicly which n bits are used to generate the output string is to prevent an attack where she asks Bob and Charlie to play the TFKW game on different bits, and uses Charlie's replies to extract information about Bob's prepared conjugate-coding basis.

2.3.4 Randomness expansion

Randomness is a precious resource for computation and cryptography. Pseudorandom generators are functions that produce large amounts of randomness from a small random seed, but the quality of this randomness is inherently based on a computational assumption, *e.g.* the existence of one-way functions. Thus, given sufficient computational power or time, an adversary can eventually break the scheme.

Quantum entanglement has long been known to provide an advantage in creating unconditionally secure randomness [Col06, AM16]. By verifying that two isolated parties violate a Bell inequality, a verifier is able to guarantee, due to the randomness inherent in quantum mechanics, that the players' outputs provide intrinsic, fresh randomness. Such schemes are able to yield exponential randomness expansion [VV12]. Further, using the rigidity of the CHSH game, it is possible to guarantee that the randomness is secure against side information, and thus allow composition, providing arbitrarily large randomness ex-

pansion [CY14]. The technical difficulty with these schemes is that they require entanglement between isolated parties, which remains difficult to generate in sufficient quantities. Based on the experimental demonstration of a loophole-free Bell inequality violation [HBD+15], recent work has been able to achieve a randomness expansion of 24% over a period of 91 hours; however, the new randomness is only secure against classical and not quantum side information [SZB+21].

Here, we give a protocol where entanglement between isolated parties is not required in order to expand randomness. In order to achieve this, we make use of an adapted version of the WSE protocol as described above. First, the questions Alice asks are pseudorandom rather than uniformly random; this allows Alice to start with only a small random seed. With polynomial overhead, we can extract statistically near-uniform randomness using the rigidity of the TFKW game. To do this, Alice uses many of the bits to verify that the shared state is near the state of an optimal strategy, and then extracts randomness using her knowledge of the remainder of the state. We thus require the computational assumption to hold during the interaction of the protocol, after which the output randomness becomes nearly indistinguishable from uniform, even to an unbounded adversary — this concept is called *everlasting* security and was previously studied in the context of quantum key distribution [SML10] and multi-party computation [Unr13]. Furthermore, we note that in our model, all of the measurement settings Alice uses can be leaked as she measures, without compromising the security or uniformity of the randomness.

Proof techniques. We use the rigidity of the TFKW game, as well as a computational assumption on the existence of pseudorandom generators, to construct a randomness expansion scheme that is everlasting, in the sense that the output randomness is guaranteed to be near-uniform in trace norm, as long as the computational assumption is not broken during the execution of the protocol. As in the previous protocol, Alice interacts with a pair of adversaries, Bob and Charlie, and they all share an adversarially-prepared state ρ_{ABC}, where Alice holds $N \in \texttt{poly}(n)$ qubits. Alice plays the TFKW game on $N - n$ of the qubits to verify that the shared state is near an optimal state. However, rather than choosing the locations and questions for the TFKW game rounds uniformly at random, she chooses them by sampling the output of a pseudorandom generator, given a random seed. Bob and Charlie, who are assumed to be computationally bounded, have only a negligible probability of distinguishing this from the uniformly random case, and thus this check has only a negligibly small probability of failure. Alice measures each of the remaining n qubits in

the basis $|+i\rangle, |-i\rangle$ that diagonalises the Pauli Y operator. Since this basis is mutually unbiased with both of the Wiesner-Breidbart bases, the outcome is nearly uniformly random, and neither Bob nor Charlie have information on what this outcome is, as long as they stay isolated.

Chapter 3

Mathematical Preliminaries

In this chapter, we review the standard mathematical objects we need and the notations we use to represent them.

3.1 Sets and Notation

We make use of two different set constructor notations: for usual sets of unlabelled elements, we construct them with the usual notation, such as $\{x_i | i \in I\}$; and for labelled sets, we construct them with subscript notation, such as $\{x_i\}_{i \in I}$. For a set X, we write the power set, which is the set of all subsets, $\mathscr{P}(X)$.

We use standard notation for the number sets: $\mathbb{N} = \{1, 2, 3, \ldots\}$ for the set of natural numbers, $\mathbb{Z}$ for the integers, $\mathbb{R}$ for the real numbers, and $\mathbb{C}$ for the complex numbers. To avoid confusion, we write the non-negative real numbers as $[0, \infty)$ and the positive real numbers as $(0, \infty)$. For conciseness, we write the set of natural numbers up to n as $[n] = \{1, 2, \cdots, n\}$. Write $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ for the ring of integers modulo $n \in \mathbb{N}$. We equate $\mathbb{Z}_2$ and the space of one bit, and in this way see the addition as the XOR operation and the multiplication as the AND operation.

We write the base e logarithm $\ln$ and the base 2 logarithm $\lg$. They are related by $\lg x = \frac{\ln x}{\ln 2}$.

3.1.1 Words and Groups

It is often useful to see a finite set Σ as an *alphabet*. That is, we see elements of Σ as letters which are concatenated to give *strings*, or *words*. In this interpretation, we call

elements of the Cartesian power $x \in \Sigma^n$ strings of length n and write them $x = x_1 \dots x_n$ for $x_i \in \Sigma$. For a subset $I \subseteq [n]$, we define $x_I := x_{i_1} x_{i_2} \dots x_{i_k}$ the string of length k, for $I = \{i_1, \dots, i_k\}$ with $i_1 < \dots < i_k$. The most important example is the space of n-bit strings $\mathbb{Z}_2^n$. In this set, we also write e_i for the string such that $(e_i)_j = \delta_{i,j}$, the Kronecker delta, and $e_I = \sum_{i \in I} e_i$. We write the space of all bit strings $\mathbb{Z}_2^* = \bigcup_{n=0}^{\infty} \mathbb{Z}_2^n$, where $\mathbb{Z}_2^0$ is considered to contain one element, the empty string ϵ.

We can also generate groups from words. For a finite set Σ, we take $\mathrm{F}\Sigma$, the *free group generated by* Σ, to be the set of words of any length in $\Sigma \cup \Sigma^{-1} \cup \{1\}$, where 1 is an identity element and Σ^{-1} represents the inverses of the elements of Σ, subject to the relations $x = 1x = x1$ and $xx^{-1} = x^{-1}x = 1$ for all $x \in \Sigma$. The concatenation of strings becomes the group product on $\mathrm{F}\Sigma$. We can represent relations on Σ by elements of $\mathrm{F}\Sigma$. In order to avoid conflation with bra-ket notation, we write the group generated by Σ with relations $R \subseteq \mathrm{F}\Sigma$ as $\mathrm{gen}\,\{\Sigma | R\}$; this is the quotient of $\mathrm{F}\Sigma$ by the normal subgroup generated by R.

3.1.2 Order Approximations

It is often useful to compare the growth rates of functions $\mathbb{N} \to [0, \infty)$ without having to appeal to their exact forms. To do so, we compare the functions asymptotically up to *order*. Let $f, g : \mathbb{N} \to [0, \infty)$. We define the sets $O(g)$, $o(g)$, and $\Omega(g)$ as follows. First, $f \in O(g)$ if there exists $N \in \mathbb{N}$ and $k \geq 0$ such that $f(n) \leq kg(n)$ for all $n \geq N$; and that $f \in o(g)$ if this holds for all $k > 0$. Next $f \in \Omega(g)$ if $g \in O(f)$. Write $O(g(n)) = O(g)$ and similar for the others. We say that f is *polynomial* if $f \in O(n^m)$ for some $m \in \mathbb{N}$, that it is *negligible* if $f \in o(1/n^m)$ for all $m \in \mathbb{N}$, and that it is *exponentially small* if $f \in O(b^{-n})$ for some $b > 1$. Write the set of polynomial functions as $\mathtt{poly}(n)$ and the set of negligible functions as $\mathtt{negl}(n)$

3.2 Vector Spaces

Most of the results here are standard. Some of the proofs follow [NC10].

We assume some familiarity with linear algebra, so we don't dwell on the basics. A *vector space* V over a field $\mathbb{F}$ is an abelian group under $+$ along with a field action $\mathbb{F} \times V \to V$ called scalar multiplication, where the addition on the field and the group and the field are compatible. The set of all linear combinations of elements in a sub-

set $S \subseteq V$ is called the *span* and denoted $\mathrm{span}_{\mathbb{F}} S$, where the subscript is omitted if the field is evident; the span is the smallest vector subspace containing S. When obvious we sometimes write v to denote the subspace $\mathbb{F}v = \mathrm{span}_{\mathbb{F}}\{v\}$. A subset $S \subseteq V$ is *linearly dependent* if there exist $v_1, \ldots, v_n \in S$, and $c_1, \ldots, c_n \in \mathbb{F}$ not all zero such that $\sum_i c_i v_i = 0$; else the collection is linearly independent. A maximal linearly independent subset of V is called a *basis*. Every basis of V has the same cardinality, called the *dimension* of V and denoted $\dim V$. V is *finite dimensional* if $\dim V < \infty$ — unless otherwise indicated, we assume any vector space we work with is finite dimensional.

3.2.1 Metrics, norms, and inner products

On many spaces, it is primordial to have a notion of distance. The most basic among these is a metric.

Definition 3.1 (Metric)**.** Let X be a set. A *metric* is a function $d : X \times X \to [0, \infty)$ that satisfies, for $x, y, z \in X$,

positive-definiteness $d(x, y) = 0$ if and only if $x = y$

symmetry $d(x, y) = d(y, x)$

triangle inequality $d(x, y) \leq d(x, z) + d(z, y)$

The pair (X, d) is called a *metric space*.

Any metric space is automatically a topological space with the topology generated by the base of open balls $B(x, \varepsilon) = \{y \in X | d(x, y) < \varepsilon\}$ for all $x \in X$, $\varepsilon > 0$.

An example of a metric that we use on multiple occasions is the *Hamming distance*. This metric is defined on any set of words Σ^n as the number of letters on which a pair of words differs $d(x, y) = |\{i \in [n] | x_i \neq y_i\}|$.

On vector spaces, we can do more. We define norms and inner products. In general, these can be defined on real or complex vector spaces, but for our purposes we consider them only on complex spaces.

Definition 3.2 (Norm)**.** Let V be a vector space over $\mathbb{C}$. A *norm* is a function $\|\cdot\| : V \to [0, \infty)$, that satisfies for $u, v \in V$ and $\lambda \in \mathbb{C}$,

positive-definiteness $\|u\| = 0$ if and only if $u = 0$

homogeneity $\|\lambda u\| = |\lambda|\|u\|$

triangle inequality $\|u + v\| \leq \|u\| + \|v\|$

The pair $(V, \|\cdot\|)$ is called a *normed vector space*.

Any norm on a vector space induces a metric, and so a topology, via $d(x, y) := \|x-y\|$.

The canonical example is the Euclidean norm on $\mathbb{C}^n$, that we write $\|v\| = \sqrt{\sum_{i=1}^{n} |v_i|^2}$. An interesting non-example is provided by the Hamming distance. On $\mathbb{Z}_2^n$, which is a vector space, the Hamming distance can be used to define the *Hamming weight* $|x| = d(x, 0)$, the number of non-zero letters in the word. This is both positive-definite and satisfies the triangle inequality, but it is not a norm as $\mathbb{Z}_2^n$ is not a $\mathbb{C}$-vector space and hence homogenity over $\mathbb{C}$ is impossible.

Definition 3.3 (Inner product)**.** Let V be a vector space over $\mathbb{C}$. An *inner product* is a map $\langle\cdot|\cdot\rangle : V \times V \to \mathbb{C}$ that satisfies, for $u, v, w \in V$ and $\alpha, \beta \in \mathbb{C}$

positive-definiteness $\langle u|u\rangle \in [0, \infty)$ and $\langle u|u\rangle = 0$ iff $u = 0$

conjugate symmetry $\langle u|v\rangle = \overline{\langle v|u\rangle}$

right-linearity $\langle u|\alpha v + \beta w\rangle = \alpha \langle u|v\rangle + \beta \langle u|w\rangle$

The pair $(V, \langle\cdot|\cdot\rangle)$ is called an *inner product space*.

Note that we use the definition of an inner product that is more common in physics with linearity on the right. In mathematics it is more common to see left linearity. In our case, the inner product is nevertheless nearly linear on the left, satisfying conjugate linearity $\langle \alpha u + \beta v|w\rangle = \bar{\alpha} \langle u|w\rangle + \bar{\beta} \langle v|w\rangle$.

The positive-definiteness implies that the inner product is *non-degenerate* in the sense that $\langle v|u\rangle = 0$ for all $v \in V$ if and only if $u = 0$.

An inner product induces a norm $\|v\| := \sqrt{\langle v|v\rangle}$, giving the inner product space the structure of a normed vector space and therefore a topological space. An inner product space that is complete in the topology generated by the inner product is called a *Hilbert space*. In finite dimensions, every inner product space is a Hilbert space as it is always complete in the inner product topology. We denote Hilbert spaces by script capitals, such

as $\mathcal{H}$. In a complex inner product space, it is possible to express the inner product in terms of the norm by means of the *polarisation identity*

$$\langle u|v\rangle = \tfrac{1}{4}\sum_{k=0}^{3}(-i)^k\|u+i^kv\|^2. \tag{3.2.1}$$

The standard inner product in $\mathbb{C}^n$ is $\langle u|v\rangle = \sum_{i=1}^n \bar{u}_i v_i$. The induced norm of this is the Euclidean norm.

In an inner product space a vector $v \in V$ is called a *unit vector* if $\|v\| = 1$, and two vectors $u, v \in V$ are called *orthogonal* if $\langle u|v\rangle = 0$. Given a subset $S \subseteq V$, the *orthogonal complement* $S^\perp = \{u \in V |\, \langle u|v\rangle = 0 \,\forall\, v \in S\}$. This is always a subspace, and in finite dimensions we have $(S^\perp)^\perp = \operatorname{span}_{\mathbb{C}} S$. For any subspace $U \subseteq V$, we can decompose as the direct sum $V = U \oplus U^\perp$, where the direct sum $\oplus$ denotes that $U \cap U^\perp = \{0\}$. The inner product structure allows us to choose a very nice basis for the space.

Definition 3.4 (Orthonormal basis)**.** Let V be an inner product space over $\mathbb{C}$. A basis $\{v_i\}_{i\in I} \subseteq V$ is

- *orthogonal* if $\langle v_i|v_j\rangle = 0$ for all $i \neq j$
- *orthonormal* if it is orthogonal and composed of unit vectors, *i.e.* $\langle v_i|v_j\rangle = \delta_{i,j}$.

Using the Gram-Schmidt orthonormalisation procedure, we can always choose an orthonormal basis for a Hilbert space.

3.2.2 Linear maps

We consider maps between vector spaces.

Definition 3.5 (Linear maps)**.** Let U, V be vector spaces over $\mathbb{F}$. A map $T : U \to V$ is *linear* if, for all $u, v \in U$ and $\alpha, \beta \in \mathbb{F}$, $T(\alpha u + \beta v) = \alpha T(u) + \beta T(v)$. The set of all linear maps $U \to V$ is denoted $\mathcal{L}(U, V)$, and if $U = V$, $\mathcal{L}(U)$, which is called the space of *operators* on U.

For a linear map T, we write $Tu := T(u)$. The *rank-nullity theorem* tells us that $\dim\ker T + \dim\operatorname{im} T = \dim U$. The set of linear maps $\mathcal{L}(U, V)$ is a vector space over $\mathbb{F}$ under addition $(T + S)(u) = Tu + Su$ and scalar multiplication $(\alpha T)(u) = \alpha(Tu)$. Linear maps also satisfy a product under composition: for $T \in \mathcal{L}(U, V)$ and $S \in \mathcal{L}(V, W)$,

their composition $ST = S \circ T \in \mathcal{L}(U, W)$. In $\mathcal{L}(U)$, the *identity operator* is denoted $\mathbb{I}_U$, omitting the subscript when evident; it is the identity under composition, and the set of invertible elements is denoted $\mathcal{GL}(U)$. This is a group under multiplication. The set of linear maps $U \to \mathbb{F}$ is called the *algebraic dual* and denoted $U' = \mathcal{L}(U, \mathbb{F})$.

Definition 3.6. Let V be a finite-dimensional vector space. An operator $T \in \mathcal{L}(V)$ is *diagonalisable* if there exists a basis of *eigenvectors* $\{v_i\}_{i \in I} \subseteq V$ and a set of *eigenvalues* $\lambda_i \in \mathbb{F}$ such that $Tv_i = \lambda_i v_i$.

In finite dimensions, we represent linear maps by matrices. Let $\beta = \{u_i\}_{i \in I}$ be a basis of U and $\gamma = \{v_j\}_{j \in J}$ be a basis of V. The *matrix representation* of $T \in \mathcal{L}(U, V)$ is the matrix $T_{\beta \to \gamma} = (T_{ji})_{j \in J, i \in I}$ where the coefficients are such that $Tu_i = \sum_j T_{ji} v_j$. The composition of linear maps becomes matrix multiplication of their matrix representations. The matrix allows us to define an important functional.

Definition 3.7 (Trace)**.** Let V be a finite-dimensional vector space over $\mathbb{F}$ with basis $\beta = \{v_i\}_{i \in I}$. The *trace* is the map $\mathcal{L}(U) \to \mathbb{F}$ defined as

$$\mathrm{Tr}(T) = \sum_i T_{ii} \tag{3.2.2}$$

The trace is a linear map, so $\mathrm{Tr} \in \mathcal{L}(U)'$. *A priori*, the trace depends on the choice of basis: however, this is not the case, due to the *cyclic property*.

Lemma 3.8 (Cyclic property of the trace)**.** Let $T \in \mathcal{L}(U, V)$ and $S \in \mathcal{L}(V, U)$. Then, $\mathrm{Tr}(ST) = \mathrm{Tr}(TS)$.

Using this property, we see that if M is a change-of-basis matrix $\beta \to \gamma$, the trace in basis β is equal to that in basis γ: $\mathrm{Tr}(MTM^{-1}) = \mathrm{Tr}(M^{-1}MT) = \mathrm{Tr}(T)$.
Proof: Treating the choice of bases implicitly, we have that

$$\mathrm{Tr}(ST) = \sum_i (ST)_{ii} = \sum_{i,j} S_{ij} T_{ji} = \sum_j (TS)_{jj} = \mathrm{Tr}(TS). \tag{3.2.3}$$

■

The norm of a normed vector space induces a norm on the linear maps.

Definition 3.9 (Operator norm)**.** Let U, V be normed vector spaces and $T \in \mathcal{L}(U, V)$. The *operator norm* of T is

$$\|T\| = \sup \{\|Tu\| | u \in U, \|u\| = 1\} . \tag{3.2.4}$$

A linear map $T \in \mathcal{L}(U, V)$ that preserves the norm — $\|Tu\| = \|u\|$ for all $u \in U$ — is called an *isometry*. Every isometry is injective and has operator norm 1, but not every injective and/or norm 1 operator is an isometry. Write the set of isometries $\mathcal{U}(U, V) \subseteq \mathcal{L}(U, V)$.

We note some important properties of the operator norm. First, for $u \in U$ and $T \in \mathcal{L}(U, V)$, $\|Tu\| \leq \|T\|\|u\|$. Similarly, for $T \in \mathcal{L}(U, V)$ and $S \in \mathcal{L}(V, W)$, $\|ST\| \leq \|S\|\|T\|$.

Now, we consider linear maps on inner product spaces.

Definition 3.10 (Adjoint)**.** Let U, V be finite-dimensional inner product spaces and let $T \in \mathcal{L}(U, V)$. The *adjoint* of T is the unique map $T^\dagger \in \mathcal{L}(V, U)$ such that, for all $u \in U$ and $v \in V$,

$$\langle u|T^\dagger v\rangle = \langle Tu|v\rangle . \tag{3.2.5}$$

The adjoint is a conjugate-linear map $\mathcal{L}(U, V) \to \mathcal{L}(V, U)$, and satisfies $(ST)^\dagger = T^\dagger S^\dagger$ and $(T^\dagger)^\dagger = T$. For the matrix representation with respect to orthonormal bases, the adjoint becomes the conjugate transpose $(T^\dagger)_{ji} = \overline{T}_{ij}$.

The adjoint interacts with the operator norm in an important way via the *C^* identity* $\|TT^\dagger\| = \|T\|^2$.

Finally, we can use this to construct an inner product on linear maps, the *Hilbert-Schmidt inner product* $(T, S) \mapsto \mathrm{Tr}(T^\dagger S)$. For a linear map between linear maps Φ, we make use of the adjoint $\Phi^\dagger$ with respect to this inner product.

3.2.2.1 Normal operators

Now, we focus on a class of operators that is well-behaved with respect to the adjoint. Fix V a finite-dimensional inner product space.

Definition 3.11 (Normal, hermitian, and unitary operators)**.** An operator $T \in \mathcal{L}(V)$ is called *normal* if $TT^\dagger = T^\dagger T$. T is called *hermitian* (or *self-adjoint*) if $T = T^\dagger$ and *unitary* if $T^\dagger = T^{-1}$.

Note that both hermitian operators and unitary operators are normal. We write the set of unitary operators $\mathcal{U}(V)$, and see that it is a subgroup of $\mathcal{GL}(V)$.

Lemma 3.12 (Characterisation of unitaries)**.** For an operator $U \in \mathcal{L}(V)$, the following are equivalent:

(i) U is unitary.

(ii) U is an isometry.

(iii) For all $u, v \in V$, $\langle Uu|Uv\rangle = \langle u|v\rangle$.

(iv) U sends orthonormal bases to orthonormal bases.

(v) U sends a fixed orthonormal basis to an orthonormal basis.

Proof: (i)⇒(ii) This is immediate as $\|Uv\|^2 = \langle Uv|Uv\rangle = \langle v|U^\dagger Uv\rangle = \langle v|v\rangle = \|v\|^2$.
(ii)⇒(iii) This follows from the polarisation identity:

$$\langle Uu|Uv\rangle = \tfrac{1}{4}\sum_{k=0}^{3}(-i)^k\|U(u+i^k v)\|^2 = \frac{1}{4}\sum_{k=0}^{3}(-i)^k\|u+i^k v\|^2 = \langle u|v\rangle\,. \tag{3.2.6}$$

(iii)⇒(iv) Direct since inner products are preserved.
(iv)⇒(v) Direct as it is a special case
(v)⇒(i) Let $\{v_i\}_{i\in I}$ be the fixed orthonormal basis. Then, $\{Uv_i\}$ is an orthonormal basis, so $\langle Uv_i|Uv_j\rangle = \delta_{i,j}$. Thus, as any vector can be expressed in the basis, that means $\langle Uu|Uv\rangle = \langle u|U^\dagger Uv\rangle = \langle u|v\rangle$ for all $u, v \in V$. By non-degeneracy of the inner product, we get $U^\dagger U = \mathbb{I}$. As $\mathcal{GL}(V)$ is a group, this means $U^\dagger = U^{-1}$. ■

Next, any operator $T \in \mathcal{L}(H)$ can be written as a linear combination of hermitian operators as $T = \frac{T+T^\dagger}{2} + i\frac{T-T^\dagger}{2i}$. An important class of hermitian operators are the positive operators.

Definition 3.13. An operator $P \in \mathcal{L}(V)$ is *positive (semidefinite)* if, for all $v \in V$, $\langle v|Pv\rangle \geq 0$. We write the set of positive operators $\mathcal{P}(V)$.

We also write $P \geq 0$ to denote $P \in \mathcal{P}(V)$. We see that sums of positive operators are positive, and positive scalar multiples of positive operators are positive. The product of any linear map and its adjoint is positive. Also, positive operators are hermitian: for $P \geq 0$,

we have $\langle v|Pv\rangle = \langle Pv|v\rangle = \langle v|P^\dagger v\rangle$ since it is real, which gives by polarisation identity and nondegeneracy of the inner product that $P = P^\dagger$. Hence, positive operators provide a partial order on the hermitian operators, defined as $S \geq T$ if $S - T \in \mathcal{P}(V)$. Finally, we see that the operator norm $\|T\| \geq T$, and hence T may be written as the difference of positive operators $T = \|T\| - (\|T\| - T)$.

Definition 3.14. A hermitian operator $P \in \mathcal{L}(V)$ is a *projector* if $P^2 = P$.

Because it is hermitian, we see that is also positive. Projectors correspond exactly to linear subspaces of V.

Lemma 3.15. $P \in \mathcal{L}(V)$ is a projector if and only if there exists a subspace $U \subseteq V$ such that P acts as identity on U and as 0 on its orthogonal complement.

This tells also us that any projector is diagonalisable with eigenvalues 1 and/or 0. Note that if P is the projector onto U, $\mathbb{I} - P$ is the projector onto $U^\perp$.

Proof of Lemma 3.15: Let P be a projector. Note that any eigenvalue of P must satisfy $\lambda^2 = \lambda$, so $\lambda = 0$ or $\lambda = 1$. Now, let $U = \{v \in V | Pv = v\}$; this is the 1-eigenspace, and it may be the 0 subspace. Consider $v \in U^\perp$. For any $u \in U$ we have that $\langle u|Pv\rangle = \langle Pu|v\rangle = \langle u|v\rangle = 0$, and so $Pv \in U^\perp$. On the other hand, $P(Pv) = P^2 v = Pv$, and so $Pv \in U$. As $U \cap U^\perp = 0$, we have $Pv = 0$, and so $U^\perp$ is the 0-eigenspace. Thus, U fully characterises P.

On the other hand, consider P the map such that $Pu = u$ for $u \in U$ and $Pw = 0$ for $w \in U^\perp$. As any vector $v \in V$ can be decomposed uniquely as $v = u + w$ for some $u \in U$ and $w \in U^\perp$, it is direct to see that P is in fact a projector. ■

3.2.2.2 Diagonalisation and decomposition

Normal operators are easily diagonalisable.

Theorem 3.16 (Spectral theorem)**.** Let $T \in \mathcal{L}(V)$ be a normal operator. Then, T is diagonalisable with an orthonormal basis of eigenvectors.

We can express the spectral theorem by means of projectors. Let $\Lambda \subseteq \mathbb{C}$ be the set eigenvalues of T and for each $\lambda \in \Lambda$, let P_λ be the projector onto the λ-eigenspace. We can write

$$T = \sum_{\lambda \in \Lambda} \lambda P_\lambda. \tag{3.2.7}$$

An important consequence of the diagonalisation is that the norm of a normal operator is simply the largest among the moduli of its eigenvalues.

Proof of Theorem 3.16: We proceed by induction on the dimension of V. If $\dim V = 1$, then every operator is diagonal so we are done. For $\dim V > 1$, we can pick an eigenvalue λ of T (just by picking a root of the characteristic polynomial). Let P be the projector onto the λ-eigenspace V_λ and write $Q = \mathbb{I} - P$. We decompose

$$T = (P+Q)T(P+Q) = PTP + PTQ + QTP + QTQ. \tag{3.2.8}$$

First, for any $v \in V$, $Pv \in V_\lambda$ and hence $PTPv = \lambda P^2 v = \lambda Pv$, giving $PTP = \lambda P$. Similarly, $QTP = \lambda QP = 0$. To see that $PTQ = 0$ also, we note first that for any $v \in V_\lambda$, $TT^\dagger v = T^\dagger T v = \lambda T^\dagger v$, and so $T^\dagger$ preserves V_λ. Hence, as the image of $T^\dagger P$ is in V_λ, $QT^\dagger P = 0$. Taking the adjoint gives $PTQ = 0$. As such $T = \lambda P + QTQ$. To finish, we want to use the induction hypothesis to diagonalise QTQ, as it is an operator on V_λ, that has dimension strictly smaller than V. It remains to show that QTQ is normal. In fact, knowing that $PTQ = QTP = 0$,

$$QTQ(QTQ)^\dagger = QTQT^\dagger Q = QT(P+Q)T^\dagger Q = QTT^\dagger Q = QT^\dagger TQ = (QTQ)^\dagger QTQ, \tag{3.2.9}$$

which completes the proof. ■

Now, we can deduce some important properties of normal operators.

Corollary 3.17. Let $T, S \in \mathcal{P}(V)$ be commuting ($TS = ST$) normal operators. Then, they are diagonalisable with the same orthonormal basis.

By induction, this extends to any finite number of pairwise commuting operators. When discussing commutation of operators, we often make use of the *commutator* $[T, S] := TS - ST$.

Proof: Let $\Lambda \subseteq \mathbb{C}$ be the set of eigenvalues of T and, for each $\lambda \in \Lambda$, let $V_\lambda \subseteq V$ be the λ-eigenspace. Let $v \in V_\lambda$. Then,

$$TSv = STv = \lambda Sv, \tag{3.2.10}$$

giving that S preserves the eigenspaces of T. Thus, S can be restricted to a map $V_\lambda \to V_\lambda$. As its adjoint can be restricted by projecting onto V_λ, S is normal on V_λ and hence it can

be diagonalised on it. Taking the union of the bases over all $\lambda \in \Lambda$, we have an orthonormal basis on which both T and S are diagonal. ■

Corollary 3.18. Let $T \in \mathcal{L}(V)$.

(i) If T is hermitian, its eigenvalues are real.

(ii) If T is unitary, its eigenvalues have modulus 1.

(iii) If T is positive, its eigenvalues are contained in $[0, \infty)$. T has a unique positive square root $\sqrt{T}$.

Proof:

(i) Let λ be an eigenvalue of T, and let v be an eigenvector. By the spectral decomposition, $\lambda v = Tv = T^\dagger v = \bar{\lambda} v$, giving that λ is real.

(ii) Let λ be an eigenvalue of T with an eigenvector v. Using the spectral decomposition, $v = T^\dagger T v = |\lambda|^2 v$, so $|\lambda| = 1$.

(iii) Since T is positive, every eigenvalue is real. Let λ be an eigenvalue with unit eigenvector v. We have that $0 \leq \langle v|Pv\rangle = \lambda$.

To find the square root, consider the spectral decomposition $T = \sum_\lambda \lambda P_\lambda$. It is direct to see that for $P = \sum_\lambda \sqrt{\lambda} P_\lambda$, P is positive and $P^2 = T$, so P is a positive square root of T. Now, let Q be a positive square root of T. As $QT = Q^3 = TQ$, they are diagonalisable on the same orthonormal basis. Let λ be an eigenvalue of Q with eigenvector v. Then, $Tv = Q^2 v = \lambda^2 v$, giving that every eigenvalue of Q is the square root of an eigenvalue of P with the same eigenspace. As such, $Q = P$ and so the square root is unique.

■

Using the square root, we define the *absolute value* of an operator $T \in \mathcal{L}(V)$, as the positive operator $|T| = \sqrt{T^\dagger T}$.

We end the section with decompositions of general operators.

Theorem 3.19 (Polar decomposition)**.** Let $T \in \mathcal{L}(V)$. There exist a unitary $U \in \mathcal{U}(V)$ and a positive $P \in \mathcal{P}(V)$ such that $T = UP$.

Proof: Let $P = |T|$, and let $\{v_i\}$ be an eigenbasis of P with eigenvalues λ_i. For $\lambda_i \neq 0$, let $u_i = \frac{1}{\lambda_i} T v_i$. Note that the u_i are orthonormal as $\langle u_i | u_j \rangle = \frac{\langle P v_i | P v_j \rangle}{\lambda_i \lambda_j} = \delta_{i,j}$. Now, we can extend the set $\{u_i\}$ to an orthonormal basis, and associate each of the added vectors to an i such that $\lambda_i = 0$. Then, define U as the linear map that sends v_i to u_i. By definition, U is unitary, and $UPv_i = \lambda_i U v_i = \lambda_i u_i = T v_i$, so $T = UP$. ■

Corollary 3.20 (Singular-value decomposition)**.** Let $T \in \mathcal{L}(V, W)$. There exist orthonormal bases $\{v_i\}$ of V and $\{w_i\}$ of W and positive numbers $\lambda_i \in [0, \infty)$ such that $T v_i = \lambda_i w_i$.

Proof: By rank-nullity, we know that $\dim(\ker T)^\perp = \dim \operatorname{im} T$, so T can be seen as an operator on a space of that dimension. Using the polar decomposition, write $T = UP$. Let $\{v_i\}$ be an eigenbasis of P be with eigenvalues λ_i. Then, taking $w_i = U v_i$, $T v_i = \lambda_i U v_i = \lambda_i w_i$. Finally, we extend $\{v_i\}$ to an orthonormal basis of V, take $\lambda_i = 0$ for those additional elements, and then extend $\{w_i\}$ to an orthonormal basis of W. ■

3.2.3 Tensor products

This section follows [Ash02, NC10].

An immensely important construction for quantum theory is the tensor product, that provides, in a sense, a product of vector spaces.

Definition 3.21 (Tensor product)**.** Let U, V be vector spaces over $\mathbb{F}$. The *tensor product* $U \otimes V$ is defined as follows. Let F be the $\mathbb{F}$-vector space with basis $U \times V$, and let $G \subseteq F$ be the subspace spanned by $(u + \alpha w, v) - (u, v) - \alpha(w, v)$ and $(u, v + \alpha x) - (u, v) - \alpha(u, x)$ for all $u, w \in U$, $v, x \in V$, and $\alpha \in \mathbb{F}$. Define $U \otimes V = F/G$. The class of a basic element $(u, v) \in F$ is called a *pure tensor* and written $u \otimes v$.

Note that, in general, the tensor product depends on the choice of field (or ring) with respect to which it is taken, but we need not worry about that because all our tensor products are with respect to $\mathbb{C}$. Every element of the tensor product is a linear combination of the pure tensors. The tensor product is associative in the sense that $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$ and distributes on the direct sum in the sense that $U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W)$, which we often use implicitly. We also have $\mathbb{F} \otimes V \cong V \otimes \mathbb{F} \cong V$. There is also an isomorphism $U \otimes V \cong V \otimes U$, but we don't see the tensor product as commutative, since on $U \otimes U$, a tensor $u \otimes v \neq v \otimes u$.

The tensor product of two inner product spaces $U \otimes V$ can be made into an inner product space by taking the inner product of pure tensors to be $\langle u \otimes v | w \otimes x \rangle := \langle u | w \rangle \langle v | x \rangle$

and extending using the linearity. Hence, if $\{u_i\}_{i\in I} \subseteq U$ and $\{v_j\}_{j\in J} \subseteq V$ are orthonormal bases, $\{u_i \otimes v_j\}_{(i,j)\in I\times J}$ is an orthonormal basis of $U \otimes V$.

Theorem 3.22. Let U, V be finite-dimensional inner product spaces, $U \otimes V \cong \mathcal{L}(U, V)$.

Proof: Let $\{u_i \otimes v_j\}_{(i,j)\in I\times J}$ be an orthonormal basis of $U \otimes V$. Take $\Phi : U \otimes V \to \mathcal{L}(U, V)$ to be the linear map such that $\Phi(u_i \otimes v_j)u = \langle u_i|u\rangle\, v_j$. We need to show $\ker \Phi = 0$ and $\operatorname{im} \Phi = \mathcal{L}(U, V)$. Let $w = \sum_{i,j} c_{ij} u_i \otimes v_j \in \ker \Phi$. Then, $0 = \Phi(w)u_i = \sum_j c_{ij} v_j$ for all i, so all the coefficients $c_{ij} = 0$, giving $w = 0$. Also, let $T \in \mathcal{L}(U, V)$. Consider the matrix representation $T_{\{u_i\}\to\{v_j\}}$ and let $w = \sum_{i,j} T_{ji} u_i \otimes v_j$. Then, $\Phi(w)u_i = \sum_j T_{ji} v_j = Tu_i$, so $T \in \operatorname{im} \Phi$. Thus, Φ is an isomorphism. ■

Note that the isomorphism we consider is not quite the same as the natural isomorphism $U' \otimes V \cong \mathcal{L}(U, V)$, and hence requires a basis-dependent map. However, it makes the Schmidt decomposition below more straightforward.

Proposition 3.23 (Schmidt decomposition)**.** Let U, V be finite-dimensional inner product spaces and let $w \in U \otimes V$. Let $d = \min\{\dim U, \dim V\}$. There exist orthonormal bases $\{u_i\}_{i=1}^{\dim U} \subseteq U$ and $\{v_i\}_{i=1}^{\dim V} \subseteq V$ and $p_i \geq 0$ for $i = 1, \ldots, d$ such that $\sum_i p_i = \langle w|w\rangle$ and

$$w = \sum_{i=1}^{d} \sqrt{p_i} u_i \otimes v_i. \tag{3.2.11}$$

Proof: Consider the isomorphism Φ of the previous theorem. Then, as $\Phi(w) \in \mathcal{L}(U, V)$, we can apply the singular-value decomposition Corollary 3.20 and find orthonormal bases $\{u_i\}_{i=1}^{\dim U} \subseteq U$ and $\{v_i\}_{i=1}^{\dim V} \subseteq V$ and $\lambda_i \geq 0$ such that $\Phi(w)u_i = \lambda_i v_i$. Let $p_i = \lambda_i^2$ and take $w' = \sum_{i=1}^{d} \sqrt{p_i}\bar{u}_i \otimes v_i$, where the complex conjugate is with respect to the basis with respect to which Φ was defined. We see that $\Phi(w')u_i = \lambda_i v_i$, so $\Phi(w) = \Phi(w')$ and hence $w = w'$. ■

We can also consider the tensor product of linear maps.

Definition 3.24. Let $T \in \mathcal{L}(U, W)$ and $S \in \mathcal{L}(V, X)$. The *tensor product of maps* $T \otimes S \in \mathcal{L}(U \otimes V, W \otimes X)$ is the map defined on pure tensors as

$$(T \otimes S)(u \otimes v) = Tu \otimes Sv, \tag{3.2.12}$$

and extended linearly.

The tensor product behaves well with respect to both the operator norm and the trace: $\|T \otimes S\| = \|T\|\|S\|$ (which follows from the diagonalisation of $T^\dagger T \otimes S^\dagger S$) and $\mathrm{Tr}(T \otimes S) = \mathrm{Tr}(T)\,\mathrm{Tr}(S)$. An important tensor product of linear maps is the *partial trace*: $\mathrm{Tr}_V : \mathcal{L}(U) \otimes \mathcal{L}(V) \to \mathcal{L}(U)$ is defined as $\mathrm{id}_U \otimes \mathrm{Tr}$. The partial trace extends directly to any number of tensor factors.

In the matrix representation, the tensor product becomes the *Kronecker product*. For matrices $A = (A_{ij})_{i,j}$ and B, the Kronecker product is the block matrix $A \otimes B = (A_{ij}B)_{i,j}$. Similarly to the tensor product, this is associative but not commutative.

3.3 Group Representations

Throughout this section, let G be a finite group.

3.3.1 Representation theory of finite groups

This section uses [Ser77, Wei03].

First, we introduce the basics of group representation theory.

Definition 3.25. Let V be a finite-dimensional inner product space over $\mathbb{C}$. Then, a *representation* of G is a homomorphism into the invertible operators of V

$$\varrho : G \to \mathcal{GL}(V). \tag{3.3.1}$$

Take two representations $\varrho_i : G \to \mathcal{GL}(V_i)$, $i = 1, 2$. An *intertwining operator* is a linear map $T : V_1 \to V_2$ such that $T\varrho_1(g) = \varrho_2(g)T$ for all $g \in G$. The representations are said to be *equivalent* if there exists an invertible intertwining operator. We often write $d_\varrho := \dim V$.

Remark. Any representation is equivalent to a unitary representation. By changing the inner product on the space to $\langle\phi|\psi\rangle \mapsto \sum_{g\in G} \langle\varrho(g)\phi|\varrho(g)\psi\rangle$, it becomes invariant under the action of G. So, ϱ is equivalent to a $\varrho' : G \to \mathcal{U}(V)$.

Definition 3.26. A representation $\varrho : G \to \mathcal{GL}(V)$ is *irreducible* if the only subspaces of V that are invariant under the action of G are the trivial ones, 0 and V itself.

Write $\mathsf{Irr}(G)$ for a set of representatives of the equivalence classes of the irreducible representations — without loss of generality, we can choose these representations to be unitary. A fundamental result on irreducible representations is Schur's lemma.

Lemma 3.27 (Schur)**.** Let $\varrho_i : G \to \mathcal{GL}(V_i)$, $i = 1, 2$, be irreducible representations.

1. Any non-zero intertwining operator $T : V_1 \to V_2$ is invertible.
2. If $\varrho_1 = \varrho_2$, then every intertwining operator is a constant multiple of the identity.

Proof:

1. Let T be a non-zero intertwining operator and let $v \in \ker T$. Since $T\rho_1(g)v = \rho_2(g)Tv = 0$, $\ker T$ is invariant under the action of G. As $\ker T \neq V_1$ and ρ_1 is irreducible, $\ker T = 0$ so T is injective. Conversely, if $w \in \operatorname{im} T$, then $w = Tv$ for some $v \in V_1$, so $\rho_2(g)w = T\rho_1(g)v \in \operatorname{im} T$, so $\operatorname{im} T$ is invariant under G. As such, as $\operatorname{im} T \neq 0$ and ρ_2 is irreducible, $\operatorname{im} T = V_2$, so T is also surjective.
2. Let $T : V_1 \to V_1$ be an intertwining operator. As it is a linear map, it has an eigenvalue λ. Thus, $T - \lambda\mathbb{I}$ is an intertwining operator. As this has a zero, it must be zero everywhere, giving $T = \lambda\mathbb{I}$.

■

Corollary 3.28. The image of a central element by an irreducible representation is a multiple of identity. Every irreducible representation of an abelian group is one-dimensional.

Proof: Let $g \in \mathcal{Z}(G)$ the centre. Then, the operator $\varrho(g)$ is intertwining, so it is a multiple of identity. For an abelian group, $G = \mathcal{Z}(G)$, so all the elements are multiples of identity. In order that there be no non-trivial subspace invariant under the action on G, the dimension of the representation must be one. ■

Definition 3.29.

- A function $f : G \to \mathbb{C}$ is called a *class function* if it is constant on all the conjugacy classes, *i.e.* $f(hgh^{-1}) = f(g)$ for all $g, h \in G$.
- A *character* of G is a function $\chi : G \to \mathbb{C}$ such that $\chi = \operatorname{Tr} \circ \gamma$ for some representation γ of G.

First, due to the cyclicity of the trace, equivalent representations have the same character. This also tells us that characters are class functions. Next, we show the classic result of representation theory that the characters of the irreducible representations form an orthonormal basis of the space of class functions, under the inner product $\langle f' | f \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f'(g)} f(g)$. Schur's lemma helps us show the orthogonality.

Lemma 3.30 (Orthogonality of characters)**.** Let $\chi, \chi' : G \to \mathbb{C}$ be characters. Then,

$$\sum_{g\in G} \overline{\chi'(g)}\chi(g) = |G|\delta_{\chi',\chi} \tag{3.3.2}$$

Proof: Let χ and χ' be the characters of ϱ and ϱ', respectively, where we may choose the representations to be unitary and that, if $\chi = \chi'$, then $\varrho = \varrho'$. Now, for any linear map $X : V \to V'$, we define $\tilde{X} = \sum_{g\in G} \varrho'(g)^\dagger X \varrho(g)$. By construction, this is an intertwining operator. Consider first the case $\chi \neq \chi'$. Then, by Schur's lemma, $\tilde{X} = 0$. Now, fixing orthonormal bases $\{u_j\}$ of V and $\{v_i\}$ of V', let E^{ij} be the map with matrix representation $E^{ij}_{i'j'} = \delta_{i,i'}\delta_{j,j'}$. We have that

$$0 = \sum_{i,j} \tilde{E}^{ij}_{ij} = \sum_{g\in G}\sum_{i,j,i',j'} (\varrho'(g)^\dagger)_{ii'} E^{ij}_{i'j'} (\varrho(g))_{jj'} = \sum_{g\in G}\sum_{i,j} \overline{\varrho'(g)_{ii}}\varrho(g)_{jj} = \sum_{g\in G} \overline{\chi'(g)}\chi(g). \tag{3.3.3}$$

Now, for the case $\chi = \chi'$, we have that $\tilde{X} = \lambda\mathbb{I}$, where, taking the trace, $\lambda = \frac{|G|}{d_\varrho}\operatorname{Tr}(X)$. Thus, using the same construction,

$$|G| = \sum_{i,j} \tilde{E}^{ij}_{ij} = \sum_{g\in G} \overline{\chi'(g)}\chi(g). \tag{3.3.4}$$

■

To show that the characters also span the class functions, we need the full strength of Maschke's theorem.

Theorem 3.31 (Maschke)**.** Every representation is equivalent to a direct sum of irreducible representations.

Proof: We prove this by showing that any representation that is not irreducible can be written as a direct sum of two nontrivial representations, which can then be continued recursively. If $\varrho : G \to \mathcal{U}(V)$ is reducible, there is a nontrivial subspace U that is closed under the action on G. Let $\Pi : V \to V$ be a projector onto U. Defining $P = \frac{1}{|G|}\sum_{g\in G} \varrho(g)^\dagger \Pi \varrho(g)$, we have that P acts on U as Π, and it is intertwining so $\ker P$ is closed under the action of G. So $V \cong \ker P \oplus \operatorname{im} P = \ker P \oplus U$ is a decomposition of V into representations of smaller dimension. ■

Now, suppose that the irreducible characters do not form a basis. Then there exists a

nonzero class function $f : G \to \mathbb{C}$ that is orthogonal to all of them: $\sum_{g\in G} \overline{f(g)}\chi(g) = 0$. Consider the operator $T = \sum_{g\in G} \overline{f(g)}\varrho(g)$, where ϱ is the irreducible representation for which χ is the character. Because f is a class function, this is intertwining, and hence $T = \lambda\mathbb{I}$. But $\operatorname{Tr} T = 0$, so $T = 0$. By Maschke's theorem, this holds for the character of every representation. Consider the regular representation $\varrho : G \to \mathcal{U}(V)$, where V is spanned by orthonormal e_g for all $g \in G$, defined by $\varrho(g)e_h = e_{gh}$. Then,

$$0 = \sum_{x\in G} \overline{f(g)}\varrho(g)e_1 = \sum_{g\in G} \overline{f(g)}e_g, \tag{3.3.5}$$

so $f = 0$. We see that the irreducible characters form a basis of the class functions.

This allows us to derive a useful relation. Consider the function $f : G \to \mathbb{C}$ defined $f(g) = \delta_{g,1}$, which is a class function as $\{1\}$ is a conjugacy class. It has an expansion in the characters $f = \sum_\chi a_\chi \chi$, and by orthonormality we have $|G|a_\chi = \sum_{g\in G} f(g)\overline{\chi(g)} = \overline{\chi}(1) = d_\chi$. Thus, for $g \in G$, we have $|G|\delta_{g,1} = \sum_{\gamma\in \mathsf{Irr}(G)} d_\gamma \operatorname{Tr}(\gamma(g))$.

3.3.2 Approximate representation theory

We now discuss the theory of approximate representations, which hinges on a result of Gowers and Hatami [GH17].

Definition 3.32. Let V and W be finite-dimensional inner product spaces and let $\psi \in V \otimes W$. For $\varepsilon \geq 0$, an (ε, ψ)-*representation* of G is a map $f : G \to \mathcal{U}(V)$ such that, for every $h \in G$,

$$\frac{1}{|G|}\sum_{g\in G} \|(f(g)f(h) - f(gh))\psi\|^2 \leq \varepsilon^2. \tag{3.3.6}$$

Note that, in the above definition, we implicitly consider $f(g)$ as acting on $V \otimes W$ as $f(g) \otimes \mathbb{I}_W$. The following theorem characterises how close an approximate representation is to a true representation.

Theorem 3.33 (Gowers-Hatami)**.** Let $f : G \to \mathcal{U}(V)$ be a (ε, ψ)-representation, where $\varepsilon \geq 0$ and $\psi \in V \otimes W$. Then, there exists a finite-dimensional inner product space V', an isometry $U : V \to V'$, and a representation $\varrho : G \to \mathcal{U}(V')$ such that, for any $g \in G$,

$$\|(Uf(g) - \varrho(g)U)\psi\| \leq \varepsilon. \tag{3.3.7}$$

Note that the above definition and theorem have a slightly different form from how they were presented in previous work [Vid18, CMMN20].

The proof given here is almost identical to the proof of [Vid18], which uses the notion of the Fourier transform of a function acting on a group. Given a function $f : G \to \mathcal{L}(V)$ for V a $\mathbb{C}$-vector space, the Fourier transform is the map $\hat{f} : \mathsf{Irr}(G) \to \mathcal{L}\big(V \otimes \bigoplus_{\gamma \in \mathsf{Irr}(G)} V_\gamma\big)$ defined as

$$\hat{f}(\gamma) = \frac{1}{|G|} \sum_{g \in G} f(g) \otimes \gamma(g). \tag{3.3.8}$$

It is straightforward to check, using the orthogonality of the characters, that the inverse transform is

$$f(g) = \sum_{\gamma \in \mathsf{Irr}(G)} d_\gamma \operatorname{Tr}_{V_\gamma}\Big((\mathbb{I}_V \otimes \gamma(g)^\dagger)\hat{f}(\gamma)\Big). \tag{3.3.9}$$

Proof of Proof of Theorem 3.33: First, we construct the necessary objects. The dilated space is

$$V' = \bigoplus_{\gamma \in \mathsf{Irr}(G)} V \otimes V_\gamma \otimes V_\gamma, \tag{3.3.10}$$

and the representation is taken to be

$$\varrho(g) = \bigoplus_{\gamma \in \mathsf{Irr}(G)} \mathbb{I} \otimes \mathbb{I}_\gamma \otimes \overline{\gamma(x)}, \tag{3.3.11}$$

where the complex conjugate on V_γ is taken with respect to a fixed basis $\{e_{\gamma,i}\}_{i \in [d_\gamma]}$. Then, we take the isometry to be

$$Uv = \bigoplus_{\gamma \in \mathsf{Irr}(G)} \sqrt{d_\gamma} \sum_{i=1}^{d_\gamma} \hat{f}(\gamma)(v \otimes e_{\gamma,i}) \otimes e_{\gamma,i}. \tag{3.3.12}$$

This is in fact an isometry as

$$\begin{aligned}
\|Uv\|^2 &= \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \sum_{i,j=1}^{d_\gamma} \langle \hat{f}(\gamma)(v\otimes e_{\gamma,i})|\hat{f}(\gamma)(v\otimes e_{\gamma,j})\rangle \ \langle e_{\gamma,i}|e_{\gamma,j}\rangle \\
&= \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \sum_{i=1}^{d_\gamma} \langle \hat{f}(\gamma)(v\otimes e_{\gamma,i})|\hat{f}(\gamma)(v\otimes e_{\gamma,i})\rangle \\
&= \frac{1}{|G|}\sum_{g,h\in G}\sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \sum_{i=1}^{d_\gamma} \langle f(g)v|f(h)v\rangle \ \langle \gamma(g)e_{\gamma,i}|\gamma(h)e_{\gamma,i}\rangle \\
&= \frac{1}{|G|}\sum_{g,h\in G} \langle f(g)v|f(h)v\rangle \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \operatorname{Tr}(\gamma(g^{-1}h)) \\
&= \frac{1}{|G|}\sum_{g,h\in G} \langle f(g)v|f(h)v\rangle \, \delta_{g,h} = \frac{1}{|G|}\sum_{g,h\in G}\|f(g)v\|^2 = \|v\|^2.
\end{aligned} \tag{3.3.13}$$

Thus, with a similarly long equation we may simplify

$$\begin{aligned}
\langle u|U^\dagger \varrho(g) U v\rangle &= \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \sum_{i,j=1}^{d_\gamma} \langle \hat{f}(\gamma)(u\otimes e_{\gamma,i})|\hat{f}(\gamma)(v\otimes e_{\gamma,j})\rangle \ \langle e_{\gamma,i}|\overline{\gamma(g)}e_{\gamma,j}\rangle \\
&= \frac{1}{|G|^2}\sum_{h,h'\in G} \langle f(h)u|f(h')v\rangle \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \sum_{i,j=1}^{d_\gamma} \langle \gamma(h)e_{\gamma,i}|\gamma(h')e_{\gamma,j}\rangle \ \langle e_{\gamma,j}|\gamma(g)^\dagger e_{\gamma,i}\rangle \\
&= \frac{1}{|G|^2}\sum_{h,h'\in G} \langle f(h)u|f(h')v\rangle \sum_{\gamma\in\mathsf{Irr}(G)} d_\gamma \operatorname{Tr}\big(\gamma(h^{-1}h'g^{-1})\big) \\
&= \frac{1}{|G|}\sum_{h,h'\in G} \langle f(h)u|f(h')v\rangle \, \delta_{h',hg} = \frac{1}{|G|}\sum_{h\in G} \langle f(h)u|f(hg)v\rangle \,,
\end{aligned} \tag{3.3.14}$$

which gives $U^\dagger \varrho(g) U = \frac{1}{|G|}\sum_{h\in G} f(h)^\dagger f(hg)$. Noting that

$$\|(f(g)f(h) - f(gh))\psi\|^2 = 2\,\langle\psi|\psi\rangle - 2\,\mathrm{Re}\ \langle\psi|f(h)^\dagger f(g)^\dagger f(gh)\psi\rangle\,, \tag{3.3.15}$$

we can use the above and the hypothesis to get

$$\begin{aligned}\|(Uf(g) - \varrho(g)U)\psi\|^2 &= 2\langle\psi|\psi\rangle - 2\,\mathrm{Re}\,\langle\psi|f(g)^\dagger U^\dagger \varrho(g) U\psi\rangle \\ &= \frac{1}{|G|}\sum_{h\in G}\big(2\langle\psi|\psi\rangle - 2\,\mathrm{Re}\,\langle\psi|f(g)^\dagger f(h)^\dagger f(hg)\psi\rangle\big) \\ &= \frac{1}{|G|}\sum_{h\in G}\|(f(h)f(g) - f(hg))|\psi\rangle\|^2 \leq \varepsilon^2,\end{aligned} \tag{3.3.16}$$

which completes the proof. ■

3.4 Semi-pre-C^*-algebras

In this section, we give a rapid tour of some of the aspects of C^*-algebra theory. Ideas from C^*-algebras are used in this work to phrase rigidity of games as an abstract noncommutative polynomial inequality. We proceed from semi-pre-C^*-algebras, following [Oza13]. We also cite [BO08] as an important resource.

Definition 3.34. A *unital $*$-algebra* is a unital algebra A over $\mathbb{C}$ equipped with an involution $x \mapsto x^*$ such that

- $1^* = 1$
- $(xy)^* = y^*x^*$ for all $x, y \in A$
- $(\lambda x + y)^* = \overline{\lambda}x^* + y^*$ for all $x, y \in A$ and $\lambda \in \mathbb{C}$.

The involution generalises the adjoint of linear maps. It is also possible to define $*$-algebras over $\mathbb{R}$, but we will not do that here. To simplify notation, we do not distinguish between $\mathbb{C}$ and the copy $\mathbb{C}1$ of it in A. For a set $S \subseteq A$, we write $\mathrm{gen}^*_{\mathbb{C}}(S)$ for the $*$-subalgebra generated by S. Finally, we will refer to the $\mathbb{R}$-subspace $A_h = \{x \in A | x = x^*\}$ of *hermitian elements*.

Definition 3.35. Let A be a unital $*$-algebra. A subset $A_+ \subseteq A_h$ is a *$*$-positive cone* if

- $\mathbb{R}_{\geq 0} \subseteq A_+$
- $\lambda a + b \in A_+$ for all $a, b \in A_+$ and $\lambda \geq 0$
- $x^*ax \in A_+$ for all $a \in A_+$ and $x \in A$.

The $*$-positive cone generalises the positive operators on a Hilbert space. In the same way, A_+ induces an order on A_h, where we say $a \geq b$ if $a - b \in A_+$.

There is always a minimal cone composed of the *sums-of-squares*

$$A_+ = \Sigma^2 A := \Big\{ \sum_{i=1}^{n} x_i^* x_i \Big| n \in \mathbb{N}; x_1, \ldots, x_n \in A \Big\}. \tag{3.4.1}$$

Definition 3.36. An element $x \in A$ is called *bounded* if there exists $R \geq 0$ such that $x^*x \leq R$; denote the set of bounded elements A_b. A $*$-algebra A endowed with a $*$-positive cone A_+ is called a *semi-pre-C^*-algebra* if every element is bounded, $A = A_b$.

In a semi-pre-C^*-algebra A, we simply call A_+ the *cone*.

Lemma 3.37. Let A be a $*$-algebra with $*$-positive cone A_+. If $S \subseteq A_b$, then $\mathrm{gen}^*_{\mathbb{C}}(S) \subseteq A_b$.

It follows that A_b is a $*$-subalgebra of A, and that A is a semi-pre-C^* algebra if and only if it has a set of bounded generators.

Proof: We need to show that boundedness is preserved under linear combinations, products, and the involution. Let $\alpha \in \mathbb{C}$ and $x, y \in A$ bounded. There exist $R, S \geq 0$ such that $x^*x \leq R$ and $y^*y \leq S$. First, we get $(\alpha x)^*(\alpha x) = |\alpha|^2 x^*x \leq |\alpha|^2 R$. Next, as $(x-y)^*(x-y) \geq 0$, we have $x^*x + y^*y \geq x^*y + y^*x$ and therefore $(x+y)^*(x+y) \leq 2(x^*x + y^*y) \leq 2(R+S)$. Thus boundedness is preserved under linear combinations. Also, $(xy)^*xy \leq y^*x^*xy \leq y^*Ry \leq RS$, so boundedness is preserved under the product. Finally, $0 \leq (R - xx^*)^2 = R^2 - 2Rxx^* + x(x^*x)x^* \leq R^2 - Rxx^*$, giving $xx^* \leq R$ as well. ■

As noted above, the canonical example of a semi-pre-C^*-algebra is the set of *bounded operators* on a Hilbert space $\mathcal{B}(\mathcal{H})$. The involution is provided by the adjoint and the positive cone is provided by the positive bounded operators. For a finite-dimensional Hilbert space, these are all the operators $\mathcal{L}(\mathcal{H}) = \mathcal{B}(\mathcal{H})$.

Definition 3.38. A *$*$-representation* of a semi-pre-C^*-algebra A is an algebra homomorphism $\pi : A \to \mathcal{B}(\mathcal{H})$, where $\mathcal{H}$ is a Hilbert space, such that $\pi(A_+) \subseteq \mathcal{P}(\mathcal{H})$ and $\pi(x^*) = \pi(x)^\dagger$ for all $x \in A$.

Example 3.39. An important example of a semi-pre-C^*-algebra is the *full group algebra*. Let Γ be a discrete group. The *group algebra* is $\mathbb{C}[\Gamma]$, the set of finitely-supported functions

$\Gamma \to \mathbb{C}$; we express $x \in \mathbb{C}[\Gamma]$ as a linear combination $x = \sum_{g\in\Gamma} x(g)g$. The product on $\mathbb{C}[\Gamma]$ is given by convolutions $xy = \sum_{g,h\in\Gamma} x(g)y(h)gh = \sum_{g\in\Gamma}\big(\sum_{h\in\Gamma} x(h)y(g^{-1}h)\big)g$, and the involution by $g^* = g^{-1}$, which makes this into a $*$-algebra. To get the full group semi-pre-C^*-algebra, we can define the cone to be the sums of squares $\mathbb{C}[\Gamma]_+ = \Sigma^2\mathbb{C}[\Gamma]$. With this cone, every unitary representation of Γ sends positive elements to positive operators. Since the group elements generate $\mathbb{C}[\Gamma]$, it suffices to show that they are bounded, which we see by $g^*g = 1$.

The $*$-representations of the algebra $\mathbb{C}[\Gamma]$ are the unitary representations of the group Γ.

Finally, we give a construction that allows us to construct new algebras.

Definition 3.40. Let A and B be semi-pre-C^*-algebras. The *max-tensor product* is the algebra $A\otimes^{\max} B = A\otimes B$, the algebraic tensor product, with involution $(a\otimes b)^* = a^*\otimes b^*$ and cone generated by the tensors of positive elements

$$(A \otimes^{\max} B)_+ = \left\{\sum_{i=1}^{k} x_i^*(a_i \otimes b_i)x_i \middle| k \in \mathbb{N}; a_i \in A_+, b_i \in B_+; x_i \in A \otimes B\right\}. \tag{3.4.2}$$

For a finite-dimensional Hilbert space $\mathcal{H}$, the algebra $\mathcal{L}(\mathcal{H}) \otimes^{\max} A$ is referred to as the *matrix algebra over* A as the elements can be represented as A-valued matrices. On group algebras, the max-tensor acts as the Cartesian product. For discrete groups Γ and H,

$$\mathbb{C}[\Gamma \times H] \cong \mathbb{C}[\Gamma] \otimes^{\max} \mathbb{C}[H], \tag{3.4.3}$$

which can be directly seen by using the isomorphism $(g, h) \mapsto g \otimes h$.

The algebra we work with will be the matrix algebra over a tensor of group algebras.

3.5 Probability

In this section, we present the standard definitions and results that we use in probability theory. We cite [Rén70] as an important reference.

Definition 3.41. Let X be a set, called the *sample space*, $\mathscr{S} \subseteq \mathscr{P}(X)$ be a set of subsets of X (containing $\varnothing$ and X, and closed under complement and countable unions), called the *event space*. A function $\pi : \mathscr{S} \to [0, 1]$ is called a *probability distribution* on X if

$\pi(X) = 1$ and, for any countable collection of disjoint sets $\Omega_1, \Omega_2, \ldots \in \mathscr{S}$,

$$\pi\Big(\bigcup_{i=1}^{\infty} \Omega_i\Big) = \sum_{i=1}^{\infty} \pi(\Omega_i). \tag{3.5.1}$$

We only consider probability distributions on finite sets, so we do not need the full strength of this definition. In this case, we can take the event space to be the whole of $\mathscr{P}(X)$ and see that $\pi(\Omega) = \sum_{x\in\Omega} \pi(\{x\})$ for any event $\Omega \subseteq X$. As such, we consider any probability distribution on a finite set as a map $\pi : X \to [0, 1]$ satisfying $\sum_{x\in X} \pi(x) = 1$, which is linked to the general definition via $\pi(x) = \pi(\{x\})$.

When the probability distribution is implicit, we often write $\Pr[\Omega] := \pi(\Omega)$ for an event Ω. The *conditional probability* of an event Ω conditioned on an event Ω' is

$$\Pr[\Omega|\Omega'] = \frac{\Pr[\Omega \cap \Omega']}{\Pr[\Omega']}. \tag{3.5.2}$$

This represents the probability that Ω occurs once Ω' has already occurred. Two events Ω and Ω' are *independent* if $\Pr[\Omega \cap \Omega'] = \Pr[\Omega] \Pr[\Omega']$. In that case, the probability of Ω does not change when conditioned on Ω'.

For a function $f : X \to V$, where V is a vector space over $\mathbb{R}$ or $\mathbb{C}$, we write the *expectation value* with respect to π as

$$\mathop{\mathbb{E}}_{x\leftarrow\pi} f(x) = \sum_{x\in X} \pi(x) f(x). \tag{3.5.3}$$

An important probability distribution defined on any finite set is the *uniform distribution*, $\mathfrak{u}_X(x) = \frac{1}{|X|}$. Write the expectation value with respect to $\mathfrak{u}_X$ as $\mathbb{E}_{x\in X}$.

Definition 3.42. A (finite) *random variable* on a set X is a function $\Gamma : A \to X$, where A is the finite sample space of a probability distribution. For $x \in X$, the probability that $\Gamma = x$ is

$$\Pr[\Gamma = x] = \Pr[\{a \in A | \Gamma(a) = x\}]. \tag{3.5.4}$$

For a random variable $\Gamma : A \to X$ and a function $f : X \to Y$, we write $f(\Gamma)$ for the random variable $f \circ \Gamma : A \to Y$. For two random variables, $\Gamma : A \to X$ and $\Delta : A \to Y$, the pair (Γ, Δ) is a random variable $A \to X \times Y$. As such, arbitrary functions of arbitrarily

many random variables on the same (finite) sample space give rise to random variables. When working with random variables, we can avoid reference to the sample space and simply use the probability of the outputs.

If Γ is a random variable on $X \subseteq V$ a vector space, the expectation value of Γ is

$$\mathbb{E}\Gamma = \sum_{x \in X} x \Pr[\Gamma = x]. \tag{3.5.5}$$

Two random variables Γ, Δ on X and Y, respectively, are said to be *independent* if, for any $x \in X$ and $y \in Y$, the probability $\Pr[\Gamma = x \wedge \Delta = y] = \Pr[\Gamma = x] \Pr[\Delta = y]$.

Theorem 3.43 (Markov's inequality)**.** Let Γ be a random variable on $[0, \infty)$. Then, for all $\varepsilon > 0$,

$$\Pr[\Gamma \geq \varepsilon] \leq \frac{\mathbb{E}\Gamma}{\varepsilon}. \tag{3.5.6}$$

Proof: Consider the random variable Δ on $[0, \infty)$ defined as $\Delta = 0$ if $\Gamma < \varepsilon$ and $\Delta = \varepsilon$ if $\Gamma \geq \varepsilon$. Then, $\Delta \leq \Gamma$, so

$$\mathbb{E}\Gamma \geq \mathbb{E}\Delta = \varepsilon \Pr[\Gamma \geq \varepsilon]. \tag{3.5.7}$$

Dividing by ε gives the result. ■

3.5.1 Hoeffding's inequality

Hoeffding's inequality provides an exponential bound on the probability that a sum of independent random variables deviates from its expectation value. We make use of this bound on multiple occasions. The proofs given here are based on the original paper of Hoeffding [Hoe63].

Lemma 3.44 (Hoeffding's lemma)**.** Let Γ be a random variable on $[a, b]$. Then, for any $s > 0$,

$$\mathbb{E}e^{s(\Gamma - \mathbb{E}\Gamma)} \leq e^{\frac{1}{8}s^2(b-a)^2}. \tag{3.5.8}$$

The proof relies on the convexity of the exponential function. A function $f : V \to \mathbb{R}$, where V is a real vector space, is called *convex* if, for all $u, v \in V$ and $p \in [0, 1]$,

$f(pu+(1-p)v) \leq pf(x)+(1-p)f(v)$. By using convexity recursively, we get *Jensen's inequality* $f(\sum_i p_i v_i) \leq \sum_i p_i f(v_i)$ for $v_i \in V$ and $p_i \in [0,1]$ such that $\sum_i p_i = 1$.

Proof: We can replace Γ with $\Gamma - \mathbb{E}\Gamma$, and similarly for the bounds, and hence suppose that $\mathbb{E}\Gamma = 0$. Next, by convexity of the exponential, $e^{sx} \leq \frac{(b-x)e^{sa}+(a-x)e^{sb}}{b-a}$, and so

$$\mathbb{E}e^{s\Gamma} \leq \frac{(b-\mathbb{E}\Gamma)e^{sa}+(\mathbb{E}\Gamma-a)e^{sb}}{b-a} = \frac{be^{sa}-ae^{sb}}{b-a} = e^{f(s(b-a))}, \tag{3.5.9}$$

where $f(x) = \ln\left(\frac{b}{b-a}e^{\frac{a}{b-a}x} - \frac{a}{b-a}e^{\frac{b}{b-a}x}\right)$. Differentiating, we have $f'(x) = \frac{ab}{b-a}\frac{1-e^x}{b-ae^x}$ and $f''(x) = \frac{1}{4\cosh^2((x+\ln(-a/b))/2)}$. Then, using Taylor series, there exists some $t \in \mathbb{R}$ such that $f(x) = f(0)+f'(0)x+f''(t)\frac{x^2}{2}$. Noting that $f(0) = f'(0) = 0$ and $f''(t) \leq \frac{1}{4}$, we get $f(x) \leq \frac{x^2}{8}$. This gives $\mathbb{E}e^{s\Gamma} \leq e^{\frac{1}{8}s^2(b-a)^2}$, as wanted. ■

Theorem 3.45 (Hoeffding's inequality)**.** Let $\Gamma_1, \ldots, \Gamma_n$ be independent random variables on $[0,1]$, and let $\Gamma = \Gamma_1 + \ldots + \Gamma_n$ be their sum. Then, for any $t > 0$

$$\Pr[\Gamma - \mathbb{E}\Gamma \geq t] \leq e^{-\frac{2t^2}{n}}. \tag{3.5.10}$$

Proof: Let $s > 0$. We see that $\Pr[\Gamma - \mathbb{E}\Gamma \geq t] = \Pr\left[e^{s(\Gamma-\mathbb{E}\Gamma)} \geq e^{st}\right]$, because the events are equal. Now, we make use of Markov's inequality (Theorem 3.43) to get

$$\Pr\left[e^{s(\Gamma-\mathbb{E}\Gamma)} \geq e^{st}\right] \leq e^{-st}\mathbb{E}e^{s(\Gamma-\mathbb{E}\Gamma)}. \tag{3.5.11}$$

Since $e^{s(\Gamma-\mathbb{E}\Gamma)} = \prod_{i=1}^n e^{s(\Gamma_i-\mathbb{E}\Gamma_i)}$ and they are independent, the expectation decomposes as the product of the expectations. Now, using the lemma,

$$e^{-st}\mathbb{E}e^{s(\Gamma-\mathbb{E}\Gamma)} = e^{-st}\prod_{i=1}^n \mathbb{E}e^{s(\Gamma_i-\mathbb{E}\Gamma_i)} \leq e^{-st}\prod_{i=1}^n e^{\frac{s^2}{8}} = e^{-st+\frac{n}{8}s^2}. \tag{3.5.12}$$

Minimising this as a function of s gives the optimal value $s = \frac{4t}{n}$, which provides the upper bound $\Pr\left[e^{s(\Gamma-\mathbb{E}\Gamma)} \geq e^{st}\right] \leq e^{-\frac{2t^2}{n}}$. ■

A stumbling block that arises in the usage of Hoeffding's inequality is the need for independence of the random variables. However, if we fix the outputs of a collection of non-independent random variables, we can still make use of Hoeffding's inequality by sampling a uniformly random subset of them as the outputs of new random variables.

Corollary 3.46 (Hoeffding's inequality for sampling)**.** Let $x_1, \ldots, x_N \in [0,1]$. Define the random variables Γ_i on $[0,1]$ for $i \in [n]$ to represent sampling without replacement: let $(\Gamma_1, \ldots, \Gamma_n)$ be the variable on $[0,1]^n$ that samples a random tuple from $\{x_1, \ldots, x_N\}$ of size n. Then, writing $\Gamma = \Gamma_1 + \ldots + \Gamma_n$,

$$\Pr[\Gamma - \mathbb{E}\Gamma \geq t] \leq e^{-\frac{2t^2}{n}}. \tag{3.5.13}$$

Proof: Let Δ_i be the random variables corresponding to sampling with replacement: each outputs a random element of $\{x_1, \ldots, x_N\}$. In particular, they are random variables with support in $[0,1]$, and are independent and identically distributed. Let $\Delta = \Delta_1 + \ldots + \Delta_n$. Hence, we know from the proof of Theorem 3.45 that $\Pr[\Gamma - \mathbb{E}\Gamma \geq t] \leq e^{-st}\mathbb{E}e^{s(\Gamma - \mathbb{E}\Gamma)}$ and $e^{-st}\mathbb{E}e^{s(\Delta - \mathbb{E}\Delta)} \leq e^{-\frac{2t^2}{n}}$. To finish the proof, it suffices to show that $\mathbb{E}e^{s\Gamma} \leq \mathbb{E}e^{s\Delta}$, noting that $\mathbb{E}\Gamma = \mathbb{E}\Delta$ as every x_i belongs to the same number of subsets of size n. To do so, we use the convexity of $f(x) = e^{sx}$. We expand $\mathbb{E}\Gamma = \mathbb{E}_{\{i_1,\ldots,i_n\}\subseteq[N]}(x_{i_1} + \ldots + x_{i_n})$ and

$$\mathbb{E}\Delta = \mathop{\mathbb{E}}_{j_1,\ldots,j_n\in[N]}(x_{j_1} + \ldots + x_{j_n}) = \mathop{\mathbb{E}}_{\{i_1,\ldots,i_n\}\subseteq[N]} \mathop{\mathbb{E}}_{j_1,\ldots,j_n\in\{i_1,\ldots,i_n\}}(x_{j_1} + \ldots + x_{j_n}), \tag{3.5.14}$$

where we can see that $x_{i_1} + \ldots + x_{i_n} = \mathbb{E}_{j_1,\ldots,j_n\in\{i_1,\ldots,i_n\}}(x_{j_1} + \ldots + x_{j_n})$. Hence, using the convexity via Jensen's inequality,

$$f(x_{i_1} + \ldots + x_{i_n}) \leq \mathop{\mathbb{E}}_{j_1,\ldots,j_n\in\{i_1,\ldots,i_n\}} f(x_{j_1} + \ldots + x_{j_n}). \tag{3.5.15}$$

Putting the expectations back gives $\mathbb{E}f(\Gamma) \leq \mathbb{E}f(\Delta)$ as wanted. ■

3.6 Linear Error-Correcting Codes

The theory of error-correcting codes deals with the problem of encoding messages in such a way that they are robust against transmission errors. Most often, messages are represented as bit strings in $\mathbb{Z}_2^n$ and errors are represented as random bit flips. Many different kinds of error-correcting codes exist, and linear codes make up the most developed and accessible family. We make use of linear codes in many of our applications. In this section, we introduce the definitions, notation, and results we need; we refer to [MS77, Pre92].

Definition 3.47. An (n, k)-*code* is a subset $C \subseteq \mathbb{Z}_2^n$ such that $|C| = 2^k$. It is called *linear* if C is a subspace of dimension k, where $\mathbb{Z}_2^n$ is seen as a vector space over the finite field $\mathbb{Z}_2$. It is called an (n, k, d)-*code* if $d = \min_{x,y \in C; x \neq y} d(x, y)$, where $d(x, y)$ is the Hamming distance.

For an (n, k, d)-code C, n is called the *block length*, k is called the *rank*, and d is called the *distance*. Additionally, we call $r := k/n$ the *rate*, and $s := n - k$ the *syndrome size*. The elements of C are called *codewords*.

An (n, k, d)-linear code C encodes message strings of length k as codewords of length n. The encoding procedure is simply a $\mathbb{Z}_2$-linear injection $G : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ with image C, called the *generator matrix*. The decoding procedure may vary, but a canonical choice is to decode a received word $\mathbb{Z}_2^n$ to a closest codeword in Hamming distance, and then act with G^{-1} to give a string in $\mathbb{Z}_2^k$. Note that this closest codeword is not necessarily unique.

Using the linearity, we see that $d = \min_{x \in C \setminus \{0\}} |x|$, the minimal Hamming weight of a codeword.

Theorem 3.48. Let C be an (n, k, d)-code.

(i) It is possible for C to detect that any error of weight at most s has occurred if and only if $s + 1 \leq d$.

(ii) It is possible for C to correct any error of weight at most s if and only if $2s + 1 \leq d$.

Proof:

(i) Suppose $s + 1 \leq d$. The code can detect that an error has occurred if the error cannot distort one code word into another codeword. Let y be the received string. Suppose that it is a codeword. By hypothesis, there is a codeword $x \in C$ such $d(x, y) \leq s < d$. Then two codewords are closer than the minimum distance, which is a contradiction. Hence, y cannot be a codeword and so the error is detected.

Conversely, suppose $s + 1 > d$. Then, as the code distance is d, there are two codewords that are $\leq s$ apart and hence the error may exchange those codewords and be undetectable.

(ii) Suppose $2s + 1 \leq d$. The code can correct an error if the codeword closest to the received string is the original message. Let y be the received word and x be the original message. By hypothesis, $d(x, y) \leq s$. Then, as for any codeword $x' \neq x$,

$d(x, x') \geq d$, $d(x', y) \geq d(x', x) - d(x, y) \geq s + 1 > d(x, y)$. So x is the closest codeword to y, and so the code corrects correctly.

Conversely, suppose $2s + 1 > d$. Let x, x' be code words of distance d. Construct the received word y as follows. Let the first $\lfloor d/2 \rfloor$ bits of y be those of x and the remaining $\lceil d/2 \rceil$ bits be those of x'. As such, y may be received upon sending x but a closest codeword to y is x'.

■

Definition 3.49. Let C be an (n, k, d)-linear code. A linear map $H : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n-k}$ is called a *check matrix* if $\ker H = C$. In that case, for $x \in \mathbb{Z}_2^n$, Hx is called the *syndrome* of x.

The syndrome gives information about the error that has occurred without divulging much information about the actual message.

There is a systematic, if inefficient, way to decode a received string, using the *standard array*. To do so, we consider the quotient space $\mathbb{Z}_2^n/C$. For any coset $y + C$, we choose a representative $\bar{y} \in y + C$ such that $|\bar{y}| = \min_{x \in C} |y + x|$. This representative is not necessarily unique, so it must be fixed for each coset. Then, to correct a received string y, it suffices to output the preimage of the codeword $\bar{y} + y \in C$. This is in fact a codeword with minimal distance to y.

Proposition 3.50. Let $y \in \mathbb{Z}_2^n$ and $x \in C$. Then, $d(y, x) \geq d(y, \bar{y} + y)$.

Proof: First, note that $d(y, \bar{y} + y) = |\bar{y}|$, the weight of the representative. As $y + x \in y + C$, we also have that $d(y, x) = |y + x| \geq |\bar{y}| = d(y, \bar{y} + y)$, as the representative is minimal. ■

The syndrome Hy uniquely determines the coset representative of y as the check matrix induces an isomorphism $\mathbb{Z}_2^n/C \cong \mathbb{Z}_2^{n-k}$.

3.6.1 Code bounds

In this section, we present upper and lower bounds on the rates, or dually on the relative syndrome sizes, which gives an idea of the strengths and limitations of possible codes.

We write the *ball of radius* m in $\mathbb{Z}_2^n$ as $B(n, m) = \{y \in \mathbb{Z}_2^n | |y| \leq m\}$. The ball around $x \in \mathbb{Z}_2^n$ is expressed $x + B(n, m)$.

First, we give an upper bound on the rate as a function of distance that is satisfied by any code.

Theorem 3.51 (Hamming bound)**.** Let C be an (n, k, d)-code. Then $k \leq n - \lg |B(n, \frac{d-1}{2})|$.

In particular, this tells us that the length of the syndrome of any linear code must be at least $\left\lceil \lg |B(n, \frac{d-1}{2})| \right\rceil$ bits.

Proof: Since the code distance is d, Theorem 3.48 tells us that the balls of radius $\frac{d-1}{2}$ around each codeword must be disjoint. Then, as there are 2^k codewords, this provides $2^k |B(n, \frac{d-1}{2})|$ distinct elements in $\mathbb{Z}_2^n$. As such, we know that $2^n \geq 2^k |B(n, \frac{d-1}{2})|$. Taking the logarithm gives the result. ■

However, the Hamming bound is almost never tight. Nonetheless, we can show that there exist codes that attain a related bound.

Theorem 3.52 (Gilbert-Varshamov bound)**.** For all $n, d \in \mathbb{N}$, there exists an (n, k, d)-code such that $k \geq n - \lg |B(n, d-1)|$.

Proof: Let $C \subseteq \mathbb{Z}_2^n$ be a code with distance d. We may suppose it is maximal in the sense that, for every string x, there exists a codeword y such that $d(x, y) < d$. Else, we could add the string that is d or further from the code without changing the distance. Hence, we see that the balls of radius $d-1$ around the elements of the maximal code cover $\mathbb{Z}_2^n$. So, the size $|\mathbb{Z}_2^n| \leq 2^k |B(n, d-1)|$. Taking the logarithm gives the wanted bound. ■

We note also that the Gilbert-Varshamov bound is attained by linear codes.

Proposition 3.53 (Linear Gilbert-Varshamov)**.** Let C be an (n, k, d)-linear code. If the rank $k < n - \lg |B(n, d-1)|$, there exists an $(n, k+1, d)$-linear code $C' \supset C$.

Proof: By hypothesis, there exists $x \in \mathbb{Z}_2^n$ such that $d(x, y) \geq d$ for all $y \in C$. Consider $C' = \mathbb{Z}_2 x + C$. By construction, this is a linear code that contains C strictly. It remains to show that the distance remains d. For $u \in C' \backslash \{0\}$, we have $u = y$ or $u = x + y$ for some $y \in C$. In the former case $|u| \geq d$ since this is the distance of C and in the latter case $|u| = d(x, y) \geq d$ by construction. ■

In the asymptotic limit $n \to \infty$, these bounds can be represented in a particularly simple way. We do so by bounding the volume of the Hamming ball.

Definition 3.54 (Binary entropy function)**.** The *binary entropy function* is the function $h : [0, 1] \to [0, 1]$ defined as $h(\gamma) = -\gamma \lg \gamma - (1 - \gamma) \lg(1 - \gamma)$.

Lemma 3.55. Let $n \in \mathbb{N}$ and $0 \leq \delta \leq \frac{1}{2}$. Then,

$$|B(n, \delta n)| \leq 2^{nh(\delta)}. \tag{3.6.1}$$

Further, $\lim_{n\to\infty} \frac{\lg |B(n,\delta n)|}{n} = h(\delta)$.

Proof: First, for any $m \leq n$, the number of strings of weight m is $\binom{n}{m}$. Thus, the size of the ball $|B(n,\delta n)| = \sum_{m=0}^{\lfloor \delta n \rfloor} \binom{n}{m}$.

$$\begin{aligned} 1 = (\delta + (1-\delta))^n &= \sum_{m=1}^{n} \binom{n}{m} \delta^m (1-\delta)^{n-m} \\ &\geq \sum_{m=1}^{\lceil \delta n \rceil} \binom{n}{m} \delta^m (1-\delta)^{n-m} \geq \sum_{m=1}^{\lceil \delta n \rceil} \binom{n}{m} (1-\delta)^n \left(\tfrac{\delta}{1-\delta}\right)^{\delta n}. \end{aligned} \tag{3.6.2}$$

Then, $|B(n,\delta n)| \leq \delta^{-\delta n}(1-\delta)^{-(1-\delta)n} = 2^{nh(\delta)}$.

For the second part, we show that a lower bound on $\frac{\lg |B(n,\delta n)|}{n}$ tends to $h(\delta)$, as the upper bound does. First, $|B(n,\delta n)| \geq \binom{n}{\lfloor \delta n \rfloor}$. We use a simple form of Stirling's approximation $\ln(n!) \in n\ln n - n + o(n)$ to see that, writing $\delta_n = \frac{\lfloor \delta n \rfloor}{n}$,

$$\begin{aligned} \ln \binom{n}{\lfloor \delta n \rfloor} &= \ln(n!) - \ln(\lfloor \delta n \rfloor !) - \ln((n - \lfloor \delta n \rfloor)!) \\ &\in n\ln n - n - \delta_n n \ln(\delta_n n) + \delta_n n - (1-\delta_n)n \ln((1-\delta_n)n) + (1-\delta_n)n + o(n) \\ &= (\ln 2) h(\delta_n) n + o(n). \end{aligned} \tag{3.6.3}$$

Therefore, as $\delta_n \to \delta$, $\frac{\lg |B(n,m)|}{n} \geq \frac{\lg \binom{n}{\lfloor \delta n \rfloor}}{n} \to h(\gamma)$. ■

Corollary 3.56. For any $0 \leq \delta \leq \frac{1}{2}$ and $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$,

- Every $(n, k, \lfloor \delta n \rfloor)$-linear code satisfies $\frac{s}{n} \geq h(\frac{\delta}{2}) - \varepsilon$
- There exists an $(n, k, \lfloor \delta n \rfloor)$-linear code such that such that

$$h(\tfrac{\delta}{2}) - \varepsilon \leq \tfrac{s}{n} \leq h(\delta), \tag{3.6.4}$$

where $\frac{s}{n} = 1 - \frac{k}{n}$ is the relative syndrome length.

This follows directly by using the asymptotic expression of the volume of the Hamming ball in the Hamming and Gilbert-Varshamov bounds.

Chapter 4

Quantum Theory

In this chapter, we introduce and provide some justification for the postulates of quantum mechanics, and discuss the implications thereof to physical reality, notably entanglement. After, we introduce the theory of quantum information, which arises from this.

4.1 Quantum Mechanics

4.1.1 Origins

In this section, we give a very terse historical introduction to quantum mechanics that omits most of the major players and developments, but should be sufficient to motivate the axiomatisation of the following section. We cite [BJ00] as a major resource.

At the end of the nineteenth century, classical physics was able to give a complete description of the world. Except for all the problems. Notably, in what is known as the ultraviolet catastrophe, blackbody radiation was theoretically expected to increase without bound at low wavelengths, which neither matched experiments nor was physically possible. In 1900, Planck gave the first derivation of the observed spectrum by assuming that light energy was only available in discrete *quanta*, integer multiples of $E = hf = \hbar\omega$ [Pla01]. Einstein [Ein05] later used those same quanta to explain the photoelectric effect; and Bohr [Boh13] noted a similar quantisation of electron energy would explain the atomic spectrum of hydrogen. Energy quantisation of matter as a function of frequency was confirmed experimentally by Franck and Hertz [FH14], and by the electron diffraction experiment of Davisson and Germer [DG28]. These results seemed to indicate that both light and matter had properties of both waves and particles.

De Broglie [de 23] noted that, since energy and frequency are the time components of the special relativistic momentum and wavenumber four-vectors, respectively, the momentum of a massive particle should quantise in the same way as the energy does, giving the de Broglie relations $E = \hbar\omega$ and $\mathbf{p} = \hbar\mathbf{k}$ expressing the wave-particle duality. With this in mind, Schrödinger [Sch26] attempted to find a wave equation for a particle. He did so by combining the classical nonrelativistic Hamiltonian equation for a single particle with energy E in a potential V, $H = \frac{p^2}{2m} + V = E$, with the basic form of a plane wave $\psi = e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)}$. To extract the momentum from this wave, we can act by the operator $-i\hbar\nabla\psi = \mathbf{p}\psi$ and to extract the energy, we can act $i\hbar\partial_t\psi = E\psi$. Using these momentum and energy operators, the Hamiltonian equation can be made into the Schrödinger equation $-\frac{\hbar^2}{2m}\nabla^2\psi + V\psi = i\hbar\partial_t\psi$. Note that this a linear partial differential equation, similarly to the wave equation. In free space, as originally proposed, we have $V = 0$ so plane waves — particles with definite momentum but indefinite position — are in fact solutions of this equation. The Schrödinger equation was first accepted as it is able to more accurately predict hydrogen spectra than Bohr's model. In general, the solution is called the *wavefunction* and describes the state of a single quantum particle.

4.1.2 Postulates of quantum mechanics

Though quantum mechanics was originally formulated to describe experiments whose results clashed with classical physics, it can be equivalently thought of as an axiomatised mathematical framework. The axioms of the theory take the form of a collection of *postulates*. In this way, we can describe quantum systems very generally and avoid reference to a particular physical representation. In this section, we introduce a formulation of the postulates similar to that of Nielsen and Chuang [NC10] that is well-adapted to quantum information and cryptography, and justify them at a high level using the discussion of the previous section.

4.1.2.1 Postulate 1: State

Postulate 1. The state of an isolated quantum system is fully described by a unit vector in a complex Hilbert space $\mathcal{H}$.

This postulate is composed of two important parts. First, the description of a quantum system as a Hilbert space relies on the principle of *superposition*. Because the Schrödinger equation is linear, any complex linear combination of wavefunctions $\alpha\psi + \beta\phi$ remains

a solution of the equation. Hence, the solution space of the Schrödinger equation is a subspace of the vector space of functions $\mathbb{R}^3 \to \mathbb{C}$. This vector space may be endowed with a norm. We can again rely on the Schrödinger equation to provide a candidate: the equation implies a continuity equation $\partial_t \rho + \nabla \cdot \mathbf{j} = 0$, where $\rho = |\psi|^2$ is interpreted as a density and $\mathbf{j} = -\frac{i\hbar}{2m}(\bar{\psi}\nabla\psi - \psi\nabla\bar{\psi})$ as a current. Using this, the total "mass" of the wavefunction can be used to define the norm $\|\psi\|^2 = \int_{\mathbb{R}^3} |\psi(x)|^2 dx$. This interpretation indicates that the wavefuctions should have finite norm (else we would have problems such as infinite energy) and hence the solution space is a normed vector space. This norm arises from an inner product $\langle\phi|\psi\rangle = \int_{\mathbb{R}^3} \bar{\phi}(x)\psi(x)dx$ so the solution space is an inner product space. Finally, we assume that this vector space is complete, so it is the Hilbert space $L^2(\mathbb{R}^3)$. Note that this means a general element of the space is a class of functions equal almost everywhere, and only on a dense subset is the Hamiltonian operator defined. However, these concerns are never a problem in finite dimensions. Generalising, this tells us that a quantum system's state should be a point in some Hilbert space $\mathcal{H}$.

Next, it follows directly by using the Schrödinger equation that a wavefunction's norm is constant, *i.e.* $\partial_t \langle\psi|\psi\rangle = 0$. As such, we may normalise and assume that the norm of any wavefunction is 1. This also gives rises to the *probabilistic interpretation* of quantum mechanics: the density $|\psi|^2$ can now be seen as a probability density where the measure of a set $E \subseteq \mathbb{R}^3$, $\int_E |\psi(x)|^2 dx$, is the probability of measuring the particle at a point in E. Thus, quantum systems also satisfy conservation of probability.

As is customary in quantum theory, we use Dirac bra-ket notation for vectors in the Hilbert space of a quantum system. A vector in $\mathcal{H}$ is denoted by a *ket* $|\psi\rangle \in \mathcal{H}$. The symbol (or symbols) such as ψ inside the ket identifies it and the $|\cdot\rangle$ denotes that it is a ket and serves as brackets in the case of multiple symbols. A functional in the dual $\mathcal{H}^* \cong \mathcal{H}$ is denoted by a *bra* $\langle\phi| \in \mathcal{H}^*$. Every ket $|\phi\rangle$ corresponds to a unique bra $\langle\phi|$ such that $\langle\phi|(|\psi\rangle) = \langle\phi|\psi\rangle$, the inner product on $\mathcal{H}$ which is called the *braket*. Finally, for kets $|\psi\rangle \in \mathcal{H}$, $|\phi\rangle \in \mathcal{K}$ we define the *ketbra* $|\phi\rangle\langle\psi| \in \mathcal{L}(\mathcal{H}, \mathcal{K})$ as the map $|\phi\rangle\langle\psi|\,(|\chi\rangle) = \langle\psi|\chi\rangle\,|\phi\rangle$. For finite-dimensional Hilbert spaces, $\mathcal{L}(\mathcal{H}, \mathcal{K})$ is the span of its ketbras; in infinite dimensions, the bounded operators are the closure of the span of the ketbras in the strong topology. Finally, the action of an operator $A \in \mathcal{L}(\mathcal{H}, \mathcal{K})$ is written as $A|\psi\rangle \in \mathcal{K}$, which is expressed as $\langle\phi|A|\psi\rangle = \langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle$ in the braket.

4.1.2.2 Postulate 2: Evolution

Postulate 2. The time evolution of an isolated quantum system is a unitary linear operator: $|\psi(t)\rangle = U(t)|\psi(0)\rangle$.

Write $U(t) : \mathcal{H} \to \mathcal{H}$ to be the time-evolution operator. First, the state evolves as $U(t)(\alpha|\psi(0)\rangle+\beta|\phi(0)\rangle) = \alpha|\psi(t)\rangle+\beta|\phi(t)\rangle = \alpha U(t)|\psi(0)\rangle+\beta U(t)|\phi(0)\rangle$, by linearity of the Schrödinger equation. So, time evolution is linear. Also, by conservation of probability, we immediately have $\langle\psi(0)|\psi(0)\rangle = \langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|U(t)^\dagger U(t)|\psi(0)\rangle$. Because time evolution in an isolated system is reversible, this implies that $U(t)^\dagger = U(t)^{-1}$, and so it is unitary.

More generally, any transformation of an isolated quantum system is described by a unitary.

4.1.2.3 Postulate 3: Measurement

Postulate 3. A measurement on a quantum system $\mathcal{H}$ with possible outcomes in a set I may be described by a function $M : I \to \mathcal{L}(\mathcal{H}, \mathcal{K})$ called a *generalised measurement* which, writing $M_i := M(i)$, satisfies $\sum_{i\in I} M_i^\dagger M_i = \mathbb{I}_\mathcal{H}$. The probability of measuring outcome i on state $|\psi\rangle$ is given by $\langle\psi|M_i^\dagger M_i|\psi\rangle = \|M_i|\psi\rangle\|^2$; and the post-measurement state conditioned on measuring i is $\frac{M_i|\psi\rangle}{\|M_i|\psi\rangle\|}$.

This notion of measurement arises as a generalisation of the quantisation of energy in quantum mechanics. This is the foundational observation that, for a bound quantum particle, such as the electron in a hydrogen atom, the energy can only take discrete values. Quantisation arises from the Schrödinger equation in that the solution space is spanned by the eigenstates of the Hamiltonian, for which time evolution simply varies the global phase. However, the postulate that the measurement changes the state discontinuously in what is infamously known as a "collapse of the wavefunction" is a significant point of contention in the interpretation of quantum mechanics. The way we formulate the postulate aligns with the *Copenhagen interpretation* of quantum mechanics originated by Bohr, which sees measurement results as the only physically-relevant knowledge available about a quantum system.

In the energy measurement example, this means that for a measured energy E, the state becomes an E-eigenstate of the Hamiltonian with probability $\langle\psi|\Pi_E|\psi\rangle$, where Π_E is the projector onto the E-eigenspace. This expression for the probability of measurement

is known as the *Born rule* after its discoverer, who first saw it to be the only possible interpretation of the solution to a scattering [Bor26]. Gleason's theorem [Gle57] puts this on a stronger mathematical footing by showing that, assuming that measurement probability depends only on the measurement projector (noncontextuality), Born's rule is the only way to assign probabilities to a measurement, in spaces of dimension greater than two.

Different interpretations of quantum mechanics handle the collapse of the wavefunction to a post-measurement state differently. From a Bayesian point of view, the wavefunction is taken to be the knowledge an observer has about the system, and as a measurement increases the knowledge, it follows that it should restrain the states of the system. As is noted later in the preliminaries, from an information-theoretic perspective, the act of measuring can be seen as a unitary operation on a larger quantum system — one that also takes into account the measurer's space. That is, wavefunction collapse becomes a consequence of a usual unitary operation on a non-closed system.

Finally, we mention what the measurement postulate indicates about phase. For any $\zeta \in \mathbb{C}$ with $|\zeta| = 1$, the measurement probability $\|M_i(\zeta|\psi\rangle)\|^2 = \|M_i|\psi\rangle\|^2$, that is that the measurement probability does not depend on the *global phase* of a state. In the Copenhagen interpretation, this tells us that the global phase of a state is not a physically relevant quantity as it cannot be measured. Formally, we can say that the space of quantum states is in fact the projective space $\mathcal{H}/\mathbb{C}^\times$, however it is usually easier to work with simply $\mathcal{H}$ due to the linearity. Nonetheless, the *relative phases* of different terms in a superposition are physically relevant since they affect measurements.

4.1.2.4 Postulate 4: Composition

Postulate 4. The joint state of two quantum systems $\mathcal{H}$ and $\mathcal{K}$ is described by the unit vectors in the tensor product Hilbert space given by the completion of $\mathcal{H} \otimes \mathcal{K}$.

Suppose a system $\mathcal{H}$ is in state $|\psi\rangle$ and a system $\mathcal{K}$ is in state $|\phi\rangle$. It is absolutely untenable to require that these states be considered separately. Naively, we can consider the state of the joint system as the pair $(|\psi\rangle, |\phi\rangle)$. However, first, we need to allow for the principle of superposition: that is, it must be possible to superpose these pairs as $\alpha(|\psi_1\rangle, |\phi_1\rangle) + \beta(|\psi_2\rangle, |\phi_2\rangle)$. Due to superpositions on only one of the systems, the two-system superposition must satisfy $\alpha(|\psi_1\rangle, |\phi\rangle) + \beta(|\psi_2\rangle, |\phi\rangle) = (\alpha|\psi_1\rangle + \beta|\psi_2\rangle, |\phi\rangle)$ and $\alpha(|\psi\rangle, |\phi_1\rangle) + \beta(|\psi\rangle, |\phi_2\rangle) = (|\psi\rangle, \alpha|\phi_1\rangle + \beta|\phi_2\rangle)$. The space generated by the addition given by superposition, modulo the above relations, is exactly the tensor product $\mathcal{H} \otimes \mathcal{K}$. The elements are linear combinations of the pure tensors $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle$. The

inner product on the tensor product space extends the inner products on each of the factors as $(\langle\psi_1| \otimes \langle\phi_1|)(|\psi_2\rangle \otimes |\phi_2\rangle) = \langle\psi_1|\psi_2\rangle\langle\phi_1|\phi_2\rangle$, which extends linearly to a unique inner product. For infinite-dimensional Hilbert spaces, the tensor product space is no longer complete, so the associated Hilbert space of this system is the completion in the topology generated by the inner product.

4.1.3 Entanglement, communication, and no-cloning

One of the most striking consequences of the formulation of quantum mechanics is *entanglement*: the property that superpositions of states in multipartite Hilbert spaces give rise to stronger-than-classical correlations between systems.

Definition 4.1 (Separability and entanglement)**.** A state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ is called *separable* if it can be expressed as $|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle$ for states $|\psi\rangle \in \mathcal{H}$ and $|\phi\rangle \in \mathcal{K}$. Else, the state is called *entangled*.

This feature was first noted by Einstein, Podolsky and Rosen [EPR35], who saw it as flaw in the theory as it meant that there are physical systems that do not admit local descriptions. Rather, they advocated that there must be local "hidden variables" that underlie any quantum system and allow a local description of the system. Bell [Bel64] developped a way to test for the existence of these hidden variables, a *Bell inequality*, a bound on the probability of measuring certain outcomes of measurements on a joint system assuming the existence of hidden variables. Thus, in order to disprove any hidden variable theory, it suffices to violate a Bell inequality by undertaking an experiment where the measurements succeed with higher-than-prescribed probability. This challenge was first succeeded by Aspect *et al.* [ADR82] and since greatly improved. As such, quantum theory must be *nonlocal* and hence allow for all the classically-unexpected consequences of entanglement. We give an important example.

Definition 4.2 (EPR state [EPR35])**.** Let $\mathcal{H} = \mathrm{span}_{\mathbb{C}}\{|0\rangle, |1\rangle\}$. The *EPR state* is the quantum state $|\mathrm{EPR}\rangle \in \mathcal{H} \otimes \mathcal{H}$ defined as

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{4.1.1}$$

It is direct to verify that for any unitary $U \in \mathcal{U}(\mathcal{H})$, $(U \otimes \overline{U})|\mathrm{EPR}\rangle = |\mathrm{EPR}\rangle$, and therefore for *any* a measurement in any basis made on the first system, there is a measurement on the second system that accurately predicts the result. This was originally seen as

a significant problem as it would seem as though this property might permit instantaneous communication, contradicting the light-speed limit of communication set by special relativity. However, this is not the case, as we highlight with the following simple thought experiment, or game. The game, which we call the *no-signalling game*, is played by two cooperating players, Alice and Bob, against a referee and proceeds as follows.

1. Alice and Bob agree on a strategy, consisting of respective quantum systems $\mathcal{H}_A$ and $\mathcal{H}_B$, generalised measurements $M^y : I \to \mathcal{P}(\mathcal{H}_A)$ and $N : \{0,1\} \to \mathcal{P}(\mathcal{H}_B)$, and a shared quantum state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. Then, they are separated and may no longer communicate.

2. The referee provides Alice with a bit $y \in \{0,1\}$ sampled uniformly at random, and she does an arbitrary action on her system, represented by her measurement M^y.

3. Bob attempts to guess y, represented by his measurement N.

4. Alice and Bob win if Bob guesses y correctly.

If the players are able to win with probability any higher than $\frac{1}{2}$, which is attained by Bob randomly guessing, then the state is allowing them to communicate information without sending a signal and using only entanglement. Otherwise, entanglement by itself does not permit communication.

Proposition 4.3. For any strategy the probability of winning the no-signalling game is $\frac{1}{2}$.

Proof: Fix a strategy and let p be the winning probability. Then, collecting the events that allow the players to win

$$p = \frac{1}{2} \sum_{y=0,1} \langle\psi| \sum_{i \in I} (M_i^y)^\dagger M_i^y \otimes N_y^\dagger N_y |\psi\rangle = \frac{1}{2} \sum_{y=0,1} \langle\psi| \mathbb{I}_A \otimes N_y^\dagger N_y |\psi\rangle = \frac{1}{2}. \tag{4.1.2}$$

■

Nonetheless, there have been attempts to show that entanglement permits communication. Most important and believable among these is the *FLASH* scheme of Herbert [Her82], and the search for its flaw was foundational in the development of quantum information. Though it was evident that it contradicted fundamental physics, it was accepted for publication as, at first, the actual source of the error was unable to be found [Per03]. The scheme attempts to make use of the strong correlation property of the EPR state, in the same context as the no-signalling game above. To send a bit y, Alice makes a measurement in one

of two bases. Then, Bob uses the fact that his register contains all the information about Alice's measurement result to retrieve her measurement setting. However, he cannot do this with one measurement. Instead, Herbert proposes to have Bob make multiple *copies* of his local state, measure half of the copies in one of the measurement bases and the other half in the other, and deduce Alice's original bit by seeing which measurement always gives the same result. It is here that the problem lies: quantum states are not in fact able to be copied, or *cloned*. Soon after the FLASH scheme was proposed, this property was shown by Dieks [Die82] and separately by Wooters and Zurek [WZ82]. In hindsight, it was later seen that the no-cloning property had already been studied implicitly by Park [Par70]. This is in opposition with classical information, for which cloning is easy — reading a classical string does not disturb it, and therefore a copy of it can be made. We give a proof of the *no-cloning theorem*, following [NC10].

Theorem 4.4 (No-cloning)**.** Let $\mathcal{H} = \mathrm{span}_{\mathbb{C}}\{|0\rangle, |1\rangle\}$ and let $\mathcal{K}$ be an arbitrary Hilbert space. For any collection of states $|\mathrm{in}\rangle, |\mathrm{out}_\psi\rangle \in \mathcal{K}$ for all $|\psi\rangle \in \mathcal{H}$, there does not exist a unitary $U \in \mathcal{U}(\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{K})$ such that

$$U(|\psi\rangle|0\rangle|\mathrm{in}\rangle) = |\psi\rangle|\psi\rangle|\mathrm{out}_\psi\rangle \tag{4.1.3}$$

for all $|\psi\rangle \in \mathcal{H}$.

For generality, we include an auxiliary register $\mathcal{K}$ that could be modified, even as a function of the input state, by the cloning operation. Note also that, although this theorem only explicitly gives no-cloning in a two-dimensional Hilbert space, it extends directly to any higher dimension as it holds on any two-dimensional subspace.

Proof: Suppose that a cloning unitary U exists. We look for a contradiction. By hypothesis, we have that $U(|0\rangle|0\rangle|\mathrm{in}\rangle) = |0\rangle|0\rangle|\mathrm{out}_0\rangle$ and $U(|1\rangle|0\rangle|\mathrm{in}\rangle) = |1\rangle|1\rangle|\mathrm{out}_1\rangle$. Consider cloning of the state $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. On one hand, again by hypothesis, we must have $U(|+\rangle|0\rangle|\mathrm{in}\rangle) = |+\rangle|+\rangle|\mathrm{out}_+\rangle$. On the other hand, by linearity of U, we must have

$$\begin{aligned} U(|+\rangle|0\rangle|\mathrm{in}\rangle) &= \tfrac{1}{\sqrt{2}}(U(|0\rangle|0\rangle|\mathrm{in}\rangle) + U(|1\rangle|0\rangle|\mathrm{in}\rangle)) \\ &= \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle|\mathrm{out}_0\rangle + |1\rangle|1\rangle|\mathrm{out}_1\rangle), \end{aligned} \tag{4.1.4}$$

so $|+\rangle|+\rangle|\mathrm{out}_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|\mathrm{out}_0\rangle + |1\rangle|1\rangle|\mathrm{out}_1\rangle)$. Acting with $\langle 0| \otimes \langle 1| \otimes \mathbb{I}_{\mathcal{K}}$ on either side gives $\frac{1}{2}|\mathrm{out}_+\rangle = 0$, which contradicts the unitarity of U. ■

The proof of the no-cloning theorem also helps show that the uncloneability of quantum information does not contradict the cloneability of classical information. The contradiction was only attained by considering states that are not in the same basis; since classical information corresponds to a fixed basis, the no-cloning theorem nevertheless permits it to be copied.

4.2 Quantum Information

In this section, we formally introduce the ideas and notation peculiar to quantum information theory, following [NC10, Wat18].

4.2.1 States, Measurements, and Channels

4.2.1.1 Registers and their states

A physical device can be used to store information by assigning values to the various physical states of the system. The concept of a register is a mathematical abstraction meant to represent such a physical device.

Definition 4.5. A *register* is a non-empty finite set X. The elements $x \in X$ are called the *classical states* of X.

We use uppercase Latin letters to represent registers and the corresponding lowercase letters to represent their states.

It is important to note that, although two registers might have the same underlying set of states, they do not correspond to the same system and hence should in general be considered distinct.

We can consider the states of multiple registers at the same time.

Definition 4.6. Let X_1 and X_2 be registers. Their *compound register* is $X_1X_2 := X_1 \times X_2$. An element of the compound register is written x_1x_2 and represents a classical state on both systems.

If X is a compound register with Y as factor, Y is called a *subregister* of X.

If a classical state on X is probabilistic, it corresponds to a probability distribution on the register. In that case, we also use X to refer to the random variable whose value is the state on X.

We can see registers as quantum systems, which provide the natural setting for quantum information and computation.

Definition 4.7. Let X be a register. The *Hilbert space on* X is $\mathcal{H}_X = \mathrm{span}_{\mathbb{C}} \{|x\rangle | x \in X\}$, where $\{|x\rangle | x \in X\}$ is an orthonormal basis called the *register basis*. A *quantum state on* X is a unit vector $|\psi\rangle \in \mathcal{H}_X$.

Compounding registers corresponds to taking the tensor product of their Hilbert spaces, as $\mathcal{H}_{XY} \cong \mathcal{H}_X \otimes \mathcal{H}_Y$. We use this isomorphism implicitly.

For simplicity, on Hilbert spaces on registers, we write $\mathcal{L}(X, Y) := \mathcal{L}(\mathcal{H}_X, \mathcal{H}_Y)$, $\mathcal{U}(X) := \mathcal{U}(\mathcal{H}_X)$, *etc*. Also, write the identity operator $\mathbb{I}_X = \mathbb{I}_{\mathcal{H}_X}$ and the identity map $\mathrm{id}_X = \mathbb{I}_{\mathcal{L}(X)}$, suppressing the subscript when obvious.

An important quantum register is the *qubit*, whose register is the space of one bit $\mathbb{Z}_2$ with corresponding Hilbert space $\mathcal{H}_{\mathbb{Z}_2} \cong \mathbb{C}^2$. In this space, the register basis $\{|0\rangle, |1\rangle\}$ is called the *computational basis*. Two other important bases are the *Hadamard basis*

$$\left\{ |+\rangle = \tfrac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\rangle = \tfrac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \tag{4.2.1}$$

and the *complex Hadamard basis*

$$\left\{ |+i\rangle = \tfrac{|0\rangle + i|1\rangle}{\sqrt{2}}, |-i\rangle = \tfrac{|0\rangle - i|1\rangle}{\sqrt{2}} \right\}. \tag{4.2.2}$$

A major property of these bases is that they are *mutually unbiased* in the sense that the overlaps $|\langle 0|+\rangle|^2 = |\langle 1|+\rangle|^2 = ... = \frac{1}{2} = \frac{1}{\dim \mathcal{H}_{\mathbb{Z}_2}}$. These three bases diagonalise the *Pauli operators*

$$\begin{aligned} Z &= |0\rangle\langle 0| - |1\rangle\langle 1| = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \\ X &= |+\rangle\langle +| - |-\rangle\langle -| = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \\ Y &= |+i\rangle\langle +i| - |-i\rangle\langle -i| = \left[\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right], \end{aligned} \tag{4.2.3}$$

where the matrix expressions are in the computational basis. Another related important operator is the *Hadamard operator* that exchanges the computational and Hadamard bases

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| = \tfrac{1}{\sqrt{2}} \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]. \tag{4.2.4}$$

The *Bloch sphere* provides a useful geometrical representation of the states on a qubit. A state $|\psi\rangle \in \mathcal{H}_{\mathbb{Z}_2}$ can be, up to global phase, represented by a point on the sphere. Expressing the point in spherical coordinates (θ, φ) for $\theta \in [0, \pi]$ and $\varphi \in (-\pi, \pi]$, we write

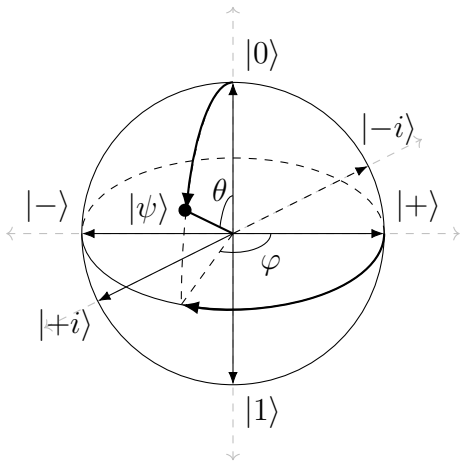


Figure 4.1: The Bloch sphere representation of a qubit. The computational, Hadamard, and complex Hadamard bases correspond to the z, x, and y axes on the sphere, respectively.

the corresponding state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$. This representation is illustrated in Fig. 4.1.

The computational and Hadamard bases generalise to the n-qubit space $\mathcal{H}_{\mathbb{Z}_2}^{\otimes n}$ as the *conjugate-coding or Wiesner states*. A conjugate-coding state is identified by a pair of strings $x, \theta \in \mathbb{Z}_2^n$ and takes the form

$$|x^\theta\rangle = H^\theta|x\rangle = H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_n}|x_n\rangle. \tag{4.2.5}$$

For fixed θ, the conjugate-coding states form a basis.

4.2.1.2 Density operator formalism

Representing quantum states as density operators allows us to synthesize quantum states and classical probability distributions. Since a physical state is represented by a quantum state, we should also be able work with a probability distribution over quantum states. Consider an ensemble of states $\{|\psi_i\rangle\}$, where the system is in state $|\psi_i\rangle$ with probability p_i. What is the probability of measuring an outcome j with generalised measurement M? If the system is in state $|\psi_i\rangle$, the probability is $\|M_j|\psi_i\rangle\|^2$, so taking the mean gives that the

probability of measuring j is

$$\begin{aligned}\sum_i p_i \|M_j|\psi_i\rangle\|^2 = \sum_i p_i \langle\psi_i|M_j^\dagger M_j|\psi_i\rangle = \sum_i p_i \operatorname{Tr}\Big(M_j^\dagger M_j \,|\psi_i\rangle\langle\psi_i|\Big) \\ = \operatorname{Tr}\Big(M_j^\dagger M_j \sum_i p_i \,|\psi_i\rangle\langle\psi_i|\Big).\end{aligned} \tag{4.2.6}$$

That is, the probability depends linearly on the operator $\rho = \sum_i p_i \,|\psi_i\rangle\langle\psi_i|$. This is called the *density operator* or *mixed state* of the ensemble. Since the measurement outcomes are the only physically relevant quantities, the density operator is all that is needed to characterise the state of a system. Also, the density operator does not depend on the global phase of the states in the ensemble, which indicates that there is a bijective correspondence between the density operators and the (probabilistic) physical states of the system. So, we consider mixed states the most general form of quantum state.

Definition 4.8. Let X be a register. A *mixed quantum state* on X is an operator $\rho \in \mathcal{P}(X)$ such that $\operatorname{Tr}(\rho) = 1$. Write the space of mixed states on X as $\mathcal{D}(X)$.

Under this general definition, we see due to the spectral decomposition (Theorem 3.16) that any mixed state can be written as the density operator of an ensemble of orthonormal states.

All the states we have considered thus far may be represented as mixed states. First, quantum states — which we contrast by referring to them as *pure quantum states* — are represented by the rank 1 mixed states $|\psi\rangle \mapsto |\psi\rangle\langle\psi|$. Classical states $x \in X$, which correspond to quantum states $|x\rangle$, give the mixed states $[x] := |x\rangle\langle x|$. Finally, probabilistic classical states, corresponding to probability distributions π on X, give the mixed states $\mu_\pi := \mathbb{E}_{x\leftarrow\pi}[x]$. The uniform probability distribution corresponds to the mixed state $\mu_X = \frac{\mathbb{I}}{|X|}$, called the *maximally mixed state*. We say a register X is *classical* if every state we work with is (probabilistic) classical on it.

We also consider states that are somewhere in between classical and quantum. A state $\rho \in \mathcal{D}(XY)$ is called *classical-quantum* (cq) or classical on X if it can be written $\rho = \sum_{x\in X} p_x[x] \otimes \rho_Y^x$ for some $\rho_Y^x \in \mathcal{D}(Y)$ and $p_x \in [0,1]$. By extension, we say a state $\rho \in \mathcal{D}(X_1 \cdots X_m Y_1 \cdots Y_n)$ is $\mathrm{c}^m\mathrm{q}^n$ if it is classical on each X_i.

To refer to a mixed state $\rho \in \mathcal{D}(X)$, we often write ρ_X. This allows us to refer to states like $\rho_{f(X)X}$, where f is a function applied coherently on the register basis to give a new register; or if ρ_{XY} is defined on multiple registers, to write ρ_X, which represents the state with register Y "forgotten" by taking the partial trace Tr_Y. This representation is due

to the fact that any measurement done locally on register X takes the form $M \otimes \mathbb{I}$, and therefore Y is removed by trace anyway. We say that a state ρ_X is *supported* on Y if Y is a subregister of X.

Similarly to random variables, mixed states can also be conditioned on events. For any cq state ρ_{XY} and any event $\Omega \subseteq X$ — which may be phrased as either a subset or as a relation — write the *partial state*

$$\rho_{\wedge\Omega} = \rho_{XY\wedge\Omega} = \sum_{x\in\Omega} p_x[x] \otimes \rho_Y^x, \tag{4.2.7}$$

and the *conditional state* $\rho_{|\Omega} = \frac{\rho_{\wedge\Omega}}{\operatorname{Tr}\rho_{\wedge\Omega}}$. Since ρ_X is classical, the probability of the event Ω is simply $\Pr[\Omega] = \operatorname{Tr}\rho_{\wedge\Omega}$.

Any mixed state can be seen as a pure state where one of the registers has been forgotten by tracing out.

Lemma 4.9 (State purification)**.** Let ρ_X be a mixed state. There exists a register Y and a state $|\psi\rangle \in \mathcal{H}_{XY}$ such that $\operatorname{Tr}_Y(|\psi\rangle\langle\psi|) = \rho_X$.

Proof: Using the spectral decomposition, we can write $\rho_X = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ where the $|\psi_i\rangle$ are orthonormal. Then, taking $Y = X$ and $|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|\psi_i\rangle$, we have $\operatorname{Tr}_Y(|\psi\rangle\langle\psi|) = \rho_X$. ■

An operator $\rho \in \mathcal{P}(X)$ is a *subnormalised state* if $\operatorname{Tr}(\rho) \leq 1$, representing a state scaled by a probability. The partial states seen above provide an important example. The definitions for mixed states extend directly to subnormalised states. We write the set of subnormalised states on X as $\mathcal{D}_{\leq}(X)$.

4.2.1.3 Representations of measurements

The measurements originally considered in quantum mechanics were projectors onto an eigenspace, which seems to be only a very specific case of the generalised measurement postulated. In this section, we see that generalised measurements reduce to projective measurements in a natural way. First, we define an intermediate type of measurement.

Definition 4.10. Let X be a register and I be a set of measurement outcomes. A *positive operator-valued measurement (POVM)* on X with outcomes in I is a map $P : I \to \mathcal{P}(X)$ such that $\sum_{i\in I} P_i = \mathbb{I}$, where $P_i := P(i)$.

Any generalised measurement $M : I \to \mathcal{L}(X, Y)$ gives rise to a POVM $P_i = M_i^\dagger M_i$; this POVM has the same distribution of outcomes as the generalised measurement. The canonical generalised measurement associated to a POVM is $\sqrt{P}$. However, this does not necessarily recover the original generalised measurement. But, using the polar decomposition (Theorem 3.19), we know that there exist isometries $U_i : \operatorname{im} P_i \to \mathcal{H}_Y$ such that $M_i = U_i\sqrt{P_i}$. As such, a generalised measurement is just a POVM followed by an isometry conditioned on the measurement outcome.

Next, we simplify POVMs.

Definition 4.11. Let X be a register and I be a set of measurement outcomes. A *projector-valued measurement (PVM)* on X with outcomes in I is a map $\Pi : I \to \mathcal{P}(X)$ such that $\sum_{i\in I} \Pi_i = \mathbb{I}$ and each $\Pi_i = \Pi(i)$ is a projector.

The projectors Π_i are in fact orthogonal, as, for any $i \neq j$, $\Pi_i + \Pi_j \leq \mathbb{I}$, and so the subspace of Π_j is contained in the orthogonal complement of the subspace of Π_i. So, for a PVM, we have $\Pi_i\Pi_j = \delta_{i,j}\Pi_i$. We can reduce POVMs to PVMs by dilating the space using Naimark's theorem.

Theorem 4.12 (Naimark)**.** Let X be a register and $P : I \to \mathcal{P}(X)$ be a POVM. There exists a register X', an isometry $V \in \mathcal{U}(X, X')$, and a PVM $\Pi : I \to \mathcal{P}(X')$ such that

$$P_i = V^\dagger \Pi_i V. \tag{4.2.8}$$

The proof we give follows the one in [TFKW13]. More general versions of the theorem exist, such as in [Pau02].

Proof: Consider the linear operator

$$\begin{array}{rccc} V: & \mathcal{H}_X & \to & \mathcal{H}_{XI} \\ & |\psi\rangle & \mapsto & \sum_{i\in I} \sqrt{P_i}|\psi\rangle \otimes |i\rangle. \end{array} \tag{4.2.9}$$

Since $\langle\varphi|V^\dagger V|\psi\rangle = \sum_i \langle\varphi|P_i|\psi\rangle = \langle\varphi|\psi\rangle$, we have that V is an isometry. Define now $\Pi : I \to \mathcal{P}(XI)$ by $\Pi_i = \mathbb{I}_X \otimes [i]$, which is immediately a PVM. Finally, Π is a dilation of P as

$$\langle\varphi|V^\dagger\Pi_i V|\psi\rangle = \sum_{j,j'} \langle\varphi|\sqrt{P_{j'}}\sqrt{P_j}|\psi\rangle \langle j'|i\rangle \langle i|j\rangle = \langle\varphi|P_i|\psi\rangle . \tag{4.2.10}$$

■

4.2.1.4 General quantum operations: channels

Since both unitary evolution and measurement are possible quantum operations, we should be able to see them as particular cases of a more general quantum operation. To do so, we first define the most general possible operation, called a *quantum channel*, see how both unitary evolution and measurement appear as special cases, and then see that this general operation can in fact be seen as a unitary on a larger system. A map must satisfy some basic properties to be an admissible quantum channel. First and most importantly, the channel must send quantum states to quantum states. Second, as both unitary evolution and measurement are positive linear on mixed states (as maps to states and probability distributions, respectively), we can assume a channel is positive linear as well. Due to the decomposition of an operator as a linear combination of positive operators, the channel extends to a complex linear map on operators.

Definition 4.13. Let X and Y be registers. A *completely positive trace-preserving (CPTP) map* from X to Y is a linear map $\Phi : \mathcal{L}(X) \to \mathcal{L}(Y)$ that is

positive For any $P \in \mathcal{P}(X)$, $\Phi(P) \geq 0$.

completely positive For any register Z, the map $\mathrm{id}_Z \otimes \Phi$ is positive.

trace preserving For all $T \in \mathcal{P}(X)$, $\mathrm{Tr}(\Phi(T)) = \mathrm{Tr}(T)$.

The CPTP maps represent the quantum channels. The complete positivity condition implies the positivity condition, however the converse does not hold (unless $|X| = 1$ or $|Y| = 1$). That is, there are linear maps that locally send quantum states to quantum states but are not well-behaved with respect to entanglement and thus cannot be considered as permissible quantum operations.

Example 4.14. The canonical example of a positive but not completely positive operation is the *transpose*. Let $\Phi_T : \mathcal{L}(\mathbb{Z}_2) \to \mathcal{L}(\mathbb{Z}_2)$ be defined as $\Phi_T(\rho) = \rho^T$. This is both positive and trace preserving. However, consider the state $\rho = |\mathrm{EPR}\rangle\langle\mathrm{EPR}| \in \mathcal{D}(\mathbb{Z}_2\mathbb{Z}_2)$. This is positive, but $(\mathrm{id} \otimes \Phi_T)(\rho) = \frac{1}{2}(\,|00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|)$, which has an eigenvalue $-\frac{1}{2}$ and hence cannot be positive.

Now that we have given a non-example, it is perhaps time to actually give some examples. A first example is the trace, because the partial trace sends quantum states to quantum states. Next, we represent the quantum operations we have previously seen as CPTP maps.

Definition 4.15. Let X, Y, I be registers. Let $V \in \mathcal{U}(X, Y)$ be an isometry, $M : I \to \mathcal{L}(X, Y)$ be a generalised measurement, and $P : I \to \mathcal{P}(X)$ be a POVM.

- The *isometric channel* is the map $\Phi_V : \mathcal{L}(X) \to \mathcal{L}(Y)$ defined $\Phi_V(\rho) = V\rho V^\dagger$. If V is a unitary, it is called the *unitary channel*.
- The *destructive measurement channels* are $\Psi_M, \Psi_P : \mathcal{L}(X) \to \mathcal{L}(I)$ defined

$$\Psi_M(\rho) = \sum_{i \in I} \operatorname{Tr}(M_i^\dagger M_i \rho)[i], \qquad \Psi_P(\rho) = \sum_{i \in I} \operatorname{Tr}(P_i \rho)[i]. \tag{4.2.11}$$

- The *nondestructive measurement channels* are the maps $\Phi_M : \mathcal{L}(X) \to \mathcal{L}(IY)$ and $\Phi_P : \mathcal{L}(X) \to \mathcal{L}(IX)$ defined

$$\Phi_M(\rho) = \sum_{i \in I} [i] \otimes M_i \rho M_i^\dagger, \qquad \Phi_P(\rho) = \sum_{i \in I} [i] \otimes \sqrt{P_i}\rho\sqrt{P_i}. \tag{4.2.12}$$

Note that if M and P represent the same measurement, then $\Psi_P = \Psi_M$, and Φ_M is the composition of Φ_P with an isometric channel. For a mixed state ρ_X, we write the cq state arising from the action of a POVM P by the nondestructive channel $\rho_{P(X)X} := \Phi_P(\rho_X)$.

Using these channels, we can consider states conditioned on events that make reference to a measurement, *e.g.* $\Omega = (P(Y) = s)$. We assume that the measurement is undertaken by the nondestructive channel, used to come up with the partial or conditional state, and then the result is forgotten by tracing out. This may perturb registers on which the state is non-classical, so we have to in particular assure ourselves that any two measurements in the same event are compatible (commuting), or that it is made obvious which measurement occurs first.

Now, we show some general results about CPTP maps. At first, the complete positivity condition may seem daunting, but we can reduce it to the positivity condition of a related quantum state.

Definition 4.16. Let X be a register. The *EPR state on* X is

$$|\mathrm{EPR}_X\rangle = \frac{1}{\sqrt{|X|}} \sum_{x \in X} |x\rangle|x\rangle \in \mathcal{H}_{XX}. \tag{4.2.13}$$

This extends the one-qubit EPR state (Definition 4.2).

Definition 4.17 (Choi representation)**.** Let X, Y be registers and $\Phi : \mathcal{L}(X) \to \mathcal{L}(Y)$ be a linear map. The *Choi representation* of Φ is operator

$$J(\Phi) = (\mathbb{I}_X \otimes \Phi)(\,|\mathrm{EPR}_X\rangle\langle\mathrm{EPR}_X|) \in \mathcal{L}(XY). \tag{4.2.14}$$

Note that this is a different normalisation from what is usually chosen for the Choi representation, for example in [Wat18, Pau02], but the normalisation we use allows for a more direct correspondence between quantum channels and states.

Theorem 4.18 (Choi)**.** Let $\Phi : \mathcal{L}(X) \to \mathcal{L}(Y)$ be a linear map. Φ is a CPTP map if and only if the Choi representation $J(\Phi) \geq 0$ and $\mathrm{Tr}_Y(J(\Phi)) = \mu_X$.

Note that this implies that the Choi representation of a CPTP map is a quantum state. However, not every quantum state is the Choi representation of some CPTP map, but every positive operator is nonetheless the Choi representation of some completely positive map.
Proof: If Φ is CPTP, then $\mathrm{id} \otimes \Phi$ is positive so $(\mathrm{id} \otimes \Phi)(\,|\mathrm{EPR}_X\rangle\langle\mathrm{EPR}_X|)$ is positive; and trace preserving, so $\mathrm{Tr}_Y(J(\Phi)) = \mathrm{id}(\mu_X) = \mu_X$.

For the converse, suppose $J(\Phi)$ is a state. Then, by the spectral decomposition, we can decompose $J(\Phi) = \sum_i p_i \,|\psi_i\rangle\langle\psi_i|$. Since $J(\Phi) = \frac{1}{|X|}\sum_{x,y\in X} \,|x\rangle\langle y| \otimes \Phi(\,|x\rangle\langle y|)$, we see that for $x, y \in X$,

$$\Phi(\,|x\rangle\langle y|) = |X|(\langle x| \otimes \mathbb{I})J(\Phi)(|y\rangle \otimes \mathbb{I}) = \sum_i |X|p_i(\langle x| \otimes \mathbb{I})\,|\psi_i\rangle\langle\psi_i|\,(|y\rangle \otimes \mathbb{I}). \tag{4.2.15}$$

Let $A_i : \mathcal{L}(X) \to \mathcal{L}(Y)$ be such that $A_i|x\rangle = \sqrt{|X|p_i}(\langle x| \otimes \mathbb{I})|\psi_i\rangle$. Then, $\Phi(\,|x\rangle\langle y|) = \sum_i A_i \,|x\rangle\langle y|\, A_i^\dagger$, and so $\Phi(\rho) = \sum_i A_i \rho A_i^\dagger$. This is called the *Kraus decomposition* of Φ. Now, since conjugation is completely positive and sums of completely positive maps are completely positive, we have that Φ is completely positive. It remains to show that it is also trace preserving. Since the partial trace $\mathrm{Tr}_Y(J(\Phi)) = \frac{1}{|X|}\sum_{x,y} \mathrm{Tr}(\Phi(\,|x\rangle\langle y|))\,|x\rangle\langle y| = \mu_X$, we have that $\Phi(\,|x\rangle\langle y|) = \delta_{x,y}$, which suffices to show it. ■

Next, we present the *Stinespring dilation*, which allows any quantum channel to be represented as an isometry. This provides a further theoretical justification of the measurement postulate, as we get that measurements may be represented as unitaries on a larger system.

Theorem 4.19 (Stinespring)**.** Let $\Phi : \mathcal{L}(X) \to \mathcal{L}(Y)$ be a CPTP map. Then, there exists a register Z and an isometry $V \in \mathcal{U}(X, YZ)$ such that

$$\Phi(\rho) = \mathrm{Tr}_Z\big(V\rho V^\dagger\big). \tag{4.2.16}$$

Proof: We make use of the Kraus decomposition from the proof of the previous theorem: $\Phi(\rho) = \sum_{i\in I} A_i \rho A_i^\dagger$. We take $Z = I$ and define $V|\psi\rangle = \sum_i A_i|\psi\rangle \otimes |i\rangle$. Using trace preservation, $\langle\psi|V^\dagger V|\psi\rangle = \sum_i \langle\psi|A_i^\dagger A_i|\psi\rangle = \mathrm{Tr}(\Phi(\,|\psi\rangle\langle\psi|)) = \langle\psi|\psi\rangle$, so V is an isometry. Finally,

$$\mathrm{Tr}_Z\big(V\rho V^\dagger\big) = \sum_{i,j\in I} A_i \rho A_j^\dagger \langle j|i\rangle = \sum_{i\in I} A_i \rho A_i^\dagger = \Phi(\rho). \tag{4.2.17}$$

■

Finally, we note that, with respect to the Hilbert-Schmidt inner product, the adjoint of a completely positive map is completely positive, and the adjoint of a trace preserving map is identity preserving ($\Phi^\dagger(\mathbb{I}_Y) = \mathbb{I}_X$) and *vice versa*.

4.2.1.5 Metrics

Metrics on states and operators allow us to understand inexact or error-prone processes. On pure states, the Euclidean norm on the Hilbert space provides a distance metric, and by construction, the induced operator norm (Definition 3.9) is the appropriate metric on operators acting on the states. However, the situation is less clear on mixed states. It turns out the appropriate norm is the *trace norm* due to its relation to measurements. First, we introduce the norm and then we justify it.

Definition 4.20. Let U, V be finite-dimensional inner product spaces and let $T \in \mathcal{L}(U, V)$. Then, the *trace norm* of T is

$$\|T\|_{\mathrm{Tr}} = \tfrac{1}{2}\,\mathrm{Tr}(|T|) = \tfrac{1}{2}\,\mathrm{Tr}\Big(\sqrt{T^\dagger T}\Big). \tag{4.2.18}$$

Note that a different normalisation is sometimes used. The normalisation we give has the property that, for quantum states ρ and σ, $\|\rho - \sigma\|_{\mathrm{Tr}} \leq 1$. We give some important properties.

Proposition 4.21. Let X be a register.

(i) For $T \in \mathcal{L}(X)$ hermitian, $\|T\|_{\mathrm{Tr}} = \sup_{0\leq P\leq \mathbb{I}_X} \mathrm{Tr}(PT) - \frac{1}{2}\mathrm{Tr}(T)$.

(ii) For $\rho, \sigma \in \mathcal{D}(X)$ and Φ a quantum channel, $\|\Phi(\rho) - \Phi(\sigma)\|_{\mathrm{Tr}} \leq \|\rho - \sigma\|_{\mathrm{Tr}}$.

(iii) For pure states $|\psi\rangle, |\varphi\rangle \in \mathcal{H}_X$, $\| \, |\psi\rangle\langle\psi| - \, |\varphi\rangle\langle\varphi|\|_{\mathrm{Tr}} \leq \||\psi\rangle - |\varphi\rangle\|$.

Proof:

(i) Using the spectral decomposition, we can write $T = A - B$ where A and B are both positive, and $AB = 0$. Thus, $|T| = A + B$, so

$$\|T\|_{\mathrm{Tr}} = \tfrac{1}{2}(\mathrm{Tr}(A) + \mathrm{Tr}(B)) = \mathrm{Tr}(A) + \tfrac{1}{2}(\mathrm{Tr}(B - A)) = \mathrm{Tr}(A) - \tfrac{1}{2}\mathrm{Tr}(T). \tag{4.2.19}$$

Since $\mathrm{Tr}(A)$ is $\mathrm{Tr}(\Pi T)$ for Π the projector onto sum of the positive eigenspaces we have $\mathrm{Tr}(A) \leq \sup_{0\leq P\leq \mathbb{I}_X} \mathrm{Tr}(PT)$; and as $\mathrm{Tr}(PT) = \mathrm{Tr}(PA) - \mathrm{Tr}(PB) \leq \mathrm{Tr}(PA)$, this is in fact an equality.

(ii) Using part (i), since $\mathrm{Tr}(\rho - \sigma) = 0$, we have $\|\rho - \sigma\|_{\mathrm{Tr}} = \sup_{0\leq P\leq \mathbb{I}_X} \mathrm{Tr}(P(\rho - \sigma))$. Thus, we get that

$$\begin{aligned} \|\Phi(\rho) - \Phi(\sigma)\|_{\mathrm{Tr}} &= \sup_{0\leq Q\leq \mathbb{I}_Y} \mathrm{Tr}(Q\Phi(\rho - \sigma)) = \sup_{0\leq Q\leq \mathbb{I}_Y} \mathrm{Tr}\big(\Phi^\dagger(Q)(\rho - \sigma)\big) \\ &\leq \|\rho - \sigma\|_{\mathrm{Tr}}. \end{aligned} \tag{4.2.20}$$

(iii) Consider the subspace $V = \mathrm{span}_{\mathbb{C}}\{|\psi\rangle, |\varphi\rangle\}$. If $\dim V = 1$, then the trace distance $\| \, |\psi\rangle\langle\psi| - \, |\varphi\rangle\langle\varphi|\|_{\mathrm{Tr}} = 0 \leq \||\psi\rangle - |\varphi\rangle\|$. Else, $\dim V = 2$, so we can choose an orthonormal basis $\{|\psi\rangle, |\perp\rangle\}$ in which we may express $|\varphi\rangle = e^{i\alpha}\cos\frac{\theta}{2}|\psi\rangle + \sin\frac{\theta}{2}|\perp\rangle$. Then,

$$\| \, |\psi\rangle\langle\psi| - \, |\varphi\rangle\langle\varphi|\|_{\mathrm{Tr}} = \left\| \begin{bmatrix} 1 - \cos^2\frac{\theta}{2} & -e^{i\alpha}\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ -e^{-i\alpha}\cos\frac{\theta}{2}\sin\frac{\theta}{2} & -\sin^2\frac{\theta}{2} \end{bmatrix} \right\|_{\mathrm{Tr}} = \left|\sin\tfrac{\theta}{2}\right|. \tag{4.2.21}$$

On the other hand, $\||\psi\rangle - |\varphi\rangle\| = \sqrt{|1 - e^{i\alpha}\cos\frac{\theta}{2}|^2 + \sin^2\frac{\theta}{2}} \geq 2|\sin\frac{\theta}{4}|$. The inequality is provided by $\left|\sin\frac{\theta}{2}\right| \leq 2|\sin\frac{\theta}{4}|$.

■

Finally, in order to justify the use of the trace norm, we relate it to an important probability. Consider the following scenario. Alice holds a quantum register X, and she knows that the register was prepared in state ρ or σ, each with probability $\frac{1}{2}$. She attempts to guess which state she holds with one measurement. Then, her optimal probability of guessing correctly

$$\begin{aligned} p &= \sup_{P:\{\rho,\sigma\}\to\mathcal{P}(X)\text{ POVM}} \tfrac{1}{2}(\mathrm{Tr}(P_\rho\rho) + \mathrm{Tr}(P_\sigma\sigma)) \\ &= \sup_{0\le P\le\mathbb{I}} \tfrac{1}{2}(\mathrm{Tr}(P\rho) + \mathrm{Tr}((\mathbb{I}-P)\sigma)) = \tfrac{1}{2} + \tfrac{1}{2}\sup_{0\le P\le\mathbb{I}} \mathrm{Tr}(P(\rho-\sigma)) \\ &= \tfrac{1}{2} + \tfrac{1}{2}\|\rho-\sigma\|_{\mathrm{Tr}}. \end{aligned} \tag{4.2.22}$$

As such, the trace distance is related to a guessing probability, which makes differences between states in trace distance very amenable to interpretation.

4.2.2 Entropy

Entropy provides a measure of the uncertainty on a system. We make use of the min-entropy, as it has an important operational interpretation. The main reference for this section is [Tom16].

First, we define the entropy of a classical probability distribution.

Definition 4.22. Let $\pi : X \to [0,1]$ be a probability distribution. The *min-entropy* of X on π is

$$H_{\min}(X)_\pi = -\lg \max_{x\in X} \pi(x), \tag{4.2.23}$$

where $\lg$ is the base-2 logarithm.

It is direct to see that $2^{-H_{\min}(X)_\pi}$ is the optimal probability of guessing the outcome. The probability of guessing can be improved by having access to some *side information* about the distribution on X. This gives rise to the conditional min-entropy.

Definition 4.23. Let $\pi : X \times Y \to [0,1]$ be a probability distribution. The *conditional min-entropy* of X knowing Y on π is

$$H_{\min}(X|Y)_\pi = -\lg \sum_{y\in Y} \max_x \pi(x,y). \tag{4.2.24}$$

As such, $2^{-H_{\min}(X|Y)_\pi}$ is the optimal probability of guessing the outcome x as a function of a known outcome on y. In the quantum setting, due to the diagonalisation of the density operator, the original min-entropy becomes $H_{\min}(X)_\rho = -\lg\|\rho\|$, where $\|\cdot\|$ is the operator norm. This is the optimal probability of guessing the outcome of an X-outcome projective measurement on ρ. The generalisation of the conditional min-entropy is the most useful.

Definition 4.24. Let ρ_{XY} be a subnormalised quantum state. The *conditional min-entropy* of X knowing Y on ρ is

$$H_{\min}(X|Y)_\rho = -\lg\inf\left\{\mathrm{Tr}(\sigma_Y)|\sigma_Y \geq 0; \rho_{XY} \leq \mathbb{I}_X \otimes \sigma_Y\right\}. \tag{4.2.25}$$

We mostly make use of the alternate expression

$$H_{\min}(X|Y)_\rho = -\lg\sup\left\{\mathrm{Tr}(T\rho)|T_{XY} \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}_Y\right\}, \tag{4.2.26}$$

which is closer to the operational interpretation. The two expressions are related as the primal and dual forms of a semi-definite program optimisation [Tom16].

Theorem 4.25. Let ρ_{XY} be a cq state. Then, $2^{-H_{\min}(X|Y)_\rho}$ is the optimal probability of guessing X by making a measurement on Y.

Proof: We use the alternate expression of the min-entropy. Writing $\rho_{XY} = \sum_x p_x[x] \otimes \rho_Y^x$ and analogously $T_{XY} = \sum_{x,x'} |x\rangle\langle x'| \otimes T_Y^{x,x'}$, we get that $\mathrm{Tr}(T\rho) = \sum_x p_x \mathrm{Tr}(T^{x,x}\rho^x)$. As positivity implies positivity of the diagonal blocks, we can restrict to those T that are zero on the off-diagonal blocks and write

$$\begin{aligned} 2^{-H_{\min}(X|Y)_\rho} &= \sup\left\{\sum_x p_x \mathrm{Tr}(T^x\rho^x)\middle| T_Y^x \geq 0; \sum_x T_Y^x \leq \mathbb{I}_Y\right\} \\ &= \sup_{P:X\to\mathcal{P}(Y)\text{ POVM}} \sum_x p_x \mathrm{Tr}(P_x\rho^x). \end{aligned} \tag{4.2.27}$$

This is exactly the probability of guessing X with a measurement on register Y. ■

We also work with a robust version of the min-entropy, that is attained by considering the entropy of all possible small perturbations of the state.

Definition 4.26 (Smooth entropy)**.** Let $\varepsilon > 0$ and ρ_{XY} be a subnormalised state. Then, the *ε-smooth conditional min-entropy*

$$H_{\min}^{\varepsilon}(X|Y)_{\rho} = \sup\left\{H_{\min}(X|Y)_{\sigma} | \sigma \in \mathrm{Tr}(\rho)\mathcal{D}_{\leq}(XY); \|\rho - \sigma\|_{\mathrm{Tr}} \leq \mathrm{Tr}(\rho)\varepsilon\right\}. \quad (4.2.28)$$

Though it is defined in terms of the norm, the smooth min-entropy is stable under inclusions in a larger space.

Proposition 4.27. Let ρ_{XY} be a subnormalised state and $U \in \mathcal{U}(X, X')$, $V \in \mathcal{U}(Y, Y')$ be isometries. Fix $\rho'_{X'Y'} = (U \otimes V)\rho_{XY}(U^{\dagger} \otimes V^{\dagger})$. Then,

$$H_{\min}^{\varepsilon}(X'|Y')_{\rho'} = H_{\min}^{\varepsilon}(X|Y)_{\rho}. \quad (4.2.29)$$

Proof: Since the ball around ρ' is compact, there exists a state σ' that maximises the min-entropy $H_{\min}^{\varepsilon}(X'|Y')_{\rho'} = H_{\min}(X'|Y')_{\sigma'}$. Now, let Π_{XY} be the projector onto $\mathrm{im}(U \otimes V)$ and Π_Y be the projector onto $\mathrm{im}(V)$. Again using compactness, there exists $\tau_{Y'}$ satisfying $\tau \geq 0$, $\sigma' \leq \mathbb{I} \otimes \tau$, and $H_{\min}(X|Y)_{\sigma'} = -\lg \mathrm{Tr}(\tau)$. Then, as conjugation preserves positivity,

$$\Pi_{XY}\sigma'\Pi_{XY} \leq \Pi_{XY}(\mathbb{I} \otimes \tau)\Pi_{XY} \leq \mathbb{I} \otimes \Pi_Y \tau \Pi_Y. \quad (4.2.30)$$

Letting $\sigma'' = \Pi_{XY}\sigma'\Pi_{XY}$ and $\tau' = \Pi_Y \tau \Pi_Y$, this gives that, since $\mathrm{Tr}(\tau') \leq \mathrm{Tr}(\tau)$, $H_{\min}(X|Y)_{\sigma'} \leq H_{\min}(X|Y)_{\sigma''}$. Finally, since $\rho' = \Pi_{XY}\rho'\Pi_{XY}$, we have that $\|\rho' - \sigma''\|_{\mathrm{Tr}} \leq \|\rho' - \sigma'\|_{\mathrm{Tr}}$, so we can restrict the search to those states that are in the image of the isometry, and so we get the wanted equality. ■

Now, we provide the important inequalities we use when dealing with entropy.

Theorem 4.28 (Data processing)**.** Let ρ_{XY} be a subnormalised state and $\Phi : \mathcal{L}(Y) \to \mathcal{L}(Y')$ be a completely positive trace non-increasing map. Then, for $\varepsilon > 0$,

$$H_{\min}^{\varepsilon}(X|\Phi(Y))_{\rho} \geq H_{\min}^{\varepsilon}(X|Y)_{\rho}. \quad (4.2.31)$$

Note that in this expression $H_{\min}^{\varepsilon}(X|\Phi(Y))_{\rho} := H_{\min}^{\varepsilon}(X|Y')_{\Phi_Y(\rho)}$. The data-processing inequality tells us that no local quantum operation can increase the knowledge about another system.

Proof: First, we work with the un-smoothed entropy. We see that

$$\begin{aligned} 2^{-H_{\min}(X|\Phi(Y))_\rho} &= \sup\{\mathrm{Tr}(T\Phi_Y(\rho))|T \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}\} \\ &= \sup\left\{\mathrm{Tr}(\Phi^\dagger_{Y'}(T)\rho))\middle|T \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}\right\} \\ &\leq \sup\{\mathrm{Tr}(T\rho))|T \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}\} = 2^{-H_{\min}(X|Y)_\rho}, \end{aligned} \tag{4.2.32}$$

since $\Phi^\dagger$ is completely positive and identity non-increasing $\Phi^\dagger(\mathbb{I}) \leq \mathbb{I}$.

Now, as in the previous proposition, let σ be a state such that $H^\varepsilon_{\min}(X|Y)_\rho = H_{\min}(X|Y)_\sigma$. Then, we have that $H_{\min}(X|Y)_\sigma \leq H^\varepsilon_{\min}(X|\Phi(Y))_\sigma \leq H^\varepsilon_{\min}(X|\Phi(Y))_\rho$, as a CP trace non-increasing map does not increase the trace distance. ■

Theorem 4.29 (Conditioning on classical information)**.** Let ρ_{XYZ} be a subnormalised state that is classical on Z. Then, for $\varepsilon > 0$,

$$H^\varepsilon_{\min}(X|YZ)_\rho \geq H^\varepsilon_{\min}(X|Y)_\rho - \lg|Z|. \tag{4.2.33}$$

This tells that n bits of classical information can only decrease the uncertainty by n.

Proof: As above, we first approach the unsmoothed case. Writing $\rho_{XYZ} = \sum_{z\in Z} \rho^z_{XY} \otimes |z\rangle\langle z|$ and $T_{XYZ} = \sum_{z,z'} T^{z,z'}_{XY} \otimes |z\rangle\langle z'|$, we have that

$$\begin{aligned} 2^{-H_{\min}(X|YZ)_\rho} &= \sup\left\{\sum_z \mathrm{Tr}(T^{z,z}\rho^z)\middle|T^{z,z} \geq 0; \mathrm{Tr}_X(T^{z,z}) \leq \mathbb{I}_Y\right\} \\ &\leq |Z| \max_{z\in Z} \sup\{\mathrm{Tr}(T\rho^z)|T \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}_Y\} \\ &\leq |Z| \max_{z\in Z} \sup\{\mathrm{Tr}(T\rho_{XY})|T \geq 0; \mathrm{Tr}_X(T) \leq \mathbb{I}_Y\} \\ &\leq |Z| 2^{-H_{\min}(X|Y)_\rho}, \end{aligned} \tag{4.2.34}$$

as $\rho_{XY} = \sum_z \rho^z_{XY}$.

For the smoothed case, let σ_{XYZ} be a state classical on Z in the ball around ρ_{XYZ} — every σ_{XY} around ρ_{XY} can be attained by tracing out the register Z. Then, by the above, $H_{\min}(X|Y)_\sigma - \lg|Z| \leq H_{\min}(X|YZ)_\sigma \leq H^\varepsilon_{\min}(X|YZ)_\rho$. Taking the supremum over σ gives the result. ■

4.2.2.1 Quantum-proof strong extractors

An important use of conditional min-entropy is for quantum-proof strong extractors. Due to the operational interpretation, the conditional min-entropy of a cq state provides a condition on the probability of guessing a classical register. However, in general, the min-entropy being high does not say that the classical register is uncorrelated. Strong extractors provide a way to remedy that.

Definition 4.30 ([KT08])**.** Let X, Y, Z be classical registers. A *quantum-proof* (k, ε)*-strong extractor* is a function $e : X \times Y \to Z$ such that for any subnormalised cq state ρ_{XQ}, where Q is a quantum register such that $H_{\min}(X|Q) \geq k$, if we take $\rho_{YXQ} = \mu_Y \otimes \rho_{XQ}$,

$$\left\| \rho_{e(X,Y)YQ} - \mu_Z \otimes \mu_Y \otimes \rho_Q \right\|_{\mathrm{Tr}} \leq \varepsilon. \tag{4.2.35}$$

Additionally, we say that e is a (k, ε)*-strong extractor* if the condition holds when there is no side information Q, and that e is a *classical-proof* (k, ε)*-strong extractor* if the condition holds whenever Q is classical.

It was shown in [KT08] that every (k, ε)-strong extractor is $(k - \lg \varepsilon, 2\varepsilon)$-classical-proof; and that, if its output $Z = \mathbb{Z}_2$, then it is also $(k - \lg \varepsilon, 3\sqrt{\varepsilon})$-quantum-proof. In [DPVR12], it was shown that a one-bit quantum-proof strong extractor can be used to construct an extractor on many bits via Trevisan's construction [Tre01]. They also give many examples of extractors based on list-decodable codes.

Though we will tend use general extractors and only specify their parameters, we give an example of the construction of [DPVR12] that is useful to keep in mind. For any $m, n \in \mathbb{N}$ and $\varepsilon > 0$, there exists a quantum-proof $(8 \lg(3m/2\varepsilon) + m, \varepsilon)$-strong extractor $e : \mathbb{Z}_2^n \times \mathbb{Z}_2^d \to \mathbb{Z}_2^m$, where $d \in O(\lg(m\sqrt{n}/\varepsilon)^2 \lg m)$. Of course, for this to be useful, we need that $k = 8 \lg(3m/2\varepsilon) + m < n$. Nevertheless, it is possible to achieve an exponentially small error $\varepsilon = \eta^m$ for any output length m by taking $n > 8 \lg(3m/2) + (1 + 8 \lg 1/\eta)m \in O(m)$, though this requires the key length d to be polynomial in m. This example absolutely defeats the original purpose of strong extractors, to extract a large amount of near-uniform randomness using a small seed, but is of great use in our cryptographic applications.

Another important construction of extractors often used, especially for QKD, is a construction based on hash functions. This is a family of functions that, when sampled randomly, minimises the probability of a collision — it is unlikely for two elements to have the same image. Hash functions are often used to approximate random functions.

Definition 4.31. Let X, Y be finite sets. A family of functions H from $X \to Y$ is *universal$_2$* if, for any distinct $x, x' \in X$, $\Pr[H(x) = H(x')] = \frac{1}{|Y|}$, where, abusing notation, H represents the uniform random variable on H.

There are constructions of hash functions whenever the cardinalities of X and Y are powers of 2 [WC81]. It is possible to use this property to construct quantum-proof strong extractors.

Lemma 4.32 (Leftover hash lemma)**.** Let H be a universal$_2$ family of functions $\mathbb{Z}_2^n \to \mathbb{Z}_2^\ell$. Then, the function $e : \mathbb{Z}_2^n \times H \to \mathbb{Z}_2^\ell$ defined as $e(x, h) = h(x)$ is a quantum-proof $(k, 2^{-(k-\ell+2)/2})$-strong extractor for all $k > 0$.

A proof of this result is given in [TL17].

Chapter 5

Uncloneability Games

In this chapter, we formally introduce the general structure of uncloneability games, expanding on the descriptions given in Chapter 1. First, in Section 5.1, we discuss the no-cloning and monogamy-of-entanglement principles that the games illustrate. Then, we present the extended nonlocal game framework in Section 5.2, which provides a general description of entanglement-based games. We specialise this to monogamy-of-entanglement games in Section 5.3. Finally, in Section 5.4, we introduce no-cloning games and discuss the duality between these and monogamy-of-entanglement games.

Much in this chapter consists of literature review, though we do include some new contributions; we indicate these with footnotes.

5.1 The Monogamy-of-Entanglement Principle

The idea of uncloneability games arises from the question of how to study the no-cloning principle. Though it may be rigorously understood via the no-cloning theorem (Theorem 4.4), the principle is often unamenable to application. Uncloneability games attempt to remedy that.

Rather than the no-cloning property of a channel, it often serves to work with a related entanglement-based property of a state. This is a property of tripartite entanglement, the *monogamy-of-entanglement* (MoE). This property is rather elusive, and has been studied from a variety of perspectives, for example by means of state shareability [Ter04] or entanglement-measure inequalities [CKW00]. We give an operational interpretation[1] that

[1] To the best of our knowledge, this way of interpreting monogamy-of-entanglement is novel.

is dual to no-cloning in the sense that, if there were a channel that permits cloning, its Choi representation (Definition 4.17) would be a state that breaks monogamy-of-entanglement. The MoE property says that no quantum system can be maximally entangled with two systems at once. Here, maximal entanglement is taken to generalise the property of the EPR state that any unitary operation on one of the systems can be counteracted by an unitary operation on the other system. Note that maximal entanglement under this definition does not exist in infinite dimensions — only approximate versions of the property exist.

Definition 5.1. Let $\mathcal{H} \cong \mathbb{C}^d$. A state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ is called *maximally entangled* if, for all $U \in \mathcal{U}(\mathcal{H})$, there exists $U' \in \mathcal{U}(\mathcal{H})$ such that

$$(U \otimes U')|\Psi\rangle = |\Psi\rangle. \tag{5.1.1}$$

In this definition, we see maximally-entangled states as those where unitary evolution on one of the systems can be undone by an operation on the other system.

Lemma 5.2. Let $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H}$ be maximally entangled and let $\{|i\rangle\}_{i\in[d]}$ be a basis of $\mathcal{H}$. Then, there exists a basis $\{|v_i\rangle\}_{i\in[d]}$ of $\mathcal{H}$ such that

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |v_i\rangle, \tag{5.1.2}$$

and for every $U \in \mathcal{U}(\mathcal{H})$, $U' = M\overline{U}M^\dagger$ where $M = \sum_i |v_i\rangle\langle i|$ is the change-of-basis matrix and the conjugate is with respect to the basis $\{|i\rangle\}$.

This tells us that every maximally-entangled state is essentially a higher-dimensional generalisation of the EPR state (Definition 4.2), up to a local unitary rotation. In particular, the result of any measurement on one system may be perfectly predicted by a corresponding measurement on the other system.

Proof: We consider the Schmidt decomposition of $|\Psi\rangle = \sum_{i=1}^{d} \sqrt{p_i}|u_i\rangle \otimes |v_i\rangle$. Using the maximal entanglement property, we can act by $U \otimes U'$ where U is a change-of-basis matrix and preserve the state, and hence assume that $|u_i\rangle = |i\rangle$. Next, we show that $p_i = \frac{1}{d}$. Suppose otherwise, that is that there exist $i, j \in [d]$ such that $p_i \neq p_j$. Consider the unitary

S_{ij} defined as

$$S_{ij}|k\rangle = \begin{cases} |j\rangle & , k = i \\ |i\rangle & , k = j \\ |k\rangle & , \text{ else} \end{cases}. \tag{5.1.3}$$

Then, as $(S_{ij} \otimes S'_{ij})|\Psi\rangle = |\Psi\rangle$, we have that

$$\sqrt{p_j} S'_{ij}|v_j\rangle = (\langle i| \otimes \mathbb{I})(S_{ij} \otimes S'_{ij})|\Psi\rangle = (\langle i| \otimes \mathbb{I})|\Psi\rangle = \sqrt{p_i}|v_i\rangle. \tag{5.1.4}$$

Taking the norm of each side gives the contradiction $p_i = p_j$. As such, we get the wanted form of the state. Now let $U \in \mathcal{U}(\mathcal{H})$. Writing $U = \sum_{i,j} U_{ij} |i\rangle\langle j|$ and $U' = \sum_{i,j} U'_{ij} |v_i\rangle\langle v_j|$, the equality $(U \otimes U')|\Psi\rangle = |\Psi\rangle$ gives, for all $j, j' \in [d]$, $\sum_j U_{ij} U'_{i'j} = \delta_{i,i'}$. Since U is unitary, this means $U'_{ij} = \overline{U}_{ij}$, giving $U' = \sum_{ij} \overline{U}_{ij} M |i\rangle\langle j| M^\dagger = M\overline{U}M^\dagger$. ■

Theorem 5.3 (Monogamy of entanglement)**.** Let $\mathcal{H} \cong \mathbb{C}^d$ for $d > 1$. There does not exist a state $|\Psi\rangle \in \mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$ such that for all $U \in \mathcal{U}(\mathcal{H})$, there exists $U' \in \mathcal{U}(\mathcal{H})$ such that

$$(U \otimes \mathbb{I} \otimes \mathbb{I})|\Psi\rangle = (\mathbb{I} \otimes U' \otimes U')|\Psi\rangle. \tag{5.1.5}$$

Proof: Suppose otherwise and let $|\Psi\rangle$ be this state. Using the Schmidt decomposition, write $|\Psi\rangle = \sum_{i=1}^d \sqrt{p_i}|v_i\rangle|\psi_i\rangle$ for $|v_i\rangle \in \mathcal{H}$ and $|\psi_i\rangle \in \mathcal{H} \otimes \mathcal{H}$. As the subspace of $\mathcal{H} \otimes \mathcal{H}$ spanned by the $|\psi_i\rangle$ has dimension d, the above lemma implies $|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |v_i\rangle \otimes |\psi_i\rangle$ and there exists an isometry $M : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ such that $U' \otimes U' = M\overline{U}M^\dagger$. In particular, for $U = \mathbb{I}$, $U' \otimes U' = MM^\dagger$. But this gives that a projector onto a subspace of $\mathcal{H} \otimes \mathcal{H}$ of dimension d is unitary, which is a contradiction. ■

5.2 Extended Nonlocal Games

Extended nonlocal games are a general class of one-round quantum interaction involving a *referee* or verifier, Alice, and two *players* or provers, Bob and Charlie. This model was first introduced in [JMRW16] and has both nonlocal games and monogamy-of-entanglement games as special cases. In an extended nonlocal game, each party holds a quantum register, where Alice's register A is fixed, and Bob and Charlie's registers, B and C, are arbitrarily

chosen by the players. The gameplay proceeds as follows.

1. Bob and Charlie prepare a shared quantum state ρ_{ABC}, after which they are isolated and may no longer communicate.

2. Next, Alice samples a pair of random questions (θ_B, θ_C) from a fixed question distribution π. She sends Bob θ_B and Charlie θ_C.

3. By making local measurements on their spaces, Bob and Charlie produce answers x_B and x_C, respectively, and send them to Alice.

4. Alice makes a fixed single-bit measurement on her space, depending on the questions and answers. Bob and Charlie win if she measures 1.

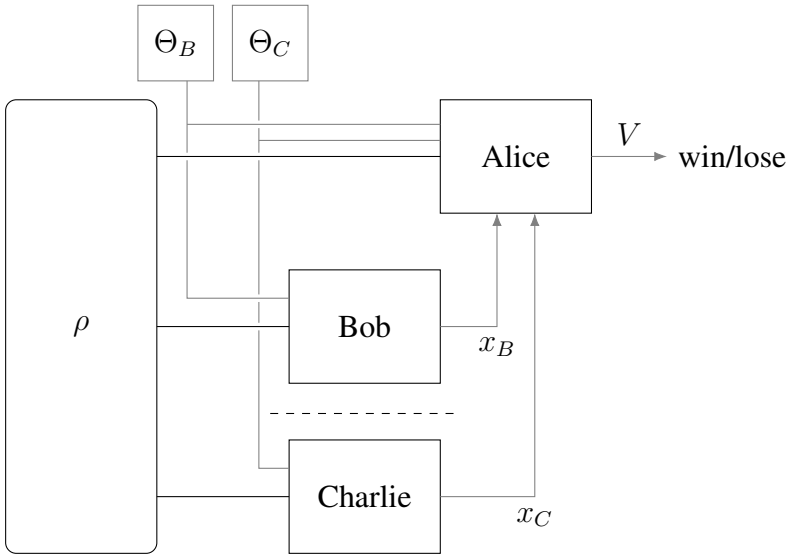


Figure 5.1: Scenario of an XNL game.

This setup is illustrated in Fig. 5.1. We can formally define games and strategies in this setting.

Definition 5.4. A *extended nonlocal (XNL) game* is a tuple $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, \pi, A, V)$ where

- Θ_B and Θ_C are finite sets, representing the possible questions
- X_B and X_C are finite sets, representing the possible answers

- $\pi : \Theta_B \times \Theta_C \to [0,1]$ is a probability distribution
- A is a register, representing Alice's quantum system
- $V : X_B \times X_C \times \Theta_B \times \Theta_C \to \mathcal{P}(A)$ is a function satisfying $V(x_B, x_C|\theta_B, \theta_C) \leq \mathbb{I}_A$, called the *predicate.*

In this definition, it is possible to pack the probability distribution and the predicate together in a function $K : X_B \times X_C \times \Theta_B \times \Theta_C \to \mathcal{P}(A)$ defined $K(x_B, x_C, \theta_B, \theta_C) = \pi(\theta_B, \theta_C)V(x_B, x_C|\theta_B, \theta_C)$, called an *assemblage*. It is possible to see the assemblage as something like a joint probability distribution of which the predicate is the conditional probability distribution with marginal π.

Next, we define the strategies that Bob and Charlie may use to play the game.

Definition 5.5. Let $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, \pi, A, V)$ be an XNL game. A *strategy* for $\mathtt{G}$ is a tuple $\mathtt{S} = \big(B, C, \{B^{\theta_B}\}_{\theta_B \in \Theta_B}, \{C^{\theta_C}\}_{\theta_C \in \Theta_C}, \rho\big)$, where

- B and C are registers, representing Bob and Charlie's quantum systems
- $B^{\theta_B} : X_B \to \mathcal{P}(B)$ and $C^{\theta_C} : X_C \to \mathcal{P}(C)$ are POVMs, representing Bob and Charlie's measurements
- $\rho \in \mathcal{D}(ABC)$ is a shared quantum state.

The *winning probability* of a strategy $\mathtt{S}$ for $\mathtt{G}$ is

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) = \mathop{\mathbb{E}}_{(\theta_B,\theta_C)\leftarrow\pi} \sum_{\substack{x_B \in X_B \\ x_C \in X_C}} \mathrm{Tr}\big[(V(x_B, x_C|\theta_B, \theta_C) \otimes B^{\theta_B}_{x_B} \otimes C^{\theta_C}_{x_C})\rho\big]. \tag{5.2.1}$$

The *optimal winning probability* of a game is $\mathfrak{w}(\mathtt{G}) = \sup_{\mathtt{S}} \mathfrak{w}_{\mathtt{G}}(\mathtt{S})$, where the supremum is over all strategies.

In this definition, we can see that the predicate is seen as a POVM element corresponding to Alice measuring a winning outcome; the other element $\mathbb{I} - V(x_B, x_C|\theta_B, \theta_C)$ corresponds to Alice measuring a losing outcome.

Note also that there is not necessarily a strategy that attains the optimal winning probability — this occurs iff the set of winning probabilities contains its supremum. In general, to work with the optimal winning probability, we would have to deal with a sequence of strategies whose winning probabilities tend to this bound.

Remark. Nonlocal games form a special case of XNL games: they correspond to the games where Alice's space is one-dimensional. Then, the predicate is just a real value in $[0, 1]$ that gives the probability of Alice accepting the set of questions and answers. That is, all Alice's operations are classical. Formally, we write a nonlocal game $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, \pi, v)$, where π is a probability distribution on $\Theta_B \times \Theta_C$ and $v : X_B \times X_C \times \Theta_B \times \Theta_C \to [0, 1]$ is the predicate. This is represented by the XNL game $(\Theta_B, \Theta_C, X_B, X_C, \pi, \{0\}, v[0])$.

Next, given a strategy for an XNL game, it is possible to simplify by purifying all the elements.

Theorem 5.6 (Strategy purification)**.** Let $\mathtt{G}$ be an XNL game and $\mathtt{S}$ be a strategy for $\mathtt{G}$. There exists a strategy $\mathtt{S}'$ such that the state is pure and the measurements are PVMs, that wins with at least the same winning probability.

We call this type of strategy a *pure strategy*, and note that we may assume that any strategy is pure.

Proof: First, we can use Lemma 4.9 to purify the state by enlarging Bob and Charlie's spaces with auxiliary registers that they ignore. Next, for each of the POVMs, we make use of Theorem 4.12 to express it as a PVM conjugated by the adjoint of an isometry. By moving the isometries to the state we find a strategy with a pure state and measurements given by PVMs conjugated by isometries. This strategy has the same winning probability by construction. The conjugated PVM elements remain projectors, but they may sum to less than identity because the conjugating isometry may not be surjective, so it remains to extend them to a full PVM to get the pure strategy. This has greater or equal winning probability. ■

It is possible to construct new XNL games by playing two games in parallel.

Definition 5.7. Let $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, \pi, A, V)$ and $\mathtt{G}' = (\Theta'_B, \Theta'_C, X'_B, X'_C, \pi', A', V')$. Then the *parallel product* of $\mathtt{G}$ and $\mathtt{G}'$ is the XNL game

$$\mathtt{G} \times \mathtt{G}' = (\Theta_B\Theta'_B, \Theta_C\Theta'_C, X_BX'_B, X_CX'_C, \pi\pi', AA', V \otimes V') \tag{5.2.2}$$

where

$$\begin{aligned}(\pi\pi')(\theta_B\theta'_B, \theta_C\theta'_C) &= \pi(\theta_B, \theta_C)\pi'(\theta_C, \theta'_C)\\ (V \otimes V')(x_Bx'_B, x_Cx'_C|\theta_B\theta'_B, \theta_C\theta'_C) &= V(x_B, x_C|\theta_B, \theta_C) \otimes V'(x'_B, x'_C|\theta'_B, \theta'_C).\end{aligned} \tag{5.2.3}$$

By playing the strategies of the two games in parallel, it is possible to see that $\mathfrak{w}(\mathtt{G}\times\mathtt{G}')\geq\mathfrak{w}(\mathtt{G})\mathfrak{w}(\mathtt{G}')$. However, the converse is not necessarily true.

The n-fold product of a game with itself $\mathtt{G}^n=\mathtt{G}\times\cdots\times\mathtt{G}$ is called the *parallel repetition* of $\mathtt{G}$. In a parallel repetition, we can consider not only the total winning probability, but also the winning probability on each of the games.

Definition 5.8. Let $\mathtt{G}=\big(\Theta_B,\Theta_C,X_B,X_C,\pi,A,\{A^\theta\}_{\theta\in\Theta}\big)$ be an XNL game, let $i\in[n]$, and let $\mathtt{S}=\big(B,C,\{B^{\theta_B}\}_{\theta_B\in\Theta_B},\{C^{\theta_C}\}_{\theta_C\in\Theta_C},\rho\big)$ be a strategy for $\mathtt{G}^n$. Then, the *i-th winning probability*[2] of $\mathtt{G}^n$ is

$$\mathfrak{w}^i_{\mathtt{G}^n}(\mathtt{S})=\mathop{\mathbb{E}}_{(\theta_B,\theta_C)\leftarrow\pi^n}\sum_{\substack{y_B\in X_B\\ y_C\in X_C}}\mathrm{Tr}\Big[\Big(V_i(y_B,y_C|\theta_B,\theta_C)\otimes B^{\theta_B}_{y_B,i}\otimes C^{\theta_C}_{y_C,i}\Big)\rho\Big],\tag{5.2.4}$$

where $V_i(y_B,y_C|\theta_B,\theta_C)=V(y_B,y_C|(\theta_B)_i,(\theta_C)_i)_i$ is the predicate acting on Alice's i-th register and $B^{\theta_B}_{y_B,i}=\sum_{\substack{x_B\in X_B^n\\(x_B)_i=y_B}}B^{\theta_B}_{x_B}$ with analogous definition for $C^{\theta_C}_{y_C,i}$.

By definition, the predicate V_i depends only on the i-th terms of the strings θ_B,θ_C. However, this does not hold for the players' measurements. Nevertheless, if they are PVMs, we can get some weaker but important relations on the operators. First, they commute for the same question

$$[B^{\theta_B}_{y_B,i},B^{\theta_B}_{y'_B,j}]=0,\tag{5.2.5}$$

and satisfy the product relation

$$B^{\theta_B}_{x_B}=B^{\theta_B}_{(x_B)_1,1}B^{\theta_B}_{(x_B)_2,2}\cdots B^{\theta_B}_{(x_B)_n,n}.\tag{5.2.6}$$

5.3 Monogamy-of-Entanglement Games

In its most general form, a monogamy-of-entanglement (MoE) game is an extended nonlocal game where Alice's predicates decompose as a measurement followed by sampling from a probability distribution that depends on the question and answer pairs as well as the measurement result. The important difference that arises here is that Alice's measurement can be undertaken *before* she receives the answers from Bob and Charlie. As such, the

[2]This idea has been studied in some form in the context of nonlocal games [Col17], but not for XNL games.

MoE game can be interpreted as measuring how well Bob and Charlie are able to each guess some aspect of Alice's measurement by making use of their entanglement. The monogamy property of entanglement is thus illustrated by the winning probability of such a game being low.

5.3.1 MoE games and generalised MoE games

First, we introduce the original form on an MoE game studied in [TFKW13, JMRW16]. The gameplay proceeds as follows.

1. Bob and Charlie prepare a shared quantum state ρ_{ABC}, after which they are isolated and may no longer communicate.

2. Next, Alice samples a random question θ from a fixed question distribution π. She sends θ to Bob and Charlie.

3. By making local measurements on their spaces, Alice, Bob, and Charlie produce answers x, x_B, and x_C, respectively. Bob and Charlie send their answers to Alice.

4. Bob and Charlie win if $x = x_B = x_C$.

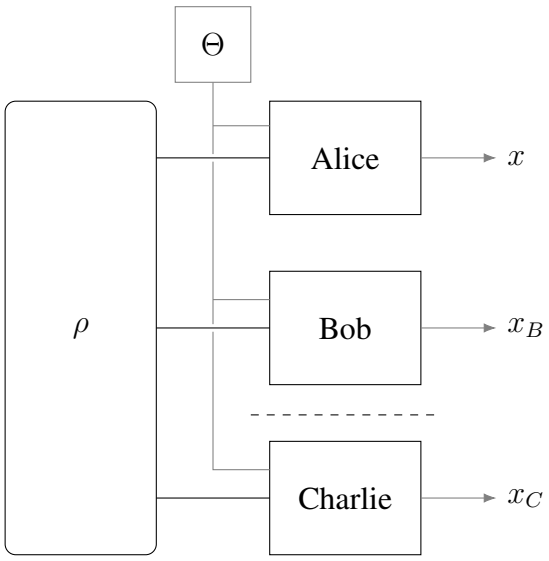


Figure 5.2: Scenario of an MoE game. The players win if the equality $x = x_B = x_C$ holds.

This setup is illustrated in Fig. 5.2. We present this formally.

Definition 5.9. A *monogamy-of-entanglement (MoE) game* is a tuple $\mathtt{G} = (\Theta, X, \pi, A, \{A^\theta\}_{\theta\in\Theta})$ where

- Θ is a finite set, representing the possible questions
- X is a finite set, representing the possible answers
- $\pi : \Theta \to [0, 1]$ is a probability distribution
- A is a register, representing Alice's quantum system
- $A^\theta : Y \to \mathcal{P}(A)$ are POVMs representing Alice's measurements.

The monogamy-of-entanglement principle (Theorem 5.3) relates to the structure of the above MoE games in an insightful way. Consider an MoE game where Alice's measurements are projective — that is where her measurement result is fully dependent on the state and not on auxiliary randomness. Then, first of all, by sharing a maximally-entangled state with Alice, either Bob or Charlie could always guess her measurement result, because he could always undo her transformation into her measurement basis with an appropriate unitary. Now, what if there existed a state that violates the monogamy of entanglement? Then, by acting simultaneously, Bob and Charlie could undo Alice's measurement basis transformation in the same way. Then, they would be able to both simultaneously guess her measurement result. In this way, MoE games would be trivial if there were a state that violates monogamy-of-entanglement. So they can be used as way to measure the influence of monogamy-of-entanglement on a system.

This original definition is too restrictive to capture many of the games highlighting MoE properties. There have been games of the same style that go beyond by allowing the guesses to have errors [TFKW13] or requiring that the players guess different aspects of the measurement result [CLLZ21]. Our more general definition intends to capture all of those that fit in the XNL game model.[3] We capture these additional properties by having Alice compute a predicate that is a function of her, Bob's, and Charlie's measurement results. For example, to allow error, Alice will be able to say that the players win if their results fall within a neighbourhood of her result; or to have the players guess different aspects of the measurement result, she may verify that their results match hers up to some equivalence class. The gameplay proceeds as follows.

[3] This is a novel generalisation.

1. Bob and Charlie prepare a shared quantum state ρ_{ABC}, after which they are isolated and may no longer communicate.

2. Next, Alice samples random questions θ_B, θ_C from a fixed question distribution π. She sends θ_B to Bob and θ_C to Charlie.

3. By making local measurements on their spaces, Alice, Bob, and Charlie produce answers y, x_B, and x_C, respectively. Bob and Charlie send their answers to Alice.

4. Alice samples from a one-bit probability distribution depending on the questions and answers. The players win if she samples 1.

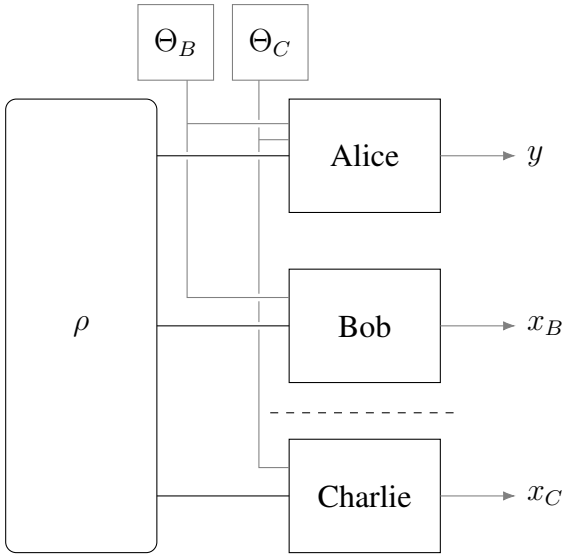


Figure 5.3: Scenario of a GMoE game. The players win with probability $p(x_B, x_C, y|\theta_B, \theta_C)$.

Next, we formalise the above discussion. The setup is presented in Fig. 5.3.

Definition 5.10. A *generalised monogamy-of-entanglement (GMoE) game* is a tuple $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, Y, \pi, p, A, \{A^{\theta_B,\theta_C}\}_{\theta_B\in\Theta_B,\theta_C\in\Theta_C})$ where

- Θ_B and Θ_C are finite sets, representing the possible questions
- X_B and X_C are finite sets, representing the possible answers
- Y is a finite set, representing Alice's intermediate answer

- $\pi : \Theta_B \times \Theta_C \to [0,1]$ is a probability distribution
- $p : X_B \times X_C \times Y \times \Theta_B \times \Theta_C \to [0,1]$ is a function representing the probability of winning with each question and answer set, called the *scalar predicate*
- A is a register, representing Alice's quantum system
- $A^{\theta_B,\theta_C} : Y \to \mathcal{P}(A)$ are POVMs representing Alice's measurements.

A GMoE game in this definition reduces to an extended nonlocal game by taking the predicate $V(x_B, x_C|\theta_B, \theta_C) = \sum_{y\in Y} p(x_B, x_C, y|\theta_B, \theta_C) A_y^{\theta_B,\theta_C}$. As such, a strategy for the GMoE game is a strategy for the equivalent XNL game $(\Theta_B, \Theta_C, X_B, X_C, \pi, A, V)$. In terms of the GMoE game, the winning probability of a strategy $\mathtt{S} = \big(B, C, \{B^{\theta_B}\}, \{C^{\theta_C}\}, \rho\big)$ is

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) = \mathop{\mathbb{E}}_{(\theta_B,\theta_C)\leftarrow\pi} \sum_{\substack{x_B\in X_B\\ x_C\in X_C\\ y\in Y}} p(x_B, x_C, y|\theta_B, \theta_C) \operatorname{Tr}\big[(A_y^{\theta_B,\theta_C} \otimes B_{x_B}^{\theta_B} \otimes C_{x_C}^{\theta_C})\rho\big]. \tag{5.3.1}$$

Further, any MoE $\mathtt{G} = \big(\Theta, X, \pi, A, \{A^\theta\}\big)$ game may be represented as the GMoE game $\big(\Theta, \Theta, X, X, X, \pi', p, A, \{A^{\theta_B,\theta_C}\}\big)$, where the distribution $\pi'(\theta_B, \theta_C) = \pi(\theta_B)\delta_{\theta_B,\theta_C}$, the scalar predicate $p(x_B, x_C, y|\theta_B, \theta_C) = \delta_{x_B,y}\delta_{x_C,y}$, and the measurements $A^{\theta_B,\theta_C} = A^{\theta_B}$. Making use of the representations as a GMoE game and then an XNL game, we see that strategies for $\mathtt{G}$ take the form $\mathtt{S} = \big(B, C, \{B^\theta\}_{\theta\in\Theta}, \{C^\theta\}_{\theta\in\Theta}, \rho\big)$, and have winning probability

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) = \mathop{\mathbb{E}}_{\theta\leftarrow\pi} \sum_{x\in X} \operatorname{Tr}\big[(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)\rho\big]. \tag{5.3.2}$$

Parallel repetition of the XNL game also carries over to MoE and GMoE games. The parallel-repeated predicate is $V^n(x_B, x_C|\theta_B, \theta_C) = \sum_{y\in Y^n} p^n(x_B, x_C, y|\theta_B, \theta_C)(A^n)_y^{\theta_B,\theta_C}$, where $p^n(x_B, x_C, y|\theta_B, \theta_C) = \prod_{i=1}^n p((x_B)_i, (x_C)_i, y_i|(\theta_B)_i, (\theta_C)_i)$ and $(A^n)_y^{\theta_B,\theta_C} = \bigotimes_{i=1}^n A_{y_i}^{(\theta_B)_i,(\theta_C)_i}$. Hence, the i-th winning probability of a strategy can be written

$$\mathfrak{w}_{\mathtt{G}^n}^i(\mathtt{S}) = \mathop{\mathbb{E}}_{(\theta_B,\theta_C)\leftarrow\pi^n} \sum_{\substack{y_B\in X_B\\ y_C\in X_C\\ y\in Y}} p(y_B, y_C, y|\theta) \operatorname{Tr}\Big[\Big((A^n)_{y,i}^{\theta_B,\theta_C} \otimes (B^n)_{y_B,i}^{\theta_B} \otimes (C^n)_{y_C,i}^{\theta_C}\Big)\rho\Big], \tag{5.3.3}$$

where $A^{\theta_B,\theta_C}_{y,i} = \sum_{\substack{x\in Y^n \\ x_i=y}} A^{n\theta_B,\theta_C}_{x} = (A^{(\theta_B)_i,(\theta_C)_i}_{y})_i$.

5.3.2 The TFKW game

To illustrate the MoE game model, we give the foundational example introduced in [TFKW13]. In the basic form of this game, which we call the *TFKW game*, Alice measures her single-qubit system in either the computational or the Hadamard basis. Then, she informs Bob and Charlie of her measurement basis, and to win, they are simultaneously required to guess her measurement result correctly. Formally, this corresponds to the MoE game $\texttt{TFKW} = (\mathbb{Z}_2, \mathbb{Z}_2, \pi, \mathbb{Z}_2, \{A^0, A^1\})$, where $A^\theta_y = |y^\theta\rangle\langle y^\theta|$. For this game, the winning probability of a strategy $\texttt{S}$ simplifies to

$$\mathfrak{w}_{\texttt{TFKW}}(\texttt{S}) = \frac{1}{2}\sum_{\theta,y\in\mathbb{Z}_2} \mathrm{Tr}\big[(\,|y^\theta\rangle\langle y^\theta| \otimes B^\theta_y \otimes C^\theta_y)\rho\big]. \tag{5.3.4}$$

A major result of [TFKW13] is to find the winning probability of this game, and its parallel repetition. They find that

$$\mathfrak{w}(\texttt{TFKW}^n) = \mathfrak{w}(\texttt{TFKW})^n = \left(\cos^2\left(\tfrac{\pi}{8}\right)\right)^n = \left(\tfrac{1}{2} + \tfrac{1}{2\sqrt{2}}\right)^n. \tag{5.3.5}$$

For the TFKW game, there is a simple strategy that wins with this optimal probability. In fact, it is *unentangled* in the sense that Bob and Charlie do not hold any entanglement with Alice on the shared state — their spaces are one-dimensional. This strategy makes use of the *Breidbart state* $|\beta\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$, which has the property of sitting directly in between the computational and Hadamard states on the Bloch sphere. To make use of this strategy, Bob and Charlie simply provide Alice with the Breidbart state and then both guess measurement result 0, irrespective of the question. Formally, this strategy is $\big(\{0\},\{0\},\{B^\theta\},\{C^\theta\},\,|\beta\rangle\langle\beta|\big)$ where $B^\theta_y = C^\theta_y = \delta_{y,0}$. By rotating the state using the Pauli operators, which preserve the computation and Hadamard measurement bases, it is possible to construct other unentangled strategies.[4] We call the states the *Wiesner-Breidbart states*, as they form a pair of mutually unbiased bases corresponding to a rotated version of the Wiesner bases. These states are illustrated in Fig. 5.4. To transform the Wiesner bases

[4] Only one of these optimal strategies was considered previously in [TFKW13].

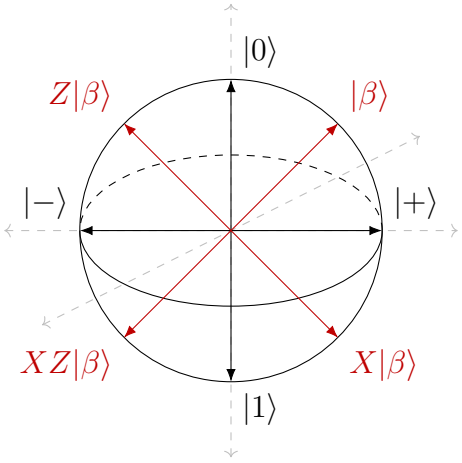


Figure 5.4: Positions of the Wiesner-Breidbart states on the Bloch sphere. They form a pair of bases analogous to the conjugate-coding bases, but rotated by $\frac{\pi}{4}$ so that each vector is located at the midpoint between a vector from the computational basis and one from the Hadamard basis.

State	$\theta = 0$	$\theta = 1$
$\|\beta\rangle$	0	0
$Z\|\beta\rangle$	0	1
$X\|\beta\rangle$	1	0
$XZ\|\beta\rangle$	1	1

Table 5.1: Answers y for the unentangled optimal strategies of the TFKW game. Bob and Charlie reply with the same answer, depending on both θ and the Wiesner-Breidbart state they chose.

to the Wiesner-Breidbart bases, we use the *Breidbart operator* with matrix representation

$$\mathfrak{b} = \begin{bmatrix} \cos\frac{\pi}{8} & \sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & -\cos\frac{\pi}{8} \end{bmatrix}. \tag{5.3.6}$$

The Breidbart operator is hermitian and diagonalises the Hadamard operator as $H = \mathfrak{b}Z\mathfrak{b}$. We have that $\mathfrak{b}|0\rangle = |\beta\rangle$, $\mathfrak{b}|1\rangle = -XZ|\beta\rangle$, $\mathfrak{b}|+\rangle = Z|\beta\rangle$, and $\mathfrak{b}|-\rangle = X|\beta\rangle$.

To construct an optimal strategy from a Wiesner-Breidbart state $X^aZ^b|\beta\rangle$, Bob and Charlie make a guess as a function of a, b, θ. These optimal guesses are given in Table 5.1. Note that for one of the Wiesner-Breidbart bases, the guesses do not depend on the question, but for the other, they do.

The Wiesner-Breidbart states form in fact the only unentangled optimal strategies.

It is a harder task to show that the winning probability of these strategies is actually optimal. We work with an adapted version of the technique of [TFKW13] in Chapter 6; and give an alternate proof of the optimality in the one-qubit case in Chapter 7.

5.4 No-Cloning Games

In XNL games, the referee Alice makes a measurement on a shared state to decide the correct answer. Often, a scenario that is not based on tripartite entanglement is more useful to consider, since the creation of reliable and long-lived entanglement is experimentally difficult. In this case, we can replace Alice's measurement by a state preparation. In such a scenario, the answers of a game are considered to be generated by Alice, rather than measured. We work with a form of game that is, in a sense, dual to GMoE games, and is again played by two players, Bob and Charlie, against an honest referee, Alice. Since these games illustrate the no-cloning property, we call the model the *no-cloning game* model.[5] A no-cloning game proceeds as follows.

1. Alice samples a pair of questions θ_B, θ_C and an index y. She prepares and sends a state $\sigma_y^{\theta_B,\theta_C}$.

2. Bob and Charlie act on the state with some channel Φ. Then, they are isolated and may no longer communicate.

3. Alice shares θ_B with Bob and θ_C with Charlie. They produce answers x_B and x_C, respectively, and send them to Alice.

4. Alice samples from a one-bit probability distribution depending on the questions and answers. The players win if she samples 1.

This setup is illustrated in Fig. 5.5. We can formally define this form of game and its strategies.

Definition 5.11. A *no-cloning (NC) game* is a tuple
$\mathtt{G} = (\Theta_B, \Theta_B, X_B, X_C, Y, \pi, p, A, \{\sigma_y^{\theta_B,\theta_C}\}_{\theta_B\in\Theta_N,\theta_C\in\Theta_C,y\in Y})$, where

- Θ_B and Θ_C are finite sets, representing the possible questions

[5] This model has generally been implicitly considered, in relation to the MoE model, for example in [CLLZ21]. To the best of our knowledge, our formalisation is novel.

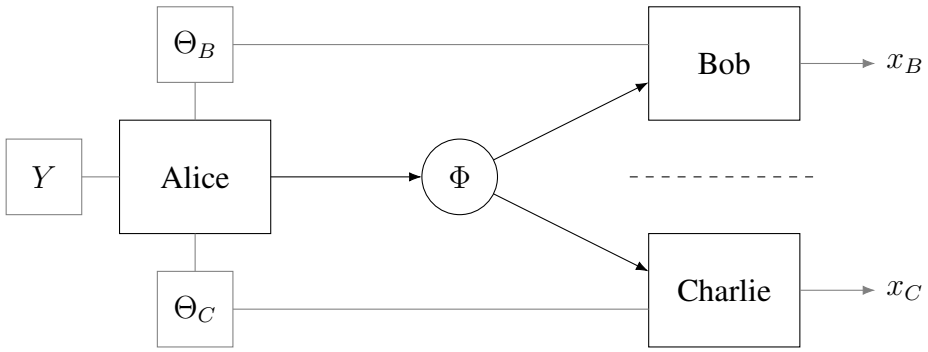


Figure 5.5: Scenario of an NC game. The players win with probability $p(x_B, x_C, y|\theta_B, \theta_C)$.

- X_B and X_C are finite sets, representing the possible answers
- Y is a finite set, representing the possible preparation indices
- $\pi : \Theta_B \times \Theta_C \times Y \to [0, 1]$ is a probability distribution
- $p : X_B \times X_C \times Y \times \Theta_B \times \Theta_C \to [0, 1]$ is a function, called the scalar predicate
- A is a register, representing the quantum system that Alice sends
- $\sigma_y^{\theta_B,\theta_C} \in \mathcal{D}(A)$ are the quantum states that Alice sends.

Definition 5.12. Let $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, Y, \pi, p, A, \{\sigma_y^{\theta_B,\theta_C}\})$ be an NC game. A *strategy* for $\mathtt{G}$ is a tuple $\mathtt{S} = \big(B, C, \{B^{\theta_B}\}_{\theta_B\in\Theta_B}, \{C^{\theta_C}\}_{\theta_C\in\Theta_C}, \Phi\big)$, where

- B and C are registers, representing Bob and Charlie's quantum systems
- $B^{\theta_B} : X_B \to \mathcal{P}(B)$ and $C^{\theta_C} : X_C \to \mathcal{P}(C)$ are POVMs, representing Bob and Charlie's measurements
- $\Phi : \mathcal{L}(A) \to \mathcal{L}(BC)$ is a quantum channel.

The *winning probability* of a strategy $\mathtt{S}$ for $\mathtt{G}$ is

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) = \mathop{\mathbb{E}}_{(\theta_B,\theta_C,y)\leftarrow\pi} \sum_{\substack{x_B\in X_B\\ x_C\in X_C}} p(x_B, x_C, y|\theta_B, \theta_C) \operatorname{Tr}\big[\big(B_{x_B}^{\theta_B} \otimes C_{x_C}^{\theta_C}\big)\Phi(\sigma_y^{\theta_B,\theta_C})\big]. \tag{5.4.1}$$

The *optimal winning probability* of a game is $\mathfrak{w}(\mathtt{G}) = \sup_{\mathtt{S}} \mathfrak{w}_{\mathtt{G}}(\mathtt{S})$, where the supremum is over all strategies.

In the same way as MoE games measure the monogamy-of-entanglement principle, NC games measure the no-cloning principle. That is, if there were a channel that violates the no-cloning theorem (Theorem 4.4), then it would make all no-cloning games trivial. The channel could be used to copy the transmitted state, and therefore Bob and Charlie would be able to win the game as well as a single player.

Remark. NC games can be seen to generalise nonlocal games in a different way to the generalisation of XNL games. Given a nonlocal game $\mathtt{G} = (\Theta_B, \Theta_C, X_B, X_C, \pi, v)$, we can represent it as the NC game $\mathtt{G}' = \left(\Theta_B, \Theta_C, X_B, X_C, \{0\}, \pi, v', \{0\}, \left\{\sigma_y^{\theta_B,\theta_C} = [0]\right\}\right)$ where $v'(x_B, x_C, y|\theta_B, \theta_C) = v(x_B, x_C|\theta_B, \theta_C)$ — that is the NC game where Alice always sends the trivial state and computes a predicate that depends only on Bob and Charlie's questions and answers. As such, there is a bijection between the strategies for these two games that preserves the winning probability, simply by taking $\Phi([0]) = \rho$.

5.4.1 Association to GMoE

It is possible to transform any GMoE game into an NC game.

Definition 5.13. Let $\mathtt{G} = \left(\Theta_B, \Theta_C, X_B, X_C, Y, \pi, p, A, \{A^{\theta_B,\theta_C}\}\right)$ be a GMoE game. The *Choi-corresponding NC game*[6] is the NC game $\mathtt{JG} = \left(\Theta_B, \Theta_C, X_B, X_C, Y, \pi', p, A, \{\sigma_y^{\theta_B,\theta_C}\}\right)$, where $\pi'(\theta_B, \theta_C, y) = \pi(\theta_B, \theta_C)\frac{\operatorname{Tr} A_y^{\theta_B,\theta_C}}{|A|}$ and $\sigma_y^{\theta_B,\theta_C} = \frac{\overline{A_y^{\theta_B,\theta_C}}}{\operatorname{Tr} A_y^{\theta_B,\theta_C}}$, for the complex conjugate with respect to the register basis.

We can see that this map is injective and its image is the set of NC games such that $\sum_{y\in Y} \pi(\theta_B, \theta_C, y)\sigma_y^\theta = \sum_{y\in Y} \pi(\theta_B, \theta_C, y)\mu_A$ for all $(\theta_B, \theta_C) \in \Theta_B \times \Theta_C$. Hence, any NC game in this image corresponds to a unique GMoE game. This correspondence also carries over to strategies.

Proposition 5.14. Let $\mathtt{G} = \left(\Theta_B, \Theta_C, X_B, X_C, Y, \pi, p, A, \{A^{\theta_B,\theta_C}\}\right)$ be a GMoE game. Then, for any strategy $\mathtt{S}$ for $\mathtt{JG}$, there exists a strategy $\tilde{\mathtt{S}}$ for $\mathtt{G}$ such that

$$\mathfrak{w}_{\mathtt{G}}(\tilde{\mathtt{S}}) = \mathfrak{w}_{\mathtt{JG}}(\mathtt{S}). \tag{5.4.2}$$

In particular, that means that $\mathfrak{w}(\mathtt{JG}) \leq \mathfrak{w}(\mathtt{G})$. However, the converse inequality does not always hold.

[6] As for the NC game model, this is a transformation that, as best we know, had only been implicitly utilised. The name was chosen due to its relationship with the Choi representation seen in Proposition 5.14.

Example 5.15. We consider an MoE game closely related to the TFKW game presented above: $\mathtt{G} = \big(\mathbb{Z}_2, \mathbb{Z}_2, \pi, \mathbb{Z}_2^3, \{A^\theta\}\big)$, where $\pi(\theta_B, \theta_C) = \frac{1}{2}$ and

$$A_y^\theta = |0^\theta\rangle\langle 0^\theta| \otimes |y\rangle\langle y| \otimes \mathbb{I} + |1^\theta\rangle\langle 1^\theta| \otimes \mathbb{I} \otimes |y\rangle\langle y| \,. \tag{5.4.3}$$

It is straightforward to see that $\mathfrak{w}(\mathtt{G}) = 1$. In fact, by taking the simple strategy $\mathtt{S} = \big(\{0\}, \{0\}, \{B^\theta\}, \{C^\theta\}, |000\rangle\langle 000|\big)$ where $B_y^\theta = C_y^\theta = \delta_{y,0}$, we have that $\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) = 1$, as the state ensures that Alice always measures 0. However, this is not the case for the Choi-corresponding game $\mathtt{JG} = \big(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \pi', p, \mathbb{Z}_2^3, \{\sigma_y^{\theta_B,\theta_C}\}\big)$. Let $\varepsilon = \frac{\sin^2\frac{\pi}{8}}{4} > 0$ and suppose that there exists a strategy $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \Phi\big)$ for $\mathtt{JG}$ that wins with probability strictly greater than $1-\varepsilon$. Then,

$$\begin{aligned} 1-\varepsilon &< \frac{1}{4}\sum_{\theta,y\in\mathbb{Z}_2} \mathrm{Tr}\big[(B_y^\theta \otimes C_y^\theta)\Phi\big(\sigma_y^\theta\big)\big] \\ &= \frac{1}{16}\sum_{\theta,p,x_0,x_1\in\mathbb{Z}_2} \mathrm{Tr}\Big[(B_{x_p}^\theta \otimes C_{x_p}^\theta)\Phi\big(\,|p^\theta x_0 x_1\rangle\langle p^\theta x_0 x_1|\big)\Big] \\ &\leq \frac{3}{4} + \frac{1}{4}\min_{x_0,x_1\in\mathbb{Z}_2}\frac{1}{4}\sum_{x,p\in\mathbb{Z}_2} \mathrm{Tr}\Big[(B_{x_p}^\theta \otimes C_{x_p}^\theta)\Phi\big(\,|p^\theta x_0 x_1\rangle\langle p^\theta x_0 x_1|\big)\Big]. \end{aligned} \tag{5.4.4}$$

This gives that every term $\frac{1}{4}\sum_{x,p\in\mathbb{Z}_2} \mathrm{Tr}\Big[(B_{x_p}^\theta \otimes C_{x_p}^\theta)\Phi\big(\,|p^\theta x_0 x_1\rangle\langle p^\theta x_0 x_1|\big)\Big]$ must be greater than $4(1-\varepsilon-\frac{3}{4}) = 1-4\varepsilon$. In particular, for $x_0x_1 = 01$, we have

$$1-4\varepsilon < \frac{1}{4}\sum_{x,p\in\mathbb{Z}_2} \mathrm{Tr}\big[(B_p^\theta \otimes C_p^\theta)\Phi\big(\,|p^\theta 01\rangle\langle p^\theta 01|\big)\big]. \tag{5.4.5}$$

This exactly expresses the winning probability of the strategy $\mathtt{S}' = \big(B, C, \{B^\theta\}, \{C^\theta\}, \Phi'\big)$ for the one-qubit TFKW NC game $\mathtt{JTFKW}$, where $\Phi'(\sigma) = \Phi(\sigma \otimes |01\rangle\langle 01|)$. Hence, we know by Proposition 5.14 and the bound on the winning probability of the TFKW game that $1-4\varepsilon < \cos^2\frac{\pi}{8}$, giving $\varepsilon > \frac{\sin^2\frac{\pi}{8}}{4}$. Contradiction. Thus, the winning probability of $\mathtt{JG}$ is strictly less than that of $\mathtt{G}$.

Proof of Proposition 5.14: Let $\mathtt{S} = \big(B, C, \{B^{\theta_B}\}, \{C^{\theta_C}\}, \Phi\big)$ be a strategy for $\mathtt{JG}$. Define the strategy $\tilde{\mathtt{S}} = \big(B, C, \{B^{\theta_B}\}, \{C^{\theta_C}\}, J(\Phi)\big)$ for $\mathtt{G}$, where $J(\Phi)$ is the Choi representa-

tion (Definition 4.17). Then,

$$\begin{aligned}
\mathfrak{w}_{\mathtt{G}}(\tilde{\mathtt{S}}) &= \sum_{\substack{\theta_B\in\Theta_B,\theta_C\in\Theta_C,y\in Y\\ x_B\in X_B,x_C\in X_C}} \pi(\theta_B,\theta_C)p(x_B,x_C,y|\theta_B,\theta_C)\operatorname{Tr}\big[\big(A_y^{\theta_B,\theta_C}\otimes B_{x_B}^{\theta_B}\otimes C_{x_C}^{\theta_C}\big)J(\Phi)\big]\\
&= \sum_{\substack{\theta_B\in\Theta_B,\theta_C\in\Theta_C,y\in Y\\ x_B\in X_B,x_C\in X_C}} \pi(\theta_B,\theta_C)p(x_B,x_C,y|\theta_B,\theta_C)\frac{1}{|A|}\sum_{a,a'\in A}\langle a'|A_y^{\theta_B,\theta_C}|a\rangle\operatorname{Tr}\big[\big(B_{x_B}^{\theta_B}\otimes C_{x_C}^{\theta_C}\big)\Phi(\,|a\rangle\langle a'|)\big]\\
&= \sum_{\substack{\theta_B\in\Theta_B,\theta_C\in\Theta_C,y\in Y\\ x_B\in X_B,x_C\in X_C}} \frac{\pi(\theta_B,\theta_C)}{|A|}p(x_B,x_C,y|\theta_B,\theta_C)\sum_{a,a'\in A}\operatorname{Tr}\Big[\big(B_{x_B}^{\theta_B}\otimes C_{x_C}^{\theta_C}\big)\Phi(\,|a\rangle\langle a|\,\overline{A_y^{\theta_B,\theta_C}}\,|a'\rangle\langle a'|)\Big]\\
&= \sum_{\substack{\theta_B\in\Theta_B,\theta_C\in\Theta_C,y\in Y\\ x_B\in X_B,x_C\in X_C}} \pi'(\theta_B,\theta_C,y)p(x_B,x_C,y|\theta_B,\theta_C)\operatorname{Tr}\big[\big(B_{x_B}^{\theta_B}\otimes C_{x_C}^{\theta_C}\big)\Phi(\sigma_y^{\theta_B,\theta_C})\big] = \mathfrak{w}_{\mathtt{JG}}(\mathtt{S}).
\end{aligned} \tag{5.4.6}$$

■

Chapter 6

Coset States and Games

In this chapter, we study the winning probabilities of the subspace coset games introduced in Section 2.1. First, in Section 6.1, we introduce the subspace coset states used to construct these games. Next, in Section 6.2, we study the coset state games introduced in [CLLZ21] and prove the conjectured upper bound on the winning probability. Next, in Section 6.3, we extend these games to leaky and then also robust versions, and analyse these. Finally, in Section 6.4, we represent the winning probability bounds as a new type of entropic uncertainty relation, which is how we approach these bounds in applications.

This chapter is based on joint work with Thomas Vidick [CV22] and Anne Broadbent [BC22].

6.1 Subspace Coset States

To define the class of subspace coset states on an n-qubit space, we consider the underlying register as the vector space of bit strings $V = \mathbb{Z}_2^n$ over the finite field $\mathbb{Z}_2$. As bit strings, the elements of the canonical basis $E = \{e_1, \ldots, e_n\}$ are the strings e_i that are 1 at position i and 0 elsewhere. Recall that the dot product $V \times V \to \mathbb{Z}_2$ is defined as $u \cdot v = \sum_i u_i v_i$. For any subspace $a \subseteq V$, the *orthogonal subspace* with respect to this dot product is

$$a^\perp = \{v \in V | u \cdot v = 0 \; \forall \; u \in a\} \,. \tag{6.1.1}$$

This satisfies $(a^\perp)^\perp = a$ and $\dim a + \dim a^\perp = \dim V = n$, but in general $\mathrm{span}_{\mathbb{Z}_2}(a \cup a^\perp) = a + a^\perp \neq V$, for example $\{00, 11\}^\perp = \{00, 11\}$, unlike the orthogonal complement for an inner product over $\mathbb{C}$.

A subspace $a \subseteq V$ is called a *register subspace* if it may be expressed as $a = \mathrm{span}_{\mathbb{Z}_2} S$ for some $S \subseteq E$ [JNV+21]. For a register subspace, we have that $a^\perp = \mathrm{span}_{\mathbb{Z}_2} S^c$, and therefore that $a + a^\perp = V$. In this case, we get the canonical isomorphisms $a^\perp \cong V/a$ and $a \cong V/a^\perp$, defined as $u \mapsto u + a$ and $u \mapsto u + a^\perp$, respectively. We can easily express any register subspace by an indicator vector $\iota(a) \in V$ defined by $\iota(a)_i = 1$ if and only if $e_i \in a$.

We define subspace coset states on the space $\mathcal{H}_V \cong (\mathbb{C}^2)^{\otimes n}$.

Definition 6.1 ([CLLZ21, VZ21])**.** Let $a \subseteq V$ be a subspace. Given $t, t' \in V$, the *subspace coset state*

$$|a_{t,t'}\rangle = \frac{1}{\sqrt{|a|}} \sum_{u \in a} (-1)^{u \cdot t'} |u + t\rangle. \tag{6.1.2}$$

If $u \in t + a$ and $u' \in t' + a^\perp$, we have that $|a_{u,u'}\rangle$ is equal to $|a_{t,t'}\rangle$ up to global phase. To make use of this, for any subspace a, we fix a linear map $\mathbb{Z}_2^{n-\dim a} \to \mathbb{Z}_2^n$, $t \mapsto t_a$ such that $t \mapsto t_a + a$ is an isomorphism $\mathbb{Z}_2^{n-\dim a} \cong \mathbb{Z}_2^n/a$, and then take, for $t \in \mathbb{Z}_2^{n-\dim a}$ and $t' \in \mathbb{Z}_2^{\dim a}$, $|a_{t,t'}\rangle := |a_{t_a, t'_{a^\perp}}\rangle$. Then, the coset states $\left\{ |a_{t,t'}\rangle \middle| t \in \mathbb{Z}_2^{n-\dim a}, t' \in \mathbb{Z}_2^{\dim a} \right\}$ are all distinct and form an orthonormal basis of $\mathcal{H}_V$.

If a is a register subspace, there is a particularly good choice of map. For $a^\perp = \mathrm{span}_{\mathbb{Z}_2}\{e_{i_1}, \ldots, e_{i_m}\}$ with $i_1 < i_2 < \ldots < i_m$, we take $t_a = \sum_{j=1}^m t_j e_{i_j}$. This allows us to write the subspace coset state in this case as a Wiesner state $|a_{t,t'}\rangle = |x^\theta\rangle$, where $x = t_a + t'_{a^\perp}$ and $\theta = \iota(a)$.

6.2 Weak and Strong Subspace Coset NC Games

The first constructions of NC games based on subspace coset states were given in [CLLZ21]. They are all played between a referee Alice, who holds the register $V = \mathbb{Z}_2^n$ where n is even, and two cooperating players, Bob and Charlie; and the questions are taken from a set of subspaces A of $\mathbb{Z}_2^n$. The simplest of these, the *weak subspace coset NC game*, matches the traditional structure of an NC game. The gameplay proceeds as follows.

1. Alice samples a uniformly random $a \in A$ and $t, t' \in \mathbb{Z}_2^{n/2}$. She prepares the state $|a_{t,t'}\rangle \in \mathcal{H}_V$ and sends it to Bob and Charlie.

2. They act by an arbitrary channel $\Phi : \mathcal{L}(V) \to \mathcal{L}(BC)$ and then are isolated, so that Bob holds B and Charlie holds C.

3. Alice shares a with Bob and Charlie, and they each make guesses of the pair (t, t').

4. Bob and Charlie win if their guesses are both correct.

This corresponds to the NC game

$$\mathtt{WSC}_{n,A} = \left(A, A, \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^{n/2}, \pi, p, V, \{\sigma_{(t,t')}^{a,b}\}\right), \tag{6.2.1}$$

where the distribution $\pi(a, b, t, t') = \frac{\delta_{a,b}}{|A|2^n}$, the predicate $p((t_B, t'_B), (t_C, t'_C), (t, t')|a, b) = \delta_{t_B,t}\delta_{t_C,t}\delta_{t'_B,t'}\delta_{t'_C,t'}$, and the state $\sigma_{(t,t')}^{a,b} = |a_{t,t'}\rangle\langle a_{t,t'}|$. Because of its simple structure, this is the Choi-corresponding NC game of an MoE game, not just of a more general GMoE game.

The more useful version of this game, the *strong subspace coset NC game* is easier to win and does not follow the traditional structure. It proceeds as follows.

1. Alice samples a uniformly random $a \in A$ and $t, t' \in \mathbb{Z}_2^{n/2}$. She prepares the state $|a_{t,t'}\rangle \in \mathcal{H}_V$ and sends it to Bob and Charlie.

2. They act by an arbitrary channel $\Phi : \mathcal{L}(V) \to \mathcal{L}(BC)$ and then are isolated, so that Bob holds B and Charlie holds C.

3. Alice shares a with Bob and Charlie. Bob makes a guess of t and Charlie makes a guess of t'.

4. Bob and Charlie win if their guesses are both correct.

Again, this may be represented formally as the NC game

$$\mathtt{SSC}_{n,A} = \left(A, A, \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^{n/2}, \pi, p, V, \{\sigma_{(t,t')}^{a,b}\}\right), \tag{6.2.2}$$

where $\pi(a, b, t, t') = \frac{\delta_{a,b}}{|A|2^n}$, $p(t_B, t'_C, (t, t')|a, b) = \delta_{t_B,t}\delta_{t'_C,t'}$, and $\sigma_{(t,t')}^{a,b} = |a_{t,t'}\rangle\langle a_{t,t'}|$.

Directly from the definitions, we see that any strategy for the weak game may be used to play the strong one (Bob does not send t'_B and Charlie does not send t_C), and therefore the winning probability $\mathfrak{w}(\mathtt{SSC}_{n,A}) \geq \mathfrak{w}(\mathtt{WSC}_{n,A})$. In particular, any upper bound on the winning probability of the strong game also provides an upper bound for the weak game.

Finally, it is easy to check that both of the games above are in the image of the Choi correspondence. Hence, we can also represent them as GMoE games where Alice measures in a basis of coset states. We will make use of this correspondence to upper-bound the winning probabilities of the games.

6.2.1 Bounding the winning probability

In this section, we prove the following theorem.

Theorem 6.2. Let $n \in \mathbb{N}$ be even and let A be either the collection of all subspaces of dimension $n/2$ or the collection of register subspaces of dimension $n/2$ in $\mathbb{Z}_2^n$. Then,

$$\mathfrak{w}(\mathtt{SSC}_{n,A}) \leq \sqrt{e}\big(\cos\tfrac{\pi}{8}\big)^n. \tag{6.2.3}$$

To upper bound the winning probability of the strong subspace coset monogamy game, we adapt a technique of [TFKW13]. This technique relies on a general bound on the norm of a sum of positive operators.

Definition 6.3. Let S be a finite set. A *family of mutually orthogonal permutations* of S is a collection of bijections $\pi_s : S \to S$ for all $s \in S$ such that $\pi_s \circ \pi_t^{-1}$ has a fixed point iff $s = t$.

Note that a family of mutually orthogonal permutations always exists. By making the identification $S \cong \mathbb{Z}_{|S|}$, we take $\pi_s(t) = s + t$. Then, $\pi_s \circ \pi_t^{-1} = \pi_{s-t}$ so it only has a fixed point if $s - t = 0$.

Lemma 6.4 (Lemma 2 in [TFKW13])**.** Let $P^s \in \mathcal{P}(\mathcal{H})$ for $s \in S$ be a collection of positive operators. For any family of mutually orthogonal permutations $\pi_s : S \to S$ then

$$\Big\|\sum_{s\in S} P^s\Big\| \leq \sum_{s\in S} \max_{t\in S} \Big\|\sqrt{P^t}\sqrt{P^{\pi_s(t)}}\Big\|.$$

Proof: Consider the operator A on $\mathcal{H}\otimes\mathcal{H}_S$ defined as $A = \sum_s \sqrt{P^s}\otimes |s\rangle\langle s_0|$ for some fixed $s_0 \in S$. Then $A^\dagger A = \sum_s P^s \otimes |s_0\rangle\langle s_0|$, so $\|A^\dagger A\| = \|\sum_s P^s\|$. By the C^* identity, this is equal to $\|AA^\dagger\| = \big\|\sum_{s,s'} \sqrt{P^s}\sqrt{P^{s'}} \otimes |s\rangle\langle s'|\big\|$. By orthogonality of the permutations, $\sum_{s,s'} \sqrt{P^s}\sqrt{P^{s'}} \otimes |s\rangle\langle s'| = \sum_s \sum_t \sqrt{P^t}\sqrt{P^{\pi_s(t)}} \otimes |t\rangle\langle \pi_s(t)|$. Then, using the triangle inequality,

$$\begin{aligned}\|AA^\dagger\| &\leq \sum_s \Big\|\sum_t \sqrt{P^t}\sqrt{P^{\pi_s(t)}} \otimes |t\rangle\langle \pi_s(t)|\Big\| = \sum_s \Big\|\sum_t \sqrt{P^t}\sqrt{P^{\pi_s(t)}} \otimes |t\rangle\langle t|\Big\| \\ &= \sum_s \max_t \Big\|\sqrt{P^t}\sqrt{P^{\pi_s(t)}}\Big\|.\end{aligned} \tag{6.2.4}$$

■

To make use of this bound, we need two things: a family of mutually orthogonal permutations of a relevant set, and the value of the overlaps of relevant operators. We begin with the former. By fixing a basis, we can represent the subspaces spanned by subsets of this basis by indicator vectors — generalising the presentation of register subspaces. As such, the relevant set for the orthogonal permutations is

$$S = \{x \in \mathbb{Z}_2^n || x| = n/2\}\,. \tag{6.2.5}$$

The size $|S| = \binom{n}{n/2} =: N$, so to find a family of mutually orthogonal permutations, it suffices to find N permutations and show that they are mutually orthogonal.

Lemma 6.5. There are mutually orthogonal permutations $\pi_1, \ldots, \pi_N$ of S such that, for each $k \in \{0, \ldots, n/2\}$, there are exactly $\binom{n/2}{k}^2$ permutations π_j such that the number of positions at which x and $\pi_j(x)$ are both 1 is $\frac{n}{2} - k$ for any $x \in S$.

We use a construction based on graph theory. It requires only some fundamental concepts, for which we refer to [Die18]. An example of the construction is given in Fig. 6.1.
Proof: Let $k \in \{1, \ldots, n/2\}$. We take $G_{n,k}$ to be the graph with vertex set S and an edge between any $x, x' \in S$ such that the number of positions at which x and x' are both 1 is exactly $\frac{n}{2} - k$.

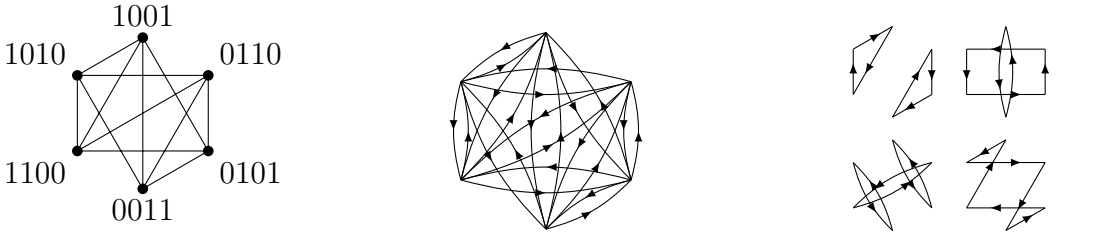
We claim that the minimum degree d_k of $G_{n,k}$ (the number of edges on each vertex) is at least $\binom{n/2}{k}^2$. Indeed, for any $x \in S$, we can define distinct x' that are connected to it in $G_{n,k}$ by choosing k locations among the $\frac{n}{2}$ 1 positions of x, k locations among the $\frac{n}{2}$ 0 positions, and flipping those values.

For each edge in $G_{n,k}$, create two directed edges to obtain a directed graph $\tilde{G}_{n,k}$. In $\tilde{G}_{n,k}$ each vertex has in-degree at least d_k, and out-degree at least d_k. Thus we can find d_k non-overlapping oriented vertex cycle covers of $\tilde{G}_{n,k}$ (closed, potentially disjoint, paths through the graph that follow the directed edges and pass through every vertex) — call them $c_{k,1}, \ldots, c_{k,d_k}$.[1] To each oriented vertex cycle cover $c_{k,i}$, associate a permutation $\pi_{k,i}$ of S by taking $\pi_{k,i}(x)$ to be the vertex connected to x on the directed edge out. By construction, for any $i \neq i'$, $\pi_{k,i}$ and $\pi_{k,i'}$ are orthogonal since the cycle covers share no edges.

For $k = 0$, set $\pi_{0,1}$ to be the identity permutation of S.

We observe that for $k \neq k'$ and any i, i', it must be that $\pi_{k,i}$ and $\pi_{k',i'}$ are orthogonal permutations. This is because two elements of S can be connected by an edge in at most

[1] To show this, find a first cycle cover in an arbitrary way and remove all edges used. This reduces both the out- and in-degrees by exactly 1. Repeat until the minimum degree reaches zero.



(a) The graph $G_{4,1}$. (b) The graph $\tilde{G}_{4,1}$. (c) A set of cycle covers.

Figure 6.1: Graph construction from Lemma 6.5 in the case of $n = 4, k = 1$.

one of the graphs $G_{n,k}$. To conclude that we have N mutually orthogonal permutations, we have by the Vandermonde identity that we have constructed

$$\sum_{k=0}^{n/2} \binom{n/2}{k}^2 = \binom{n}{n/2} = N \tag{6.2.6}$$

permutations, as desired. ■

Now, we work out the next preliminary result: the overlap we use.

Lemma 6.6. For any $a, b \subseteq \mathbb{Z}_2^n$ subspaces of dimension $n/2$, and $t', s \in \mathbb{Z}_2^{n/2}$ we have that the overlap

$$\left\| \sum_{t \in \mathbb{Z}_2^{n/2}} |a_{t,t'}\rangle\langle a_{t,t'}| \sum_{s' \in \mathbb{Z}_2^{n/2}} |b_{s,s'}\rangle\langle b_{s,s'}| \right\| \leq \sqrt{2^{\dim(a \cap b) - \frac{n}{2}}}. \tag{6.2.7}$$

Proof: First, we note that

$$\begin{aligned} \sum_{s' \in \mathbb{Z}_2^{n/2}} |b_{s,s'}\rangle\langle b_{s,s'}| &= \sum_{s' \in \mathbb{Z}_2^{n/2}} \frac{1}{|b|} \sum_{v,v' \in b} (-1)^{s'_{b^\perp} \cdot (v+v')} |v + s_b\rangle\langle v' + s_b| \\ &= \sum_{v \in b} |v + s_b\rangle\langle v + s_b| =: \Pi_{b+s_b}, \end{aligned} \tag{6.2.8}$$

the projector onto $\operatorname{span}\{|v\rangle | v \in b + s_b\}$. Then, the norm we want to bound may be expressed as

$$\left\| \sum_{t \in \mathbb{Z}_2^{n/2}} |a_{t,t'}\rangle\langle a_{t,t'}| \, \Pi_{b+s_b} \right\| = \left\| \sum_{t \in \mathbb{Z}_2^{n/2}} \Pi_{b+s_b} \, |a_{t,t'}\rangle\langle a_{t,t'}| \, \Pi_{b+s_b} \right\|^{1/2}, \tag{6.2.9}$$

using the fact that $\|A\|^2 = \|A^\dagger A\|$ and the operators $|a_{t,t'}\rangle\langle a_{t,t'}|$ are orthogonal projectors. Next, noting that $\Pi_{b+s_b}|a_{t,t'}\rangle$ is a superposition over elements of $(b+s_b)\cap(a+t_a)$, they are orthogonal for different values of t. Thus, bounding the norm as a sum of hermitian operators with orthogonal support,

$$\Big\| \sum_{t\in\mathbb{Z}_2^{n/2}} \Pi_{b+s_b}\,|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+s_b} \Big\| = \max_t \|\Pi_{b+s_b}\,|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+s_b}\|. \tag{6.2.10}$$

Finally, using the fact that each term is the norm of a rank one operator

$$\|\Pi_{b+s_b}\,|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+s_b}\| = \langle a_{t,t'}|\Pi_{b+s_b}|a_{t,t'}\rangle = \tfrac{|(b+s_b)\cap(a+t_a)|}{|a|} \le \tfrac{|a\cap b|}{|a|}, \tag{6.2.11}$$

so we have the upper bound $\sqrt{\frac{|a\cap b|}{|a|}} = \sqrt{2^{\dim(a\cap b)-n/2}}$. ■

Before we proceed to the proof of the theorem, we need a generic bound that we use to simplify the final result.

Lemma 6.7. For any even integer $n \ge 2$,

$$\frac{1}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 \sqrt{2^{-k}} \le \sqrt{e}\Big(\cos\frac{\pi}{8}\Big)^n. \tag{6.2.12}$$

Proof: We bound $\binom{n/2}{k} \le \binom{n/2}{\lfloor n/4\rfloor}$ for any $k \in \{0,\ldots,\frac{n}{2}\}$ and

$$\begin{aligned} \frac{\binom{n/2}{\lfloor n/4\rfloor}}{\binom{n}{n/2}} &= \frac{1}{2^{\frac{n}{2}}}\Big(1+\frac{1}{n-1}\Big)\Big(1+\frac{1}{n-3}\Big)\cdots\Big(1+\frac{1}{2\lfloor\frac{n}{4}\rfloor+1}\Big) \\ &\le \frac{1}{2^{\frac{n}{2}}}\Big(1+\frac{2}{n}\Big)^{\frac{n}{4}} \le \frac{\sqrt{e}}{2^{\frac{n}{2}}}, \end{aligned} \tag{6.2.13}$$

which gives

$$\begin{aligned} \frac{1}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 \sqrt{2^{-k}} \le \frac{\binom{n/2}{\lfloor n/4\rfloor}}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k} \sqrt{2^{-k}} &\le \frac{\sqrt{e}}{2^{\frac{n}{2}}}\Big(1+\frac{1}{\sqrt{2}}\Big)^{\frac{n}{2}} \\ &= \sqrt{e}\Big(\cos\frac{\pi}{8}\Big)^n, \end{aligned} \tag{6.2.14}$$

as claimed. ■

Now, we can prove the theorem of this section. The proof proceeds in three steps: first, we bound the winning probability using overlaps; then, we simplify the overlaps to be able to use Lemma 6.6; and then we simplify the resulting bound.

Proof of Theorem 6.2: First, since $\mathtt{SSC}_{n,A}$ is in the image of the Choi correspondence, there exists a GMoE game $\mathtt{G}$ such that $\mathtt{JG} = \mathtt{SSC}_{n,A}$. Let $\mathtt{S} = (B, C, \{B^a\}, \{C^a\}, \rho)$ be a strategy for $\mathtt{G}$. Using Theorem 5.6, we may in particular assume that the POVM elements are all projectors. Then, the winning probability

$$\begin{aligned}\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) &= \mathop{\mathbb{E}}_{a\in A} \sum_{t,t'\in\mathbb{Z}_2^n} \mathrm{Tr}[(\,|a_{t,t'}\rangle\langle a_{t,t'}| \otimes B_t^a \otimes C_{t'}^a)\rho] \\ &\leq \Big\| \mathop{\mathbb{E}}_{a\in A} \sum_{t,t'\in\mathbb{Z}_2^n} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes B_t^a \otimes C_{t'}^a \Big\|.\end{aligned} \tag{6.2.15}$$

By setting $P^a = \sum_{t,t'\in\mathbb{Z}_2^n} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes B_t^a \otimes C_{t'}^a$, this is the norm of a sum of positive operators — in fact, of projectors. Next, we split the expectation over A into two: first, a uniform expectation over the bases of $\mathbb{Z}_2^n$, then over the subspaces spanned by subsets of that basis. In the case that A is the set of all subspaces of dimension $n/2$, this gives

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) \leq \Big\| \mathop{\mathbb{E}}_{\substack{\beta\subseteq\mathbb{Z}_2^n \\ \text{basis}}} \mathop{\mathbb{E}}_{\substack{\gamma\subseteq\beta \\ |\gamma|=n/2}} P^{\mathrm{span}_{\mathbb{Z}_2}\gamma} \Big\| \leq \mathop{\mathbb{E}}_{\substack{\beta\subseteq\mathbb{Z}_2^n \\ \text{basis}}} \frac{1}{\binom{n}{n/2}} \Big\| \sum_{\substack{\gamma\subseteq\beta \\ |\gamma|=n/2}} P^{\mathrm{span}_{\mathbb{Z}_2}\gamma} \Big\|. \tag{6.2.16}$$

In the case that A is only the set of all register subspaces, we only need to consider one basis $\beta = E$, and so we can express the winning probability similarly as $\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) \leq \frac{1}{\binom{n}{n/2}} \Big\| \sum_{\gamma\subseteq E,|\gamma|=n/2} P^{\mathrm{span}_{\mathbb{Z}_2}\gamma} \Big\|$. In either case, fix an ordered basis β and for $x \in \mathbb{Z}_2^n$, write a_x for the subspace spanned by $\gamma \in \beta$ with indicator vector x. With this, we can use the construction of Lemma 6.5 in Lemma 6.4 to bound

$$\frac{1}{\binom{n}{n/2}} \Big\| \sum_{\substack{\gamma\subseteq\beta \\ |\gamma|=n/2}} P^{\mathrm{span}_{\mathbb{Z}_2}\gamma} \Big\| = \frac{1}{\binom{n}{n/2}} \Big\| \sum_{x\in S} P^{a_x} \Big\| \leq \frac{1}{N} \sum_{i=1}^{N} \max_{x\in S} \|P^{a_x} P^{a_{\pi_i(x)}}\|, \tag{6.2.17}$$

where $N = \binom{n}{n/2}$. Now, we fix subspaces a, b, and simplify the overlap $\|P^a P^b\|$. Defining operators $P = \sum_{t,t'} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes \mathbb{I}_B \otimes C_{t'}^a$ and $Q = \sum_{s,s'} |b_{s,s'}\rangle\langle b_{s,s'}| \otimes B_s^b \otimes \mathbb{I}_C$, we have that $P^a \leq P$ and $P^b \leq Q$. Then, the norm

$$\|P^a P^b\|^2 = \sup_{|v\rangle\in\mathrm{im}\, P^b, \||v\rangle\|\leq 1} \langle v|P^a|v\rangle \leq \sup_{|v\rangle\in\mathrm{im}\, Q, \||v\rangle\|\leq 1} \langle v|P|v\rangle = \|PQ\|^2. \tag{6.2.18}$$

Thus,

$$\begin{aligned}\|P^a P^b\| &\leq \Big\|\sum_{t',s}\sum_{t} |a_{t,t'}\rangle\langle a_{t,t'}| \sum_{s'} |b_{s,s'}\rangle\langle b_{s,s'}| \otimes B_s^b \otimes C_{t'}^a\Big\| \\ &\leq \max_{t',s}\Big\|\sum_{t} |a_{t,t'}\rangle\langle a_{t,t'}| \sum_{s'} |b_{s,s'}\rangle\langle b_{s,s'}|\Big\|,\end{aligned} \tag{6.2.19}$$

since the terms $B_s^b \otimes C_{t'}^a$ are orthogonal projectors. Then, using Lemma 6.6, we get $\|P^a P^b\| \leq \sqrt{2^{\dim(a\cap b)-n/2}}$. For indicator vectors $x, y \in \mathbb{Z}_2^n$, the dimension of the intersection $\dim(a_x \cap a_y) = |x \wedge y|$, the number of bits on which the two strings are both 1. By construction of the family of mutually orthogonal permutations, there are $\binom{n/2}{k}^2$ values of i such that $|x \wedge \pi_i(x)| = n/2 - k$ for all x. Thus, we get that

$$\frac{1}{N}\Big\|\sum_{x\in S} P^{a_x}\Big\| \leq \frac{1}{N}\sum_{i=1}^{N}\max_{x\in S}\sqrt{2^{|x\wedge\pi_i(x)|-\frac{n}{2}}} = \frac{1}{\binom{n}{n/2}}\sum_{k=1}^{n/2}\binom{n/2}{k}^2\sqrt{2^{-k}}. \tag{6.2.20}$$

Finally, using Lemma 6.7, we can bound this by $\sqrt{e}\big(\cos\frac{\pi}{8}\big)^n$, which provides the bound for any strategy $\mathfrak{w}(\mathtt{SSC}_{n,A}) \leq \mathfrak{w}(\mathtt{G}) \leq \sqrt{e}\big(\cos\frac{\pi}{8}\big)^n$ ■

6.3 Leaky Subspace Coset NC Game

We exhibit an even stronger version of the NC properties above by showing that the same bound holds on a family of games that can only be easier to win. In the same setting as above, the game proceeds as follows:

1. Alice samples a uniformly random subspace $a \in A$ and $t, t' \in \mathbb{Z}_2^{n/2}$. She prepares the state $|a_{t,t'}\rangle \in \mathcal{H}_V$ and sends it to Bob and Charlie.

2. They act by an arbitrary channel $\Phi : \mathcal{L}(V) \to \mathcal{L}(BC)$ and then are isolated, so that Bob holds B and Charlie holds C.

3. Alice shares a with Bob and Charlie.

4. Bob makes a guess t_B of t, which is then given to Charlie; Charlie makes a guess t'_C of t'.

5. Bob and Charlie win if their guesses are both correct.

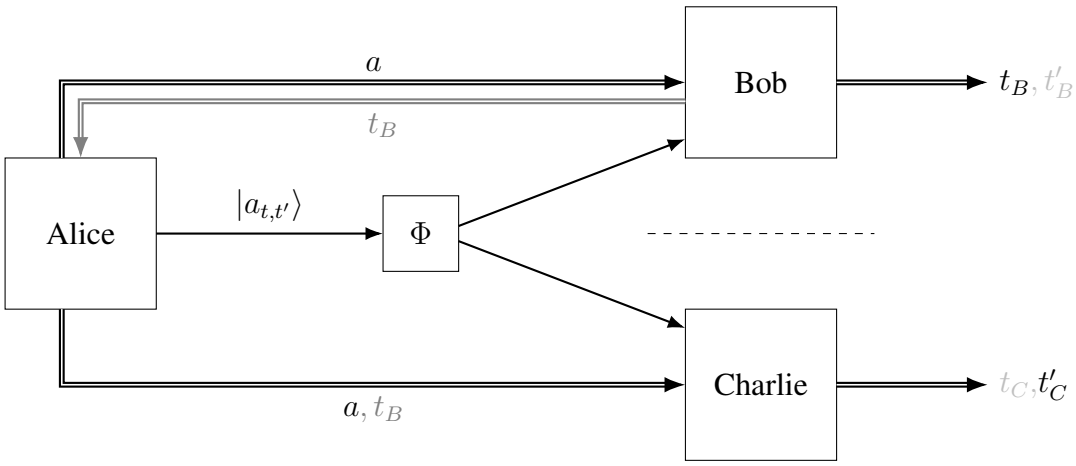


Figure 6.2: The subspace coset NC games. The additional guesses Bob and Charlie need to make in the weak NC game are given in light gray, and the additional interaction step in the leaky NC game is given in dark gray.

We call this the *leaky subspace coset NC game*. The scenario is illustrated in Fig. 6.2. The description of the game above does not immediately allow it to be expressed as an NC game. An alternate but equivalent way to play the game is to have Alice provide Charlie with the correct value of t rather than Bob's guess. The equivalence can be seen by noting that, in the original interpretation, only the cases when Bob's guess is correct are relevant to the computation of the winning probability. In this way, the game admits a description as the NC game

$$\mathtt{LSC}_{n,A} = \left(A, A \times \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2}, \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^{n/2}, \pi, p, V, \{\sigma_{t,t'}^{a,(b,t_0)}\}\right), \tag{6.3.1}$$

where the distribution $\pi(a,(b,t_0),t,t') = \frac{\delta_{a,b}\delta_{t,t_0}}{|A|2^n}$, the predicate $p(t_B,t'_C,t,t'|a,(b,t_0)) = \delta_{t_B,t}\delta_{t'_C,t'}$, and the state $\sigma_{t,t'}^{a,(b,t_0)} = |a_{t,t'}\rangle\langle a_{t,t'}|$.

However, unlike the weak and strong NC games, this NC game is not in the image of GMoE games by the Choi correspondence. Nevertheless, this does not stop us from effecting the transformation to the entanglement-based picture in the same way. That is,

for a strategy $\mathtt{S}$ for $\mathtt{LSC}_{n,A}$, we can express the winning probability

$$\begin{aligned}\mathfrak{w}_{\mathtt{LSC}_{n,A}}(\mathtt{S}) &= \mathop{\mathbb{E}}_{a\in A;t,t'\in\mathbb{Z}_2^{n/2}} \mathrm{Tr}\big[(B_t^a\otimes C_{t'}^{a,t})\Phi(\,|a_{t,t'}\rangle\langle a_{t,t'}|)\big] \\ &= \mathop{\mathbb{E}}_{a\in A}\sum_{t,t'\in\mathbb{Z}_2^{n/2}} \mathrm{Tr}\big[(\,|a_{t,t'}\rangle\langle a_{t,t'}|\otimes B_t^a\otimes C_{t'}^{a,t})J(\Phi)\big].\end{aligned} \tag{6.3.2}$$

6.3.1 Bounding the winning probability

Now, we can formally express the bound on the leaky subspace coset NC game.

Theorem 6.8. Let $n\in\mathbb{N}$ and A be either the collection of register subspaces of dimension $n/2$ or the collection of all subspaces of dimension $n/2$ of $\mathbb{Z}_2^n$. Then,

$$\mathfrak{w}(\mathtt{LSC}_{n,A})\leq\sqrt{e}(\cos\tfrac{\pi}{8})^n. \tag{6.3.3}$$

To show this, we proceed in a very similar way to Theorem 6.2. First, we adapt Lemma 6.6.

Lemma 6.9. For any $a,b\in A$, $\|P^aP^b\|\leq\sqrt{2^{\dim(a\cap b)-n/2}}$, where the projectors are $P^a=\sum_{t,t'\in\mathbb{Z}_2^{n/2}}|a_{t,t'}\rangle\langle a_{t,t'}|\otimes B_t^a\otimes C_{t'}^{a,t}$ for B^a and $C^{a,t}$ PVMs.

Proof: First, note that $P^a\leq\sum_{t,t'}|a_{t,t'}\rangle\langle a_{t,t'}|\otimes\mathbb{I}_B\otimes C_{t'}^{a,t}$ and

$$P^b\leq\sum_{u,u'}|b_{u,u'}\rangle\langle b_{u,u'}|\otimes B_u^b\otimes\mathbb{I}_C=\sum_u\Pi_{b+u_b}\otimes B_u^b\otimes\mathbb{I}_C, \tag{6.3.4}$$

where $\Pi_{b+u_b}=\sum_{v\in b+u_b}|v\rangle\langle v|$ is the projector onto $b+u_b$. Then,

$$\begin{aligned}\big\|P^aP^b\big\| &\leq\Big\|\sum_{t,t',u}|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+u_b}\otimes B_u^b\otimes C_{t'}^{a,t}\Big\| \\ &= \max_{u\in\mathbb{Z}_2^{n/2}}\Big\|\sum_{t,t'}|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+u_b}\otimes C_{t'}^{a,t}\Big\|,\end{aligned} \tag{6.3.5}$$

since the B_u^b are orthogonal projectors. Next, by the C^* identity,

$$\Big\|\sum_{t,t'}|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+u_b}\otimes C_{t'}^{a,t}\Big\|=\Big\|\sum_{t,t'}\Pi_{b+u_b}|a_{t,t'}\rangle\langle a_{t,t'}|\,\Pi_{b+u_b}\otimes C_{t'}^{a,t}\Big\|^{1/2}. \tag{6.3.6}$$

Now, the terms in this sum are Hermitian with orthogonal supports, because the operators $\Pi_{b+u_b} |a_{t,t'}\rangle\langle a_{t,t'}| \Pi_{b+u_b}$ provide the orthogonality for different values of t, and for any fixed value of t, $C_{t'}^{a,t}$ provide it for different values of t'. Therefore, we can again decompose this norm as the maximum of the norms of each term. Putting this together, we get

$$\left\|P^a P^b\right\| \leq \max_{t,t',u\in\mathbb{Z}_2^{n/2}} \|\Pi_{b+u_b} |a_{t,t'}\rangle\langle a_{t,t'}| \Pi_{b+u_b}\|^{1/2} = \max_{t,t',u\in\mathbb{Z}_2^{n/2}} \sqrt{\langle a_{t,t'}|\Pi_{b+u_b}|a_{t,t'}\rangle}, \tag{6.3.7}$$

and we complete the proof by noting that

$$\langle a_{t,t'}|\Pi_{b+u_b}|a_{t,t'}\rangle = \frac{1}{2^{n/2}} \sum_{v\in(a+t_a)\cap(b+u_b)} |(-1)^{t'_a{}^{\perp}\cdot v}|^2 \leq \frac{|a\cap b|}{2^{n/2}}. \tag{6.3.8}$$

■

Now, we can proceed to the proof of Theorem 6.8, which follows the method of Theorem 6.2.

Proof of Theorem 6.8: First, for any strategy, we use the Choi representation to upper bound

$$\mathfrak{w}_{\mathrm{LSC}_{n,A}}(\mathtt{S}) \leq \left\|\mathop{\mathbb{E}}_{a\in A} \sum_{t,t'\in\mathbb{Z}_2^{n/2}} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes B_t^a \otimes C_{t'}^{a,t}\right\|. \tag{6.3.9}$$

Using the notation of the previous lemma, this is $\mathfrak{w}_{n,A}(\mathtt{S}) \leq \|\mathbb{E}_a P^a\|$. As before, we split the expectation into two: first we take the average over the bases β of $\mathbb{Z}_2^n$, and then over the subspaces than can be spanned by that basis. Fix an ordered basis β, so that subspaces may be expressed by indicator vectors. It remains to upper bound the norm for that basis, $\|\mathbb{E}_{x\in S} P^{a_x}\|$. Using Lemma 6.4 with the permutations of Lemma 6.5 and then Lemma 6.9, we have, since P^a is a projector,

$$\begin{aligned}\left\|\mathop{\mathbb{E}}_{x\in S} P^{a_x}\right\| &\leq \frac{1}{N}\sum_{i=1}^{N} \max_{x\in S} \|P^{a_x} P^{a_{\pi_i(x)}}\| \leq \frac{1}{N}\sum_{i=1}^{N} \max_{x\in S} \sqrt{2^{|x\wedge\pi_i(x)|-n/2}} \\ &= \frac{1}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 \sqrt{2^{-k}}.\end{aligned} \tag{6.3.10}$$

Using Lemma 6.7 again, this is upper-bounded by $\sqrt{e}(\cos\frac{\pi}{8})^n$, finishing the proof. ■

6.3.2 Robust Subspace Coset Game: Beyond the XNL Model

We construct a more general game based on the subspace coset states by making the leaky NC game robust against errors. To do so, we fix neighbourhoods of 0 $U, U' \subseteq \mathbb{Z}_2^{n/2}$, and modify the leaky MoE game winning condition by saying that Alice accepts if Bob's answer is in $t + U$ and Charlie's is in $t' + U'$. To warrant the name "leaky", we suppose that Charlie gets Bob's potentially erroneous guess of t — but never the actual value of t chosen by Alice — before making his guess. We call this the *robust leaky subspace coset game* $\texttt{RLSC}_{n,A,U,U'}$. In the case of $U = U' = \{0\}$, this reduces to the original leaky MoE game. The gameplay proceeds as follows.

1. Alice samples a uniformly random $a \in A$ and $t, t' \in \mathbb{Z}_2^{n/2}$. She prepares the state $|a_{t,t'}\rangle \in \mathcal{H}_V$ and sends it to Bob and Charlie.

2. They act by an arbitrary channel $\Phi : \mathcal{L}(V) \to \mathcal{L}(BC)$ and then are isolated, so that Bob holds B and Charlie holds C.

3. Alice shares a with Bob and Charlie.

4. Bob makes a guess t_B of t, which is then given to Charlie; Charlie makes a guess t'_C of t'.

5. Bob and Charlie win if $t_B \in t + U$ and $t'_C \in t' + U'$.

Unlike the leaky NC game, this game *cannot* be expressed as an NC game, and consequently it cannot be reformulated as an XNL game. This is because the string t_B that is leaked to Charlie may in part be chosen by Bob — the string is not sampled from a distribution fixed by Alice. Nevertheless, the game constitutes a straightforward generalisation of the leaky NC game. Due to this similarity, we can approach it in the same way.

Definition 6.10. A *strategy* for $\texttt{RLSC}_{n,A,U,U'}$ is a strategy $\mathtt{S} = (B, C, \{B^a\}, \{C^{a,t}\}, \Phi)$ for $\texttt{LSC}_{n,A}$. The *winning probability* of $\mathtt{S}$ is

$$\mathfrak{w}_{\texttt{RLSC}_{n,A,U,U'}}(\mathtt{S}) = \mathop{\mathbb{E}}_{a\in A; t,t'\in\mathbb{Z}_2^n} \sum_{u\in U, u'\in U'} \mathrm{Tr}\big[(B^a_{t+u} \otimes C^{a,t+u}_{t'+u'})\Phi(\,|a_{t,t'}\rangle\langle a_{t,t'}|)\big]. \tag{6.3.11}$$

The winning probability also admits an analogous entanglement-based presentation

$$\mathfrak{w}_{\texttt{RLSC}_{n,A,U,U'}}(\mathtt{S}) = \mathop{\mathbb{E}}_{a\in A} \sum_{t,t'\in\mathbb{Z}_2^n} \sum_{u\in U, u'\in U'} \mathrm{Tr}\big[(\,|a_{t,t'}\rangle\langle a_{t,t'}| \otimes B^a_{t+u} \otimes C^{a,t+u}_{t'+u'})J(\Phi)\big]. \tag{6.3.12}$$

We use the same technique as above to provide a bound on the winning probability of the game. Since the neighbourhoods U, U' are supposed to represent bitwise errors, we make two important restrictions. First, we work only with register subspaces, as each basis element is weight 1. Also, we take the error neighbourhoods to be Hamming balls $U = B(n/2, m)$, $U' = B(n/2, m')$, so that they represent all errors of at most a given weight.

Theorem 6.11. Let A be the set of register subspaces of $\mathbb{Z}_2^n$ of dimension $n/2$. Then, for $m, m' \leq n/4$

$$\mathfrak{w}(\texttt{RLSC}_{n,A,B(n/2,m),B(n/2,m')}) \leq \sqrt{e} 2^{\frac{n}{2}h(\frac{2m}{n})+\frac{n}{4}h(\frac{2m'}{n})} \left(\cos\tfrac{\pi}{8}\right)^n. \tag{6.3.13}$$

Recall that $h(\gamma)$ is the binary entropy function (Definition 3.54).

Note that this bound is not particularly tight. We try to stick with the tightest possible expression throughout the proof before passing to this simple closed-form expression at the very end.

The proof proceeds similarly to Theorem 6.8. First, we need a further robust generalisation of Lemma 6.9.

Lemma 6.12. Let $a, b \subseteq \mathbb{Z}_2^n$ be subspaces of dimension $n/2$, and $U, U' \subseteq \mathbb{Z}_2^{n/2}$ be neighbourhoods of 0. Then,

$$\left\| \sqrt{P^a}\sqrt{P^b} \right\| \leq \max_{t \in \mathbb{Z}_2^n} \left(|(a+b+t) \cap U_b||U||U'| \frac{|a \cap b|}{|a|} \right)^{1/2}, \tag{6.3.14}$$

where $P^a = \sum_{t,t'\mathbb{Z}_2^{n/2}} \sum_{u \in U, u' \in U'} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes B^a_{t+u} \otimes C^{a,t+u}_{t'+u'}$.

Proof: Since $\sum_{v' \in U'} C^{b,s+v}_{s'+v'} \leq \mathbb{I}$ for any $s, s', v \in \mathbb{Z}_2^{n/2}$, we get the bound

$$\begin{aligned} P^b &\leq \sum_{s,s' \in \mathbb{Z}_2^{n/2}; v \in U} |b_{s,s'}\rangle\langle b_{s,s'}| \otimes B^b_{s+v} \otimes \mathbb{I} = \sum_{s \in \mathbb{Z}_2^{n/2}; v \in U} \Pi_{b+s_b} \otimes B^b_{s+v} \otimes \mathbb{I} \\ &= \sum_{s \in \mathbb{Z}_2^{n/2}} \Pi_{\bigcup_{v \in U}(b+(s+v)_b)} \otimes B^b_s \otimes \mathbb{I}. \end{aligned} \tag{6.3.15}$$

Since the right hand side is a projector, we have by the operator monotonicity of the square

root that it is also a bound on $\sqrt{P^b}$. We also bound

$$P^a \leq \sum_{t,t',u,u'} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes \mathbb{I} \otimes C^{a,t+u}_{t'+u'} = \sum_{t,t',u,u'} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \otimes \mathbb{I} \otimes C^{a,t}_{t'}. \tag{6.3.16}$$

Using these,

$$\begin{aligned}
&\left\|\sqrt{P^a}\sqrt{P^b}\right\| \leq \|\sqrt{P^b}P^a\sqrt{P^b}\|^{1/2} \\
&\leq \Big\| \sum_{\substack{t,t',s\in\mathbb{Z}_2^{n/2} \\ u\in U,u'\in U'}} \Pi_{\bigcup_{v\in U}(b+(s+v)_b)} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \, \Pi_{\bigcup_{v\in U}(b+(s+v)_b)} \otimes B^b_s \otimes C^{a,t}_{t'} \Big\|^{1/2} \\
&\leq \max_{s\in\mathbb{Z}_2^{n/2}} \Big\| \sum_{t,t',u,u'} \Pi_{\bigcup_{v\in U}(b+(s+v)_b)} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \, \Pi_{\bigcup_{v\in U}(b+(s+v)_b)} \otimes C^{a,t}_{t'} \Big\|^{1/2}.
\end{aligned} \tag{6.3.17}$$

Next, using the triangle inequality,

$$\left\|\sqrt{P^a}\sqrt{P^b}\right\| \leq \max_s \Big(\sum_u \Big\| \sum_{t,t',u'} \Pi_{\bigcup_v(b+(s+v)_b)} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \, \Pi_{\bigcup_v(b+(s+v)_b)} \otimes C^{a,t}_{t'} \Big\| \Big)^{1/2}. \tag{6.3.18}$$

Now, as the terms $\sum_{u'} \Pi_{\bigcup_v(b+(s+v)_b)} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \, \Pi_{\bigcup_v(b+(s+v)_b)} \otimes C^{a,t}_{t'}$ of the sum are Hermitian with orthogonal supports, we can bound

$$\begin{aligned}
\left\|\sqrt{P^a}\sqrt{P^b}\right\| &\leq \max_s \Big(\sum_u \max_{t,t'} \Big\| \sum_{u'} \Pi_{\bigcup_v(b+(s+v)_b)} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}| \, \Pi_{\bigcup_v(b+(s+v)_b)} \otimes C^{a,t}_{t'} \Big\| \Big)^{1/2} \\
&\leq \max_s \Big(|U| \max_{t,t'} \Big\| \sum_{u'} \Pi_{\bigcup_v(b+(s+v)_b)} |a_{t,t'+u'}\rangle\langle a_{t,t'+u'}| \, \Pi_{\bigcup_v(b+(s+v)_b)} \Big\| \Big)^{1/2}.
\end{aligned} \tag{6.3.19}$$

For each of these terms,

$$\begin{aligned}
&\Big\|\sum_{u'} \Pi_{\bigcup_v (b+(s+v)_b)} \, |a_{t,t'+u'}\rangle\langle a_{t,t'+u'}| \, \Pi_{\bigcup_v (b+(s+v)_b)}\Big\| \\
&\leq \sum_{u'} \Big\| \Pi_{\bigcup_v (b+(s+v)_b)} \, |a_{t,t'+u'}\rangle\langle a_{t,t'+u'}| \, \Pi_{\bigcup_v (b+(s+v)_b)}\Big\| \\
&= \sum_{u'} \langle a_{t,t'+u'}|\Pi_{\bigcup_v (b+(s+v)_b)}|a_{t,t'+u'}\rangle = |U'|\frac{|(a+t_a)\cap \bigcup_v (b+(s+v)_b)|}{|a|}.
\end{aligned} \tag{6.3.20}$$

The cardinality of the intersection may be written as

$$\begin{aligned}
\Big|(a+t_a)\cap \bigcup_v (b+(s+v)_b)\Big| &= |a\cap b||\{v\in U|(a+t_a)\cap(b+(s+v)_b)\neq \varnothing\}| \\
&= |a\cap b||\{v\in U|t_a+s_b+v_b\in a+b\}| \\
&= |a\cap b||(a+b+t_a+s_b)\cap U_b|.
\end{aligned} \tag{6.3.21}$$

This gives the wanted bound

$$\begin{aligned}
\Big\|\sqrt{P^a}\sqrt{P^b}\Big\| &\leq \max_s \Big(|U|\max_{t,t'}|U'||a\cap b||(a+b+t_a+s_b)\cap U_b|\frac{|a\cap b|}{|a|}\Big)^{1/2} \\
&\leq \max_{t\in\mathbb{Z}_2^n} \Big(|U||U'||(a+b+t)\cap U_b|\frac{|a\cap b|}{|a|}\Big)^{1/2}.
\end{aligned} \tag{6.3.22}$$

■

Now, we proceed to the proof of the theorem.

Proof of Proof of Theorem 6.11: Write $U = B(n/2, m)$ and $U' = B(n/2, m')$. First, we bound the winning probability by an operator norm

$$\mathfrak{w}_{\mathtt{RLSC}_{n,A,U,U'}}(\mathtt{S}) \leq \Big\|\mathop{\mathbb{E}}_{a\in A} P^a\Big\| = \Big\|\mathop{\mathbb{E}}_{x\in S} P^{a_x}\Big\|, \tag{6.3.23}$$

so that we can apply Lemma 6.4 using the same permutations of Lemma 6.5, giving

$$\mathfrak{w}_{\mathtt{RLSC}_{n,A,U,U'}}(\mathtt{S}) \leq \frac{1}{N}\sum_{i=1}^{N} \max_{x\in S} \Big\|\sqrt{P^{a_x}}\sqrt{P^{a_{\pi_i(x)}}}\Big\|. \tag{6.3.24}$$

We use Lemma 6.12 to write the overlap $\left\|\sqrt{P^a}\sqrt{P^b}\right\|$ in terms of $\dim(a \cap b)$. Suppose the spaces $a = \operatorname{span}\gamma$ and $b = \operatorname{span}\eta$. Then $U_b = \{u \in \mathbb{Z}_2^n | u_\eta = 0, |u| \leq m\}$. Thus, as $a + b = \operatorname{span}(\eta \cup \gamma)$, for any $t \in \mathbb{Z}_2^n$,

$$(a + b + t) \cap U_b = \{u \in \mathbb{Z}_2^n | u_{\eta^c \cap \gamma^c} = t_{\eta^c \cap \gamma^c}, u_\eta = 0, |u| \leq m\}. \tag{6.3.25}$$

To maximise the cardinality of this set, we take $t_{\eta^c \cap \gamma^c} = 0$, so

$$\begin{aligned} |(a + b + t) \cap U_b| &= |\{u \in \mathbb{Z}_2^n | u_{\eta \cup \gamma^c} = 0, |u| \leq m\}| \\ &= |B(|\eta^c \cap \gamma|, m)| = |B(n/2 - \dim(a \cap b), m)|. \end{aligned} \tag{6.3.26}$$

This gives $\left\|\sqrt{P^a}\sqrt{P^b}\right\| \leq \sqrt{|B(n/2,m)||B(n/2,m')||B(n/2-\dim(a\cap b),m)|}2^{\dim(a\cap b)/2-n/4}$. Putting this into the bound on the winning probability,

$$\mathfrak{w}_{\mathtt{RLSC}_{n,A,U,U'}}(\mathtt{S}) \leq \frac{1}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 \sqrt{|B(n/2,m)||B(n/2,m')||B(k,m)|2^{-k}}. \tag{6.3.27}$$

We can bound $B(k, m) \leq B(n/2, m)$ and therefore

$$\begin{aligned} \mathfrak{w}_{\mathtt{RLSC}_{n,A,U,U'}}(\mathtt{S}) &\leq \frac{|B(n/2,m)|\sqrt{|B(n/2,m')|}}{\binom{n}{n/2}} \sum_{k=0}^{n/2} \binom{n/2}{k}^2 2^{-k/2} \\ &\leq \sqrt{e}|B(n/2,m)|\sqrt{|B(n/2,m')|}(\cos\tfrac{\pi}{8})^n. \end{aligned} \tag{6.3.28}$$

Using the bound on the volume of a ball $B(n/2, m) \leq 2^{\frac{n}{2}h(\frac{2m}{n})}$ gives the result. ■

6.4 Representation as Entropic Uncertainty Relations

Uncertainty relations have played a foundational role in quantum mechanics, beginning with Heisenberg's uncertainty principle $\Delta x \Delta p \geq \frac{\hbar}{2}$ [Hei27], which states that it is impossible to know the value of the position and momentum of a quantum particle at the same time. Here, the lack of knowledge is quantified using the variances of the respective observables. In quantum information, lack of knowledge is expressed using entropies: Hirschmann [Hir57] first showed a position-momentum entropic uncertainty relation for the differential von Neumann entropy. Deutsch [Deu83] found an entropic uncertainty relation for the von Neumann entropy of finite-dimensional systems, and Maassen and Uffink

[MU88] extended this to a relation in terms of the min-entropy, providing bounds on guessing probability using entropy. On the other hand, Christandl and Winter [CW05] show an entropic uncertainty relation that considers quantum side-information. Tomamichel, Fehr, Kaniewski, and Wehner [TFKW13] synthesize the use of min-entropy and the inclusion of side-information with their entropic uncertainty relation related to an MoE game.

6.4.1 Sequential min-entropy

To pass from the winning probability of an NC game to an entropic uncertainty relation, we define a novel generalisation of the min-entropy.

Definition 6.13. Let ρ be a state supported on not necessarily distinct classical registers $X_1, \ldots, X_n$ and quantum registers $A_1, \ldots, A_n$. For POVMs $M^i : X_i \to \mathcal{P}(A_i)$, write

$$H_{\min}(X_1|M^1(A_1); \ldots; X_n|M^n(A_n))_\rho = -\lg \operatorname{Tr}\left[(\cdots(\rho_{\wedge(M^1(A_1)=X_1)})\cdots)_{\wedge(M^n(A_n)=X_n)}\right], \tag{6.4.1}$$

where $\rho_{\wedge\Omega}$ is the partial state of the event Ω (Eq. (4.2.7)). Then, we define the *sequential min-entropy* of $X_1, \ldots, X_n$ knowing $A_1, \ldots, A_n$ as

$$H_{\min}(X_1|A_1; \ldots; X_n|A_n)_\rho = \inf_{M^1,\ldots,M^n \text{ POVMs}} H_{\min}(X_1|M^1(A_1); \ldots; X_n|M^n(A_n)). \tag{6.4.2}$$

The sequential min-entropy represents the uncertainty of guessing X_1 knowing A_1, followed by guessing X_2 knowing A_2, and so on. Note that the sequential min-entropy is a generalisation of the conditional min-entropy in the sense that they are the same for $n = 1$.

Now, we present a way to expand the sequential min-entropy as an entropic uncertainty relation.

Proposition 6.14. Let ρ be a state supported on classical registers X, Y and quantum registers A, B. Then,

$$H_{\min}(X|A; Y|B)_\rho = \inf_{M:X\to\mathcal{P}(A) \text{ POVM}} \Big(H_{\min}(X|M(A))_\rho + H_{\min}(Y|B)_{\rho_{|(M(A)=X)}} \Big). \tag{6.4.3}$$

Note the contrast between this entropic uncertainty relation and that found in [TFKW13]. Most importantly, their relation considers the min-entropy of the same state on both terms,

whereas ours uses different, albeit closely related, states. This avoids the shortcoming of their entropic uncertainty relation — that the entropy can remain bounded for any dimension of Alice's space — and thus allows us to make use of the full power of the winning probability bound in terms of an entropy.

Proof of Proposition 6.14: This follows immediately from the definition. We have

$$\begin{aligned} H_{\min}(X|A;Y|B) &= \inf_{M,N} -\lg \mathrm{Tr}\left[(\rho_{\wedge(M(A)=X)})_{\wedge(N(B)=Y)}\right] \\ &= \inf_{M,N} -\lg \mathrm{Tr}\left[\rho_{\wedge(M(A)=X)}\right] \mathrm{Tr}\left[(\rho_{|(M(A)=X)})_{\wedge(N(B)=Y)}\right] \\ &= \inf_{M}\Big(-\lg \mathrm{Tr}\left[\rho_{\wedge(M(A)=X)}\right] + \inf_{N} -\lg \mathrm{Tr}\left[(\rho_{|(M(A)=X)})_{\wedge(N(B)=Y)}\right]\Big) \\ &= \inf_{M}\Big(H_{\min}(X|M(A))_{\rho} + H_{\min}(Y|B)_{\rho_{|(M(A)=X)}}\Big) \end{aligned} \tag{6.4.4}$$

■

6.4.2 Relation for the leaky NC game

The winning probability of the leaky NC game $\mathtt{LSC}_{n,A}$ may be phrased using this entropy. First, for registers $T = T' = \mathbb{Z}_2^{n/2}$ and A representing either the register subspaces or all subspaces of $\mathbb{Z}_2^n$ of dimension $n/2$, Alice prepares $\rho_{ATT'} = \mu_A \otimes \mu_T \otimes \mu_{T'}$, and then prepares coset states on $V = \mathbb{Z}_2^n$ accordingly to get

$$\rho_{AA'TT'V} = \mathop{\mathbb{E}}_{a,t,t'} [aatt'] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \,. \tag{6.4.5}$$

Bob and Charlie act with a channel Φ, giving $\rho_{AA'TT'BC} = (\mathrm{id}_{AA'TT'} \otimes \Phi)(\rho_{AA'TT'V})$. In terms of the sequential min-entropy, the leaky NC property is the statement that

$$H_{\min}(T|AB;T'|A'TC)_{\rho} \geq -\lg \mathfrak{w}(\mathtt{LSC}_{n,A}) \geq (-\lg \cos \tfrac{\pi}{8})n - \tfrac{1}{2\ln 2}. \tag{6.4.6}$$

This expression follows directly from the definition. Bob's measurements B_t^a provide a measurement $M : T \to \mathcal{P}(AB)$ where $M_t = \sum_{a\in A}[a] \otimes B_t^a$ and Charlie's measurements $C_{t'}^{a,t}$ provide $N : T' \to \mathcal{P}(A'TC)$ where $N_{t'} = \sum_{a\in A, t\in\mathbb{Z}_2^{n/2}}[at] \otimes C_{t'}^{a,t}$, giving

$$H_{\min}(T|M(AB);T'|N(A'TC))_{\rho} = -\lg \mathfrak{w}_{\mathtt{LSC}_{n,A}}(\mathtt{S}). \tag{6.4.7}$$

The only snarl is that, in general in the definition of the sequential min-entropy, Bob's measurement may not preserve A, since in general M might not be diagonal on A; and similarly Charlie's measurement may not preserve $A'T$. However, since the classical registers are not reused, only the diagonal blocks have any effect, and therefore, we may assume that the measurements are diagonal on the classical registers. As such, the infimum over the measurements is attained by those measurements that correspond to strategies. Note that any MoE or NC game admits an entropic expression of this form.

Using Proposition 6.14, we may express the leaky NC property as an entropic uncertainty relation.

Corollary 6.15 (Leaky NC entropic uncertainty relation)**.** For any POVM $M : T \to \mathcal{P}(AB)$ Bob uses in the leaky NC game, we have

$$H_{\min}(T|M(AB))_\rho + H_{\min}(T'|A'TC)_{\rho_{|(M(AB)=T)}} \geq (-\lg\cos\tfrac{\pi}{8})n - \tfrac{1}{2\ln 2}. \tag{6.4.8}$$

This follows immediately by combining Theorem 6.8 with Proposition 6.14 via Eq. (6.4.6). This is the form of the bound that we make use of for applications.

6.4.3 Relation for the robust game

It will prove useful to express the winning probability of the robust leaky subspace coset game $\texttt{RLSC}_{n,A,U,U'}$ as a sequential min-entropy as well.

Corollary 6.16. Fix a strategy for the (n, A, U, U')-robust leaky monogamy game with $U = B(n/2, m)$ and $U' = 0$. Let the state

$$\sigma_{AA'TT'BC} = \mathop{\mathbb{E}}_{a,t,t',u,u'} [aatt'] \otimes \Phi(\,|a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}|\,). \tag{6.4.9}$$

Then, the sequential min-entropy

$$H_{\min}(T|AB;T'|A'TC)_\sigma \geq \left(-\lg\cos\tfrac{\pi}{8} - \tfrac{1}{(2\ln 2)n}\right)n. \tag{6.4.10}$$

Note that we pack the approximate guessing into the state, so we can derive a result on the sequential min-entropy of that state.

Proof: First, the winning probability may be rewritten as

$$\begin{aligned}\mathfrak{w}_{n,A,U,U'}(\mathtt{S}) &= \mathop{\mathbb{E}}_{a,t,t'} \operatorname{Tr}\Big[(B_t^a \otimes C_{t'}^{a,t})\Phi\Big(\sum_{u,u'} |a_{t+u,t'+u'}\rangle\langle a_{t+u,t'+u'}|\Big)\Big] \\ &= |U||U'| \mathop{\mathbb{E}}_{a,t,t'} \operatorname{Tr}\Big[(B_t^a \otimes C_{t'}^{a,t})\sigma_{BC}^{a,t,t'}\Big],\end{aligned} \tag{6.4.11}$$

Thus, using the bound $\mathfrak{w}_{n,A,U,U'}(\mathtt{S}) \leq \sqrt{e}|U|\sqrt{|U'|}\big(\cos\frac{\pi}{8}\big)^n$ of Theorem 6.11 with $|U'| = 1$, $\mathbb{E}_{a,t,t'} \operatorname{Tr}\Big[(B_t^a \otimes C_{t'}^{a,t})\sigma_{BC}^{a,t,t'}\Big] \leq \sqrt{e}\big(\cos\frac{\pi}{8}\big)^n$. Since this takes a similar form to the winning probability of the original leaky NC game, we can apply the definition of sequential min-entropy to get the wanted result

$$H_{\min}(T|AB;T'|A'TC)_\sigma \geq \Big(-\lg\cos\tfrac{\pi}{8} - \tfrac{1}{(2\ln 2)n}\Big)n. \tag{6.4.12}$$

■

Finally, we get an entropic uncertainty relation.

Corollary 6.17 (Robust leaky MoE entropic uncertainty relation)**.** For any measurement made by Bob $M : T \to \mathcal{P}(AB)$ in the robust leaky game, we have

$$H_{\min}(T|M(AB))_\sigma + H_{\min}(T'|A'TC)_{\sigma_{|(M(AB)=T)}} \geq \Big(-\lg\cos\tfrac{\pi}{8} - \tfrac{1}{(2\ln 2)n}\Big)n. \tag{6.4.13}$$

Chapter 7

Rigidity for MoE Games

In this chapter, study the rigidity property of strategies of the TFKW game, as introduced in Section 2.2. This provides the first example of rigidity in the setting of MoE games. First, we introduce rigidity via the well-studied example of the CHSH game in Section 7.4. Then, in Sections 7.2 and 7.3, we introduce the main tools we use: approximate representations of $\mathbb{Z}_2^n$ and a sum-of-squares decomposition for the TFKW game polynomial, respectively. Next, we prove the main rigidity theorems in Section 7.4. Finally, in Section 7.5, we phrase rigidity in a way that is amenable to applications.

This chapter is based on joint work with Anne Broadbent [BC21].

7.1 Rigidity for Nonlocal Games

Rigidity, the property that observed correlations can be used to constrain (or *self-test*) the state of a joint quantum system, was first studied by Mayers and Yao [MY04] using nonlocal games. In this context, the necessary correlation to be attained is given by the optimal winning probability of the game. This property was first noted by Tsirelson [Tsi93] for the CHSH game, for which it was shown that the state of an optimal strategy must be maximally entangled between the players' systems. The CHSH game, introduced by Clauser, Horne, Shimony, and Holt [CHSH69] as a discrete-variable Bell inequality [Bel64], may be expressed as the extended nonlocal game

$$\texttt{CHSH} = (\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{u}, \{0\}, v), \tag{7.1.1}$$

where v is the (scalar) predicate $v(b,c|x,y) = \delta_{xy,b+c}$. Then, the winning probability of a strategy $\mathtt{S}$ is expressed

$$\mathfrak{w}_{\mathtt{CHSH}}(\mathtt{S}) = \frac{1}{4} \sum_{\substack{x,y,b,c\in\mathbb{Z}_2 \\ b+c=xy}} \mathrm{Tr}[(B_b^x \otimes C_c^y)\rho]. \tag{7.1.2}$$

The optimal winning probability of the CHSH game is $\mathfrak{w}(\mathtt{CHSH}) = \cos^2 \frac{\pi}{8}$ [Tsi80]. Next, we sketch why the state of any strategy that attains this optimal probability must be maximally entangled, following [CMMN20]. Many other nonlocal games are known to be rigid, *e.g.* the Mermin-Peres magic square game, but we will focus on CHSH as this will serve as a blueprint for the proof in the MoE game case.

First, we can reexpress the winning probability in a simpler way. Since it is a two-answer game, it helps to work with the *bias* rather than the winning probability: $\mathfrak{b}_{\mathtt{CHSH}}(\mathtt{S}) = 8\mathfrak{w}_{\mathtt{CHSH}}(\mathtt{S}) - 4$; the optimal bias $\mathfrak{b}(\mathtt{CHSH}) = 2\sqrt{2}$. The bias is contained in $[-4,4]$ and quantifies how much better the strategy does than random guessing. The scaling coefficient is chosen so that the bias admits a particularly simple expression using the measurement observables.

Definition 7.1. Let $M : \mathbb{Z}_2 \to \mathcal{P}(\mathcal{H})$ be a two-answer POVM. Then, the *observable* of M is $\bar{M} = M_0 - M_1$.

Note in particular that $\bar{M}$ is hermitian, and unitary iff M is a PVM. In this way, the observable uniquely determines the measurement if it is a PVM, but not if it is a more general POVM. With the observables $B_\theta := \bar{B^\theta}$, $C_\theta := \bar{C^\theta}$, the bias of a pure strategy $\mathtt{S} = (B, C, \{B^0, B^1\}, \{C^0, C^1\}, |\psi\rangle\langle\psi|)$ is

$$\mathfrak{b}_{\mathtt{CHSH}}(\mathtt{S}) = \langle\psi|B_0 \otimes C_0 + B_0 \otimes C_1 + B_1 \otimes C_0 - B_1 \otimes C_1|\psi\rangle\,. \tag{7.1.3}$$

A simple but powerful observation is that a value β upper bounds the optimal bias $\beta \geq 2\sqrt{2}$ if and only if $\beta \geq B_0 \otimes C_0 + B_0 \otimes C_1 + B_1 \otimes C_0 - B_1 \otimes C_1$ as operators, for any strategy. Hence, we can handle the calculation of the bias by a positivity argument.

Since the relation must hold for any hermitian unitary choice of observables, we can consider the positivity to hold on an algebra $\mathcal{A}$ whose representations correspond to the observables of the strategies. The algebra $\mathcal{A}$ is the $*$-algebra generated by b_0, b_1, c_0, c_1 satisfying $b_x^2 = c_y^2 = 1$, $b_x c_y = c_y b_x$, $b_x^* = b_x$, and $c_y^* = c_y$. Thus, $\mathcal{A} \cong \mathbb{C}[\Gamma \times \Gamma]$, where $\Gamma = \mathrm{gen}\{a, b | a^2, b^2\}$ is the free group over two generators of order two. In order to only

require the inner product to hold on the tensor-product representations, we should take the positive cone on $\mathcal{A}$ given by the min-tensor product of free group algebras [HMN+21]. However, for simplicity, we will work with the smaller positive cone of sums of squares, corresponding to the max-tensor. In the space of strategies, this corresponds to *commuting-operator strategies* where Bob and Charlie may make any compatible (commuting) measurement on the same joint Hilbert space. In finite dimensions, this does not affect the winning probability [SW08].

In the game algebra $\mathcal{A}$, we call $P = b_0c_0 + b_0c_1 + b_1c_0 - b_1c_1$ the *game polynomial*. If we are able to find a sum-of-squares (SOS) decomposition $\beta - P = \sum_i S_i^* S_i$ for $\beta \in \mathbb{R}$, then we know that β upper bounds the optimal bias. In fact, it is always possible to find such a decomposition if $\beta > 2\sqrt{2}$ [Oza13]. In the case of the CHSH, we can find the SOS decomposition

$$2\sqrt{2} - P = \tfrac{1}{2\sqrt{2}}\Big(b_0 + b_1 - \sqrt{2}c_0\Big)^2 + \tfrac{1}{2\sqrt{2}}\Big(b_0 - b_1 - \sqrt{2}c_1\Big)^2. \tag{7.1.4}$$

Each of these terms must act on the state of an optimal strategy as 0, which provides a family of relations, with respect to the state, on the operators. The algebra $\mathcal{A}$ acts on the state $|\psi\rangle$ via the representation $b_x \mapsto B_x$, $c_y \mapsto C_y$. These relations give rise to rigidity. By noting that $B_0B_1|\psi\rangle = -B_1B_0|\psi\rangle$, Bob's operators generate a $|\psi\rangle$-representation $f : D_4 \to \mathcal{U}(B)$ of the dihedral group $D_4 = \mathrm{gen}\{t, r | t^4, r^2, (rt)^2\}$ via $r \mapsto B_0$, $t \mapsto B_0B_1$, and identically for Charlie. It is important to note that this representation has the special property that $t^2 \mapsto -1$. As such, the Gowers-Hatami theorem (Theorem 3.33) gives that there exists an isometry $V \in \mathcal{U}(B, B')$ and a representation $\pi : D_4 \to \mathcal{U}(B')$ such that for all $g \in D_4$ $Vf(g)|\psi\rangle = \pi(g)V|\psi\rangle$. Then, as this is a true representation, it can be decomposed into a direct sum of irreducible representations using Maschke's theorem (Theorem 3.31). But we must have $\pi(t^2) = -1$ and there is only one irreducible representation that satisfies that: the unique non-abelian irreducible representation, which is two-dimensional. Thus, the representation must be a direct sum of copies of this irreducible representation.

Finally, by using the structure of the operators of this two-dimensional irreducible representation, it can be shown that the shared state must be maximally entangled, in the sense that for certain local dilations of Bob and Charlie's spaces, the state takes $|\mathrm{EPR}\rangle|\mathrm{aux}\rangle$ where the players act trivially on the auxiliary state $|\mathrm{aux}\rangle$. In this way, the CHSH game is rigid and self-tests a maximally entangled state.

This rigidity property has been extended in a variety of ways. First, it is *robust* in

the sense that, for strategies with near-optimal winning probability, the shared state dilated by local isometries is close, in norm, to a maximally entangled state [MYS12]. Also, the rigidity property was shown to hold for multiple copies of the game played sequentially [RUV13] or in parallel [Col17]. Lastly, the rigidity property can be ascertained from observed correlations: if many rounds of the CHSH game are played and at least around 85% of them win, then a large proportion of them must correspond to an EPR state [RUV13]. This is of paramount importance for experimental verification of rigidity, and therefore for applications to quantum cryptography and computing.

7.2 Approximate representations of the group of n-bit strings

An important technical step for our rigidity result makes use of approximate representations of $\mathbb{Z}_2^n$, similarly to how the CHSH rigidity result uses approximate representations of D_4. As $\mathbb{Z}_2^n$ is abelian, the irreducible representations of $\mathbb{Z}_2^n$ are all 1-dimensional, and can be parametrised by elements of the group. On $\mathbb{Z}_2^n$, recall that the *dot product* is the bilinear map $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2$, $x \cdot y = \sum_{i=1}^n x_i y_i$. This provides the representations $\gamma_x(y) = (-1)^{x \cdot y}$. These representations are all distinct and irreducible, and since there are 2^n of them, they constitute all the irreducible representations. Since $\mathbb{Z}_2^n$ is abelian, the irreducible representations are also the elements of the *dual group* of homomorphisms to the circle group.

The approximate representations (Definition 3.32) are induced by approximate commutation relations of the generators. To show they are in fact approximate representations, we need to relate approximate commutation of the generators to approximate commutation of all the elements so that we may use the Gowers-Hatami theorem (Theorem 3.33). First, we tackle the case that needs no extra assumptions, $G = \mathbb{Z}_2^2$.

Lemma 7.2. Let V and W be finite-dimensional inner product spaces, let $\psi \in V \otimes W$, and let $U_0, U_1 \in \mathcal{U}(V)$ be self-inverse such that

$$\|[U_0, U_1]\psi\| \leq \delta, \tag{7.2.1}$$

for some $\delta \geq 0$. Then, the function $f : \mathbb{Z}_2^2 \to \mathcal{U}(V)$ defined by $f(00) = \mathbb{I}$, $f(01) = U_0$, $f(10) = U_1$, and $f(11) = U_0 U_1$ is an $(\delta/\sqrt{2}, \psi)$-representation of $\mathbb{Z}_2^2$.

Proof: This is straightforward to check using the hypothesis and the fact that the action by a unitary does not change the norm. Write $\Delta(y) = \frac{1}{4}\sum_{x \in G} \|(f(x)f(y) - f(x+y))\psi\|^2$.

For $y = 00$,

$$\Delta(00) = \frac{1}{4}\sum_{x\in G}\|(f(x) - f(x))\psi\|^2 = 0 \leq \frac{\delta^2}{2}. \tag{7.2.2}$$

For $y = 01$,

$$\begin{aligned}\Delta(01) = \frac{1}{4}\big(&\|(U_0 - U_0)\psi\|^2 + \|(U_0^2 - \mathbb{I})\psi\|^2 \\ &+ \|(U_1U_0 - U_0U_1)\psi\|^2 + \|(U_0U_1U_0 - U_1)\psi\|^2\big) \leq \frac{\delta^2}{2}.\end{aligned} \tag{7.2.3}$$

For $y = 10$,

$$\begin{aligned}\Delta(10) = \frac{1}{4}\big(&\|(U_1 - U_1)\psi\|^2 + \|(U_0U_1 - U_0U_1)\psi\|^2 \\ &+ \|(U_1^2 - \mathbb{I})\psi\|^2 + \|(U_0U_1U_1 - U_0)\psi\|^2\big) = 0 \leq \frac{\delta^2}{2}.\end{aligned} \tag{7.2.4}$$

And finally, for $y = 11$,

$$\begin{aligned}\Delta(11) = \frac{1}{4}\big(&\|(U_0U_1 - U_0U_1)\psi\|^2 + \|(U_0U_0U_1 - U_1)\psi\|^2 \\ &+ \|(U_1U_0U_1 - U_0)\psi\|^2 + \|(U_0U_1U_0U_1 - \mathbb{I})\psi\|^2\big) \leq \frac{\delta^2}{2}.\end{aligned} \tag{7.2.5}$$

■

Extending a result of this form to $\mathbb{Z}_2^n$ for $n > 2$ requires another condition on the unitaries, in order to be able to use the commutation with respect to ψ even when there are operators sitting between the state and the unitaries. To do this, we impose an additional relation, arising from our sum-of-squares decomposition, which allows to swap operators onto another register while incurring only a small error.

Lemma 7.3. Let V, W be finite-dimensional inner product spaces, let $\psi \in V \otimes W$, and let $U_1, ..., U_n \in \mathcal{U}(V)$ be a collection of self-inverse unitaries such that

$$\|[U_i, U_j]\psi\| \leq \delta \tag{7.2.6}$$

and there exist self-inverse $V_1, ..., V_n \in \mathcal{U}(V \otimes W)$ such that

$$\|U_i\psi - V_i\psi\| \leq \epsilon \tag{7.2.7}$$
$$[U_i, V_j] = 0 \tag{7.2.8}$$

for some $\delta, \epsilon \geq 0$. Then, the map

$$\begin{array}{rccc} f: & \mathbb{Z}_2^n & \to & \mathcal{U}(V) \\ & x & \mapsto & U^x, \end{array} \tag{7.2.9}$$

where $U^x := U_1^{x_1} \cdots U_n^{x_n}$, is an $(n^2(3\epsilon + \delta), |\psi\rangle)$-representation of $\mathbb{Z}_2^n$.

Proof: Let $x, y \in \mathbb{Z}_2^n$. Then $f(x)f(y) - f(x+y) = U^x U^y - U^{x+y}$. Write $V^x = V_n^{x_n} \cdots V_1^{x_1}$. Suppose the first nonzero term of y is at position i_0. Write $x^1 = x_1 \ldots x_{i_0-1} 0 \ldots 0$ and $x^2 = 0 \ldots 0 x_{i_0+1} \ldots x_n$ and similarly for y. By hypothesis, this gives via Eq. (7.2.7)

$$\begin{aligned} \|(U^x U^y - U^{x+y})\psi\| &= \|(U^{x^1} U_{i_0}^{x_{i_0}} U^{x^2} U_{i_0} U^{y^2} - U^{x+y})\psi\| \\ &\leq \|(U^{x^1} U_{i_0}^{x_{i_0}} U^{x^2} U_{i_0} V^{y^2} - U^{x+y})\psi\| + |y^2|\epsilon. \end{aligned} \tag{7.2.10}$$

Now, we can shift U_{i_0} up through U^{x^2} by using the commutation relations Eqs. (7.2.6) and (7.2.8) and then replacing that term of U^{x^2} with the corresponding V term, and continuing recursively. This adds an error

$$\|(U^{x^1} U_{i_0}^{x_{i_0}} U^{x^2} U_{i_0} V^{y^2} - U^{x+y})\psi\| \leq \|(U^{x^1} U_{i_0}^{x_{i_0}+y_{i_0}} V^{y^2} V^{x^2} - U^{x+y})\psi\| + |x^2|(\epsilon + \delta). \tag{7.2.11}$$

We can then shift V^{x^2} and the first term, i_1, of y^2 back:

$$\begin{aligned} \|(U^{x^1} U_{i_0}^{x_{i_0}} U^{x^2} U_{i_0} V^{y^2} - U^{x+y})\psi\| &\leq \|(U^{x^1} U_{i_0}^{x_{i_0}+y_{i_0}} U^{x^2} U_{i_1}^{y_{i_1}} V^{y^{2\,2}} - U^{x+y})\psi\| + |x^2|(2\epsilon + \delta) + \epsilon \\ &\leq \|(U^{x^1} U_{i_0}^{x_{i_0}+y_{i_0}} U^{x^2} U_{i_1}^{y_{i_1}} V^{y^{2\,2}} - U^{x+y})\psi\| + n(2\epsilon + \delta) \end{aligned} \tag{7.2.12}$$

Note that the above estimate is relatively crude. This process can be repeated another $|y^2|$ times to get

$$\|(U^x U^y - U^{x+y})\psi\| \leq n|y|(2\epsilon + \delta) + |y^2|\epsilon \leq n^2(2\epsilon + \delta) + n\epsilon, \tag{7.2.13}$$

which gives the result. ■

7.3 Sum-of-Squares Decomposition

In this section, we follow the model of the CHSH game to construct a game polynomial for the TFKW game, and then present an SOS decomposition for it.

Definition 7.4. Let $\mathtt{S}$ be a strategy for $\mathtt{TFKW}$. Then, the *bias* of $\mathtt{S}$ is $\mathfrak{b}_{\mathtt{TFKW}}(\mathtt{S}) = 8\mathfrak{w}_{\mathtt{TFKW}}(\mathtt{S})-4$. The *optimal bias* is $\mathfrak{b}(\mathtt{TFKW}) = \sup_{\mathtt{S}} \mathfrak{b}_{\mathtt{TFKW}}(\mathtt{S})$, the supremum over all strategies.

As for the CHSH game, we can first assume that the strategy is pure, and then re-express the bias in terms of the hermitian unitary measurement observables. Note that as the referee Alice also makes a measurement here, she also has observables, corresponding to the Pauli operators $A_0 = Z$ and $A_1 = X$. Let $\mathtt{S} = (B, C, \{B^0, B^1\}, \{C^0, C^1\}, |\psi\rangle\langle\psi|)$ be a pure strategy for $\mathtt{TFKW}$. Then, the bias is expressed as

$$\begin{aligned}\mathfrak{b}_{\mathtt{TFKW}}(\mathtt{S}) = \langle\psi| Z\otimes(B_0\otimes\mathbb{I}+\mathbb{I}\otimes C_0) - \mathbb{I}\otimes(\mathbb{I}-B_0\otimes C_0) \\ + X\otimes(B_1\otimes\mathbb{I}+\mathbb{I}\otimes C_1) - \mathbb{I}\otimes(\mathbb{I}-B_1\otimes C_1)|\psi\rangle.\end{aligned} \tag{7.3.1}$$

We can again interpret the expression in the expectation value as the representation of a game polynomial in a $*$-algebra. Since each player has two measurement observables, the game algebra arises from the same discrete group $\Gamma = \mathrm{gen}\{a, b | a^2, b^2\}$ for each player. Then. the algebra is the two-by-two matrix algebra over the algebra generated by b_0, b_1, c_0, c_1 such that $b_x^2 = c_y^2 = 1$, $b_x c_y = c_y b_x$, $b_x^* = b_x$, and $c_y^* = c_y$ (isomorphic to the group algebra of $\Gamma\times\Gamma$), $\mathcal{A} \cong \mathcal{L}(\mathbb{Z}_2)\otimes^{\max}\mathbb{C}[\Gamma\times\Gamma]$. Here the positivity as a semi-pre-C^*-algebra is given by the sums-of-squares. As such, the game polynomial is

$$P = Z\otimes(b_0+c_0) + X\otimes(b_1+c_1) - \mathbb{I}\otimes(1-b_0c_0) - \mathbb{I}\otimes(1-b_1c_1) \in \mathcal{A}. \tag{7.3.2}$$

Since the optimal bias is again $\mathfrak{b}(\mathtt{TFKW}) = 2\sqrt{2}$, we want an SOS decomposition of $2\sqrt{2} - P$. One such decomposition is

$$\frac{1}{2\sqrt{2}}\Big[(Z\otimes b_0 + X\otimes c_1 - \sqrt{2})^2 + (Z\otimes c_0 + X\otimes b_1 - \sqrt{2})^2\Big] + \frac{1}{2}\big[(b_0-c_0)^2 + (b_1-c_1)^2\big]. \tag{7.3.3}$$

First, this directly implies that $2\sqrt{2}$ upper bounds the bias of $\mathtt{TFKW}$, giving an alternate

proof of the winning probability to that of [TFKW13]. Conversely, the state of an optimal strategy must be in the 0 eigenspace of a representation of this operator, and therefore it must be in the 0 eigenspace of each of the squared terms. We use this idea to work out the rigidity for this game.

7.4 Rigidity Theorems

In this section, we prove the rigidity of the TFKW game, first in the exact case, then the robust case, and finally for the parallel repetitions of both cases. Each part builds upon the previous one, so we proceed in order of difficulty.

7.4.1 Exact rigidity

We can get a lot of intuition from working with the exact case, where we assume the strategy wins with exactly optimal probability.

In order to later be able to generalise to the case where the shared state is mixed, we work with the class of *purified strategies*. These are pure strategies, where the shared state is supported on an additional register R, to which none of the parties have access. By tracing out this additional register, we can attain the state of any strategy.

Theorem 7.5 (exact rigidity)**.** Let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, |\psi\rangle\langle\psi|\big)$ be a purified strategy for TFKW. If this strategy is optimal, then there exist registers B' and C', and isometries $V \in \mathcal{U}(B, B')$ and $W \in \mathcal{U}(C, C')$ such that we have a decomposition of the state

$$(V \otimes W)|\psi\rangle = \sum_{s \in \mathbb{Z}_2 \times \mathbb{Z}_2} X^{s_0} Z^{s_1} |\beta\rangle \otimes |\psi_s\rangle, \tag{7.4.1}$$

where the supports of the $|\psi_s\rangle \in \mathcal{H}_{B'C'R}$ on both B' and C' are orthogonal; and there exist commuting operators $B'_\theta \in \mathcal{U}(B')$ and $C'_\theta \in \mathcal{U}(C')$ such that

$$\begin{aligned} VB_\theta|\psi\rangle &= B'_\theta V|\psi\rangle \\ WC_\theta|\psi\rangle &= C'_\theta W|\psi\rangle, \end{aligned} \tag{7.4.2}$$

$$B'_\theta|\psi_s\rangle = C'_\theta|\psi_s\rangle = (-1)^{s_\theta}|\psi_s\rangle. \tag{7.4.3}$$

It is a straightforward computation to show that a strategy of this form wins in fact optimally. Intuitively, the result says that what the players must do in order to win optimally

is to agree on a Wiesner-Breidbart state to give Alice, which they can do without communicating after deciding on the shared state using the simultaneous distinguishability of their parts of the state, and then guess accordingly. The Wiesner-Breidbart states can be seen as a family of states corresponding to the conjugate-coding states rotated by a Breidbart operator, as seen in Fig. 5.4. However, this form of rigidity is unlike that known for the CHSH game as there is not a single unique strategy up to isomorphism, but an infinite family of related strategies. Nevertheless, there is a known nonlocal game that exhibits rigidity in this way [MNP21].

Proof: Letting P be the game polynomial (Eq. (7.3.2)), we know $\langle\psi|2\sqrt{2} - P|\psi\rangle = 0$, acting by the representation induced by the strategy. Then, each of the terms in the sum of squares (Eq. (7.3.3)) is positive so they must all act as zero, giving four relations

$$(Z \otimes B_0 + X \otimes C_1)|\psi\rangle = \sqrt{2}|\psi\rangle \tag{7.4.4}$$
$$(Z \otimes C_0 + X \otimes B_1)|\psi\rangle = \sqrt{2}|\psi\rangle \tag{7.4.5}$$
$$B_0|\psi\rangle = C_0|\psi\rangle \tag{7.4.6}$$
$$B_1|\psi\rangle = C_1|\psi\rangle. \tag{7.4.7}$$

We can combine Eq. (7.4.4) and Eq. (7.4.7) to get a relation solely in terms of Alice and Bob's observables, $(Z \otimes B_0 + X \otimes B_1)|\psi\rangle = \sqrt{2}|\psi\rangle$. Squaring this

$$2|\psi\rangle = (Z \otimes B_0 + X \otimes B_1)^2|\psi\rangle = 2|\psi\rangle + ZX \otimes [B_0, B_1]|\psi\rangle, \tag{7.4.8}$$

we get that the commutator $[B_0, B_1]|\psi\rangle = 0$, that is B_0 and B_1 commute with respect to $|\psi\rangle$. The commutation means that this generates a $(0, |\psi\rangle)$-representation f of $\mathbb{Z}_2^2$ as $f(00) = \mathbb{I}_B$, $f(01) = B_0$, $f(10) = B_1$, $f(11) = B_0B_1$; this is analogous to Lemma 7.2 with $U_0 = B_0$, $U_1 = B_1$, and $\delta = 0$. By the Gowers-Hatami theorem (Theorem 3.33), there exists an isometry $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and a representation $g : \mathbb{Z}_2^2 \to \mathcal{U}(B')$ such that $Vf(x)|\psi\rangle = g(x)V|\psi\rangle$. Defining $B'_0 = g(01)$ and $B'_1 = g(10)$, these are commuting unitaries such that $VB_\theta|\psi\rangle = B'_\theta V|\psi\rangle$. Further, as g is a representation, the dilated space decomposes orthogonally as a direct sum of irreducible representations

$$\mathcal{H}_{B'} = \bigoplus_{s\in\mathbb{Z}_2^2} \mathcal{B}_s, \tag{7.4.9}$$

such that the operators act as $B'_\theta = \sum_{s\in\mathbb{Z}_2^2}(-1)^{s_\theta}\mathbb{I}_{B,s}$, where $\mathbb{I}_{B,s}$ is the projection onto $\mathcal{B}_s$.

Following an identical line of reasoning for Charlie's observables, there exists an isometry $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ and commuting unitaries $C'_0, C'_1 \in \mathcal{U}(C')$ such that $WC_\theta|\psi\rangle = C'_\theta W|\psi\rangle$; and the space decomposes as $\mathcal{H}_{C'} = \bigoplus_{s\in\mathbb{Z}_2^2} \mathcal{C}_s$ so that $C'_\theta = \sum_{s\in\mathbb{Z}_2^2}(-1)^{s_\theta}\mathbb{I}_{C,s}$. Defining the dilated state $|\psi'\rangle = (V \otimes W)|\psi\rangle$, we have that Eqs. (7.4.4) to (7.4.7) extend to the dilated spaces:

$$(Z \otimes B'_0 + X \otimes B'_1)|\psi'\rangle = \sqrt{2}|\psi'\rangle \tag{7.4.10}$$

$$B'_0|\psi'\rangle = C'_0|\psi'\rangle \tag{7.4.11}$$

$$B'_1|\psi'\rangle = C'_1|\psi'\rangle. \tag{7.4.12}$$

Now, since $|\psi'\rangle \in \mathcal{H}_{AB'C'R} = \bigoplus_{s,s'\in\mathbb{Z}_2^2} \mathcal{H}_A \otimes \mathcal{B}_s \otimes \mathcal{C}_{s'} \otimes \mathcal{H}_R$, we can decompose it accordingly as $|\psi'\rangle = \sum_{s,s'\in\mathbb{Z}_2^2}|v_{s,s'}\rangle$. Then, Eq. (7.4.11) gives that $\sum_{s,s'\in\mathbb{Z}_2^2}(-1)^{s_0}|v_{s,s'}\rangle = \sum_{s,s'\in\mathbb{Z}_2^2}(-1)^{s'_0}|v_{s,s'}\rangle$, so $|v_{s,s'}\rangle = 0$ if $s_0 \neq s'_0$. Doing the same with Eq. (7.4.12) gives that $|v_{s,s'}\rangle = 0$ if $s \neq s'$ so

$$|\psi'\rangle = \sum_{s\in\mathbb{Z}_2^2}|v_{s,s}\rangle \in \bigoplus_{s\in\mathbb{Z}_2^2} \mathcal{H}_A \otimes \mathcal{B}_s \otimes \mathcal{C}_s \otimes \mathcal{H}_R. \tag{7.4.13}$$

Next, the decomposition of the spaces means that

$$(Z \otimes B_0 + X \otimes B_1) \otimes \mathbb{I}_{CR} = \sum_{s\in\mathbb{Z}_2^2}((-1)^{s_0}Z + (-1)^{s_1}X) \otimes \mathbb{I}_{B,s} \otimes \mathbb{I}_{CR}; \tag{7.4.14}$$

and Eq. (7.4.10) says that $|\psi'\rangle$ must belong to the $\sqrt{2}$-eigenspace of this operator. Since

$$(-1)^{s_0}Z + (-1)^{s_1}X = \sqrt{2}X^{s_0}Z^{s_1}HZ^{s_1}X^{s_0}, \tag{7.4.15}$$

the $\sqrt{2}$-eigenspace is simply the span of $X^{s_0}Z^{s_1}|\beta\rangle$. Thus,

$$|\psi'\rangle \in \bigoplus_{s,s'\in\mathbb{Z}_2^2} X^{s_0}Z^{s_1}|\beta\rangle \otimes \mathcal{B}_s \otimes \mathcal{C}_{s'} \otimes \mathcal{H}_R. \tag{7.4.16}$$

Taking the intersection of the spaces $|\psi'\rangle$ belongs to, we have that

$$|\psi'\rangle \in \bigoplus_{s\in\mathbb{Z}_2^2} X^{s_0}Z^{s_1}|\beta\rangle \otimes \mathcal{B}_s \otimes \mathcal{C}_s \otimes \mathcal{H}_R, \tag{7.4.17}$$

which gives the result. ■

7.4.2 Robust rigidity

Now, we move on to the study of the robust rigidity, where we assume that the winning probability is in some small neighbourhood of the optimal probability. We can approach the proof in about the same way as the exact case, while keeping track of the error.

Theorem 7.6 (robust rigidity)**.** Let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, |\psi\rangle\langle\psi|\big)$ be a purified strategy for TFKW that wins with probability $\mathfrak{w}_{\mathtt{TFKW}}(\mathtt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$ for some $\varepsilon \geq 0$. Then there exists a constant $K \geq 0$ and isometries $V \in \mathcal{U}(B, B')$ and $W \in \mathcal{U}(C, C')$ such that the distance between quantum states

$$\Big\|(V \otimes W)|\psi\rangle - \sum_{s\in\mathbb{Z}_2^2} X^{s_0} Z^{s_1}|\beta\rangle \otimes |\psi_s\rangle\Big\| \leq K\sqrt{\varepsilon}, \tag{7.4.18}$$

where the $|\psi_s\rangle \in \mathcal{H}_{B'C'R}$ have orthogonal supports on both B' and C'; and there exists a constant $L \geq 0$, and commuting observables $B'_\theta \in \mathcal{U}(B')$ and $C'_\theta \in \mathcal{U}(C')$ such that

$$\begin{aligned} &\|VB_\theta|\psi\rangle - B'_\theta V|\psi\rangle\| \leq L\sqrt{\varepsilon} \\ &\|WC_\theta|\psi\rangle - C'_\theta W|\psi\rangle\| \leq L\sqrt{\varepsilon}, \end{aligned} \tag{7.4.19}$$

$$B'_\theta|\psi_s\rangle = C'_\theta|\psi_s\rangle = (-1)^{s_\theta}|\psi_s\rangle. \tag{7.4.20}$$

The proof below allows us to take $K = 110$ and $L = 18$ as the necessary constants. Note also that, as seen for the CHSH game in [RUV13], the order $\sqrt{\varepsilon}$ dependence of this upper bound is in fact necessary, though it may be possible to improve the constants: if we take an unentangled optimal strategy for TFKW and perturb by a vector of length δ in an orthogonal direction, the winning probability decreases on the order of δ^2.

Proof: By hypothesis, $\mathfrak{w}_{\mathtt{TFKW}}(\mathtt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$, so the bias $\mathfrak{b}_{\mathtt{TFKW}}(\mathtt{S}) \geq 2\sqrt{2} - 8\varepsilon$, giving that $\langle\psi|2\sqrt{2} - P|\psi\rangle \leq 8\varepsilon$, which, using the sum-of-squares decomposition, is

$$\begin{aligned} 16\sqrt{2}\varepsilon \geq\ &\langle\psi|(Z\otimes B_0 + X\otimes C_1 - \sqrt{2})^2|\psi\rangle + \langle\psi|(Z\otimes C_0 + X\otimes B_1 - \sqrt{2})^2|\psi\rangle \\ &+ \sqrt{2}\big[\,\langle\psi|(B_0 - C_0)^2|\psi\rangle + \langle\psi|(B_1 - C_1)^2|\psi\rangle\big]. \end{aligned} \tag{7.4.21}$$

Since each of the terms is positive, we must have that $16\varepsilon \geq \langle\psi|(B_\theta - C_\theta)^2|\psi\rangle$ and $8\sqrt{2}\varepsilon \geq \min\big\{\langle\psi|(Z\otimes B_0 + X\otimes C_1 - \sqrt{2})^2|\psi\rangle\,, \langle\psi|(Z\otimes C_0 + X\otimes B_1 - \sqrt{2})^2|\psi\rangle\big\}$. This

can be converted to Euclidean norm conditions by taking square roots:

$$2(8)^{1/4}\sqrt{\varepsilon} \geq \min\Big\{\|(Z\otimes B_0 + X\otimes C_1 - \sqrt{2})|\psi\rangle\|, \|(Z\otimes C_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\|\Big\} \tag{7.4.22}$$

$$4\sqrt{\varepsilon} \geq \|(B_\theta - C_\theta)|\psi\rangle\|. \tag{7.4.23}$$

Using Eq. (7.4.23) in Eq. (7.4.22), we get

$$\|(Z\otimes B_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\| \leq \|(Z\otimes B_0 + X\otimes C_1 - \sqrt{2})|\psi\rangle\| + \|X\otimes(B_1 - C_1)|\psi\rangle\| \tag{7.4.24}$$

and

$$\|(Z\otimes B_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\| \leq \|(Z\otimes C_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\| + \|Z\otimes(B_0 - C_0)|\psi\rangle\|. \tag{7.4.25}$$

which gives $\big\|(Z\otimes B_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\big\| \leq 2(2+8^{1/4})\sqrt{\varepsilon}$. Noting that

$$\begin{aligned}(Z\otimes B_0 + X\otimes B_1 + \sqrt{2})(Z\otimes B_0 + X\otimes B_1 - \sqrt{2}) &= (Z\otimes B_0 + X\otimes B_1)^2 - 2\\ &= ZX\otimes[B_0, B_1],\end{aligned} \tag{7.4.26}$$

we have that

$$\begin{aligned}\|[B_0,B_1]|\psi\rangle\| &= \|ZX\otimes[B_0,B_1]|\psi\rangle\|\\ &\leq \Big\|Z\otimes B_0 + X\otimes B_1 + \sqrt{2}\Big\|\Big\|(Z\otimes B_0 + X\otimes B_1 - \sqrt{2})|\psi\rangle\Big\|\\ &\leq 2(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon},\end{aligned} \tag{7.4.27}$$

that is, Bob's operators almost commute with respect to $|\psi\rangle$. As in the exact case, we use Lemma 7.2 with $U_0 = B_0$ and $U_1 = B_1$ to generate a $\big(\sqrt{2}(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon}, |\psi\rangle\big)$-representation f of $\mathbb{Z}_2^2$. By Gowers-Hatami, there exists an isometry $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ to some Hilbert space and a representation $g : \mathbb{Z}_2^2 \to \mathcal{U}(B')$ such that

$$\|(Vf(x) - g(x)V)|\psi\rangle\| \leq \sqrt{2}(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon}. \tag{7.4.28}$$

Defining $B'_0 = g(01)$ and $B'_1 = g(10)$, they are commuting observables such that

$$\|(VB_\theta - B'_\theta V)|\psi\rangle\| \leq \sqrt{2}(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon}; \tag{7.4.29}$$

and since g is a representation, there exists an orthogonal decomposition $\mathcal{H}_{B'} = \bigoplus_{s\in\mathbb{Z}_2^2} \mathcal{B}_s$ where the observables decompose accordingly as $B'_\theta = \sum_{s\in\mathbb{Z}_2^2}(-1)^{s_\theta}\mathbb{I}_{B,s}$. Applying the same reasoning for Charlie's observables gives that there exists a Hilbert space with orthogonal decomposition $\mathcal{H}_{C'} = \bigoplus_{s\in\mathbb{Z}_2^2} \mathcal{C}_s$, commuting observables $C'_\theta = \sum_{s\in\mathbb{Z}_2^2}(-1)^{s_\theta}\mathbb{I}_{C,s}$, and an isometry $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ such that $\|(WC_\theta - C'_\theta W)|\psi\rangle\| \leq \sqrt{2}(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon}$. Defining $|\psi'\rangle = (V\otimes W)|\psi\rangle$, we can extend Eq. (7.4.22) and Eq. (7.4.23) to the dilated spaces as

$$\left\|(Z\otimes B'_0 + X\otimes B'_1 - \sqrt{2})|\psi'\rangle\right\| \leq 2(3+2\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon} \tag{7.4.30}$$

$$\|B'_\theta|\psi'\rangle - C'_\theta|\psi'\rangle\| \leq 4((1+\sqrt{2})(2+8^{1/4})+1)\sqrt{\varepsilon}. \tag{7.4.31}$$

From the decomposition of Bob and Charlie's spaces, we have that the shared space is $\mathcal{H}_{AB'C'R} = \bigoplus_{s,s'\in\mathbb{Z}_2^2} \mathcal{H}_A \otimes \mathcal{B}_s \otimes \mathcal{C}_{s'} \otimes \mathcal{H}_R$, thus the state decomposes accordingly as $|\psi'\rangle = \sum_{s,s'\in\mathbb{Z}_2^2}|v_{s,s'}\rangle$. Using this in Eq. (7.4.31) gives

$$4((1+\sqrt{2})(2+8^{1/4})+1)\sqrt{\varepsilon} \geq \Big\|\sum_{s,s'\in\mathbb{Z}_2^2}\Big((-1)^{s_\theta}-(-1)^{s'_\theta}\Big)|v_{s,s'}\rangle\Big\| = 2\Big\|\sum_{s_\theta\neq s'_\theta}|v_{s,s'}\rangle\Big\| \tag{7.4.32}$$

We write $|v_0\rangle = \sum_s |v_{s,s}\rangle$ and $|v_1\rangle = \sum_{s\neq s'}|v_{s,s'}\rangle$, so that $|\psi'\rangle = |v_0\rangle + |v_1\rangle$ and

$$\||v_1\rangle\| \leq \Big\|\sum_{s_0\neq s'_0}|v_{s,s'}\rangle\Big\| + \Big\|\sum_{s_1\neq s'_1}|v_{s,s'}\rangle\Big\| \leq 4((1+\sqrt{2})(2+8^{1/4})+1)\sqrt{\varepsilon}. \tag{7.4.33}$$

Writing $|\beta_s\rangle = X^{s_0}Z^{s_1}|\beta\rangle$, we can decompose

$$\begin{aligned} Z\otimes B'_0 + X\otimes B'_1 - \sqrt{2} &= \sum_s((-1)^{s_0}Z + (-1)^{s_1}X - \sqrt{2})\otimes\mathbb{I}_{B,s} \\ &= 2\sqrt{2}\sum_s(\,|\beta_s\rangle\langle\beta_s| - \mathbb{I})\otimes\mathbb{I}_{B,s}. \end{aligned} \tag{7.4.34}$$

Also, define the projection $|v_\beta\rangle = \sum_s (\,|\beta_s\rangle\langle\beta_s| \otimes \mathbb{I})|v_{s,s}\rangle$, so that Eq. (7.4.30) implies

$$\begin{aligned} \||\psi'\rangle - |v_\beta\rangle\| &\leq \Big\|\sum_{s,s'}(\,|\beta_s\rangle\langle\beta_s| - \mathbb{I})|v_{s,s'}\rangle\Big\| + \Big\|\sum_{s\neq s'}(\,|\beta_s\rangle\langle\beta_s| \otimes \mathbb{I})|v_{s,s'}\rangle\Big\| \\ &\leq \frac{1}{2\sqrt{2}}\Big\|(Z\otimes B'_0 + X\otimes B'_1 - \sqrt{2})|\psi'\rangle\Big\| + \||v_1\rangle\| \\ &\leq (\tfrac{3}{2}\sqrt{2}+2)(2+8^{1/4})\sqrt{\varepsilon} + 4((1+\sqrt{2})(2+8^{1/4})+1)\sqrt{\varepsilon} \\ &= [(6+\tfrac{11}{2}\sqrt{2})(2+8^{1/4})+4]\sqrt{\varepsilon}. \end{aligned} \tag{7.4.35}$$

Note that although $|v_\beta\rangle$ is not necessarily normalised, it must be subnormalised and the above implies that

$$\left\|\frac{|v_\beta\rangle}{\||v_\beta\rangle\|} - |v_\beta\rangle\right\| = 1 - \||v_\beta\rangle\| \leq \||\psi'\rangle - |v_\beta\rangle\| \leq [(6+\tfrac{11}{2}\sqrt{2})(2+8^{1/4})+4]\sqrt{\varepsilon}. \tag{7.4.36}$$

Defining $|\phi\rangle = \frac{|v_\beta\rangle}{\||v_\beta\rangle\|}$, we have by construction that $|\phi\rangle = \sum_s |\beta_s\rangle \otimes |\psi_s\rangle$, where

$$|\psi_s\rangle = \frac{1}{\|v_\beta\|}(\langle\beta_s| \otimes \mathbb{I})|v_{s,s}\rangle \in \mathcal{B}_s \otimes \mathcal{C}_s \otimes \mathcal{H}_R, \tag{7.4.37}$$

so simultaneously distinguishable by Bob and Charlie. Thus, to complete the proof, note that

$$\||\psi'\rangle - |\phi\rangle\| \leq \||\psi'\rangle - |v_\beta\rangle\| + \||v_\beta\rangle - |\phi\rangle\| \leq 2[(6+\tfrac{11}{2}\sqrt{2})(2+8^{1/4})+4]\sqrt{\varepsilon}. \tag{7.4.38}$$

■

We can use the properties of purified strategies and the trace norm to directly extend this result to a general strategy.

Corollary 7.7. Let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \rho\big)$ be an arbitrary strategy for TFKW that wins with probability $\mathfrak{w}_{\texttt{TFKW}}(\mathtt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$ for some $\varepsilon \geq 0$. Then there exists a constant $K \geq 0$ and isometries $V \in \mathcal{U}(B, B')$ and $W \in \mathcal{U}(C, C')$ such that

$$\big\|(V\otimes W)\rho(V\otimes W)^\dagger - \mathrm{Tr}_R(\,|\phi\rangle\langle\phi|)\big\|_{\mathrm{Tr}} \leq K\sqrt{\varepsilon}, \tag{7.4.39}$$

where R is an auxiliary register such that $|\phi\rangle = \sum_{s\in\mathbb{Z}_2^2} X^{s_0}Z^{s_1}|\beta\rangle \otimes |\psi_s\rangle$ for some vectors $|\psi_s\rangle \in \mathcal{H}_{B'C'R}$ with orthogonal supports on both B' and C'.

The proof of Corollary 7.7 follows directly by using the inequality between the Euclidean distance and the trace distance (Proposition 4.21), tracing out the auxiliary register R, and finally using the fact that the purification of the measurements only requires an isometric extension of the state space (Theorem 5.6).

7.4.3 Parallel-repeated rigidity

Similarly to the case of a single game, we begin with the parallel repetition in the exact case. That is, we assume n copies of the TFKW game are played and the adversaries win each of the copies with optimal probability. We aim to show that, in this case, Bob and Charlie must behave as for a single game on each of the copies, i.e. they agree upon a Wiesner-Breidbart state and guess accordingly.

Theorem 7.8 (parallel-repeated exact rigidity)**.** Let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \rho = |\psi\rangle\langle\psi|\big)$ be a purified strategy for $\mathtt{TFKW}^n$ for some $n \in \mathbb{N}$ that guesses each bit optimally, that is for each $i \in [n]$, $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) = \cos^2\big(\frac{\pi}{8}\big)$. Then, there exist registers B' and C', and isometries $V \in \mathcal{U}(B, B')$ and $W \in \mathcal{U}(C, C')$ such that

$$(V \otimes W)|\psi\rangle = \sum_{t\in(\mathbb{Z}_2^2)^n} X^{t_{10}}Z^{t_{11}}|\beta\rangle \otimes \cdots \otimes X^{t_{n0}}Z^{t_{n1}}|\beta\rangle \otimes |\psi_t\rangle, \tag{7.4.40}$$

where the supports of the $|\psi_t\rangle \in \mathcal{H}_{B'C'R}$ on both B' and C' are orthogonal.

Note that we are writing strings $t \in (\mathbb{Z}_2^2)^n$ as $t = t_{10}t_{11}t_{20}t_{21}\ldots t_{n0}t_{n1}$. To prove this theorem, we want to reduce to the single-game case as much as possible and use the rigidity we know there. As such, we extract a collection of optimal strategies for a single TFKW game. In fact, we may express the i-th winning probability as

$$\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) = \mathop{\mathbb{E}}_{\substack{\varphi\in\mathbb{Z}_2^n \\ \varphi_i=0}} \left(\frac{1}{2} \sum_{\substack{\theta\in\mathbb{Z}_2^n \\ \theta_j=\varphi_j \forall j\neq i}} \sum_{y\in\mathbb{Z}_2} \mathrm{Tr}\big[\big((A^n)^\theta_{y,i} \otimes B^\theta_{y,i} \otimes C^\theta_{y,i}\big)\rho\big] \right). \tag{7.4.41}$$

In order for this average to be $\cos^2\big(\frac{\pi}{8}\big)$, each of the inner terms must also be $\cos^2\big(\frac{\pi}{8}\big)$, and thus they must correspond to an optimal strategy of $\mathtt{TFKW}$. Then we get $n2^{n-1}$ optimal strategies: for every $i \in [n]$ and $\varphi \in \mathbb{Z}_2^n$ such that $\varphi_i = 0$, the strategy ${}^{\varphi,i}\mathtt{S} =$

$\Big(B, C, \{{}^{\varphi,i}B^{\theta}\}, \{{}^{\varphi,i}C^{\theta}\}, \rho\Big)$ where ${}^{\varphi,i}B^{\theta}_{y} = B^{\varphi+\theta e_i}_{y,i}$ and ${}^{\varphi,i}C^{\theta}_{y} = C^{\varphi+\theta e_i}_{y,i}$ is an optimal strategy for TFKW, assuming that Alice measures on her i-th qubit, i.e. $A^{\theta}_{y} = (A^n)^{\theta e_i}_{y,i}$. Before going ahead to the proof, we prove an important lemma that allows us to relate strategies of this form.

Lemma 7.9. Let ${}^0\mathtt{S}$ and ${}^1\mathtt{S}$ be two purified optimal strategies for TFKW. Suppose their shared states are equal, $|\psi\rangle = |{}^0\psi\rangle = |{}^1\psi\rangle$. Then we can choose that the local dilation operations be the same for both strategies and, in that case, the rigidity decompositions of the two states must be identical.

As before, we write $|\beta_s\rangle = X^{s_0}Z^{s_1}|\beta\rangle$.

Proof: Using Theorem 7.5, for each $i = 0, 1$ there exist Hilbert spaces with orthogonal decompositions $\mathcal{H}_{{}^iB'} = \bigoplus_{s\in\mathbb{Z}_2^2} {}^i\mathcal{B}_s$ and $\mathcal{H}_{{}^iC'} = \bigoplus_{s\in\mathbb{Z}_2^2} {}^i\mathcal{C}_s$; isometries ${}^iV : \mathcal{H}_B \to \mathcal{H}_{{}^iB'}$ and ${}^iW : \mathcal{H}_C \to \mathcal{H}_{{}^iC'}$; and for each $s \in \mathbb{Z}_2^2$ vectors $|\psi^i_s\rangle \in {}^i\mathcal{B}_s \otimes {}^i\mathcal{C}_s \otimes \mathcal{H}_R$ such that

$$({}^iV \otimes {}^iW)|\psi\rangle = \sum_{s\in\mathbb{Z}_2^2} |\beta_s\rangle \otimes |\psi^i_s\rangle. \tag{7.4.42}$$

Further, again following from the exact rigidity, for each $\theta \in \mathbb{Z}_2$ there exist PVMs ${}^iB'^{\theta} : \mathbb{Z}_2 \to \mathcal{P}({}^iB')$ and ${}^iC'^{\theta} : \mathbb{Z}_2 \to \mathcal{P}({}^iC')$ such that ${}^iV\,{}^iB^{\theta}_y|\psi\rangle = {}^iB'^{\theta}_y{}^iV|\psi\rangle$, ${}^iB'^{\theta}_y|\psi^i_s\rangle = \delta_{y,s_\theta}|\psi^i_s\rangle$, and $[{}^iB'^0_y, {}^iB'^1_{y'}] = 0$; and identically for the ${}^iC'^{\theta}_y$. First we show that the dilation unitaries can be constructed so that they are identical for $i = 0, 1$. Let $\mathcal{H}_{B'} = \mathcal{H}_{{}^0B'} \oplus \mathcal{H}_{{}^1B'} = \mathcal{H}_{{}^0B'\cup{}^1B'}$ and $\mathcal{H}_{C'} = \mathcal{H}_{{}^0C'} \oplus \mathcal{H}_{{}^1C'}$, so the isometries ${}^iV$ and ${}^iW$ can be seen as isometries into $\mathcal{H}'_B$ and $\mathcal{H}'_C$ respectively. Since the images of ${}^0V$ and ${}^1V$ have the same dimension in $\mathcal{H}_{B'}$, there exist unitaries ${}^0U, {}^1U \in \mathcal{U}(B')$ such that ${}^0U{}^0V = {}^1U{}^1V =: V$. Thus, we may redefine ${}^0V$ and ${}^1V$ to be this. Doing the same for C, to get W, we may assume that the dilation operators are the same for both strategies.

Define $|\psi'\rangle = (V \otimes W)|\psi\rangle$, and ${}^i\Pi^B_s = {}^iB'^0_{s_0}{}^iB'^1_{s_1}$ and ${}^i\Pi^C_s = {}^iC'^0_{s_0}{}^iC'^1_{s_1}$, the projectors onto ${}^i\mathcal{B}_s$ and ${}^i\mathcal{C}_s$, respectively. Expanding the two expressions of $|\psi'\rangle$ in the basis $\{|\beta_{00}\rangle, |\beta_{11}\rangle\}$ of A, we get the relations

$$\begin{aligned} |\psi^0_{00}\rangle + \tfrac{1}{\sqrt{2}}\big(|\psi^0_{01}\rangle + |\psi^0_{10}\rangle\big) &= |\psi^1_{00}\rangle + \tfrac{1}{\sqrt{2}}\big(|\psi^1_{01}\rangle + |\psi^1_{10}\rangle\big) \\ |\psi^0_{11}\rangle + \tfrac{1}{\sqrt{2}}\big(|\psi^0_{01}\rangle - |\psi^0_{10}\rangle\big) &= |\psi^1_{11}\rangle - \tfrac{1}{\sqrt{2}}\big(|\psi^1_{01}\rangle + |\psi^1_{10}\rangle\big). \end{aligned} \tag{7.4.43}$$

Projecting the second line onto ${}^0\mathcal{B}_{00}\otimes\mathcal{H}_{C'}$ gives $0 = {}^0\Pi^B_{00}|\psi^1_{11}\rangle - \frac{1}{\sqrt{2}}\big({}^0\Pi^B_{00}|\psi^1_{01}\rangle + {}^0\Pi^B_{00}|\psi^1_{10}\rangle\big)$, and projecting this onto ${}^0\mathcal{B}_{00} \otimes {}^1\mathcal{C}_s$ for $s = 01, 10, 11$ gives ${}^0\Pi^B_{00}|\psi^1_s\rangle = 0$. Thus, projecting

the first relation onto ${}^0\mathcal{B}_{00} \otimes \mathcal{H}_{C'}$ gives $|\psi^0_{00}\rangle = {}^0\Pi^B_{00}|\psi^1_{00}\rangle$. Repeating a similar procedure for each $s \in \mathbb{Z}_2^2$ gives $|\psi^0_s\rangle = {}^0\Pi^B_s|\psi^1_s\rangle$. It remains to show that the projectors act as the identity on these states. Suppose there exists s such that ${}^0\Pi^B_s$ does not preserve $|\psi^1_s\rangle$. Then, $\langle\psi^0_s|\psi^0_s\rangle = \langle\psi^1_s|{}^0\Pi^B_s|\psi^1_s\rangle < \langle\psi^1_s|\psi^1_s\rangle$. However, we have then

$$1 = \langle\psi'|\psi'\rangle = \sum_{t\in\mathbb{Z}_2^2} \langle\psi^0_t|\psi^0_t\rangle < \sum_{t\in\mathbb{Z}_2^2} \langle\psi^1_t|\psi^1_t\rangle = 1, \tag{7.4.44}$$

which is a contradiction. Thus, $|\psi^0_s\rangle = |\psi^1_s\rangle$, so the rigidity decompositions are identical. ■

Proof of Theorem 7.8: Knowing that the strategies ${}^{\varphi,i}\mathtt{S}$ are optimal, we can use the exact rigidity of Theorem 7.5 to get that there exist Hilbert spaces with orthogonal decompositions $\mathcal{H}_{\varphi,iB'} = \bigoplus_{s\in\mathbb{Z}_2^2} {}^{\varphi,i}\mathcal{B}_s$ and $\mathcal{H}_{\varphi,iC'} = \bigoplus_{s\in\mathbb{Z}_2^2} {}^{\varphi,i}\mathcal{C}_s$; isometries ${}^{\varphi,i}V : \mathcal{H}_B \to \mathcal{H}_{\varphi,iB'}$ and ${}^{\varphi,i}W : \mathcal{H}_C \to \mathcal{H}_{\varphi,iC'}$; and vectors $|\psi^{\varphi,i}_s\rangle \in \mathcal{H}_{A_1\cdots A_{i-1}A_{i+1}\cdots A_n} \otimes {}^{\varphi,i}\mathcal{B}_s \otimes {}^{\varphi,i}\mathcal{C}_s \otimes \mathcal{H}_R$ such that

$$({}^{\varphi,i}V \otimes {}^{\varphi,i}W)|\psi\rangle = \sum_{s\in\mathbb{Z}_2^2} |\beta_s\rangle_i \otimes |\psi^{\varphi,i}_s\rangle, \tag{7.4.45}$$

where we use the subscript i to indicate that the state is supported on register A_i. Using the same construction as the first part of Lemma 7.9, we can assume that there is equality between the registers ${}^{\varphi,i}B' = B'$ and the isometries ${}^{\varphi,i}V = V$ for all φ, i; and similarly for Charlie's. Then, by the lemma again, $|\psi^{\varphi,i}_s\rangle$ is constant over all values of φ, so we write $|\psi^i_s\rangle$ for this state. Still using the rigidity, there exist unitary observables ${}^{\varphi,i}B'_\theta \in \mathcal{U}(B')$ and ${}^{\varphi,i}C'_\theta \in \mathcal{U}(C')$ such that

$$V\ {}^{\varphi,i}B_\theta|\psi\rangle = {}^{\varphi,i}B'_\theta V|\psi\rangle \tag{7.4.46}$$

$${}^{\varphi,i}B'_\theta|\psi^i_s\rangle = (-1)^{s_\theta}|\psi^i_s\rangle \tag{7.4.47}$$

$$[{}^{\varphi,i}B'_\theta, {}^{\varphi,i}B'_{\theta+1}] = 0; \tag{7.4.48}$$

and identically for Charlie's observables. Note that, writing $|\psi'\rangle = (V \otimes W)|\psi\rangle$, these relations imply that like the original observables

$${}^{\varphi,i}B'_\theta|\psi'\rangle = {}^{\varphi,i}C'_\theta|\psi'\rangle. \tag{7.4.49}$$

The rigidity relations also imply that

$$ {}^{\varphi,i}B'_\theta|\psi'\rangle = {}^{\varphi',i}B'_\theta|\psi'\rangle \tag{7.4.50} $$

for valid values of φ, φ'.

The first goal is to show that all of the ${}^{\varphi,i}B'_\theta$ commute with respect to $|\psi'\rangle$. For $\chi \in \mathbb{Z}_2^n$, write ${}^iB_\chi = {}^{\chi+\chi_i e_i,i}B_{\chi_i}$ and similarly for the dilated operators, which simplifies the work a bit. From Eq. (5.2.5), the operator ${}^iB_\chi$ commutes with ${}^jB_\chi$. This extends directly to the dilated operators as

$$ \begin{aligned} {}^iB'_\chi {}^jB'_\chi|\psi'\rangle &= {}^iB'_\chi \otimes {}^jC'_\chi|\psi'\rangle = (V\otimes W){}^iB_\chi \otimes {}^jC_\chi|\psi\rangle \\ &= (V\otimes W){}^iB_\chi {}^jB_\chi|\psi\rangle = (V\otimes W){}^jB_\chi {}^iB_\chi|\psi\rangle \\ &= {}^jB'_\chi {}^iB'_\chi|\psi'\rangle, \end{aligned} \tag{7.4.51} $$

so ${}^iB'_\chi$ and ${}^jB'_\chi$ commute with respect to $|\psi'\rangle$. We extend this to all the observables using Lemma 7.9. Take any $i, j \in [n]$, $\chi, \chi' \in \mathbb{Z}_2^n$. If $i = j$, then let $\xi = \chi + (\chi_i + \chi'_i)e_i$. We have that ${}^iB'_\chi$ and ${}^iB'_\xi$ commute as they are the observables from the same game and ${}^iB'_{\chi'}|\psi'\rangle = {}^iB'_\xi|\psi'\rangle$ as they are equal on the i-th bit, so

$$ {}^iB'_\chi {}^iB'_{\chi'}|\psi'\rangle = {}^iB'_\chi {}^iB'_\xi|\psi'\rangle = {}^iB'_\xi {}^iB'_\chi|\psi'\rangle = {}^iB'_\xi \otimes {}^iC'_\chi|\psi'\rangle = {}^iB'_{\chi'} \otimes {}^iC'_\chi|\psi'\rangle = {}^iB'_{\chi'} {}^iB'_\chi|\psi'\rangle. \tag{7.4.52} $$

If $i \neq j$, there exists a ξ such that $\xi_i = \chi_i$ and $\xi_j = \chi'_j$. Then, we have that

$$ {}^iB'_\chi {}^jB'_{\chi'}|\psi'\rangle = {}^iB'_\chi \otimes {}^jC'_{\chi'}|\psi'\rangle = {}^iB'_\xi \otimes {}^jC'_\xi|\psi'\rangle = {}^iB'_\xi {}^jB'_\xi|\psi'\rangle = {}^jB'_\xi {}^iB'_\xi|\psi'\rangle = {}^jB'_{\chi'} {}^iB'_\chi|\psi'\rangle. \tag{7.4.53} $$

Thus, all of the observables commute.

Consider the group generated by the observables ${}^iB'_{\theta e_i}$ for $\theta \in \mathbb{Z}_2$ and $i \in [n]$. The commutation implies that this is a $(0, |\psi\rangle)$-representation f of $(\mathbb{Z}_2^2)^n$. This holds in the same way for Charlie's observables. Applying Gowers-Hatami, there exist Hilbert spaces with orthogonal decompositions $\mathcal{H}_{B''} = \bigoplus_{t\in(\mathbb{Z}_2^2)^n} \mathcal{B}_t$ and $\mathcal{H}_{C''} = \bigoplus_{t\in(\mathbb{Z}_2^2)^n} \mathcal{C}_t$; isometries $V' : \mathcal{H}_{B'} \to \mathcal{H}_{B''}$ and $W' : \mathcal{H}_{C'} \to \mathcal{H}_{C''}$; and observables that align with the decomposition ${}^iB''_\theta = \sum_{t\in(\mathbb{Z}_2^2)^n} (-1)^{t_{i\theta}} \mathbb{I}_{B,t}$ and ${}^iC''_\theta = \sum_{t\in(\mathbb{Z}_2^2)^n} (-1)^{t_{i\theta}} \mathbb{I}_{C,t}$ such that $V' {}^iB'_{\theta e_i}|\psi'\rangle = {}^iB''_\theta V'|\psi'\rangle$ and $W' {}^iC'_{\theta e_i}|\psi'\rangle = {}^iC''_\theta W'|\psi'\rangle$. By construction, ${}^iB''_\theta V'|\psi^i_s\rangle = (-1)^{s_\theta} V'|\psi^i_s\rangle$. Thus, the support of $V'|\psi^i_s\rangle$ on B'' is contained in the span of the subspaces $\mathcal{B}_t$ such that

$t_i = s$. Since an analogous inclusion holds for Charlie's space, we get that

$$(V' \otimes W')|\psi_s^i\rangle \in \bigoplus_{t_i = t_i' = s} \mathcal{H}_{A_1 \cdots A_{i-1} A_{i+1} \cdots A_n} \otimes \mathcal{B}_t \otimes \mathcal{C}_{t'} \otimes \mathcal{H}_R. \tag{7.4.54}$$

Defining $|\psi''\rangle = (V' \otimes W')|\psi\rangle$, this gives that

$$|\psi''\rangle \in \bigoplus_{\substack{t,t' \in (\mathbb{Z}_2^2)^n \\ t_i = t_i'}} \mathcal{H}_{A_1 \cdots A_{i-1}} \otimes |\beta_{t_i}\rangle \otimes \mathcal{H}_{A_{i+1} \cdots A_n} \otimes \mathcal{B}_t \otimes \mathcal{C}_{t'} \otimes \mathcal{H}_R \tag{7.4.55}$$

for all i. Taking the intersection of all these spaces, which is easy as the $\mathcal{B}_t$ and $\mathcal{C}_{t'}$ are orthogonal, we end up with

$$|\psi''\rangle \in \bigoplus_{t \in (\mathbb{Z}_2^2)^n} |\beta_{t_1}\rangle \otimes \cdots \otimes |\beta_{t_n}\rangle \otimes \mathcal{B}_t \otimes \mathcal{C}_t \otimes \mathcal{H}_R \tag{7.4.56}$$

■

We see also from the proof that ${}^{\varphi,i}B'_\theta|\psi_t\rangle = {}^{\varphi,i}C'_\theta|\psi_t\rangle = (-1)^{t_{i\theta}}|\psi_t\rangle$.

7.4.4 Robust parallel-repeated rigidity

Now, we consider the robust rigidity of the parallel-repeated game. We want to approach it in about the same way in the exact case, so first we need a generalisation of Lemma 7.9 to the approximate case.

Lemma 7.10. Let ${}^0\mathtt{S}$ and ${}^1\mathtt{S}$ be purified strategies for TFKW that both win with probability $\mathfrak{w}_{\mathtt{TFKW}}({}^i\mathtt{S}) \geq \cos^2\left(\frac{\pi}{8}\right) - \delta$ for some $\delta \geq 0$. If we suppose their shared states are equal, $|\psi\rangle = |^0\psi\rangle = |^1\psi\rangle$, then there is a constant $Q \geq 0$ such that for every $\theta \in \mathbb{Z}_2$,

$$\begin{aligned} \left\| {}^0B_\theta|\psi\rangle - {}^1B_\theta|\psi\rangle \right\| &\leq Q\sqrt{\delta} \\ \left\| {}^0C_\theta|\psi\rangle - {}^1C_\theta|\psi\rangle \right\| &\leq Q\sqrt{\delta}. \end{aligned} \tag{7.4.57}$$

The proof below lets us take $Q = 6300$.

Proof: For each of the strategies, we use robust rigidity of Theorem 7.6 where, by the method of Lemma 7.9, we may assume that the dilation operators are equal. Then, there exist constants $K, L \geq 0$; Hilbert spaces with two orthogonal decompositions $\mathcal{H}_{B'} = \bigoplus_{s \in \mathbb{Z}_2^2} {}^i\mathcal{B}_s$ and $\mathcal{H}_{C'} = \bigoplus_{s \in \mathbb{Z}_2^2} {}^i\mathcal{C}_s$; isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$; and

for each $s \in \mathbb{Z}_2^2$ vectors $|\psi_s^i\rangle \in {}^i\mathcal{B}_s \otimes {}^i\mathcal{C}_s \otimes \mathcal{H}_R$ such that

$$\left\|(V \otimes W)|\psi\rangle - \sum_{s\in\mathbb{Z}_2^2} |\beta_s\rangle \otimes |\psi_s^i\rangle\right\| \leq K\sqrt{\delta}. \tag{7.4.58}$$

Further, for each $\theta \in \mathbb{Z}_2$, there exist unitary observables (and related PVMs) ${}^iB'_\theta \in \mathcal{U}(B')$ and ${}^iC'_\theta \in \mathcal{U}(C')$ such that

$$\begin{aligned}
&\left\|(V\,{}^iB_\theta - {}^iB'_\theta V)|\psi\rangle\right\| \leq L\sqrt{\delta},\\
&\left\|(W\,{}^iC_\theta - {}^iC'_\theta W)|\psi\rangle\right\| \leq L\sqrt{\delta},\\
&{}^iB'_\theta|\psi_s^i\rangle = {}^iC'_\theta|\psi_s^i\rangle = (-1)^{s_\theta}|\psi_s^i\rangle,\\
&[{}^iB'_0, {}^iB'_1] = 0,\\
&[{}^iC'_0, {}^iC'_1] = 0.
\end{aligned} \tag{7.4.59}$$

First, using the triangle inequality, the distance between the two rigidity decompositions is

$$\left\|\sum_{s\in\mathbb{Z}_2^2} |\beta_s\rangle \otimes |\psi_s^0\rangle - \sum_{s\in\mathbb{Z}_2^2} |\beta_s\rangle \otimes |\psi_s^1\rangle\right\| \leq 2K\sqrt{\delta}. \tag{7.4.60}$$

Expanding the state on A in the basis $\{|\beta_{00}\rangle, |\beta_{11}\rangle\}$, this gives that both

$$\begin{aligned}
&\left\|\left(|\psi_{00}^0\rangle + \tfrac{1}{\sqrt{2}}(|\psi_{01}^0\rangle + |\psi_{10}^0\rangle)\right) - \left(|\psi_{00}^1\rangle + \tfrac{1}{\sqrt{2}}(|\psi_{01}^1\rangle + |\psi_{10}^1\rangle)\right)\right\| \leq 2K\sqrt{\delta}\\
&\left\|\left(|\psi_{11}^0\rangle + \tfrac{1}{\sqrt{2}}(|\psi_{01}^0\rangle - |\psi_{10}^0\rangle)\right) - \left(|\psi_{11}^1\rangle - \tfrac{1}{\sqrt{2}}(|\psi_{01}^1\rangle - |\psi_{10}^1\rangle)\right)\right\| \leq 2K\sqrt{\delta}.
\end{aligned} \tag{7.4.61}$$

Again as in Lemma 7.9, we act by projectors of the form ${}^i\Pi_s^B = {}^iB'^0_{s_0}\,{}^iB'^1_{s_1}$ and ${}^i\Pi_s^C = {}^iC'^0_{s_0}\,{}^iC'^1_{s_1}$. Since the action of a projector cannot increase the norm, acting by ${}^0\Pi_{00}^B \otimes {}^1\Pi_s^C$ on the second inequality of Eq. (7.4.61) gives

$$\|{}^0\Pi_{00}^B|\psi_{11}^1\rangle\| \leq 2K\sqrt{\delta} \text{ and } \|{}^0\Pi_{00}^B|\psi_{01}^1\rangle\|, \|{}^0\Pi_{00}^B|\psi_{10}^1\rangle\| \leq 2\sqrt{2}K\sqrt{\delta}. \tag{7.4.62}$$

Then, acting by ${}^0\Pi_{00}^B$ on the first inequality of Eq. (7.4.61) leads to $\||\psi_{00}^0\rangle - {}^0\Pi_{00}^B|\psi_{00}^1\rangle\| \leq 6K\sqrt{\delta}$. Similar is true for other values of s for the projectors, so

$$\left\||\psi_{00}^0\rangle - |\psi_{00}^1\rangle\right\| \leq \left\||\psi_{00}^0\rangle - {}^0\Pi_{00}^B|\psi_{00}^1\rangle\right\| + \sum_{s\neq 00}\left\|{}^0\Pi_s^B|\psi_{00}^1\rangle\right\| \leq 4(2+\sqrt{2})K\sqrt{\delta}. \tag{7.4.63}$$

The same thing holds in the same way for the other values of s in the ket. Then

$$\begin{aligned}\big\|({}^0B_\theta - {}^1B_\theta)|\psi\rangle\big\| &= \big\|(V\otimes W)({}^0B_\theta - {}^1B_\theta)|\psi\rangle\big\| \\ &\leq \big\|({}^0B'_\theta - {}^1B'_\theta)(V\otimes W)|\psi\rangle\big\| + 2L\sqrt{\delta} \\ &\leq \Big\|{}^0B'_\theta \sum_{s\in\mathbb{Z}_2^2}|\beta_s\rangle\otimes|\psi_s^0\rangle - {}^1B'_\theta\sum_{s\in\mathbb{Z}_2^2}|\beta_s\rangle\otimes|\psi_s^1\rangle\Big\| + 2K\sqrt{\delta} + 2L\sqrt{\delta} \\ &= \Big\|\sum_{s\in\mathbb{Z}_2^2}(-1)^{s_\theta}|\beta_s\rangle\otimes(|\psi_s^0\rangle - |\psi_s^1\rangle)\Big\| + 2K\sqrt{\delta} + 2L\sqrt{\delta} \\ &\leq 2\Big[(17+8\sqrt{2})K + L\Big]\sqrt{\delta}\end{aligned} \tag{7.4.64}$$

We can do the same with Charlie's observables. ■

Theorem 7.11 (robust parallel-repeated rigidity)**.** Let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \rho = |\psi\rangle\langle\psi|\big)$ be a purified strategy for $\mathtt{TFKW}^n$ for some $n\in\mathbb{N}$. Suppose that for some $\varepsilon\geq 0$, for each $i\in[n]$, the i-th game wins with probability $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$. Then, there exists a constant $K\geq 0$, registers B' and C', and isometries $V\in\mathcal{U}(B,B')$ and $W\in\mathcal{U}(C,C')$ such that the distance between quantum states

$$\Big\|(V\otimes W)|\psi\rangle - \sum_{t\in(\mathbb{Z}_2^2)^n} X^{t_{10}}Z^{t_{11}}|\beta\rangle\otimes\cdots\otimes X^{t_{n0}}Z^{t_{n1}}|\beta\rangle\otimes|\psi_t\rangle\Big\| \leq Kn^3\sqrt{\varepsilon}, \tag{7.4.65}$$

where the $|\psi_t\rangle\in\mathcal{H}_{B'C'R}$ have orthogonal supports on both B' and C'; and there exists a constant $L\geq 0$ and commuting observables ${}^{\varphi,i}B'_\theta\in\mathcal{U}(B')$ and ${}^{\varphi,i}C'_\theta\in\mathcal{U}(C')$ such that

$$\begin{aligned}\big\|V\,{}^{\varphi,i}B_\theta|\psi\rangle - {}^{\varphi,i}B'_\theta V|\psi\rangle\big\| &\leq Ln^2\sqrt{\varepsilon} \\ \big\|W\,{}^{\varphi,i}C_\theta|\psi\rangle - {}^{\varphi,i}C'_\theta W|\psi\rangle\big\| &\leq Ln^2\sqrt{\varepsilon}\end{aligned} \tag{7.4.66}$$

$${}^{\varphi,i}B'_\theta|\psi_t\rangle = {}^{\varphi,i}C'_\theta|\psi_t\rangle = (-1)^{t_{i\theta}}|\psi_t\rangle, \tag{7.4.67}$$

for at least one value of φ for each i.

The proof below gives that we may take values $L = 230\ 000$, and for large enough n, $K = 320\ 000$.

We make use of the fact that, as in the exact case, the i-th winning probability is $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) = \mathbb{E}_{\substack{\varphi\in\mathbb{Z}_2^n\\ \varphi_i=0}}\mathfrak{w}_{\mathtt{TFKW}}({}^{\varphi,i}\mathtt{S})$. However, since the i-th winning probability is not quite optimal, showing that the ${}^{\varphi,i}\mathtt{S}$ win near-optimally proves to be an obstacle. To get past this,

we adapt a technique of [Col17] for parallel repetition of CHSH games. It guarantees that there is a "good set" of strategies that win with only slightly relaxed probability, and the set is large enough to continue the proof as for the exact case.

Proof: Define $\varepsilon_{\varphi,i} \geq 0$ such that $\mathfrak{w}_{\texttt{TFKW}}({}^{\varphi,i}\mathtt{S}) = \cos^2 \frac{\pi}{8} - \varepsilon_{\varphi,i}$. Then, we have that, for each i, $\varepsilon \geq \mathbb{E}_{\substack{\varphi\in\mathbb{Z}_2^n \\ \varphi_i=0}} \varepsilon_{\varphi,i}$. We want to collect a large enough number of terms where $\varepsilon_{\varphi,i}$ is not too large with respect to ε. To that effect, define the set of good values of φ for i as

$$G_i = \{\varphi \in \mathbb{Z}_2^n | \varphi_i = 0, \varepsilon_{\varphi,i} \leq 5\varepsilon\}. \tag{7.4.68}$$

As in [Col17], we claim that $|G_i| \geq 2^{n-2}+2^{n-3}+1$. In fact, suppose $|G_i| < 2^{n-2}+2^{n-3}+1$. Then, there are at least 2^{n-3} values of φ where $\varepsilon_{\varphi,i} > 5\varepsilon$. This gives however that

$$\varepsilon \geq \frac{1}{2^{n-1}} \sum_{\varphi} \varepsilon_{\varphi,i} > \frac{1}{2^{n-1}} 2^{n-3}(5\varepsilon) = \frac{5}{4}\varepsilon > \varepsilon, \tag{7.4.69}$$

which is a contradiction. Now, as for the case of a single game, for $\varphi \in G_i$, the SOS decomposition implies

$$\left\| (Z_i \otimes {}^{\varphi,i}B_0 + X_i \otimes {}^{\varphi,i}B_1 - \sqrt{2})|\psi\rangle \right\| \leq 2\sqrt{5}(2 + 8^{1/4})\sqrt{\varepsilon} \tag{7.4.70}$$

$$\left\| {}^{\varphi,i}B_\theta|\psi\rangle - {}^{\varphi,i}C_\theta|\psi\rangle \right\| \leq 4\sqrt{5}\sqrt{\varepsilon}. \tag{7.4.71}$$

This gives the commutation of ${}^{\varphi,i}B_0$ and ${}^{\varphi,i}B_1$ with respect to $|\psi\rangle$ as

$$\left\| [{}^{\varphi,i}B_0, {}^{\varphi,i}B_1]|\psi\rangle \right\| \leq 2\sqrt{5}(2+\sqrt{2})(2+8^{1/4})\sqrt{\varepsilon} =: K_0\sqrt{\varepsilon}. \tag{7.4.72}$$

Now, we need commutation between operators for different values of i. Let $i \neq i' \in [n]$, $\theta, \theta' \in \mathbb{Z}_2$ and $\varphi, \varphi' \in \mathbb{Z}_2^n$ such that $\varphi_i = \varphi'_{i'} = 0$. By the pigeonhole principle, there exists a $\chi \in (G_i + \theta 1^i) \cap (G_{i'} + \theta' 1^{i'})$, so using Lemma 7.10 with $\delta = 5\varepsilon$, there exists $Q \geq 0$ such that

$$\begin{aligned} \left\| ({}^{\varphi,i}B_\theta - {}^{\chi+\theta 1^i,i}B_\theta)|\psi\rangle \right\| &\leq \sqrt{5}Q\sqrt{\varepsilon} \\ \left\| ({}^{\varphi',i'}B_{\theta'} - {}^{\chi+\theta' 1^{i'},i'}B_{\theta'})|\psi\rangle \right\| &\leq \sqrt{5}Q\sqrt{\varepsilon}, \end{aligned} \tag{7.4.73}$$

and identically for Charlie's observables. Thus, knowing $\left\| [{}^{\chi+\theta 1^i,i}B_\theta, {}^{\chi+\theta' 1^{i'},i'}B_{\theta'}]|\psi\rangle \right\| \leq$

$K_0\sqrt{\varepsilon}$, we have

$$\begin{aligned}\left\|[{}^{\varphi,i}B_\theta, {}^{\varphi',i'}B_{\theta'}]|\psi\rangle\right\| &\leq \left\|({}^{\varphi,i}B_\theta \otimes {}^{\varphi',i'}C_{\theta'} - {}^{\varphi',i'}B_{\theta'} \otimes {}^{\varphi,i}C_\theta)|\psi\rangle\right\| + 8\sqrt{5}\sqrt{\varepsilon} \\ &\leq \left\|({}^{\chi+\theta 1^i,i}B_\theta \otimes {}^{\chi+\theta' 1^{i'},i'}C_{\theta'} - {}^{\chi+\theta' 1^{i'},i'}B_{\theta'} \otimes {}^{\chi+\theta 1^i,i}C_\theta)|\psi\rangle\right\| \\ &\quad + (4\sqrt{5}Q + 8\sqrt{5})\sqrt{\varepsilon} \\ &\leq (4\sqrt{5}(Q+4) + K_0)\sqrt{\varepsilon}.\end{aligned} \tag{7.4.74}$$

Now, for any i, we may pick some $\varphi \in G_i$, and define ${}^iB_\theta := {}^{\varphi,i}B_\theta$. We have

$$\|[{}^iB_\theta, {}^{i'}B_{\theta'}]|\psi\rangle\| \leq (4\sqrt{5}(Q+4) + K_0)\sqrt{\varepsilon}. \tag{7.4.75}$$

Then, we use Lemma 7.3 with $U_{i\theta} = {}^iB_\theta$ and $V_{i\theta} = {}^iC_\theta$ so $\epsilon = 4\sqrt{5}\sqrt{\varepsilon}$ and $\delta = (4\sqrt{5}(Q+4) + K_0)\sqrt{\varepsilon}$ to generate an $(Ln^2\sqrt{\varepsilon}, |\psi\rangle)$-representation of $(\mathbb{Z}_2^2)^n$, where $L = 4(4\sqrt{5}(Q+7) + K_0)$. The same holds in the same way for Charlie's observables.

So, this puts us in the right place to use the Gowers-Hatami theorem again. There exist Hilbert spaces with orthogonal decompositions $\mathcal{H}_{B'} = \bigoplus_{t\in(\mathbb{Z}_2^2)^n} \mathcal{B}_t$ and $\mathcal{H}_{C'} = \bigoplus_{t\in(\mathbb{Z}_2^2)^n} \mathcal{C}_t$; isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$; and unitary observables ${}^iB'_\theta = \sum_{t\in(\mathbb{Z}_2^2)^n}(-1)^{t_{i\theta}}\mathbb{I}_{B,t} \in \mathcal{U}(B')$ and ${}^iC'_\theta = \sum_{t\in(\mathbb{Z}_2^2)^n}(-1)^{t_{i\theta}}\mathbb{I}_{C,t} \in \mathcal{U}(C')$ such that

$$\begin{aligned}\left\|(V\,{}^iB_\theta - {}^iB'_\theta V)|\psi\rangle\right\| &= Ln^2\sqrt{\varepsilon} \\ \left\|(W\,{}^iC_\theta - {}^iC'_\theta W)|\psi\rangle\right\| &= Ln^2\sqrt{\varepsilon}.\end{aligned} \tag{7.4.76}$$

Let $|\psi'\rangle = (V \otimes W)|\psi\rangle$. We can put these observables back into the original inequalities to get

$$\left\|(Z_i \otimes {}^iB'_0 + X_i \otimes {}^iB'_1 - \sqrt{2})|\psi'\rangle\right\| \leq (2Ln^2 + 2\sqrt{5}(2 + 8^{1/4}))\sqrt{\varepsilon} \tag{7.4.77}$$

$$\left\|({}^iB'_\theta - {}^iC'_\theta)|\psi'\rangle\right\| \leq (2Ln^2 + 4\sqrt{5})\sqrt{\varepsilon}. \tag{7.4.78}$$

Since the quantum state $|\psi'\rangle \in \bigoplus_{t,t'\in(\mathbb{Z}_2^2)^n} \mathcal{H}_{A_1\cdots A_n} \otimes \mathcal{B}_t \otimes \mathcal{C}_{t'} \otimes \mathcal{H}_R$, we can write it as $|\psi'\rangle = \sum_{t,t'\in(\mathbb{Z}_2^2)^n}|v_{t,t'}\rangle$. Using

$$Z_i \otimes {}^iB'_0 + X_i \otimes {}^iB'_1 - \sqrt{2} = 2\sqrt{2}\sum_t (\,|\beta_{t_i}\rangle\langle\beta_{t_i}|_i - \mathbb{I}) \otimes \mathbb{I}_{B,t} \tag{7.4.79}$$

and defining $|v_{\beta,i}\rangle = \sum_{t,t'\in(\mathbb{Z}_2^2)^n}(|\beta_{t_1}\rangle\langle\beta_{t_1}|_1 \otimes \cdots \otimes |\beta_{t_i}\rangle\langle\beta_{t_i}|_i)|v_{t,t'}\rangle$, we have

$$\begin{aligned}\||\psi'\rangle - |v_{\beta,n}\rangle\| &\leq \sum_{i=1}^{n-1}\||v_{\beta,i}\rangle - |v_{\beta,i+1}\rangle\| \\ &\leq \frac{1}{2\sqrt{2}}\sum_{i=1}^{n-1}\Big\|(Z_i\otimes {}^iB'_0 + X_i\otimes {}^iB'_1 - \sqrt{2})|\psi'\rangle\Big\| \\ &\leq \tfrac{n}{\sqrt{2}}(Ln^2 + \sqrt{5}(2+8^{1/4}))\sqrt{\varepsilon}.\end{aligned} \tag{7.4.80}$$

On the other hand, Eq. (7.4.78) implies

$$(2Ln^2 + 4\sqrt{5})\sqrt{\varepsilon} \geq \Big\|\sum_{t,t'}((-1)^{t_{i\theta}} - (-1)^{t'_{i\theta}})|v_{t,t'}\rangle\Big\| = 2\Big\|\sum_{t_{i\theta}\neq t'_{i\theta}}|v_{t,t'}\rangle\Big\| \tag{7.4.81}$$

Write $|\psi'\rangle = |v_0\rangle + |v_1\rangle$ where $|v_0\rangle = \sum_{t\in(\mathbb{Z}_2^2)^n}|v_{t,t}\rangle$ and $|v_1\rangle = \sum_{t\neq t'}|v_{t,t'}\rangle$. Then,

$$\||v_1\rangle\|^2 = \sum_{t\neq t'}\langle v_{t,t'}|v_{t,t'}\rangle \leq \sum_{\theta}\sum_{i=1}^{n}\sum_{t_{i\theta}\neq t'_{i\theta}}\langle v_{t,t'}|v_{t,t'}\rangle \leq 2n\Big[(Ln^2+2\sqrt{5})\sqrt{\varepsilon}\Big]^2. \tag{7.4.82}$$

Now, let $|v_\beta\rangle = \sum_{t\in(\mathbb{Z}_2^2)^n}(|\beta_{t_1}\rangle\langle\beta_{t_1}| \otimes \cdots |\beta_{t_n}\rangle\langle\beta_{t_n}|)|v_{t,t}\rangle$. Then $\||v_\beta\rangle - |v_{\beta,n}\rangle\| \leq \||v_1\rangle\|$, so

$$\begin{aligned}\||\psi'\rangle - |v_\beta\rangle\| &\leq \||\psi'\rangle - |v_{\beta,n}\rangle\| + \||v_{\beta,n}\rangle - |v_\beta\rangle\| \\ &\leq \Big[\tfrac{n}{\sqrt{2}}(Ln^2 + \sqrt{5}(2+8^{1/4})) + \sqrt{2n}(Ln^2+2\sqrt{5})\Big]\sqrt{\varepsilon}.\end{aligned} \tag{7.4.83}$$

Now, $|v_\beta\rangle$ has the form we want, but it may not be normalised. Define $|\phi\rangle = \frac{|v_\beta\rangle}{\||v_\beta\rangle\|}$. We have

$$\||\phi\rangle - |v_\beta\rangle\| = 1 - \||v_\beta\rangle\| \leq \||\psi'\rangle - |v_\beta\rangle\|, \tag{7.4.84}$$

giving

$$\||\psi'\rangle - |\phi\rangle\| \leq 2\||\psi'\rangle - |v_\beta\rangle\| \leq \sqrt{2}\Big[n(Ln^2 + \sqrt{5}(2+8^{1/4})) + 2\sqrt{n}(Ln^2+2\sqrt{5})\Big]\sqrt{\varepsilon} \tag{7.4.85}$$

■

We can, as in the single-round case, generalise this result slightly to a general strategy.

Corollary 7.12. Let $n \in \mathbb{N}$ and let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \rho\big)$ be an arbitrary strategy for $\mathtt{TFKW}^n$. Suppose that for some $\varepsilon \geq 0$, for each $i \in [n]$, the i-th game wins with probability $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) \geq \cos^2 \frac{\pi}{8} - \varepsilon$. Then there exists a constant $K \geq 0$ and isometries $V \in \mathcal{U}(B, B')$ and $W \in \mathcal{U}(C, C')$ such that

$$\big\|(V \otimes W)\rho(V \otimes W)^\dagger - \mathrm{Tr}_R(\,|\phi\rangle\langle\phi|)\big\|_{\mathrm{Tr}} \leq K n^3 \sqrt{\varepsilon}, \tag{7.4.86}$$

where R is an auxiliary register such that

$$|\phi\rangle = \sum_{t \in (\mathbb{Z}_2^2)^n} X^{t_{10}} Z^{t_{11}} |\beta\rangle \otimes \cdots \otimes X^{t_{n0}} Z^{t_{n1}} |\beta\rangle \otimes |\psi_t\rangle \tag{7.4.87}$$

for some vectors $|\psi_t\rangle \in \mathcal{H}_{B'C'R}$ with orthogonal supports on both B' and C'.

The proof follows the same method as Corollary 7.7.

7.5 Rigidity and Observed Statistics

In any self-testing scenario, the referee cannot actually query the winning probability of the adversaries' strategy. To get around this, she may play many rounds of the game in parallel and use the players' winning statistics to approximate their winning probability. The difficulty that arises, however, is that the players' strategies need not be independent for the different rounds of the game, and therefore the information Alice receives might not be meaningful. A technique of [RUV13] allows us to get around this: first, we bound the probability of winning too many of the games if enough are too far from optimal, and then find good values of the bounding constants, depending on the application, so Alice may extract information about the state.

Lemma 7.13. Let $0 < \varepsilon, \eta < 1$ and let $\delta > 0$ such that $\delta \leq \eta\varepsilon$. Let $\mathtt{S}$ be a strategy for $\mathtt{TFKW}^n$. Let $E \subseteq \{0, \ldots, n\}$ be the set of rounds i such that $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) \geq \cos^2 \frac{\pi}{8} - \varepsilon$, and let $W \in \{0, \ldots, n\}$ be the number of rounds the adversaries win. Then, if $|E| < (1 - \eta)n$,

$$\Pr\big(W \geq (\cos^2 \tfrac{\pi}{8} - \delta)n\big) \leq e^{-2n(\eta\varepsilon - \delta)^2}. \tag{7.5.1}$$

We can make use of this in contrapositive. That is, other than with small probability, if the adversaries win at least $(\cos^2 \frac{\pi}{8} - \delta)n$ games, then at least $(1 - \eta)n$ of the games win

with near-optimal winning probability. The proof proceeds in the same way as a similar result for sequentially repeated games in [RUV13].

Proof: Write $w^* = \cos^2 \frac{\pi}{8}$ for convenience. Let W_i be the random variable that is 1 if the adversaries won round i and 0 if they lost. Then, we have that W is the random variable $W = \sum_{i=1}^n W_i$. Since $\Pr(W_i = 1) = \mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S})$, if $i \in E$, we know that $\Pr(W_i = 1) \leq w^*$, and if $i \notin E$, $\Pr(W_i = 1) \leq w^* - \varepsilon$. Let $\Gamma_1, \ldots, \Gamma_n, \Lambda_1, \ldots, \Lambda_n$ be independent Bernoulli variables such that the $\Pr(\Gamma_i = 1) = w^*$ and $\Pr(\Lambda_i = 1) = w^* - \varepsilon$. By the above, we can couple them to the W_i so that $W_i \leq \Gamma_i$ if $i \in E$ and $W_i \leq \Lambda_i$ if $i \notin E$. This implies directly that $W \leq \sum_{i\in E} \Gamma_i + \sum_{i\notin E} \Lambda_i$, so

$$\Pr(W \geq (w^* - \delta)n) \leq \Pr\Big(\sum_{i\in E} \Gamma_i + \sum_{i\notin E} \Lambda_i \geq (w^* - \delta)n\Big). \tag{7.5.2}$$

Since $\mathbb{E}\Big(\sum_{i\in E} \Gamma_i + \sum_{i\notin E} \Lambda_i\Big) = |E|w^* + (n - |E|)(w^* - \varepsilon)$, Hoeffding's inequality implies

$$Pr(W \geq (w^* - \delta)n) \leq e^{-\frac{2}{n}((n-|E|)\varepsilon - \delta n)^2} \leq e^{-2n(\eta\varepsilon - \delta)^2} \tag{7.5.3}$$

■

A simple canonical choice of variables for large n is $\varepsilon = \eta = \delta = \frac{1}{n^{1/4}}$, which allows Alice to test sets of $k \sim n^{1/25}$ parallel rounds, where she is able say that the state is $\sim \frac{1}{k^{1/8}}$ near-optimal for those rounds with probability exponentially close to 1 in k.

In view of applications, we give in Theorem 7.14 a version of Corollary 7.12 where Alice has less information about the winning probabilities of the strategy. Rather than assuming that she knows that they win each round near-optimally, we will assume that Alice only knows with high probability that each round wins near-optimally. Then, we are able to ascertain the behaviour of the shared state in expectation. This will allow us to directly apply the result of Lemma 7.13 to get conclusions about the rigidity of the state.

Theorem 7.14. Let $n \in \mathbb{N}$ and let $\mathtt{S} = \big(B, C, \{B^\theta\}, \{C^\theta\}, \rho\big)$ be a strategy for $\mathtt{TFKW}^n$. Suppose that for some $\varepsilon, \eta \in [0, 1]$, for each $i \in [n]$, there is a probability $1 - \eta$ that the i-th game wins with probability $\mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}) \geq \cos^2 \frac{\pi}{8} - \varepsilon$. Then, there exists a constant $K \geq 0$, registers B' and C', and isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ such that the expected value of the distance between quantum states

$$\mathbb{E}\big\|(V \otimes W)\rho(V \otimes W)^\dagger - \mathrm{Tr}_R(\,|\phi\rangle\langle\phi|)\big\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta, \tag{7.5.4}$$

where $|\phi\rangle = \sum_{t\in(\mathbb{Z}_2^2)^n} X^{t_{10}}Z^{t_{11}}|\beta\rangle \otimes \cdots \otimes X^{t_{n0}}Z^{t_{n1}}|\beta\rangle \otimes |\psi_t\rangle$ for some auxiliary register R and $|\psi_t\rangle \in \mathcal{H}_{B'C'R}$ with orthogonal supports on both B' and C'.

Proof: For each $i \in [n]$, let H_i be the random variable indicating if $\mathfrak{w}^i_{\texttt{TFKW}^n}(\texttt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$. We have $\Pr(H_i = 1) = 1 - \eta$. Let $H \subseteq [n]$ be the register-valued random variable such that $i \in H$ if and only if $H_i = 1$; let $L = [n]\backslash H$ be the complement. Since for any round in H, $\mathfrak{w}^i_{\texttt{TFKW}^n}(\texttt{S}) \geq \cos^2\frac{\pi}{8} - \varepsilon$, we can apply the rigidity of Corollary 7.12 to those rounds. Then, there exists a constant $K \geq 0$, register B' and C', isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$, and a state $|\phi\rangle \in \mathcal{H}_{A_HA_LB'C'R}$ of the form $|\phi\rangle = \sum_{t\in(\mathbb{Z}_2^2)^{|H|}} |\beta_t\rangle_{A_H} \otimes |\psi_t\rangle$ where the supports of the $|\psi_t\rangle \in \mathcal{H}_{A_LB'C'R}$ on both B' and C' are orthogonal such that

$$\left\|(V\otimes W)\rho(V\otimes W)^\dagger - \mathrm{Tr}_R(|\phi\rangle\langle\phi|)\right\|_{\mathrm{Tr}} \leq K|H|^3\sqrt{\varepsilon} \leq Kn^3\sqrt{\varepsilon}. \tag{7.5.5}$$

Let $\sigma = |\beta\rangle\langle\beta|^{\otimes L}_{A_L} \otimes \mathrm{Tr}_{A_LR}(|\phi\rangle\langle\phi|)$. Then, σ has the form we want and $\|\mathrm{Tr}_R(|\phi\rangle\langle\phi|) - \sigma\|_{\mathrm{Tr}} \leq n - |H|$, giving that $\mathbb{E}\|\mathrm{Tr}_R(|\phi\rangle\langle\phi|) - \sigma\|_{\mathrm{Tr}} \leq n - \sum_i H_i = n\eta$. Using the triangle inequality, we get the wanted result. ■

We give an example of the use of the results of this section by considering an explicit choice of parameters.

Example 7.15. Fix some large $n \in \mathbb{N}$. Take $\varepsilon = n^{-8}$, $\eta = n^{-2}$, and $\delta = \frac{1}{2}n^{-10}$. Suppose Alice plays $N = n^{21}$ rounds of the TFKW game in parallel with Bob and Charlie, and that the players are able to win at least $\cos^2\frac{\pi}{8}N - \frac{1}{2}n^{11}$ of them. Then Lemma 7.13 implies that, other than with probability $e^{-\frac{n}{2}}$, there are at least $(1 - n^{-2})N$ rounds that won with probability $\mathfrak{w}^i_{\texttt{TFKW}^n}(\texttt{S}) \geq \cos^2\frac{\pi}{8} - n^{-8}$. Then Alice can check the winning probability on n rounds chosen uniformly at random: call this register A'. Due to the uniform randomness, each of the n has probability $1 - n^{-2}$ of being within n^{-8} of optimal. Then, we can use the rigidity of Theorem 7.14 to say that there exists a constant $K \geq 0$, registers B' and C', and isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$ such that the expected value of the distance between quantum states

$$\mathbb{E}\left\|(V\otimes W)\rho_{A'BCR}(V\otimes W)^\dagger - \mathrm{Tr}_R(|\phi\rangle\langle\phi|)\right\|_{\mathrm{Tr}} \leq \frac{K+1}{n}, \tag{7.5.6}$$

where $|\phi\rangle = \sum_{t\in(\mathbb{Z}_2^2)^n} X^{t_{10}}Z^{t_{11}}|\beta\rangle \otimes \cdots \otimes X^{t_{n0}}Z^{t_{n1}}|\beta\rangle \otimes |t\rangle_{BCR}$ for some auxiliary register R and $|t\rangle_{BCR} \in \mathcal{H}_{B'C'R}$ with orthogonal supports on both B' and C'.

Chapter 8

Cryptographic Applications

In this chapter, we study the cryptographic applications of our uncloneability game results, introduced in Section 2.3. In Section 8.1 we provide a high-level introduction to cryptography in classical and quantum contexts. Then in Sections 8.2, 8.3, 8.4 and 8.5, we formally introduce uncloneable encryption, quantum key distribution, bit commitment, and randomness expansion, respectively, and study applications to these.

This chapter is based on joint work with Anne Broadbent [BC21, BC22].

8.1 Introduction to Cryptography

In this section, we briefly introduce the field of cryptography, following Katz and Lindell [KL07]. Put very generally, cryptography is concerned with the integrity of information in an adversarial setting. It seeks to describe and study scenarios where honest parties attempt to use information without having it fall into the hands of a dishonest adversary.

To illustrate this, we discuss the most basic type of cryptographic protocol: the *encryption scheme*. An encryption scheme is simply a map that takes as input a message m and a key k, and outputs a ciphertext c. It should also be possible to decrypt: there exists a map that, given the key and ciphertext as input, outputs the correct message. The necessity of decryption means that the encryption map cannot simply act by deleting the message. The encryption scheme is *secure* if, for keys sampled according to some given distribution, it is hard to guess the original message for an adversary who has access to the ciphertext but not the key. The method the adversary uses to come up with a guess of the message is called an *attack*. It is important to note that the adversary is assumed to know everything about the encryption scheme, except for the key. This idea is called *Kerckhoffs' principle*,

after its originator, who was the first to note that encryption whose security is based on obfuscation of the scheme is very susceptible to attack, as the description of the scheme is all that needs to be learned in order to break its security completely.

An important question remains: how do we quantify that a message is hard to guess? The strongest way to do this is to ensure *perfect security*. This is the guarantee that the distribution of ciphertexts is independent of the distribution of messages. In this setting, an adversary can only make a guess of the message based on its frequency in the message distribution. A fundamental scheme satisfying perfect security is the *one-time pad*. The messages and the keys for this scheme are bit strings of the same length, and the ciphertext $c = m + k$ is their XOR. Then, as long as the keys are sampled uniformly, the ciphertext distribution is uniformly random for any message. Any perfectly secure encryption scheme is equivalent to a one-time pad, in the sense that there must be as many keys as there are messages and they must be uniformly random [Sha49]. This is often not practicable, as the key generation and distribution is highly inefficient.

A common way to bypass this problem is to weaken the condition of being hard to guess. A first, slight, weakening is *information-theoretic security*. Here, the scheme needs again to be secure against any adversary, but we allow the adversary to be able to guess the message with small *advantange* ε, the difference between the real guessing probability and the probability in the case of perfect security. We see below that this is a sufficient weakening for many of the cryptographic tasks we consider.

However, it is often both necessary and practical to further assume that the adversary's abilities are restricted in some way. Chief among these is *computational security*, restricting adversaries to only be able to make computations that are efficient for a computer to run. Efficiency is phrased asymptotically in some security parameter λ, that often scales with the length of the message: to achieve security, the adversary's advantage must be negligibly small in the security parameter, for any attack that takes polynomially-many steps of computation. Formally, computational time complexity is understood by converting the algorithm to a Turing machine. We do not go into depth about the theory of computation; we refer to [AB09] for a full discussion. Importantly, we may additionally assume that an adversary is unable to efficiently undertake some computation for which no efficient algorithm is known, but it is unknown if such an algorithm exists; this is a *computational assumption*.

In the computational model, the natural notion of security is *indistinguishability*. To be indistinguishably secure, the probability that an adversary is able to distinguish the encryp-

tions of two messages should be negligibly close to $\frac{1}{2}$, even if the messages were provided by the adversary themselves. A perfectly secure scheme satisfies this, so indistinguishable security can be seen as a generalisation of perfect security.

These ideas of security can be generalised to a wide range of cryptographic scenarios beyond encryption. Basic cryptographic procedures, from which other more complicated protocols may be constructed, are called *cryptographic primitives*. We work with a variety of them in the body of this chapter.

8.1.1 Quantum cryptography

So far, however, we have only considered cryptography with resources provided by classical physics. By extending the resource model to also include quantum information, we enter the domain of *quantum cryptography*. The inclusion of quantum information has been able to improve the strength of cryptographic protocols, and also allow for the development of new ones.

Many of the ideas of classical cryptography carry over to the quantum setting. Here, both the honest parties and the adversaries are able to make use of quantum computers. In the information-theoretic setting, the trace distance between quantum states is often used to represent indistinguishability, due to the relation of Eq. (4.2.22), which represents the trace norm via the optimum over all, potentially computationally unfeasible, distinguishing measurements. On the other hand, in the computational setting, the adversaries make use of only the quantum polynomial-time (QPT) algorithms, potentially subject to further computational assumptions. For a full formal introduction to quantum computation, we refer again to [AB09]; nonetheless, we provide a definition of what it means for an algorithm to be QPT.

Definition 8.1. An algorithm $Q : \mathbb{Z}_2^* \to \mathbb{Z}_2^*$ is *quantum polynomial-time* (QPT) if there exists a Turing machine T such that, for each $n \in \mathbb{N}$, $T(n)$ outputs in polynomial time the description of a quantum circuit that, on input $x \in \mathbb{Z}_2^n$, outputs $Q(x)$. Similarly, we can consider a family of states $\{\rho_n\}_{n\in\mathbb{N}}$ QPT if $T(n)$ outputs a quantum circuit that constructs ρ_n from $|0\rangle$; a family of unitaries $\{U_n\}_{n\in\mathbb{N}}$ QPT if $T(n)$ provides a quantum circuit that acts as U_n; and a family of measurements $\{A_n\}_{n\in\mathbb{N}}$ QPT if the measurement A_n can be undertaken by first acting by some QPT unitary U_n and then measuring in the computational basis.

An early quantum cryptographic primitive is the *quantum money* of Wiesner [Wie83]. Apart from being interesting in its own right, it is a useful example of how the no-cloning principle can manifest itself in cryptography. A quantum money scheme is a quantum algorithm that, when run honestly, creates a token — a quantum money state — in such a way that it is immune to forgery. The original protocol creates a quantum money state by encoding a random string in a random conjugate-coding basis; and verifies by measuring in the correct basis. Because a prospective dishonest forger does not know the preparation basis, they are unable to learn the encoded string and to forge the state. This property can be justified using the no-cloning principle, but the actual security proof requires a more involved study of the quantum states. We study a variety of quantum cryptographic primitives that make use of uncloneability in a similar way to quantum money.

8.2 Interactive Uncloneable Encryption

8.2.1 Quantum encryption of classical messages

Encryption of messages can be carried over to the quantum setting. Though it is possible to consider encryption of quantum messages [AMTdW00, BR03], we focus on the encryption of classical messages as quantum states. The benefit of such an encryption is to allow classical messages to also benefit from the cryptographic properties satisfied by quantum states, such as no-cloning. The idea of a quantum encryption of classical messages was formalised in [BL20]; we introduce a variant of this definition.

Definition 8.2. A *quantum encryption of classical messages (QECM)* scheme is a tuple $\mathtt{Q} = (\mathtt{Key}, \mathtt{Enc}, \mathtt{Dec})$.

- $\mathtt{Key} : \mathcal{D}(\{0\}) \to \mathcal{D}(K)$ is CPTP map representing the *key-generation algorithm*, where K is the classical key register.
- $\mathtt{Enc} : \mathcal{D}(KM) \to \mathcal{D}(KMC)$ is the CPTP map representing the *encryption algorithm*, where M is the classical message register and C is the quantum ciphertext register. $\mathtt{Enc}$ preserves KM, *i.e.* $\mathtt{Enc}([km]) = [km] \otimes \sigma_C^{km}$.
- $\mathtt{Dec} : \mathcal{D}(KC) \to \mathcal{D}(M)$ is the CPTP map representing the *decryption algorithm*.

In order to simplify the security definitions, we assume that the encryption algorithm preserves the key and message registers that are inputted. However, only the ciphertext register C is sent.

In an asymptotic setting, the algorithms would also be functions of a security parameter λ. Here, we can remain in a simpler information-theoretic setting, and in particular we have that the key generation just produces a fixed random key, with no input.

A QECM scheme should satisfy the standard properties of an encryption scheme. That is it should be correct, in the sense that decryption should return the original message; and indistinguishable, in the sense that the ciphertexts of two messages cannot be distinguished, even when chosen by the adversary. We give these definitions in the information-theoretic setting, and we allow small errors.

Definition 8.3. Let $\mathtt{Q} = (\mathtt{Key}, \mathtt{Enc}, \mathtt{Dec})$ be a QECM scheme. We say that $\mathtt{Q}$ is

ε_0-correct if, for any classical state ρ_M,

$$\|\rho_{M\hat{M}} - \rho_{MM}\|_{\mathrm{Tr}} \leq \varepsilon_0, \tag{8.2.1}$$

where $\rho_{M\hat{M}} = (\mathrm{id}_M \otimes \mathtt{Dec}_{KC}) \circ \mathtt{Enc}(\mathtt{Key}([0]) \otimes \rho_M)$.

ε_1-indistinguishable for fixed $m_0 \in M$ if, for a cq state ρ_{MS} where S holds any side information,

$$\|\rho_{CS|(Y=0)} - \rho_{CS|(Y=1)}\|_{\mathrm{Tr}} \leq \varepsilon_1, \tag{8.2.2}$$

where $Y = \mathbb{Z}_2$ is a classical register indicating whether the message is replaced with a fixed message m_0 or preserved, and

$$\rho_{KMCSY} = (\mathtt{Enc} \otimes \mathrm{id}_S)\big(\mathtt{Key}([0]) \otimes \tfrac{1}{2}([m_0] \otimes \rho_S \otimes [0] + \rho_{MS} \otimes [1])\big). \tag{8.2.3}$$

It is possible to generalise to the asymptotic or computational settings by taking the register sizes to be functions of a security parameter λ, on the order of the ciphertext register size. Then, rather than considering the trace distance between states, we would consider the distinguishability by a QPT algorithm, which should be negligible.

As studied in [BL20], a QECM scheme might also satisfy uncloneability properties. However, it is unknown whether such a scheme actually exists. Due to [BL20], it is only known that an encryption scheme they construct is uncloneable in the quantum random oracle model (QROM). To remedy this, we consider a variant of the QECM model where the decryption requires an interaction between the sender Alice and the receiver Bob. Due to

the interaction, Alice produces an additional bit that indicates whether she accepts Bob's responses during the interaction. We can always assume, in the information-theoretic setting, that the message remains perfectly secure unless Alice accepts, by for example padding with an additional one-time pad, the key to which she only reveals if she accepts. We formalise this in the same way as the definitions above.

Definition 8.4. A *quantum encryption of classical messages with interactive decryption (QECM-ID)* scheme is a tuple $\mathtt{Q} = (\mathtt{Key}, \mathtt{Enc}, \mathtt{Dec})$.

- $\mathtt{Key} : \mathcal{D}(\{0\}) \to \mathcal{D}(K)$ is the CPTP map representing the key-generation algorithm, where K is the classical key register.
- $\mathtt{Enc} : \mathcal{D}(KM) \to \mathcal{D}(KMC)$ is the quantum channel representing the encryption algorithm, where M is the classical message register and C is the quantum ciphertext register. $\mathtt{Enc}$ preserves KM, *i.e.* $\mathtt{Enc}([km]) = [km] \otimes \sigma_C^{km}$.
- The decryption algorithm $\mathtt{Dec}$ is an interaction between Alice and Bob that takes a state on KMB to a state on $KMF\hat{M}B'$, where Alice holds K, M, and $F = \mathbb{Z}_2$ (a classical register that indicates whether Alice aborts (0) or accepts the decryption (1)); and Bob holds $\hat{M}$ (a classical register holding Bob's decryption of the message), and B and B' (additional quantum registers).

Correctness and indistinguishability generalise in a straightforward way to this setting. The correctness must change to account for the interactive decryption, but as the indistinguishability does not depend on the decryption, it can remain identical.

Definition 8.5. Let $\mathtt{Q} = (\mathtt{Key}, \mathtt{Enc}, \mathtt{Dec})$ be a QECM-ID scheme. We say that $\mathtt{Q}$ is

ε_0**-correct** if, for any classical state ρ_M, when Alice and Bob run $\mathtt{Dec}$ as intended on $\rho_{KMC} = \mathtt{Enc}(\mathtt{Key}([0]) \otimes \rho_M)$ for $B = C$ and $B' = \{0\}$, they get $\rho_{KMF\hat{M}}$ such that

$$\|\rho_{M\hat{M}\wedge(F=1)} - \rho_{MM}\|_{\mathrm{Tr}} \leq \varepsilon_0. \tag{8.2.4}$$

ε_1**-indistinguishable** for fixed $m_0 \in M$ if, for any cq state ρ_{MS},

$$\|\rho_{CS|(Y=0)} - \rho_{CS|(Y=1)}\|_{\mathrm{Tr}} \leq \varepsilon_1, \tag{8.2.5}$$

where $Y = \mathbb{Z}_2$ is a classical register indicating whether the message is replaced with a fixed message m_0 or preserved, and

$$\rho_{KMCSY} = (\texttt{Enc} \otimes \mathrm{id}_S)\big(\texttt{Key}([0]) \otimes \tfrac{1}{2}([m_0] \otimes \rho_S \otimes [0] + \rho_{MS} \otimes [1])\big). \quad (8.2.6)$$

Note that this reduces to the original definition of a QECM if the decryption is a simple one-round interaction: Alice sends the key k to Bob, who uses it to decrypt the ciphertext, and Alice always accepts the decryption.

8.2.2 Uncloneable security definitions

We extend the security properties of uncloneable and uncloneable-indistinguishable security of a QECM from [BL20] to the setting of a QECM-ID as well. Intuitively, the definitions are meant to replace the condition of Bob guessing correctly with Alice accepting the decryption.

First, we can describe the security properties by means of security games. Uncloneable security guarantees that, even if a colluding party decrypts, it is difficult for an eavesdropper to guess the message. The *uncloneable security game* is played by two cooperating adversaries Bob and Eve against a challenger Alice.

1. Alice samples a message uniformly at random. She samples a key and encrypts the message. She sends the ciphertext to the adversaries.

2. The adversaries split the state between them using a quantum channel, and then may no longer communicate.

3. Alice and Bob decrypt with the interaction `Dec`, and Eve eavesdrops on their interactions.

4. Eve attempts to guess the message. The adversaries win if Alice accepts the decryption ($f = 1$) and Eve guesses correctly.

Uncloneable security is achieved if the winning probability is only slightly above the probability of Alice accepting and Eve guessing the message given no information $\frac{\Pr[F=1]}{|M|}$.

Uncloneable-indistinguishable security combines uncloneable and indistinguishable security: it guarantees that, even if a colluding party decrypts, an eavesdropper cannot distinguish between the encryptions of an intended message and a fixed message. The

uncloneable-indistinguishable security game is also played by two cooperating adversaries against a challenger.

1. The adversaries prepare a cq state ρ_{MS} and send register M to Alice.
2. Alice samples a bit y uniformly at random. If $y = 0$ she replaces M with a fixed message m_0; else she preserves M.
3. Alice samples a key and encrypts the message. She sends the ciphertext to the adversaries.
4. The adversaries split the state between them using a quantum channel, and then may no longer communicate.
5. Alice and Bob decrypt with the interaction $\mathtt{Dec}$, and Eve eavesdrops on their interactions.
6. Eve tries to guess y. The adversaries win if Alice accepts the decryption and Eve guesses correctly.

Uncloneable-indistinguishable security is achieved if the winning probability is only slightly above $\frac{1}{2}\Pr[F = 1]$, half the probability of accepting.

We now formalise the intuition of these security games in a way that is amenable to security proofs in the information-theoretic setting.

Definition 8.6. Let $\mathtt{Q} = (\mathtt{Key}, \mathtt{Enc}, \mathtt{Dec})$ be a QECM-ID. We say the scheme satisfies

ε_2**-uncloneable security** if

$$\Pr\big[M = \check{M} \wedge F = 1\big]_\rho \leq \frac{1}{|M|}\Pr[F = 1]_\rho + \varepsilon_2, \tag{8.2.7}$$

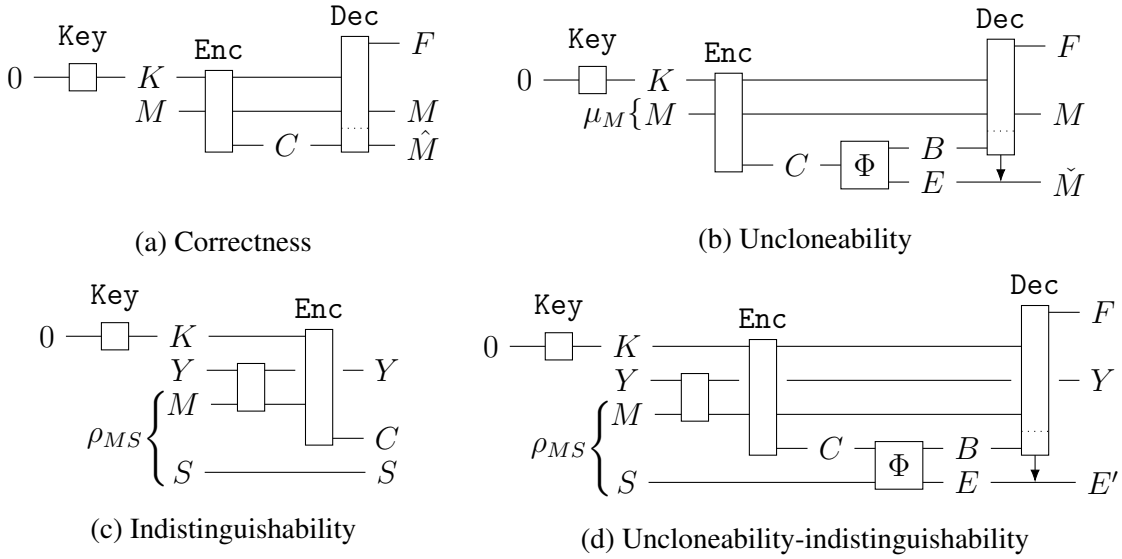
for ρ prepared as follows. Let $\rho_M = \mu_M$ the maximally mixed state. Alice encrypts $\rho_{KMC} = \mathtt{Enc}(\mathtt{Key}([0]) \otimes \rho_M)$ and an eavesdropper Eve acts with a quantum channel $\Phi : \mathcal{L}(C) \to \mathcal{L}(BE)$ to get $\rho_{KMBE} = (\mathrm{id}_{KM} \otimes \Phi)(\rho_{KMC})$. Then, after eavesdropping on all the interactions during $\mathtt{Dec}$, Eve produces a guess of the message on M, stored in the register $\check{M}$.

ε_3**-uncloneable-indistinguishable security** if

$$\big\|\rho_{E'|(Y=0)\wedge(F=1)} - \rho_{E'|(Y=1)\wedge(F=1)}\big\|_{\mathrm{Tr}} \leq \varepsilon_3, \tag{8.2.8}$$

for ρ prepared as follows. Fix $m_0 \in M$, and let $Y = \mathbb{Z}_2$ and ρ_{MS} be any cq state. Alice prepares the state $\rho_{MSY} = \frac{1}{2}([m_0] \otimes \rho_S \otimes [0] + \rho_{MS} \otimes [1])$, then encrypts to get $\rho_{KMCSY} = (\texttt{Enc} \otimes \mathrm{id}_{SY})(\texttt{Key}([0]) \otimes \rho_{MSY})$. Next, an eavesdropper Eve acts with a quantum channel $\Phi : \mathcal{L}(CS) \to \mathcal{L}(BE)$ to get $\rho_{KMBEY} = (\mathrm{id}_{KM} \otimes \Phi \otimes \mathrm{id}_Y)(\rho_{KMCSY})$ and after eavesdropping on all the interactions during Dec, Eve holds a register E'.

All the security definitions are illustrated in Fig. 8.1.



(a) Correctness

(b) Uncloneability

(c) Indistinguishability

(d) Uncloneability-indistinguishability

Figure 8.1: Schematics of the state constructions in the QECM-ID security definitions. Blocks represent operations, with interactions if they are split by a dotted line. Horizontal lines represent registers; they take part in the operations they touch. Vertical arrows represent eavesdropping.

8.2.3 General properties

In this section, we show some relations on the uncloneable security properties for QECM-IDs. These generalise similar properties shown for QECMs in [BL20].

Lemma 8.7. Let Q be an ε-uncloneable QECM-ID. Then, if the uncloneable security game is played with a classical state ρ_M not necessarily uniform, the winning probability

$$\Pr\left[M = \check{M} \wedge F = 1\right]_\rho \leq 2^{-H_{\min}(M)_\rho} \Pr[F = 1] + |M| 2^{-H_{\min}(M)_\rho} \varepsilon. \tag{8.2.9}$$

Proof: We relate this to the winning probability with $\rho_M = \mu_M$. In fact,

$$\begin{aligned}\Pr[M = \check{M} \wedge F = 1]_\rho &= \sum_{m \in M} \Pr[M = m] \Pr[\check{M} = m \wedge F = 1 | M = m] \\ &\leq \max_m \Pr[M = m] \sum_m \Pr[\check{M} = m \wedge F = 1 | M = m] \\ &= |M| 2^{-H_{\min}(M)_\rho} \Pr[M = \check{M} \wedge F = 1]_\mu \\ &\leq 2^{-H_{\min}(M)_\rho} \Pr[F = 1] + |M| 2^{-H_{\min}(M)_\rho} \varepsilon\end{aligned} \tag{8.2.10}$$

■

Theorem 8.8. Let $\mathtt{Q}$ be a perfectly indistinguishable QECM-ID.

(i) If $\mathtt{Q}$ is ε-uncloneable secure then it is $|M|\varepsilon$-uncloneable-indistinguishable secure.

(ii) If $\mathtt{Q}$ is ε-uncloneable-indistinguishable secure then it is ε-uncloneable secure.

In the asymptotic regime, this provides an equivalence between the two notions of uncloneable security.

Proof: First, we show assertion (i). We proceed by contrapositive. Suppose there exists an attack for the uncloneable-indistinguishable security game that wins with advantage greater than $|M|\varepsilon$. An important observation we make to help simplify the proof is that we may always assume that $\rho_{MS} = [m_1]$ for some message $m_1 \in M$ [KT22]. This is because the trace norm is convex, so

$$\left\| \rho_{E'|(Y=0)\wedge(F=1)} - \rho_{E'|(Y=1)\wedge(F=1)} \right\|_{\mathrm{Tr}} \leq \sum_{m \in M} p_m \left\| \rho^m_{E'|(Y=0)\wedge(F=1)} - \rho^m_{E'|(Y=1)\wedge(F=1)} \right\|_{\mathrm{Tr}}, \tag{8.2.11}$$

and thus we can take m_1 to be the value whose term in this convex combination is maximal. Finally, we can remove the side information by redefining the splitting channel $\Phi'(\sigma) = \Phi(\sigma \otimes \rho_S^{m_1})$.

With such an attack, we construct an attack against the uncloneable security game. The splitting operation and Bob act in the same way. To attempt to guess the message, Charlie makes the measurement that optimally distinguishes the cases $y = 0$ and $y = 1$,

and guess m_0 or m_1, respectively. Then, the guessing probability

$$\begin{aligned}\Pr\big[M = \check{M} \wedge F = 1\big] &= \Pr\big[M = \check{M} \wedge F = 1 \wedge M \notin \{m_0, m_1\}\big] \\ &\quad + \Pr[M \in \{m_0, m_1\}] \Pr\big[M = \check{M} \wedge F = 1 | M \in \{m_0, m_1\}\big] \\ &= \frac{2}{|M|} \Pr\big[M = \check{M} \wedge F = 1 | M \in \{m_0, m_1\}\big]\end{aligned} \tag{8.2.12}$$

Since $\Pr\big[M = \check{M} \wedge F = 1 | M \in \{m_0, m_1\}\big]$ is the probability of distinguishing messages m_0 and m_1, we have by hypothesis that this is greater than $\frac{\Pr[F=1|M\in\{m_0,m_1\}]+|M|\varepsilon}{2}$. Finally, as $\mathtt{Q}$ is perfectly indistinguishable, $\Pr[F = 1 | M \in \{m_0, m_1\}] = \Pr[F = 1]$ — otherwise Bob could distinguish the messages without access to the key. Putting this together,

$$\Pr\big[M = \check{M} \wedge F = 1\big] > \frac{\Pr[F = 1]}{|M|} + \varepsilon. \tag{8.2.13}$$

Now, we show assertion (ii). Let $\rho_{ME'\wedge(F=1)} = \mathbb{E}_{m\in M}[m] \otimes \rho^m_{E'\wedge(F=1)}$ be the final state in the uncloneable security game. Since we have by hypothesis that $\mathtt{Q}$ is uncloneable-indistinguishable secure, $\|\rho^{m_0}_{E'\wedge(F=1)} - \rho^m_{E'\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon$ for all $m \in M$. Setting the state $\tau_{ME'\wedge(F=1)} = \mu_M \otimes \rho^{m_0}_{E'\wedge(F=1)}$, we have that

$$\|\tau_{ME'\wedge(F=1)} - \rho_{ME'\wedge(F=1)}\|_{\mathrm{Tr}} = \mathop{\mathbb{E}}_{m\in M} \|\rho^{m_0}_{E'\wedge(F=1)} - \rho^m_{E'\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon. \tag{8.2.14}$$

Because the registers M and E' are independent on τ, *i.e.* $\tau_{ME'} = \tau_M \otimes \tau_{E'}$, the guessing probability $\Pr[M = \check{M} \wedge F = 1]_\tau \leq \frac{\Pr[F=1]_\tau}{|M|}$. Finally, because τ is only ε away from ρ in trace norm and $\Pr[F = 1]_\tau = \Pr[F = 1 | M = m_0]_\rho = \Pr[F = 1]_\rho$ by perfect indistinguishability, we get that $\Pr[M = \check{M} \wedge F = 1]_\rho \leq \frac{\Pr[F=1]_\rho}{|M|} + \varepsilon$. ■

8.2.4 Instantiation using coset states

Now, we give a construction of a QECM-ID. We base this construction on the structure of the leaky subspace coset NC game Section 6.3, and then show its security by making use of the entropic uncertainty relation of Corollary 6.15.

Let $e : \mathbb{Z}_2^{n/2} \times R \to \mathbb{Z}_2^\ell$ be a quantum-proof (κ, ε)-strong extractor (Section 4.2.2.1) and let A be the set of all subspaces of $V = \mathbb{Z}_2^n$ of dimension $n/2$.

Protocol 8.9 (Coset state QECM-ID)**.**

Key generation Let $T = T' = \mathbb{Z}_2^{n/2}$ and take $K = ATT'R$. The channel is

$$\texttt{Key}([0]) = \mathop{\mathbb{E}}_{a,t,t',r} [att'r]. \tag{8.2.15}$$

Encryption Let $M = \mathbb{Z}_2^\ell$ and $C = V$. Take

$$\texttt{Enc}([att'r] \otimes [m]) = [att'r] \otimes [m] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| . \tag{8.2.16}$$

Decryption Dec proceeds as follows. First, Alice sends a to Bob. Then, Bob measures in the coset state basis to get measurements $\hat{t}, \hat{t}'$ of t, t'. Bob sends $\hat{t}$ to Alice: if $\hat{t} = t$, Alice sets $f = 1$, else she sets $f = 0$ and aborts. Alice sends r and $\bar{m} = e(t', r) + m$ to Bob. Bob computes $\hat{m} = \bar{m} + e(\hat{t}', r)$.

Proposition 8.10. Protocol 8.9 is perfectly correct, *i.e.* 0-correct.

Proof: First, writing $\rho_M = \sum_m p_m [m]$,

$$\rho_{KMC} = \rho_{ATT'RMV} = \mathop{\mathbb{E}}_{a,t,t',r} \sum_m p_m [att'r] \otimes [m] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| . \tag{8.2.17}$$

To begin the decryption, Bob measures in the coset state basis and gets

$$\rho_{ATT'RM\hat{T}\hat{T}'} = \mathop{\mathbb{E}}_{a,t,t',r} \sum_m p_m [att'r] \otimes [m] \otimes [tt']. \tag{8.2.18}$$

Sending $\hat{t} = t$ to Alice, she always sets $F = 1$, and then gives r and $\bar{m} = e(t', r) + m$ to Bob. Then, the state become

$$\rho_{ATT'RMF\bar{M}\hat{T}'} = \mathop{\mathbb{E}}_{a,t,t',r} \sum_m p_m [att'r] \otimes [m] \otimes [1] \otimes [e(t', r) + m] \otimes [t']. \tag{8.2.19}$$

Finally, Bob computes $\hat{m} = e(\hat{t}', r) + \bar{m} = m$, getting

$$\rho_{KMF\hat{M}} = \mathop{\mathbb{E}}_{a,t,t',r} \sum_m p_m [att'r] \otimes [m] \otimes [1] \otimes [m]. \tag{8.2.20}$$

Thus, $\rho_{M\hat{M}\wedge(F=1)} = \sum_m p_m [m] \otimes [m] = \rho_{MM}$. ■

Proposition 8.11. Protocol 8.9 is perfectly indistinguishable.

Proof: Writing $\rho_{MS} = \sum_m p_m [m] \otimes \rho_S^m$, we see that

$$\begin{aligned}\rho_{KMCSY} &= \frac{1}{2}(\mathtt{Enc}(\mathtt{Key}(0) \otimes [m_0]) \otimes \rho_S \otimes [0] + (\mathtt{Enc} \otimes \mathrm{id}_S)(\mathtt{Key}(0) \otimes \rho_{MS}) \otimes [1]) \\ &= \frac{1}{2}\sum_m \mathtt{Enc}(\mathtt{Key}(0) \otimes [m]) \otimes (\delta_{m,m_0}\rho_S \otimes [0] + p_m \rho_S^m \otimes [1]) \\ &= \frac{1}{2}\sum_m \mathop{\mathbb{E}}_{a,t,t',r} [att'rm] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \otimes (\delta_{m,m_0}\rho_S \otimes [0] + p_m \rho_S^m \otimes [1]).\end{aligned} \tag{8.2.21}$$

Hence,

$$\begin{aligned}\rho_{CSY} &= \frac{1}{2}\sum_m \mathop{\mathbb{E}}_{a,t,t',r} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes (\delta_{m,m_0}\rho_S \otimes [0] + p_m \rho_S^m \otimes [1]) \\ &= \frac{1}{2}\mathop{\mathbb{E}}_{a,t,t'} |a_{t,t'}\rangle\langle a_{t,t'}| \otimes \sum_m (\delta_{m,m_0}\rho_S \otimes [0] + p_m \rho_S^m \otimes [1]) \\ &= \frac{1}{2}\mu_V \otimes (\rho_S \otimes [0] + \rho_S \otimes [1]) = \mu_V \otimes \rho_S \otimes \mu_Y.\end{aligned} \tag{8.2.22}$$

Thus, $\rho_{CS|(Y=0)} = \rho_{CS|(Y=1)}$. ■

Theorem 8.12. Suppose $\kappa \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$. Then, Protocol 8.9 is $\max\{\varepsilon, e^{1/4}(\cos\frac{\pi}{8})^{n/2}\}$-uncloneable.

Proof: We have the state before decryption

$$\rho_{ATT'RM\bar{M}BE} = \mathop{\mathbb{E}}_{a,t,t',r} \sum_m p_m [att'r] \otimes [m] \otimes [e(t',r) + m] \otimes \Phi(|a_{t,t'}\rangle\langle a_{t,t'}|), \tag{8.2.23}$$

where we assume both Bob and Eve have access to $\bar{M}$ if Bob provides t correctly. To begin the decryption, Alice shares a, and Bob makes a measurement N on B to determine a guess $\hat{t}$ of t. Fix $m \in M$. Then, taking Φ to be the cloning channel in the leaky NC game, we get by the leaky NC property that $H_{\min}(T|AB;T'|A'TE)_{\rho_{|(M=m)}} \geq (-\lg\cos\frac{\pi}{8})n - \frac{1}{2\ln 2}$, where A' is a copy of A. Thus, we must have either $H_{\min}(T|N(AB))_{\rho_{|(M=m)}} \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$ or $H_{\min}(T'|A'TE)_{\rho_{|(N(AB)=T\wedge M=m)}} \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$. In the former case, as AB is the

register Bob has access to by that point, we have

$$\Pr[F=1] = \Pr[\hat{T}=T] = \Pr[N(AB)=T] \leq e^{1/4}(\cos\tfrac{\pi}{8})^{n/2}. \tag{8.2.24}$$

In the latter case, we have by hypothesis and the strong extractor property,

$$\begin{aligned} &\|\rho_{e(T',R)RATE|(F=1\wedge M=m)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE|(F=1\wedge M=m)}\|_{\mathrm{Tr}} \\ &= \|\rho_{e(T',R)RATE|(N(AB)=T\wedge M=m)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE|(N(AB)=T\wedge M=m)}\|_{\mathrm{Tr}} \leq \varepsilon, \end{aligned} \tag{8.2.25}$$

where $\tilde{M} = \mathbb{Z}_2^\ell$ is the register containing $e(T', R)$. Combining the two cases,

$$\begin{aligned} &\|\rho_{e(T',R)RATE\wedge(F=1)|(M=m)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE\wedge(F=1)|(M=m)}\|_{\mathrm{Tr}} \\ &= \Pr[F=1]_\rho \|\rho_{e(T',R)RATE|(F=1\wedge M=m)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE|(F=1\wedge M=m)}\|_{\mathrm{Tr}} \\ &\leq \varepsilon^*, \end{aligned} \tag{8.2.26}$$

where we set $\varepsilon^* = \max\{\varepsilon, e^{1/4}(\cos\frac{\pi}{8})^{n/2}\}$. This implies that

$$\begin{aligned} \rho_{Me(T',R)RATE\wedge(F=1)} &= \sum_m p_m[m] \otimes \rho_{e(T',R)RATE\wedge(F=1)|(M=m)} \\ &\approx_{\varepsilon^*} \sum_m p_m[m] \otimes \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE\wedge(F=1)|(M=m)}, \end{aligned} \tag{8.2.27}$$

hence $\|\rho_{\tilde{M}RMATE\wedge(F=1)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{MATE\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon^*$. Supposing $f = 1$, the decryption continues and Eve also gets $\bar{m} = m + \tilde{m}$ and tries to guess m. As classical computations are CPTP maps, we see that

$$\begin{aligned} &\|\rho_{R\tilde{M}MATE\wedge(F=1)} - \mu_R \otimes \mu_{\tilde{M}} \otimes \rho_{MATE\wedge(F=1)}\|_{\mathrm{Tr}} \\ &\geq \|\rho_{R\tilde{M}(\tilde{M}+M)MATE\wedge(F=1)} - \mu_R \otimes \sigma_{\tilde{M}(\tilde{M}+M)MATE\wedge(F=1)}\|_{\mathrm{Tr}} \\ &\geq \|\rho_{R(\tilde{M}+M)MATE\wedge(F=1)} - \mu_R \otimes \sigma_{(\tilde{M}+M)MATE\wedge(F=1)}\|_{\mathrm{Tr}}, \end{aligned} \tag{8.2.28}$$

where $\sigma_{\tilde{M}MATE\wedge(F=1)} = \mu_{\tilde{M}} \otimes \rho_{MATE\wedge(F=1)}$, so

$$\begin{aligned} \sigma_{(\tilde{M}+M)MATE\wedge(F=1)} &= \mathop{\mathbb{E}}_{\tilde{m}} \sum_m p_m[\tilde{m}+m] \otimes [m] \otimes \rho_{ATE\wedge(F=1)|(M=m)} \\ &= \mu_{\bar{M}} \otimes \rho_{MATE\wedge(F=1)}. \end{aligned} \tag{8.2.29}$$

Let $\tau_{R\bar{M}MATE} = \mu_R \otimes \mu_{\bar{M}} \otimes \rho_{MATE\wedge(F=1)}$. Note first that R and $\bar{M}$ are independent of M

so they do not help in guessing it. As the procedure that takes $\rho_{ATVMS} = \rho_{ATV} \otimes \rho_{MS}$ to $\rho_{MATE\wedge(F=1)}$ is a trace non-increasing channel, we have by the data-processing inequality that

$$\begin{aligned} H_{\min}(M|R\bar{M}ATE)_\tau &= H_{\min}(M|ATES)_{\rho_{\wedge(F=1)}} \\ &\geq H_{\min}(M|ATVS)_\rho = H_{\min}(M|S)_\rho. \end{aligned} \tag{8.2.30}$$

Thus, the probability of guessing M given registers $E' = \bar{M}RATE$ of τ is at most $2^{-H_{\min}(M|S)_\rho}$. This implies that the probability of guessing M given E' of $\rho_{ME'\wedge(F=1)}$ is at most $2^{-H_{\min}(M|S)_\rho} + \varepsilon^*$, giving $\Pr[M = \check{M} \wedge F = 1] \leq 2^{-H_{\min}(M|S)_\rho} + \varepsilon^*$, as wanted. ■

Theorem 8.13. Suppose $\kappa \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$. Then, Protocol 8.9 is $\max\{2\varepsilon, 2e^{1/4}(\cos\frac{\pi}{8})^{n/2}\}$-indistinguishable-uncloneable.

Proof: With $\rho_{MS} = \sum_m p_m[m] \otimes \rho_S^m$, we have again

$$\rho_{ATT'RMVSY} = \frac{1}{2}\sum_m \mathop{\mathbb{E}}_{a,t,t',r} [att'rm] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \otimes (\delta_{m,m_0}\rho_S \otimes [0] + p_m\rho_S^m \otimes [1]), \tag{8.2.31}$$

so given the cloning attack $\Phi : \mathcal{L}(VS) \to \mathcal{L}(BE)$, the state before decryption is

$$\rho_{ATT'RMBEY} = \frac{1}{2}\sum_m \mathop{\mathbb{E}}_{a,t,t',r} [att'rm] \otimes \begin{pmatrix} \delta_{m,m_0}\Phi(|a_{t,t'}\rangle\langle a_{t,t'}| \otimes \rho_S) \otimes [0] \\ +p_m\Phi(|a_{t,t'}\rangle\langle a_{t,t'}| \otimes \rho_S^m) \otimes [1] \end{pmatrix}. \tag{8.2.32}$$

On $\rho_{|(Y=0)}$, the cloning attack is $\sigma \mapsto \Phi(\sigma\otimes\rho_S)$, so we have $H_{\min}(T|AB;T'|A'TE)_{\rho_{|(Y=0)}} \geq (-\lg\cos\frac{\pi}{8})n - \frac{1}{2\ln 2}$ where as above A' is a copy of A, and hence similarly

$$\|\rho_{e(T',R)RATE|(Y=0)\wedge(F=1)} - \mu_{\check{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=0)\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon^*, \tag{8.2.33}$$

and then

$$\|\rho_{M\bar{M}RATE|(Y=0)\wedge(F=1)} - [m_0] \otimes \mu_{\bar{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=0)\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon^*. \tag{8.2.34}$$

In the same way, we get that on $\rho_{|(Y=1\wedge M=m)}$, the cloning attack is $\sigma \mapsto \Phi(\sigma \otimes \rho_S^m)$, so the

entropy $H_{\min}(T|AB;T'|A'TE)_{\rho_{|(Y=1\wedge M=m)}} \geq (-\lg\cos\frac{\pi}{8})n - \frac{1}{2\ln 2}$, and hence as above

$$\|\rho_{e(T',R)RATE|(Y=1\wedge M=m)\wedge(F=1)} - \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=1\wedge M=m)\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon^*. \quad (8.2.35)$$

To include M,

$$\begin{aligned}\rho_{Me(T',R)RATE|(Y=1)\wedge(F=1)} &= \sum_m p_m[m] \otimes \rho_{e(T',R)RATE|(Y=1\wedge M=m)\wedge(F=1)} \\ &\approx_{\varepsilon^*} \sum_m p_m[m] \otimes \mu_{\tilde{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=1\wedge M=m)\wedge(F=1)},\end{aligned} \quad (8.2.36)$$

and then $\bar{M}$,

$$\begin{aligned}\rho_{M\bar{M}RATE|(Y=1)\wedge(F=1)} &= \mathrm{Tr}_{\tilde{M}}\big(\rho_{Me(T',R)\bar{M}RATE|(Y=1)\wedge(F=1)}\big) \\ &\approx_{\varepsilon^*} \mathrm{Tr}_{\tilde{M}} \sum_m \mathop{\mathbb{E}}_{\tilde{m}} p_m[m] \otimes [\tilde{m}] \otimes [m+\tilde{m}] \otimes \mu_R \otimes \rho_{ATE|(Y=1\wedge M=m)\wedge(F=1)} \\ &= \sum_m \mathop{\mathbb{E}}_{\tilde{m}} p_m[m] \otimes [m+\tilde{m}] \otimes \mu_R \otimes \rho_{ATE|(Y=1\wedge M=m)\wedge(F=1)} \\ &= \sum_m p_m[m] \otimes \mu_{\bar{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=1\wedge M=m)\wedge(F=1)}\end{aligned} \quad (8.2.37)$$

giving that

$$\|\rho_{\bar{M}RMATE|(Y=1)\wedge(F=1)} - \mu_{\bar{M}} \otimes \mu_R \otimes \rho_{MATE|(Y=1)\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon^*. \quad (8.2.38)$$

As $E' = R\bar{M}ATE$, this gives

$$\begin{aligned}&\|\rho_{E'|(Y=0)\wedge(F=1)} - \rho_{E'|(Y=1)\wedge(F=1)}\|_{\mathrm{Tr}} \\ &\leq \|\mu_{\bar{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=0)\wedge(F=1)} - \mu_{\bar{M}} \otimes \mu_R \otimes \rho_{ATE|(Y=1)\wedge(F=1)}\|_{\mathrm{Tr}} + 2\varepsilon^* \\ &= \|\rho_{ATE|(Y=0)\wedge(F=1)} - \rho_{ATE|(Y=1)\wedge(F=1)}\|_{\mathrm{Tr}} + 2\varepsilon^*.\end{aligned} \quad (8.2.39)$$

To finish the proof, we study the state $\rho_{ATEY\wedge(F=1)}$. The cloning attack and the first decryption step takes ρ_{ATVSY} to $\rho_{ATEY\wedge(F=1)}$ via a trace non-increasing channel. Therefore,

if $\rho_{ATVS|(Y=0)} = \rho_{ATVS|(Y=1)}$, then $\rho_{ATE|(Y=0)\wedge(F=1)} = \rho_{ATE|(Y=1)\wedge(F=1)}$. To that end,

$$\begin{aligned}\rho_{ATVSY} &= \frac{1}{2}\sum_m \mathop{\mathbb{E}}_{a,t,t',r} [at] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \otimes (\delta_{m,m_0}\rho_S \otimes [0] + p_m \rho_S^m \otimes [1]) \\ &= \frac{1}{2}\mathop{\mathbb{E}}_{a,t,t'} [at] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \otimes (\rho_S \otimes [0] + \rho_S \otimes [1]) = \rho_{ATV} \otimes \rho_S \otimes \mu_Y,\end{aligned} \tag{8.2.40}$$

so $\rho_{ATVS|(Y=0)} = \rho_{ATVS|(Y=1)}$, giving the result. ■

8.3 Receiver-Independent Quantum Key Distribution

8.3.1 Quantum key distribution

Quantum key distribution (QKD) is the first quantum cryptographic primitive to garner widespread interest. Its basic premise is to use the uncloneability properties of quantum mechanics to securely share a secret key. This key can then be used as the secret key for a one-time pad, allowing perfectly secure encryption without prior key agreement. In this way, QKD allows a major problem with the implementation of perfectly secure encryption to be overcome.

The first scheme for QKD was introduced by Bennett and Brassard [BB84]. It relies on the use of conjugate-coding bases. We give a simplified explanation of the construction. A sender Alice prepares a uniformly random conjugate-coding state $|x^\theta\rangle$, and sends it to a receiver Bob. Bob measures the state in a random conjugate-coding basis φ to get a string $\hat{x}$. On those qubits i where $\theta_i = \varphi_i$, $\hat{x}_i = x_i$ (these are on average half the bits); and on those where $\theta_i \neq \varphi_i$, $\hat{x}_i$ and x_i are uniformly random and independent. Then, Alice and Bob broadcast their bases, and each may learn the substring on which the bases match, the *raw key*. This step is called *sifting*. A malicious eavesdropper Eve could not learn raw key, even by modifying the transmitted state arbitrarily — she does not know which qubits the key will be extracted from while she has access to the state, and she cannot copy the state because she does not know the preparation bases. Next, Alice and Bob undertake a few additional classical steps to increase the security of the key: a *parameter estimation* step, where they share a small random portion of the bits to gauge the error in the key, caused by either imperfect transmission or a malicious Eve, and then abort if the error is too high; an *error correction* step, where Alice shares the error-correcting code syndrome (Section 3.6) of her raw key with Bob, so he may correct it to the same string, provided

the error is on few enough bits; and finally a *privacy amplification* step, where Alice and Bob act with a quantum-proof strong extractor (Section 4.2.2.1) to get a key that is, to Eve, indistinguishable from a uniformly random string.

There have been multiple proofs of security of the BB84 scheme since its invention [LC99, SP00, Ren05] as the definition of security for QKD protocols has passed through a few iterations. We use a modern version of the definition, following [MR22], which gives three properties that need to be satisfied. First is correctness. A QKD scheme is *correct* if the probability that the protocol is not aborted when Alice and Bob's final keys are unequal is low. This guarantees that the parties receive the same shared key. Next, a QKD scheme is *complete* for a given error channel if, when Eve acts only by that channel, the probability of aborting is low. A common choice of channel is an independent identically-distributed channel $\Phi^{\otimes n}$ to simulate random noise. Completeness assures us that, under reasonable noise parameters, there will actually be a key distributed. Finally, a QKD scheme is *secret*, if, whenever the protocol does not abort, Eve cannot distinguish the final key from a uniformly random string. This is the property that allows the key to be seen as secure from eavesdropping.

Often, QKD is considered in the asymptotic regime — the limit where the number of qubits tends to infinity. This allows a scheme to more intuitively understood, on a large number of qubits. Two properties are of interest in this regime: the *key rate* and the *asymptotic error tolerance*. The key rate is the ratio of the final key length to the number of qubits, and can be seen as the efficiency of the scheme. The asymptotic error tolerance is the proportion of raw key bits that can be flipped by error before either completeness or secrecy fails. Often, there is a tradeoff between these two values.

8.3.2 Device-independence and receiver-independence

A relatively strong assumption implicit in the original discussion of QKD is that Bob and Charlie's devices are assumed to be trusted. Realistically, this is not always a reasonable assumption, due to noisiness of near-term quantum devices. Many variants of QKD that require only weaker assumptions on the honest parties have been proposed. In particular, device-independent (DI) protocols, initiated by Ekert [Eke91], seek to allow QKD with few, if any, assumptions on the behaviour of Alice and Bob's devices. One-sided (1S) DI QKD, shown in [TFKW13], allows Bob's quantum device to be fully untrusted, relying on a monogamy-of-entanglement game winning probability bound for security; and fully DI QKD, shown by Vazirani and Vidick [VV14], allows both Alice and Bob's quantum

devices to be untrusted, with security coming from the rigidity of a nonlocal game. These varying assumptions allow implementations of QKD to balance practicality and security, depending on available resources.

We consider QKD in a model that strengthens one-sided DI QKD by also assuming that Bob's *classical* device is untrusted. To motivate this, we recall the one-sided DI QKD protocol given as Figure 1 of [TFKW13], with one small difference: they considered an entanglement-based model whereas we will work directly in the usual and more practical prepare-and-measure model, knowing that security in the former model implies security in the latter.

Protocol 8.14 (one-sided device independent QKD of [TFKW13])**.**

State preparation Alice samples $x \in X = \mathbb{Z}_2^n$ and $\theta \in \Theta = \mathbb{Z}_2^n$ uniformly at random and sends the state $|x^\theta\rangle$ to Bob.

Measurement Bob confirms receipt of the state, then Alice sends θ to Bob. He measures to get a string y.

Parameter estimation Alice samples a random subset $T \subseteq \{1, \ldots, n\}$ of size t and sends T, x_T to Bob. If the Hamming distance $d(x_T, y_T) > \gamma n$, Bob aborts.

Error correction Alice sends an error-correction syndrome $\mathrm{syn}(x_{T^c})$ and a random hash function $F \in \mathcal{F}$ to Bob. Bob corrects y_{T^c} using the syndrome to get $\hat{x}_{T^c}$

Privacy amplification Alice computes the output $k = F(x_{T^c})$ and Bob computes $\hat{k} = F(\hat{x}_{T^c})$.

In our model, the security of this QKD scheme can be broken, because we cannot trust Bob's classical device to honestly do parameter estimation. Bob would simply control the communication to and from the device, and receive the message $\hat{k}$ or an abort message once the protocol finishes. Consider the following attack involving a malicious device provided by an eavesdropper Eve. When Alice sends the state $|x^\theta\rangle$, Eve intercepts it and holds on to it, and sends Bob's device $|0^n\rangle$. Then, Eve intercepts every message Alice sends and is able to compute Bob's intended output $\hat{k}$, while Bob's device simply outputs a uniformly random string to him. Neither Alice nor Bob have learned that an attack has happened. In this way, Eve succeeds in completely breaking the security of the one-sided device-independent QKD protocol in the receiver-independent model.

To avoid this sort of attack, we need a QKD protocol where only Bob's communication is trusted but none of his devices are. Due to the fact that only Bob's communication needs to be trusted, in the sense that he sends no messages privately to an eavesdropper, we refer to this model as *receiver-independent (RI) QKD*.

Since Bob's classical computations are untrusted, the idea of correctness must also be altered from that of usual QKD. Neither Alice nor Bob can in general check that Bob's final key matches Alice's, since Bob's device can always, once all the checks have been passed, output a uniformly random string to Bob. As such, all Alice can assure herself of is that Bob's device has all the necessary information allowing it to compute the key. So, we only require correctness to hold for the device's computed key, though Bob may not actually receive it.

Definition 8.15. A *receiver-independent QKD protocol* is an interaction between Alice, who is trusted, and Bob, who has trusted communication but untrusted quantum and classical devices, and which is eavesdropped by an eavesdropper Eve. The interaction produces the state $\rho_{FK\hat{K}E}$ where $F = \mathbb{Z}_2$ holds a flag set to 1 if the protocol accepts and 0 otherwise, $K = \mathbb{Z}_2^\ell$ holds Alice's outputted key, $\hat{K} = \mathbb{Z}_2^\ell$ holds Bob's device's key, and E is Eve's side information. The protocol is

- ε_1-*correct* if $\Pr\left[K \neq \hat{K} \wedge F = 1\right] \leq \varepsilon_1$.
- ε_2-*secret* if $\|\rho_{KE\wedge(F=1)} - \mu_K \otimes \rho_{E\wedge(F=1)}\|_{\mathrm{Tr}} \leq \varepsilon_2$.
- (Φ, ε_3)-*complete* if, when Eve acts as the fixed channel Φ and Bob's device works as intended, $\Pr[F = 0] \leq \varepsilon_3$.

As noted, the subtle but important difference between this and the usual QKD definition is in Bob's key $\hat{k}$. Here, the key is produced by Bob's device, but as the device is untrusted, Alice cannot be sure that the key is actually given to Bob at the end of the protocol. However, even if Bob does not learn the key due to his malicious device, it remains secure from the eavesdropper.

8.3.3 Construction and security

We present a protocol for RI QKD. Its security is based on the robust leaky subspace coset game (Section 6.3.2), which we make use of via the entropic uncertainty relation Corollary 6.17. Let $e : \mathbb{Z}_2^{n/2} \times R \to \mathbb{Z}_2^\ell$ be a quantum-proof (κ, ε)-strong extractor and $C \subseteq \mathbb{Z}_2^{n/2}$ be a $(n/2, n/2 - s, d)$-linear error correcting code with syndrome $\mathrm{syn} : \mathbb{Z}_2^{n/2} \to \mathbb{Z}_2^s$.

Protocol 8.16 (receiver-independent QKD)**.**

State preparation Alice chooses $a \in A$, and $t, t' \in \mathbb{Z}_2^{n/2}$ uniformly at random, then sends the state $|a_{t,t'}\rangle$ to Bob.

Parameter estimation Alice sends a, and Bob replies with a measurement $\hat{t}$ of t. If the distance $d(\hat{t}, t) > \gamma\frac{n}{2}$, Alice aborts the protocol.

Error correction Bob makes a measurement $\hat{t}'$ of t', and sends $\mathrm{syn}(\hat{t}')$ to Alice. She uses it to correct[1] t' and get $\bar{t}'$

Information reconciliation Alice sends $j \subseteq \{1, \ldots, \frac{n}{2}\}$ of cardinality $\eta\frac{n}{2}$ to Bob, and he replies with $\hat{t}'_j$. If $\hat{t}'_j \neq \bar{t}'_j$, Alice aborts.

Privacy amplification Alice sends uniformly random $r \in R$ to Bob. Alice outputs $k = e(\bar{t}', r)$ and Bob outputs $\hat{k} = e(\hat{t}', r)$.

We note that, unlike usual QKD, Alice has full control over whether to abort the protocol. This allows us to consider the case where the checks that Bob makes are untrusted.

We now show that Protocol 8.16 satisfies the security properties of Definition 8.15 under some conditions on the parameters.

Proposition 8.17. Protocol 8.16 is $\left(1 - \frac{2d}{n}\right)^{\eta\frac{n}{2}}$-correct.

Note that, in our protocol, in order for Bob to actually receive the key, Bob's classical device is only required to do one computation honestly: the final privacy amplification step.
Proof: First, the event that $F = 1$ is equivalent to $d(T, \hat{T}) \leq \gamma\frac{n}{2} \wedge \bar{T}'_J = \hat{T}'_J$. Then,

$$\Pr[K \neq \hat{K} \wedge F = 1] \leq \Pr[e(\bar{T}', R) \neq e(\hat{T}', R) \wedge \bar{T}'_J = \hat{T}'_J] \leq \Pr[\bar{T}' \neq \hat{T}' \wedge \bar{T}'_J = \hat{T}'_J] \tag{8.3.1}$$

We claim that the event $\bar{T}' \neq \hat{T}'$ implies the event $d(\bar{T}', \hat{T}') \geq d$. To see this, (writing for $x \in \mathbb{Z}_2^{n/2}$, $\mathrm{corr}(x) \in C$ the correction from the error-correcting code, *i.e.* the nearest point in C to x) first note that if $\bar{t}' \neq \hat{t}'$, then $\mathrm{corr}(t') = \mathrm{corr}(\bar{t}') \neq \mathrm{corr}(\hat{t}')$. Then,

[1] The correction here is not simply the natural one of the error-correcting code. Rather, Alice sets $\bar{t}'$ to be the string that corrects to the same point in C as t' but has syndrome $\mathrm{syn}(\hat{t}')$. In the notation of Proposition 8.17, $\bar{t}' = \mathrm{corr}(t') + (\hat{t}' + \mathrm{corr}(\hat{t}'))$

as the code distance is d, $d(\mathrm{corr}(t'), \mathrm{corr}(\hat{t}')) \geq d$. Since $\bar{t}' + \mathrm{corr}(t') = \hat{t}' + \mathrm{corr}(\hat{t}')$, $d(\bar{t}', \hat{t}') = d(\mathrm{corr}(t'), \mathrm{corr}(\hat{t}')) \geq d$.

Thus, as j is sampled uniformly at random among the substrings of length $\eta\frac{n}{2}$,

$$\Pr[d(\bar{T}', \hat{T}') \geq d \wedge \bar{T}'_J = \hat{T}'_J] \leq \frac{\binom{n/2-d}{\eta n/2}}{\binom{n/2}{\eta n/2}} \leq \left(1 - \frac{2d}{n}\right)^{\eta\frac{n}{2}}. \tag{8.3.2}$$

■

Theorem 8.18. Let $0 \leq \delta \leq \gamma, \frac{2d}{n}$; Protocol 8.16 is $(\Phi^{\otimes n}, (e^{-(\gamma-\delta)^2})^n + (e^{-(2d/n-\delta)^2})^n)$-complete, where $\Phi^{\otimes n} : \mathcal{L}(V) \to \mathcal{L}(V)$ is any iid noise channel where $\langle 0|\Phi(|1\rangle\langle 1|)|0\rangle \leq \delta$, $\langle 1|\Phi(|0\rangle\langle 0|)|1\rangle \leq \delta$, $\langle +|\Phi(|-\rangle\langle -|)|+\rangle \leq \delta$, and $\langle -|\Phi(|+\rangle\langle +|)|-\rangle \leq \delta$.

In particular, note that this gives an exponentially small abort rate if the error $\delta < \gamma, \frac{2d}{n}$. We make use of Hoeffding's inequality (Theorem 3.45) in the proof.

Proof: First, recall that Alice sends states of the form $|a_{t,t'}\rangle = |x^\theta\rangle$, for $x = t_a + t'_{a^\perp}$ and $\theta = \iota(a)$, the indicator vector. Thus, the conditions on Φ are simply that there is an independent probability at most δ of a bit flip on any of the bits of the measured strings. Next, since $\hat{t}' = \bar{t}'$ implies that $\hat{t}'_j = \bar{t}'_j$, we have that

$$\begin{aligned} \Pr[F = 0] &= \Pr\left[d(\hat{T}, T) > \tfrac{n}{2}\gamma \vee \bar{T}'_J \neq \hat{T}'_J\right] \\ &\leq \Pr\left[d(\hat{T}, T) > \tfrac{n}{2}\gamma\right] + \Pr\left[\hat{T}' \neq \bar{T}'\right]. \end{aligned} \tag{8.3.3}$$

First, the probability of more than $\gamma\frac{n}{2}$ bit flips occurring on $\hat{t}$ is

$$\Pr\left[d(\hat{T}, T) > \tfrac{n}{2}\gamma\right] \leq \sum_{k=n\gamma/2+1}^{n/2} \binom{n/2}{k} \delta^k (1-\delta)^{n/2-k} = \Pr\left[\Gamma \geq \gamma\frac{n}{2} + 1\right], \tag{8.3.4}$$

where the binomial random variable $\Gamma \sim \mathrm{Bin}(n/2, \delta)$. Consider the independent identically distributed Bernoulli random variables $\Gamma_1, \ldots, \Gamma_{n/2} \sim \mathrm{B}(\delta)$. Since we know $\Gamma = \sum_i \Gamma_i$ and $\mathbb{E}\Gamma = \delta\frac{n}{2}$, Hoeffding's inequality provides

$$\Pr\left[d(\hat{T}, T) > \tfrac{n}{2}\gamma\right] \leq \exp\left(-\frac{4((\gamma-\delta)n/2 + 1)^2}{n}\right) \leq \left(\exp(-(\gamma-\delta)^2)\right)^n. \tag{8.3.5}$$

To proceed similarly for the second term, first note that, in the same way as in Proposi-

tion 8.17, $\bar{t}' \neq \hat{t}'$ implies $d(\hat{t}', t') \geq d$. Thus, as before

$$\Pr\Big[\hat{T}' \neq \bar{T}'\Big] \leq \Pr\Big[d(\hat{T}', T') \geq d\Big] \leq \big(\exp(-(\tfrac{2d}{n} - \delta)^2)\big)^n. \tag{8.3.6}$$

■

Lemma 8.19. Let $Y = \mathbb{Z}_2^n$ and A be registers, ρ_{YA} be a cq state, and $U = B(n, m) \subseteq \mathbb{Z}_2^n$ be a ball. For $\sigma = \mathbb{E}_{u \in U} X_Y^u \rho_{YA} X_Y^u$ where X is the Pauli operator and any POVM $M : Y \to \mathcal{P}(A)$, we have

$$\rho_{M(A)A \wedge (d(M(A),Y) \leq m)} = |U| \sigma_{M(A)A \wedge (M(A)=Y)}. \tag{8.3.7}$$

Proof: First, writing $\rho_{YA} = \sum_{y \in Y} [y] \otimes \rho_A^y$, we see that

$$\rho_{YM(A)A} = \sum_{y,z \in Y} [yz] \otimes \sqrt{M_z} \rho_A^y \sqrt{M_z}, \tag{8.3.8}$$

and so

$$\rho_{M(A)A \wedge (d(M(A),Y) \leq m)} = \sum_{\substack{y,z \in Y \\ d(y,z) \leq m}} [z] \otimes \sqrt{M_z} \rho_A^y \sqrt{M_z} = \sum_{z \in Y} [z] \otimes \sqrt{M_z} \sum_{u \in U} \rho_A^{z+u} \sqrt{M_z}. \tag{8.3.9}$$

On the other hand, $|U|\sigma_{YA} = \sum_{y \in Y, u \in U} [y] \otimes \rho_A^{y+u}$, so

$$|U| \sigma_{M(A)A \wedge (M(A)=Y)} = \sum_{y \in Y, u \in U} [y] \otimes \sqrt{M_y} \rho_A^{y+u} \sqrt{M_y}, \tag{8.3.10}$$

which completes the proof. ■

Lemma 8.20. Let X, Y, A be registers and ρ_{XYA} be a ccq state. Then, for any $y_0 \in Y$,

$$H_{\min}(X|A)_{\rho_{\wedge(Y=y_0)}} \geq H_{\min}(X|AY)_\rho. \tag{8.3.11}$$

Proof: We interpret this via the guessing probability. Writing $\rho_{XYA} = \sum_{x,y} [xy] \otimes \rho_A^{x,y}$,

the probability of guessing X given AY is

$$\begin{aligned} 2^{-H_{\min}(X|AY)_\rho} &= \sup_{M^y:X\to\mathcal{P}(A)\text{ POVMs}} \sum_{x,y} \operatorname{Tr}[M_x^y \rho_A^{x,y}] \\ &\geq \sup_{M:X\to\mathcal{P}(A)\text{ POVM}} \sum_x \operatorname{Tr}[M_x \rho_A^{x,y_0}] = 2^{-H_{\min}(X|A)_{\rho_{\wedge(Y=y_0)}}}, \end{aligned} \tag{8.3.12}$$

as $\rho_{XYA\wedge(Y=y_0)} = \sum_x [xy_0] \otimes \rho_A^{x,y_0}$. ■

Theorem 8.21. Suppose that $\kappa \leq \left(-\lg\cos\frac{\pi}{8} - \frac{2s}{n} - 2\eta - \frac{1}{(2\ln 2)n}\right)\frac{n}{2}$. Then, the QKD protocol Protocol 8.16 is $\max\{2^{\frac{n}{2}h(\gamma)}\varepsilon, 2^{-(-\lg\cos\frac{\pi}{8}-h(\gamma)-\frac{1}{(2\ln 2)n})\frac{n}{2}}\}$-secret.

Asymptotically, in order for the QKD protocol to produce a secure key, we require only

$$\left(-\lg\cos\tfrac{\pi}{8} - h(\gamma) - \tfrac{1}{(2\ln 2)n}\right)\tfrac{n}{2} > 0, \left(-\lg\cos\tfrac{\pi}{8} - \tfrac{2s}{n} - 2\eta - \tfrac{1}{(2\ln 2)n}\right)\tfrac{n}{2} > 0, \tag{8.3.13}$$

as we can make ε arbitrarily small by enlarging the key. These provide the asymptotic noise tolerance. First $\frac{1}{2\ln 2n} \to 0$ and we can choose η small enough to have $\eta \to 0$ while preserving subexponential correctness (for example $\eta = 1/\sqrt{n}$), so we don't need to worry about those terms. Also, the Gilbert-Varshamov bound (Theorem 3.52) provides an attainable value for the syndrome length $s = \frac{n}{2}h(\gamma)$. Therefore, the inequalities reduce to $-\lg\cos\frac{\pi}{8} > h(\gamma)$ asymptotically, so approximately $\gamma < 0.0153$; thus the asymptotic noise tolerance is $\approx 1.5\%$. Note that this is the same tolerance as in [TFKW13].

This bound does take into account the relation between κ and ε for the extractor, and so needs an ideal extractor in general. By using the hash-function based extractor of Lemma 4.32, we can get the error tolerance for a more realistic construction. With this construction, taking $\kappa = \left(-\lg\cos\frac{\pi}{8} - \frac{2s}{n} - 2\eta - \frac{1}{(2\ln 2)n}\right)\frac{n}{2}$, we get that the protocol is $2^{\frac{n}{2}h(\gamma)}2^{-\left(-\lg\cos\frac{\pi}{8}-\frac{2s}{n}-2\eta-\frac{1}{(2\ln 2)n}-\frac{2(\ell-2)}{n}\right)\frac{n}{4}}$-secret. As above, in the asymptotic limit, this gives the inequality $-\lg\cos\frac{\pi}{8} - 3h(\gamma) > 2r$, where $r = \frac{\ell}{n}$ is the rate. Thus, the optimal error tolerance satisfies $h(\gamma) = -\frac{1}{3}\lg\cos\frac{\pi}{8}$ so $\gamma \approx 0.41\%$, and the optimal rate $r = -\frac{1}{2}\cos\frac{\pi}{8} \approx 5.7\%$. It is possible to improve these values with a hash-function-only analysis. These, and how they compare to the rate and error tolerance of the protocol of [TFKW13], in the asymptotic limit are plotted in Fig. 8.2.

Proof of Theorem 8.21: At the start of the protocol, Alice prepares the cccq state $\rho_{ATT'V} = \mathbb{E}_{a,t,t'}[att'] \otimes |a_{t,t'}\rangle\langle a_{t,t'}|$, where she holds onto ATT' and sends V. Eve acts with some channel $\Phi : \mathcal{L}(V) \to \mathcal{L}(BE)$ and sends the register B to Bob. Bob sends $\hat{T}$ to Alice,

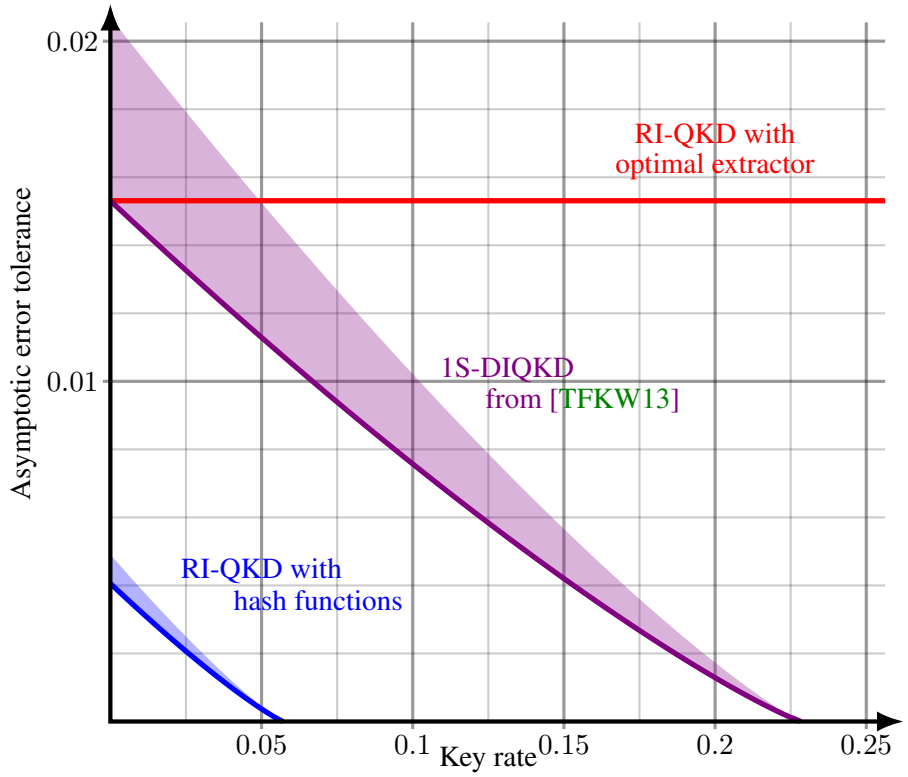


Figure 8.2: Asymptotic error tolerance as a function of rate. Possible values for codes that overcome the Gilbert-Varshamov bound are given as pale regions, where the Hamming bound (Theorem 3.51) is used to give the asymptotic value of the syndrome length.

which Eve may intercept and copy. We work first with the state $\sigma_{ATT'BE} = \mathbb{E}_{u\in U} X_T^u \rho X_T^u$, and then exchange it for ρ later, using Lemma 8.19. At the parameter estimation step, the robust leaky NC property implies that the sequential min-entropy $H_{\min}(T|AB;T'|A'TE)_\sigma \geq \left(-\lg\cos\frac{\pi}{8} - \frac{1}{(2\ln 2)n}\right)n$, where A' is a copy of A. Let $M : T \to \mathcal{P}(AB)$ be the measurement Bob's device uses to get the guess of T. Then, by the entropic uncertainty relation Corollary 6.17, we must have either

$$\begin{aligned} &H_{\min}(T|M(AB))_\sigma \geq \left(-\lg\cos\tfrac{\pi}{8} - \tfrac{1}{(2\ln 2)n}\right)\frac{n}{2} \qquad \text{or} \\ &H_{\min}(T'|A'TE)_{\sigma_{|(M(AB)=T)}} \geq \left(-\lg\cos\tfrac{\pi}{8} - \tfrac{1}{(2\ln 2)n}\right)\frac{n}{2}. \end{aligned} \tag{8.3.14}$$

In the former case, we have

$$\mathrm{Tr}\big(\sigma_{\wedge(\hat{T}=T)}\big) = \Pr\big[M(AB)=T\big]_{\sigma} \leq 2^{-\left(-\lg\cos\frac{\pi}{8}-\frac{1}{(2\ln 2)n}\right)\frac{n}{2}}, \tag{8.3.15}$$

as $\hat{T} = M(AB)$. In the latter case, by the error correction step, Eve holds the register $E_0 = A'\hat{T}\,\mathrm{syn}(\hat{T}')J\hat{T}'_J E$ and thus, making use of Lemma 8.20

$$\begin{aligned} H_{\min}(T'|A'\hat{T}\,\mathrm{syn}(\hat{T}')J\hat{T}'_J E)_{\sigma_{|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)}} &\geq H_{\min}(T'|A'\hat{T}\,\mathrm{syn}(\hat{T}')J\hat{T}'_J\bar{T}'_J E)_{\sigma_{|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)}} \\ &\geq H_{\min}(T'|A'TE)_{\sigma_{|(M(AB)=T)}} - s - 2\eta\tfrac{n}{2} \\ &\geq \left(-\lg\cos\tfrac{\pi}{8} - \tfrac{2s}{n} - 2\eta - \tfrac{1}{(2\ln 2)n}\right)\tfrac{n}{2}. \end{aligned} \tag{8.3.16}$$

Next, as Eve has access to the syndrome $\mathrm{syn}(\hat{t}')$, her probability of guessing t' is equal to that of guessing $\bar{t}'$, giving

$$H_{\min}(\bar{T}'|A'\hat{T}\,\mathrm{syn}(\hat{T}')E)_{\sigma_{|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)}} \geq \left(-\lg\cos\tfrac{\pi}{8} - \frac{2s}{n} - 2\eta - \tfrac{1}{(2\ln 2)n}\right)\frac{n}{2}. \tag{8.3.17}$$

By hypothesis on the strong extractor, we have that

$$\|\sigma_{e(\bar{T}',R)RE_0|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)} - \mu_Z\otimes\mu_R\otimes\sigma_{E_0|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)}\|_{\mathrm{Tr}} \leq \varepsilon, \tag{8.3.18}$$

where the register $Z = \mathbb{Z}_2^{\ell}$. Before passing to the information reconciliation step, we combine the two cases. Writing $\varepsilon^* = \max\{\varepsilon, 2^{-\left(-\lg\cos\frac{\pi}{8}-\frac{1}{(2\ln 2)n}\right)\frac{n}{2}}\}$, we get

$$\begin{aligned} &\|\sigma_{e(\bar{T}',R)RE_0\wedge(\hat{T}=T\wedge\hat{T}'_J=\bar{T}'_J)} - \mu_Z\otimes\mu_R\otimes\sigma_{E_0\wedge(\hat{T}=T\wedge\hat{T}'_J=\bar{T}'_J)}\|_{\mathrm{Tr}} \\ &\quad = \mathrm{Tr}(\sigma_{\wedge(\hat{T}=T)})\|\sigma_{e(\bar{T}',R)RE_0|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)} - \mu_Z\otimes\mu_R\otimes\sigma_{E_0|(\hat{T}=T)\wedge(\hat{T}'_J=\bar{T}'_J)}\|_{\mathrm{Tr}} \leq \varepsilon^*. \end{aligned} \tag{8.3.19}$$

Now, we can pass to the real state ρ. Using Lemma 8.19 with $X = T$,

$$\begin{aligned} &\|\rho_{e(\bar{T}',R)RE_0\wedge(d(\hat{T},T)\leq\gamma n/2\wedge\hat{T}'_J=\bar{T}'_J)} - \mu_Z\otimes\mu_R\otimes\rho_{E_0\wedge(d(\hat{T},T)\leq\gamma n/2\wedge\hat{T}'_J=\bar{T}'_J)}\|_{\mathrm{Tr}} \\ &\quad = |U|\|\sigma_{e(\bar{T}',R)RE_0\wedge(\hat{T}=T\wedge\hat{T}'_J=\bar{T}'_J)} - \mu_Z\otimes\mu_R\otimes\sigma_{E_0\wedge(\hat{T}=T\wedge\hat{T}'_J=\bar{T}'_J)}\|_{\mathrm{Tr}} \leq 2^{\frac{n}{2}h(\gamma)}\varepsilon^*. \end{aligned} \tag{8.3.20}$$

As the event $F = 1$ is equivalent to $d(\hat{T}, T) \leq \gamma n/2 \wedge \hat{T}'_J = \bar{T}'_J$, this means

$$\|\rho_{e(\bar{T}',R)RE_0\wedge(F=1)} - \mu_K \otimes \rho_{RE_0\wedge(F=1)}\|_{\mathrm{Tr}} \leq 2^{\frac{n}{2}h(\gamma)}\varepsilon^*. \tag{8.3.21}$$

Finally, as Eve's register is $E' = RE_0 = RA\hat{T}\,\mathrm{syn}(\hat{T}')J\hat{T}_J E$ at the end of the privacy amplification step, we get the wanted result

$$\|\rho_{KE'\wedge(F=1)} - \mu_K \otimes \rho_{E'\wedge(F=1)}\|_{\mathrm{Tr}} \leq 2^{\frac{n}{2}h(\gamma)}\varepsilon^*. \tag{8.3.22}$$

■

8.4 Bit Commitment

8.4.1 Bit commitment and its impossibility

Bit commitment is a cryptographic primitive involving two parties: a sender, Alice, and a receiver, Bob. In its simplest form, it seeks to allow the communication of a single bit of information from Alice to Bob, in two steps. First, Alice *commits* to a bit b, and then at any point later in time, Alice *reveals* the bit to Bob. A bit commitment must satisfy two security properties. It must be *hiding*, in the sense that Bob is unable to learn the bit before Alice chooses to reveal; and *binding*, in the sense that Alice must reveal the same bit b to which she had committed. The two parties in bit commitment are mutually untrusting, and each of the security properties is ensured when one of the parties is honest: if Alice is honest, she requires the scheme to be hiding, and if Bob is honest, he requires it to be binding.

The use of bit commitment permits some powerful cryptographic constructions. First, bit commitment is used in zero-knowledge proofs, which allow the validity of a proof to be verified by an honest prover, without sharing any additional information with a dishonest verifier [BCC88]. Many other applications are enabled by the relationship between bit commitment and oblivious transfer. Oblivious transfer is a primitive between a sender and a receiver, who are mutually untrusting, and has a variety of equivalent forms [Cré88]. In the form of 1-out-of-2 oblivious transfer, the sender sends two messages to the receiver, and the receiver can only read one of the messages, of their choice, but the sender does not learn which message the receiver has read [BS16]. In the classical world, bit commitment is strictly weaker than oblivious transfer, but quantumly they are equivalent [BBCS01, Unr10]. Oblivious transfer can be used to construct secure two-party computation, where

two parties jointly compute a function in such a way that no dishonest party may learn the input of an honest party beyond what they can guess from the output [Kil88].

However, secure bit commitment in this information-theoretic plain model is impossible, even when the parties can hold quantum information. This impossibility was first spotted by Mayers [May96], and generalised to arbitrary quantum protocols by Mayers [May97], and Lo and Chau [LC97]. We sketch the argument, following [BS16], which proceeds by showing that a hiding protocol cannot be binding. First, we may purify any bit commitment scheme and have Alice and Bob always act by isometries and prepare a pure state, by using state purification (Lemma 4.9), Naimark's theorem (Theorem 4.12), and Stinespring's dilation theorem (Theorem 4.19). Then, by the hiding property, the marginal on Bob's register must be identical for both values of b. As such, by considering the Schmidt decomposition of the shared states (Proposition 3.23), Alice can act by a unitary on her register to make the state consistent with either the $b = 0$ or $b = 1$ at will (Uhlmann's theorem). As such, the commitment cannot be binding. This result can be generalised to the case where the hiding property is not perfect, and gives a tradeoff between the hiding and binding [LC97].

Nevertheless, it is possible to achieve bit commitment in different models, by making additional assumptions on the parties. First, commitment may be achieved under the computational assumption of one-way permutations [DMS00]. Also, it may be achieved with no computational assumptions, but rather the assumption of noisy quantum storage [KWW12].

Finally, we formally define a commitment protocol, keeping in mind that additional assumptions on the model are required to keep the definition non-vacuous. We consider two slight generalisations of the bit commitment protocol. First, we allow for longer bit strings to be committed at once, rather than just single bits. And, we assume that the output of the commitment is uniformly random in the honest case. This can be transformed into any commitment protocol by using the committed random string as the key to a one-time pad concealing the intended string, and sending the encryption at the time of commitment. The definition is a more compact version of the definition in [KWW12].

Definition 8.22. An $(\ell, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-*randomised bit string commitment (RBC) scheme* is a pair of interactive protocols between two parties Alice and Bob: a protocol `commit` that creates a state ρ_{YAB}, and a protocol `reveal` that creates a state $\rho_{YA'\hat{Y}FB'}$. Here $Y = \mathbb{Z}_2^\ell$ is a classical register holding the committed string; $\hat{Y} = \mathbb{Z}_2^\ell$ is a classical register holding the revealed string; $F = \mathbb{Z}_2$ is a classical register that indicates whether Bob accepts (1) or

rejects (0) the reveal; and A, A' and B, B' are additional quantum registers that Alice and Bob hold, respectively. The scheme additionally satisfies

ε_1**-correctness** If Alice and Bob are honest, then $\|\rho_{Y\hat{Y}F} - \sigma_{YYF}\|_{\mathrm{Tr}} \leq \varepsilon_1$, for state $\sigma_{YF} = \mu_Y \otimes [1]$ so $\sigma_{YYF} = \mathbb{E}_{y \in Y}[yy1]$.

ε_2**-hiding** If Alice is honest, then after `commit`, $\|\rho_{YB} - \mu_Y \otimes \rho_B\|_{\mathrm{Tr}} \leq \varepsilon_2$.

ε_3**-binding** If Bob is honest, there exists a state σ_{YAB} such that $\|\rho_{YAB} - \sigma_{YAB}\|_{\mathrm{Tr}} \leq \varepsilon_3$, and if `reveal` is run to get $\sigma_{YA'\hat{Y}FB'}$, $\Pr[Y \neq \hat{Y} \wedge F = 1]_\sigma \leq \varepsilon_3$.

8.4.2 Uncloneable bit commitment

In this section, we extend usual bit commitment protocols to be uncloneable, in the sense that an honest Alice can use an interactive check step to verify that only one recipient can reveal the commitment. Commitment protocols are usually inherently cloneable — in fact, the reveal step is often seen as a public broadcast by Alice. To instantiate a construction of such a protocol we use the leaky NC game Section 6.3 and then show its security by making use of the entropic uncertainty relation of Corollary 6.15.

8.4.2.1 Strong extractors for commitment

As preliminary to the main result of this section, we describe a slight strengthening of a quantum-proof strong extractor (Section 4.2.2.1) that we use in our commitment protocol.

Definition 8.23. A *hashed quantum-proof* (k, ε)*-strong extractor* $e : X \times Y \to Z$ is a quantum-proof (k, ε)-strong extractor such that, if Y is uniformly random, then $e(X, Y)$ is uniformly random for any distribution on X.

Of course, in the information-theoretic setting, in order that $e(x, Y)$ be a uniformly random variable in Z, we need that Y gives at least $\lg |Z|$ bits of randomness, so the cardinality $|Y| \geq |Z|$. In particular, if we make no computational assumptions, this kind of extractor is by its very nature no good at extracting randomness from a weak random source, as it uses more uniform randomness than it creates. However, we find it is useful in cryptographic applications. We provide a simple way to hash an extractor.

Proposition 8.24. Let $e : \mathbb{Z}_2^n \times \mathbb{Z}_2^d \to \mathbb{Z}_2^m$ be a quantum-proof (k, ε)-extractor. Then, the map $e' : \mathbb{Z}_2^n \times \mathbb{Z}_2^{d+m} \to \mathbb{Z}_2^m$ defined as $e'(x, (y, z)) = e(x, y) + z$ is a hashed quantum-proof (k, ε)-strong extractor.

Note that this extractor is simply the original extractor followed by a one-time pad. Using the example above, we can see that there are hashed extractors with exponentially small error and polynomial-size key.

Proof: Write the registers $X = \mathbb{Z}_2^n$, $Y = \mathbb{Z}_2^d$, and $Z = \mathbb{Z}_2^m$. Assuming Y and Z are both distributed uniformly, we see that for any distribution on X, $\Pr[e(X,Y) + Z = z_1] = \Pr[e(X,Y) + Z = z_2]$, so the distribution $e'(X,(Y,Z))$ is uniform. Next it remains to show that this is still an extractor, so suppose that $H_{\min}(X|E) \geq k$. Then, as $\rho_{YZXE} = \mu_Y \otimes \mu_Z \otimes \rho_{XE}$, we have

$$\rho_{(e(X,Y)+Z)YZE} = \mathop{\mathbb{E}}_{y,z} \sum_x p_x [(e(x,y) + z)yz]_{Z'YZ} \otimes \rho_E^x, \tag{8.4.1}$$

so, writing Z' for the register containing $e(X,Y) + Z$,

$$\begin{aligned} &\|\rho_{e'(X,Y)YZE} - \mu_{Z'YZ} \otimes \rho_E\|_{\mathrm{Tr}} \\ &\quad = \mathop{\mathbb{E}}_{z} \Big\| \mathop{\mathbb{E}}_{y} \sum_x p_x [(e(x,y) + z)y] \otimes \rho_E^x - \mathop{\mathbb{E}}_{z'y} [(z' + z)y] \otimes \rho_E \Big\|_{\mathrm{Tr}} \\ &\quad = \mathop{\mathbb{E}}_{z} \|X_{Z'}^z (\rho_{e(X,Y)YE} - \mu_{Z'Y} \otimes \rho_E) X_{Z'}^z\|_{\mathrm{Tr}} \leq \varepsilon, \end{aligned} \tag{8.4.2}$$

where $X_{Z'}^z$ is the Pauli X operator acting as $X^{z_1} \otimes \cdots \otimes X^{z_m}$ on the register Z'. ■

8.4.2.2 Definition of uncloneable bit commitment

We extend the randomised bit string commitment of Definition 8.22 to the uncloneability setting by adding an eavesdropper Eve, from whom Alice wishes to hide her commitment. In order to check for cloning, the protocol will have an additional `check` step which is used to verify whether it is in fact Bob who received the commitment. The separation of the check step also allows us to consider various models: Eve can be allowed to freely communicate with Bob prior to that step, but not afterwards, as Bob could in that case simply give his register that passed the check to her.

Definition 8.25. A $(\ell, \varepsilon_1, \varepsilon_2, \varepsilon_3, \delta)$-*uncloneable randomised bit string commitment (URBC) scheme* is a triple of protocols between two parties Alice and Bob, eavesdropped by an eavesdropper Eve: a protocol `commit` that creates a state ρ_{YABE}, a protocol `check` that creates a state $\rho_{YGA'B'E'}$, and a protocol `reveal` that creates a state $\rho_{YGA''\hat{Y}FB''E''}$. Here, $Y = \mathbb{Z}_2^\ell$ is a classical register holding the committed string; $\hat{Y} = \mathbb{Z}_2^\ell$ is a classical register

holding the revealed string; $G = \mathbb{Z}_2$ is a classical register that indicates whether Alice accepts (1) or rejects (0) the check; $F = \mathbb{Z}_2$ is a classical register that indicates whether Bob accepts (1) or rejects (0) the reveal; and A, A', A'', B, B', B'', and E, E', E'' are additional quantum registers that Alice, Bob, and Eve hold, respectively. The scheme additionally satisfies

ε_1**-correctness** If Alice and Bob are honest, and Eve does not act, then the trace distance $\|\rho_{YG\hat{Y}F} - \sigma_{YGYF}\|_{\mathrm{Tr}} \leq \varepsilon_1$, where $\sigma_{YGF} = \mu_Y \otimes [1] \otimes [1]$.

ε_2**-hiding** If Alice is honest, then after `commit`, $\|\rho_{YBE} - \mu_Y \otimes \rho_{BE}\|_{\mathrm{Tr}} \leq \varepsilon_2$, and after `check`, $\|\rho_{YB'E'} - \mu_Y \otimes \rho_{B'E'}\|_{\mathrm{Tr}} \leq \varepsilon_2$.

ε_3**-binding** If Bob is honest, there exists a state σ_{YABE} such that $\|\rho_{YABE} - \sigma_{YABE}\|_{\mathrm{Tr}} \leq \varepsilon_3$ and $\Pr[Y \neq \hat{Y} \wedge F = 1]_\sigma \leq \varepsilon_3$.

δ**-uncloneability** If Alice is honest, $\left\|\rho_{YE''\wedge(G=1)} - \mu_Y \otimes \rho_{E''\wedge(G=1)}\right\|_{\mathrm{Tr}} \leq \delta$.

Since uncloneability requires only an honest Alice, it should hold for any malicious Bob, even one who colludes with Eve, as long as they do not communicate after the check. Similarly to interactive uncloneable encryption, the commitment can be seen as not having an intended recipient prior to the check step — in particular, Bob and Eve may have arbitrary communication before then. This illustrates an important aspect of the uncloneability, as only Bob will be able to open despite a lack of an agreement between him an Alice, such as a pre-shared secret key.

Remark. Note that the above definitions do not hold as given in the computational setting. However, it is straightforward to adapt them by replacing the supremum in the trace norm $\|A\|_{\mathrm{Tr}} = \sup_{0 \leq P \leq \mathbb{I}} \mathrm{Tr}(PA)$ with the supremum over computationally feasible positive operators, corresponding to a computationally-bounded guessing strategy. This allows adaptation to a wide range of computational settings where different computational assumptions that give rise to commitments can be considered. For simplicity, we use the trace norm definition to prove security of our URBC construction, but the proofs work as well in such computational settings simply because the trace norm upper bounds any seminorm given as a supremum over fewer operators. Nevertheless, in our instantiation, the information-theoretic nature of the uncloneability property may be preserved as this does not depend on the choice of commitment assumption.

Now, we can define a candidate URBC scheme. We do so by taking an RBC scheme and turning it into an uncloneable one on polynomially shorter bit strings using the leaky

NC property, implicitly working under the assumptions that are required for the commitment.

Let $c = (\texttt{commit}_0, \texttt{reveal}_0)$ be a $(k, \varepsilon_1, \varepsilon_2, \varepsilon_3)$-RBC scheme, let A be the set of all subspaces of $V = \mathbb{Z}_2^n$ of dimension $n/2$, let $e : \mathbb{Z}_2^{n/2} \times \mathbb{Z}_2^k \to \mathbb{Z}_2^\ell$ be hashed quantum-proof (κ, ε')-strong extractor, and let $C \subseteq \mathbb{Z}_2^{n/2}$ be an $(n/2, n/2 - s, d)$-linear error-correcting code with syndrome $\mathrm{syn} : \mathbb{Z}_2^{n/2} \to \mathbb{Z}_2^s$.

Protocol 8.26 (Uncloneable bit string commitment)**.**

Commit Let $R = \mathbb{Z}_2^k$ and $T = T' = \mathbb{Z}_2^{n/2}$. Alice and Bob commit to $r \in R$ using c. Then, Alice samples $a \in A$, $t \in T$, and $t' \in T'$ uniformly at random, after which she prepares the state $|a_{t,t'}\rangle$ and sends it to Bob. Alice stores t, t', a and Bob stores $|a_{t,t'}\rangle$, and they both store what is needed to reveal the commitment of r.

Check Alice sends Bob a and he measures in the coset state basis to get measurements $\hat{t}, \hat{t}'$ of t, t', then sends $\hat{t}$ to Alice. If $\hat{t} = t$, Alice sets $g = 1$, else she sets $g = 0$. Alice stores t' and Bob stores $\hat{t}'$, and they both store what is needed to reveal the commitment of r.

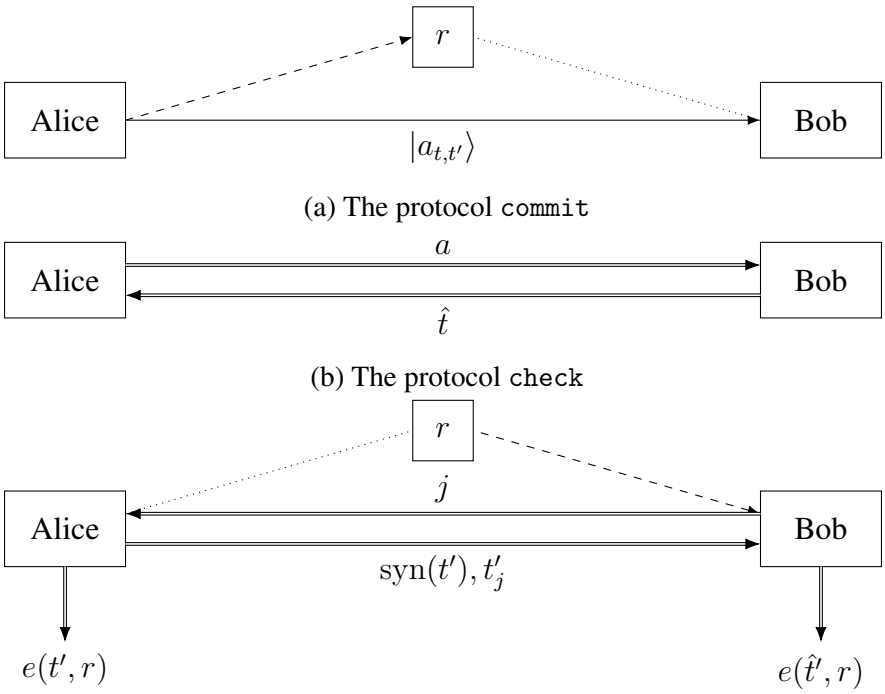
Reveal Bob selects a random subset $j \subseteq \{1, \ldots, n/2\}$ of cardinality $\eta n/2$ and sends it to Alice. She replies with $\mathrm{syn}(t')$ and t'_j. Then, they reveal the commitment c to get $\hat{r}$. If $\mathrm{syn}(\hat{t}') = \mathrm{syn}(t')$, $t'_j = \hat{t}'_j$, and $f_0 = 1$, Bob sets $f = 1$; else he sets $f = 0$. Alice's output is $e(t', r)$ and Bob's output is $e(\hat{t}', \hat{r})$

This protocol is illustrated in Fig. 8.3.

8.4.2.3 Security proofs

Proposition 8.27. Protocol 8.26 is ε_1-correct.

Proof: We suppose Alice and Bob are honest, and Eve does not act. First, Alice and Bob run $\texttt{commit}_0$ to get $\rho_{RA_0B_0}$. Then, in the commit and check phases, Alice sends $|a_{t,t'}\rangle$ and a to Bob, and he is able to measure t, t' exactly, so $\hat{t} = t$ and $\hat{t}' = t'$. Bob sends $\hat{t}$ to Alice, and she sets $g = 1$. At that point, the shared state has the form $\rho_{RA_0B_0T'\hat{T}'G} = \rho_{RA_0B_0} \otimes \sigma_{T'T'} \otimes [1]$ for $\sigma_{T'} = \mu_{T'}$. Next, in the reveal phase, we have that $\mathrm{syn}(\hat{t}') = \mathrm{syn}(t')$ and $\hat{t}'_j = t'_j$, so Bob's flag $f = f_0$. When Alice and Bob run $\texttt{reveal}_0$, the shared state



(a) The protocol `commit`

(b) The protocol `check`

(c) The protocol `reveal`

Figure 8.3: Illustration of the commitment protocol Protocol 8.26. Solid arrows represent transmission of quantum states, double arrows represent transmission of classical information, dashed arrows represent commitment and opening, and dotted lines represent other interactions involved in the commitment without transmission of relevant information.

becomes $\rho_{RA'_0\hat{R}B'_0F_0FT'\hat{T}'G} = \rho_{RA'_0\hat{R}B'_0F_0F_0} \otimes \sigma_{T'T'} \otimes [1]$, where we know by correctness of c that $\|\rho_{R\hat{R}F_0} - \sigma_{RRF_0}\|_{\mathrm{Tr}} \leq \varepsilon_1$ for $\sigma_{RF_0} = \mu_R \otimes [1]$. Thus, for $\sigma_{T'RF_0} = \mu_{T'} \otimes \mu_R \otimes [1]$, we see that

$$\|\rho_{T'\hat{T}'R\hat{R}F_0F} - \sigma_{T'T'RRF_0F_0}\|_{\mathrm{Tr}} \leq \|\sigma_{T'T'} \otimes (\rho_{R\hat{R}F_0} - \sigma_{RRF_0})\|_{\mathrm{Tr}} \leq \varepsilon_1. \tag{8.4.3}$$

We see that $\sigma_{e(T',R)F} = \sigma_{YF} = \mu_Y \otimes [1]$, as e is hashed. Then, as classical computations are quantum channels,

$$\|\rho_{e(T',R)Ge(\hat{T}',\hat{R})F} - \sigma_{YGYF}\|_{\mathrm{Tr}} \leq \|\rho_{T'\hat{T}'R\hat{R}F_0F} - \sigma_{T'T'RRF_0F_0}\|_{\mathrm{Tr}} \leq \varepsilon_1. \tag{8.4.4}$$

■

Proposition 8.28. Protocol 8.26 is ε_2-hiding.

Proof: As Alice is assumed to be honest, the commitment c is hiding in the sense that $\|\rho_{RB_0} - \mu_R \otimes \rho_{B_0}\|_{\mathrm{Tr}} \leq \varepsilon_2$. Consider the state $\sigma_{RATT'VB_0} = \mu_R \otimes \rho_{ATT'VB_0}$. As e is hashed, for each $t' \in T'$, $e(t', R)$ is uniformly random. Hence,

$$\sigma_{e(T',R)AVB_0} = \mathop{\mathbb{E}}_{a,t,t',r} [e(t',r)a] \otimes |a_{t,t'}\rangle\langle a_{t,t'}| \otimes \rho_{B_0} = \mu_Y \otimes \rho_{AVB_0}. \tag{8.4.5}$$

As Bob and Eve's registers after `commit` and `check` are given by quantum channels acting on AVB_0, we get, noting that $\rho_{RB_0ATT'V} = \rho_{RB_0} \otimes \rho_{ATT'V}$

$$\begin{aligned} \|\rho_{YBE} - \mu_Y \otimes \rho_{BE}\|_{\mathrm{Tr}} &\leq \|\rho_{e(T',R)AVB_0} - \mu_Y \otimes \rho_{AVB_0}\|_{\mathrm{Tr}} \\ &= \|\rho_{e(T',R)AVB_0} - \sigma_{e(T',R)AVB_0}\|_{\mathrm{Tr}} \\ &\leq \|\rho_{RATT'VB_0} - \sigma_{RATT'VB_0}\|_{\mathrm{Tr}} \\ &= \|\rho_{ATT'V} \otimes (\rho_{RB_0} - \mu_R \otimes \rho_{B_0})\|_{\mathrm{Tr}} \leq \varepsilon_2. \end{aligned} \tag{8.4.6}$$

In the same way $\|\rho_{YB'E'} - \mu_Y \otimes \rho_{B'E'}\|_{\mathrm{Tr}} \leq \varepsilon_2$. ■

Proposition 8.29. Protocol 8.26 is $\varepsilon_3 + \left(1 - \frac{2d}{n}\right)^{\eta\frac{n}{2}}$-binding.

Proof: Since c is ε_3-binding, we use the state $\sigma_{RA_0B_0}$ such that $\|\sigma_{RA_0B_0} - \rho_{RA_0B_0}\|_{\mathrm{Tr}} \leq \varepsilon_3$. As all the actions undertaken are quantum channels, we know that at the end of the commit phase, $\|\sigma_{YABE} - \rho_{YABE}\|_{\mathrm{Tr}} \leq \varepsilon_3 \leq \varepsilon_3 + \left(1 - \frac{2d}{n}\right)^{\eta\frac{n}{2}}$. Now, we continue the argument, implicitly assuming that the state is σ. In the reveal phase, Bob sets $f = 1$ if and only if $\mathrm{syn}(t') = \mathrm{syn}(\hat{t}')$, $t'_j = \hat{t}'_j$, and $f_0 = 1$. Thus,

$$\begin{aligned} \Pr\left[Y \neq \hat{Y} \wedge F = 1\right] &= \Pr\left[e(T',R) \neq e(\hat{T}',\hat{R}) \wedge \mathrm{syn}(T') = \mathrm{syn}(\hat{T}') \wedge T'_J = \hat{T}'_J \wedge F_0 = 1\right] \\ &\leq \Pr\left[(T' \neq \hat{T}' \vee R \neq \hat{R}) \wedge \mathrm{syn}(T') = \mathrm{syn}(\hat{T}') \wedge T'_J = \hat{T}'_J \wedge F_0 = 1\right] \\ &\leq \Pr\left[R \neq \hat{R} \wedge F_0 = 1\right] + \Pr\left[T' \neq \hat{T}' \wedge \mathrm{syn}(T') = \mathrm{syn}(\hat{T}') \wedge T'_J = \hat{T}'_J\right]. \end{aligned} \tag{8.4.7}$$

First, as c is binding, $\Pr\left[R \neq \hat{R} \wedge F_0 = 1\right] \leq \varepsilon_3$. Next, suppose that $\mathrm{syn}(t') = \mathrm{syn}(\hat{t}')$ but $t' \neq \hat{t}'$. Then as the code C has distance d, the Hamming distance $d(t', \hat{t}') \geq d$. But, as j is a subset of $\eta\frac{n}{2}$ indices chosen uniformly at random, the probability that $t'_j = \hat{t}'_j$ is no more

than $\frac{\binom{n/2-d}{\eta n/2}}{\binom{n/2}{\eta n/2}}$. Simplifying,

$$\begin{aligned}\Pr\left[T' \neq \hat{T}' \wedge \mathrm{syn}(T') = \mathrm{syn}(\hat{T}') \wedge T'_J = \hat{T}'_J\right] &\leq \Pr\left[T' \neq \hat{T}' \wedge d(T', \hat{T}') \geq d \wedge T'_J = \hat{T}'_J\right] \\ &\leq \frac{\binom{n/2-d}{\eta n/2}}{\binom{n/2}{\eta n/2}} = \frac{(n/2-d)\cdots(n/2-d-\eta n/2+1)}{(n/2)\cdots(n/2-\eta n/2+1)} \\ &= \left(1-\frac{d}{n/2}\right)\left(1-\frac{d}{n/2-1}\right)\cdots\left(1-\frac{d}{n/2-\eta n/2+1}\right) \\ &\leq \left(1-\frac{2d}{n}\right)^{\eta\frac{n}{2}},\end{aligned} \tag{8.4.8}$$

which gives the result. ■

Theorem 8.30. Suppose $\kappa \leq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2} - s - \eta\frac{n}{2}$. Then, the commitment Protocol 8.26 is $\max\{\varepsilon', e^{1/4}(\cos\frac{\pi}{8})^{n/2}\}$-uncloneable.

Proof: We must have $H_{\min}(T|AB, T'|ATE) \geq (-\lg\cos\frac{\pi}{8})n - \frac{1}{2\ln 2}$ when Bob guesses t during the check phase, due to the leaky NC property. This implies that, for any measurement M Bob might have made to get $\hat{t}$, either $H_{\min}(T|M(AB))_\rho \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$ or $H_{\min}(T'|ATE)_{\rho_{|(M(AB)=T)}} \geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2}$. In the former case, the probability that $\hat{t} = t$, and hence that $g = 1$, is at most $e^{1/4}(\cos\frac{\pi}{8})^{n/2}$. In the latter case, the additional information that Eve gets about t' during the reveal phase is $\mathrm{syn}(t')$ and t'_j, so knowing that her final register $E'' = ATE\mathrm{syn}(T')T'_J J$,

$$\begin{aligned}H_{\min}(T'|E'')_{\rho_{|(M(AB)=T)}} &\geq H_{\min}(T'|ATE)_{\rho_{|(M(AB)=T)}} - \lg|\mathrm{syn}(T')| - |J| \\ &\geq \frac{-\lg\cos\frac{\pi}{8}}{2}n - \frac{1}{4\ln 2} - s - \eta\frac{n}{2}.\end{aligned} \tag{8.4.9}$$

Then, by hypothesis on the extractor, $\left\|\rho_{YE''|(M(AB)=T)} - \mu_Y \otimes \rho_{E''|(M(AB)=T)}\right\|_{\mathrm{Tr}} \leq \varepsilon'$. Thus, combining the two cases and noting that the events $M(AB) = T$ and $G = 1$ are equivalent,

$$\begin{aligned}&\left\|\rho_{YE''\wedge(G=1)} - \mu_Y \otimes \rho_{E''\wedge(G=1)}\right\|_{\mathrm{Tr}} \\ &\quad= \Pr[M(AB) = T]\left\|\rho_{YE''|(M(AB)=T)} - \mu_Y \otimes \rho_{E''|(M(AB)=T)}\right\|_{\mathrm{Tr}} \\ &\quad\leq \max\{\varepsilon', e^{1/4}(\cos\tfrac{\pi}{8})^{n/2}\}.\end{aligned} \tag{8.4.10}$$

■

8.4.3 Weak string erasure

In this section, we introduce the cryptographic primitive of weak string erasure, that can be used to construct bit string commitment, and then provide an instantiation in a new three-party model, based on the rigidity of the TFKW game, as given in Theorem 7.14.

8.4.3.1 Definitions

Weak string erasure (WSE) is a fundamental cryptographic primitive, introduced in [KWW12]. It is a simple yet powerful way to share partial information between a sender Alice and a receiver Bob. A WSE protocol provides Alice with a random string $x \in \mathbb{Z}_2^n$, and Bob with a string $\hat{x} \in \mathbb{Z}_2^n$ and a subset $\iota \subseteq [n]$ such that $|\iota|$ is on average $n/2$. The strings satisfy the property that they are equal on the positions indexed by the elements of ι: $x_\iota = \hat{x}_\iota$. Security for such a scheme consists of Alice being unable to guess which substring of x Bob knows, while Bob is unable to guess the remaining bits of x, *i.e.* the substring x_{ι^c}. WSE was used in [KWW12] to create bit commitment and oblivious transfer schemes. In their construction of a BC scheme, the roles of the sender and the receiver are preserved: the string Alice commits to is the image of her WSE output x by a randomness extractor, and in the reveal phase, Bob uses the part of the string he knows x_ι to verify that Alice had in fact committed to this string. Hence, however, since bit commitment is impossible with no additional assumptions [BS16], WSE needs some assumptions about the model to hold. Accordingly, [KWW12] used a quantum noisy-storage model to achieve it, generalising results on bounded quantum storage used to achieve oblivious transfer [DFSS08]. We formally define security for WSE in the original two-party model.

Definition 8.31 ([KWW12])**.** A $(n, \lambda, \varepsilon)$-*weak string erasure (WSE) scheme* is a protocol between two parties, Alice and Bob, that creates a state $\rho_{XAI\hat{X}B}$, where X, I, and $\hat{X}$ are classical registers such that $X = \mathbb{Z}_2^n$ holds string x, $\hat{X} = \mathbb{Z}_2^n$ holds Bob's guess of x, and $I = P([n])$ holds ι; and A and B are optional quantum registers corresponding to Alice and Bob's remaining quantum states. The scheme must satisfy *correctness*, and *security* for both Alice and Bob:

Correctness: If both Alice and Bob are honest, $\rho_{XI\hat{X}_I} = \rho_{XIX_I}$ and $\rho_{XI} = \mu_X \otimes \mu_I$.

Security for Alice: If Alice is honest $H_{\min}^{\varepsilon}(X|B)_\rho \geq \lambda n$.

Security for Bob: If Bob is honest, $\rho_{AI} = \rho_A \otimes \mu_I$ in the event that Alice does not abort.

We say that a protocol is a $(n, \lambda, \varepsilon)$-*WSE scheme that fails with probability* p if any one of the three conditions does not hold with probability at most p.

Here, we show WSE in an alternative model. Instead of resorting to limitations on the quantum devices of parties as in [KWW12], we add an additional dishonest prover, Charlie, who colludes with the receiver.[2] Instead of the storage limitation, we place restrictions on the communications: the prover is not allowed to communicate with the receiver, and the sender is required to communicate by publicly broadcasting. The former restriction helps an honest sender constrain the action of a dishonest receiver; the latter condition blocks a subtle cheating method of a dishonest sender, where she attempts to extract different information from the receiver and the prover.

Definition 8.32. A WSE scheme in the *three-party model* consists of a sender, Alice, a receiver, Bob, and a prover, Charlie. It satisfies the following:

- Charlie is dishonest if and only if Bob is dishonest.
- Alice communicates by publicly broadcasting.
- Bob and Charlie are isolated from each other once Alice starts broadcasting.

In this model, there is an additional prover Charlie, so the state takes the form $\rho_{XAI\hat{X}BC}$, where C is an additional register held by Charlie. If he is dishonest, he should not be able to get more information out of the protocol than his collaborator, Bob. Thus, we require that the security for Alice from Definition 8.31 is satisfied with respect to either Bob or Charlie's registers. We state this formally.

Definition 8.33. A $(n, \lambda, \varepsilon)$-*WSE scheme in the three-party model* is a protocol that produces a shared state $\rho_{XAI\hat{X}BC}$ such that it is a two-party scheme for Alice and Bob, and the security for Alice is symmetric:

Two-party WSE: $\rho_{XAI\hat{X}B}$, the state with Charlie's register traced out, satisfies Definition 8.31.

Symmetric security for Alice: If Alice is honest $H_{\min}^{\varepsilon}(X|C) \geq \lambda n$.

[2]Note that oblivious transfer in yet another three-party model has been considered before. In [YXTZ14], they consider a model where an untrusted third party prepares entangled states for Alice and Bob to use. However, they make use of much stronger assumptions: the third party produces each state identically and independently, Alice and Bob need to cooperate to verify that these states are correct before running the protocol, and the third party does not collude with any of the other parties.

For our protocol in this model, as Bob colludes with Charlie but may not communicate with him, an honest sender exploits the rigidity of the TFKW game to constrain their actions. Note that an honest Alice would need Charlie to remain out of the reach of Bob's communication for as long as Bob is using his output data in order for it to stay secure. Since Alice must broadcast publicly, Bob and Charlie will receive the same TFKW game questions even if she is dishonest.

Now, we formally present our protocol.

Protocol 8.34 (three-party weak string erasure)**.**

1. Bob prepares the shared state $\mathfrak{G}^{\otimes N}|x^{\varphi}\rangle_A \otimes |x\varphi\rangle_B \otimes |x\varphi\rangle_C$ for $x, \varphi \in \mathbb{Z}_2^N$ chosen uniformly at random. Bob and Charlie are then no longer allowed to communicate.

2. Alice chooses a set of n indices $J \subseteq [N]$ and a string $\theta \in \mathbb{Z}_2^N$ uniformly at random. She measures each of her qubits $1 \leq i \leq N$ in basis $\{|0^{\theta_i}\rangle, |1^{\theta_i}\rangle\}$ if $i \notin J$ and in basis $\{\mathfrak{G}|0^{\theta_i}\rangle, \mathfrak{G}|1^{\theta_i}\rangle\}$ if $i \in J$. This produces a string $y \in \mathbb{Z}_2^N$ that she keeps; and she broadcasts J and θ.

3. Bob and Charlie, without communicating, each measure their subspaces to get strings corresponding to their optimal guess at the TFKW game on J^c, $y^B = y^C = x + 1^{J^c} \wedge \theta \wedge \varphi \in \mathbb{Z}_2^N$, and they then send $y^B_{J^c}$ and $y^C_{J^c}$, respectively, to Alice.

4. Alice checks if her string everywhere but the index set, y_{J^c}, matches $y^B_{J^c}$ and $y^C_{J^c}$ simultaneously on at least $(\cos^2 \frac{\pi}{8} - \delta)N$ bits. If it does not, she aborts.

5. Alice takes as output y_J, and Bob takes as output the set $\iota(\theta, \varphi) \subseteq J$ where the bits of θ and φ match, and the string y^B_J.

In Fig. 8.4, we give a setup for our WSE scheme, where we see that the single round of communication makes it possible to devise a way to run the protocol relativistically.

Note that the protocol requires no quantum storage to run honestly by considering it in a prepare-and-measure way. That is, Alice may come up with the random θ and J before Bob prepares the state, measure her register one qubit at a time as soon she receives it from Bob — rather than wait until she receives all the qubits and measure all at once — and only reveal θ and J once she knows that Bob and Charlie are no longer communicating. Since her measurements are local, this has the same effect on the state as if she waited until Bob and Charlie finish communicating to make her measurements.

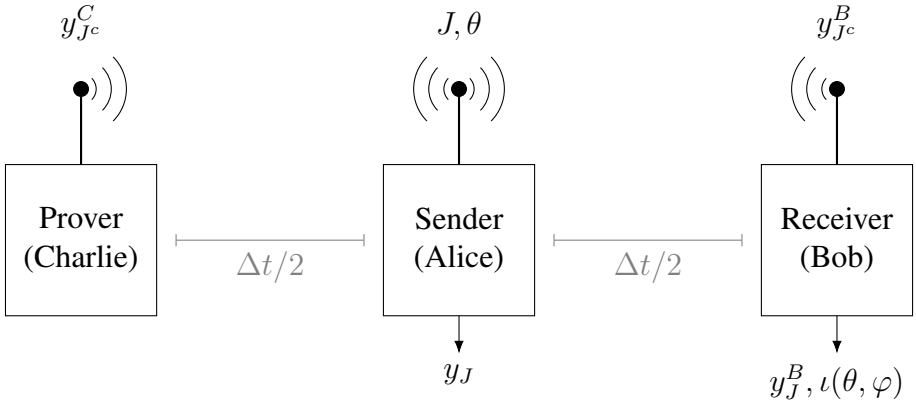


Figure 8.4: A setup for the three-party weak string erasure scheme Protocol 8.34. The parties communicate by broadcasting publicly, and as there is only one round of communication, the spacelike separation between Bob and Charlie ensures they do not communicate in the time Δt needed to run the protocol.

To illustrate the protocol, we consider in more detail the case where the players are honest. Bob should prepare some unentangled optimal state for the TFKW game uniformly at random:

$$\rho_{ABC} = \mathop{\mathbb{E}}_{x,\varphi\in\mathbb{Z}_2^N} \mathfrak{G}^{\otimes N} |x^\varphi\rangle\langle x^\varphi|_A \mathfrak{G}^{\otimes N} \otimes [x\varphi]_B \otimes [x\varphi]_C. \tag{8.4.11}$$

Alice then comes up with uniformly random θ and J and makes her measurements, so the state becomes

$$\rho_{YBC} = \mathop{\mathbb{E}}_{x,\varphi,\theta,J} \sum_y \left| \langle y^\theta | \mathfrak{G}^{1^{J^c}} | x^\varphi \rangle \right|^2 [y]_Y \otimes [x\varphi\theta J]_B \otimes [x\varphi\theta J]_C. \tag{8.4.12}$$

Now, the honest Bob measures his register in the computational basis and gets full information about x and φ. Knowing J, Bob sends $y^B_{J^c} = x_{J^c} + \theta_{J^c} \wedge \varphi_{J^c}$ corresponding to his best guess of y in the TFKW game, and keeps $y^B_J = x_J$ to himself. Charlie does the same and sends $y^C_{J^c} = y^B_{J^c}$ to Alice. Bob and Charlie win at each copy of TFKW with probability exactly $\cos^2 \frac{\pi}{8}$, so with overwhelming probability for large N, they do not cause Alice to abort. Assuming the protocol does not abort, Bob defines $\iota(\theta, \varphi) \subseteq (\mathbb{Z}_2^N)_J = \mathbb{Z}_2^n$ as the set $\iota(\theta, \varphi) = \{i \in J | \theta_i = \varphi_i\}$. Alice and Bob have no use for x_{J^c}, φ, y_{J^c}, θ, and J and may forget them. Alice calls her remaining register X and Bob calls his remaining registers I

and $\hat{X}$, so the state becomes

$$\rho_{XI\hat{X}C} = \mathop{\mathbb{E}}_{x,\varphi,\theta,J} \sum_{y_J} \left| \langle y_J | H^{\theta_J+\varphi_J} | x_J \rangle \right|^2 [y_J]_X \otimes [\iota(\theta,\varphi)]_I \otimes [x_J]_{\hat{X}} \otimes \rho_C^{x,\varphi,\theta,J}, \quad (8.4.13)$$

where each $\rho_C^{x,\varphi,\theta,J}$ is a quantum state representing what Charlie continues to hold, but the structure of this state is unimportant. From the coefficients $\left| \langle y_J | H^{\theta_J+\varphi_J} | x_J \rangle \right|^2 = \left| \langle y_J | H^{1^{\iota(\theta,\varphi)^c}} | x_J \rangle \right|^2$, we see that $(y_J)_i = (x_J)_i$ for $i \in \iota(\theta,\varphi)$ while for $i \notin \iota(\theta,\varphi)$, $(x_J)_i$ is uniformly random with respect to $(y_J)_i$. Therefore, Alice holds the string y_J, Bob has the substring $(y_J)_{\iota(\theta,\varphi)}$ and full information about where in the string they are found, but Bob has no information about the remaining bits. Formally, this gives correctness of the protocol.

8.4.3.2 Security proofs

Lemma 8.35. Protocol 8.34 is correct as a WSE scheme.

Proof:

We need to show that $\rho_{XI} = \mu_X \otimes \mu_I$ and $\rho_{XIX_I} = \rho_{XI\hat{X}_I}$ for honest Alice and Bob. By the above argument,

$$\rho_{XI\hat{X}} = \mathop{\mathbb{E}}_{x,\varphi,\theta,J} \sum_{\substack{y_J \\ (y_J)_{\iota(\theta,\varphi)} = \\ (x_J)_{\iota(\theta,\varphi)}}} \frac{1}{2^{|\theta_J+\varphi_J|}} [y_J]_X \otimes [\iota(\theta,\varphi)]_I \otimes [x_J]_{\hat{X}}, \quad (8.4.14)$$

and therefore

$$\rho_{XI} = \mathop{\mathbb{E}}_{y_J,\varphi,\theta,J} [y_J]_X \otimes [\iota(\theta,\varphi)]_I = \mu_X \otimes \mu_I. \quad (8.4.15)$$

This gives that the bit string x and the subset ι are both uniformly random. We also want Bob's substring of x to be correct. For this, padding Bob's space implicitly to keep every

term the same dimension,

$$\begin{aligned}\rho_{XI\hat{X}_I} &= \mathop{\mathbb{E}}_{x,\varphi,\theta,J} \sum_{\substack{y_J \\ (y_J)_{\iota(\theta,\varphi)}= \\ (x_J)_{\iota(\theta,\varphi)}}} \frac{1}{2^{|\theta_J+\varphi_J|}} [y_J]_X \otimes [\iota(\theta,\varphi)]_I \otimes [(x_J)_{\iota(\theta,\varphi)}]_{\hat{X}_I} \\ &= \mathop{\mathbb{E}}_{x,\varphi,\theta,J} \sum_{\substack{y_J \\ (y_J)_{\iota(\theta,\varphi)}= \\ (x_J)_{\iota(\theta,\varphi)}}} \frac{1}{2^{|\theta_J+\varphi_J|}} [y_J]_X \otimes [\iota(\theta,\varphi)]_I \otimes [(y_J)_{\iota(\theta,\varphi)}]_{\hat{X}_I} \qquad (8.4.16) \\ &= \rho_{XIX_I}.\end{aligned}$$

■

We now show security.

Theorem 8.36. Let K be the constant from Theorem 7.14. For any $N, n \in \mathbb{N}$ and $\varepsilon, \eta, \delta \in (0,1)$ such that $\eta\varepsilon > \delta$, Protocol 8.34 is a $(n, \lg(\frac{4}{3}), Kn^3\sqrt{\varepsilon} + n\eta)$-WSE scheme that fails with probability $e^{-2N(\eta\varepsilon-\delta)^2}$.

For example, taking the parameter values from Example 7.15 gives exponentially small failure probability, and requires only polynomially many qubits to run.

Proof: First, we show security for Bob. This is essentially because an honest Bob provides Alice no information about any of his strings on J. Bob, as he is honest, prepares the shared state

$$\rho_{ABC} = \mathop{\mathbb{E}}_{x,\varphi\in\mathbb{Z}_2^N} \mathfrak{G}^{\otimes N} |x^\varphi\rangle\langle x^\varphi|_A \mathfrak{G}^{\otimes N} \otimes [x\varphi]_B \otimes [x\varphi]_C. \qquad (8.4.17)$$

Alice can do anything to her state but she must send Bob and Charlie J and θ. Note that Bob and Charlie must both receive the same pair by hypothesis. Therefore, as Alice must get y, θ, J by some channel $\Phi : \mathcal{L}(A) \to \mathcal{L}(YA')$,

$$\rho_{YA'BC} = \mathop{\mathbb{E}}_{x,\varphi} \sum_{y,\theta,J} [y\theta J]_Y \otimes \langle y\theta J|_Y \Phi(\mathfrak{G}^{\otimes N} |x^\varphi\rangle\langle x^\varphi|_A \mathfrak{G}^{\otimes N})_{YA'} |y\theta J\rangle_Y \otimes [x\varphi\theta J]_B \otimes [x\varphi\theta J]_C. \qquad (8.4.18)$$

Since Bob is honest, Alice knows that he must provide her with $y^B_{J^c} = x_{J^c} + \theta_{J^c} \wedge \varphi_{J^c}$ and Charlie provides her with the same. If Alice chooses not to abort, Bob produces $\iota(\theta, \varphi)$ so

the state becomes

$$\rho_{Y'A'I\hat{X}C} = \mathop{\mathbb{E}}_{x,\varphi} \sum_{y,\theta,J} [y\theta J y^B_{J^c}]_{Y'} \otimes \langle y\theta J|_Y \Phi(\mathfrak{G}^{\otimes N} |x^\varphi\rangle\langle x^\varphi|_A \mathfrak{G}^{\otimes N})_{YA'} |y\theta J\rangle_Y \otimes [\iota(\theta,\varphi)]_I \otimes [x_J]_{\hat{X}} \otimes \rho_C^{x,\varphi,\theta,J}. \tag{8.4.19}$$

From this state and the definition of $\iota(\theta,\varphi)$ as the set of indices where θ_J and φ_J match for honest Bob, in order for Alice to guess ι, she needs to guess φ_J. Since she has no information about x_J she may not do better than uniformly random. Formally,

$$\begin{aligned}\rho_{Y'A'I} &= \mathop{\mathbb{E}}_{x,\varphi} \sum_{y,\theta,J} [y\theta J y^B_{J^c}]_{Y'} \otimes \langle y\theta J|_Y \Phi(\mathfrak{G}^{\otimes N} |x^\varphi\rangle\langle x^\varphi|_A \mathfrak{G}^{\otimes N})_{YA'} |y\theta J\rangle_Y \otimes [\iota(\theta,\varphi)]_I \\ &= \sum_{y,\theta,J} \mathop{\mathbb{E}}_{x_{J^c},\varphi_{J^c}} [y\theta J y^B_{J^c}]_{Y'} \otimes \langle y\theta J|_Y \Phi(\mathfrak{G}^{\otimes |J^c|} |x^{\varphi_{J^c}}_{J^c}\rangle\langle x^{\varphi_{J^c}}_{J^c}|_{A_{J^c}} \mathfrak{G}^{\otimes |J^c|} \otimes \mu_{A_J})_{YA'} |y\theta J\rangle_Y \\ &\qquad \otimes \mathop{\mathbb{E}}_{\varphi_J} [\iota(\theta,\varphi)]_I = \rho_{Y'A'} \otimes \mu_I,\end{aligned} \tag{8.4.20}$$

which implies that, since Alice's actions are local, any action she may do on her space gives rise to an uncorrelated final state $\rho_{AI} = \rho_A \otimes \mu_I$.

Now, we study security for Alice. That is, Alice is honest but Bob and Charlie are dishonest and colluding. We want to show that $H_{\min}^{Kn^3\sqrt{\varepsilon}+n\eta}(X|B)_\rho \geq -\ln\left(\frac{3}{4}\right)n$. As Bob is dishonest, for the first step of the protocol, he may produce any shared state ρ_{ABC}. The next three steps of the protocol consist of Alice playing $N-n$ TFKW games in parallel with Bob and Charlie, and verifying the rigidity condition. Therefore, if Alice does not abort, she knows by Lemma 7.13 that, with probability $1-e^{-2N(\eta\varepsilon-\delta)^2}$, there are at least $(1-\eta)N$ games that win with probability greater than $\cos^2\frac{\pi}{8}-\varepsilon$. We can apply the rigidity from Theorem 7.14 to get that there exists a constant $K \geq 0$, isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$, an auxiliary register R, and a state $|\phi\rangle = \sum_{x,\varphi\in\mathbb{Z}_2^n} \mathfrak{G}^{\otimes n}|x^\varphi\rangle \otimes |x,\varphi\rangle_{BCR}$ where the $|x,\varphi\rangle_{BCR} \in \mathcal{H}_{B'C'R}$ have orthogonal support on both B' and C' such that

$$\mathop{\mathbb{E}}_J \left\| (V\otimes W)\rho_{A_JBC}(V\otimes W)^\dagger - \mathrm{Tr}_R(|\phi\rangle\langle\phi|) \right\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta. \tag{8.4.21}$$

Let $\sigma_{A_JBC} = \mathrm{Tr}_R(|\phi\rangle\langle\phi|)$ and we study first what happens if the shared state is σ. Since Bob and Charlie may not communicate and Charlie provides no additional information in the protocol, we may safely trace out Charlie's state. However, we must include the copy

of θ that Bob gets during the protocol. By the orthogonality of Charlie's state's support from the rigidity theorem,

$$\sigma_{A_J\Theta B} = \mathop{\mathbb{E}}_{\theta} \sum_{x,\varphi} \mathfrak{G}^{\otimes n} |x^\varphi\rangle\langle x^\varphi| \, \mathfrak{G}^{\otimes n} \otimes [\theta]_\Theta \otimes \mathrm{Tr}_{CR}(\, |x,\varphi\rangle\langle x,\varphi|)_B. \tag{8.4.22}$$

Alice's measurement gives her X and makes the state

$$\begin{aligned} \sigma_{X\Theta B} &= \mathop{\mathbb{E}}_{\theta} \sum_{x,y,\varphi} \left| \langle y|H^{\theta_J+\varphi}|x\rangle \right|^2 [y]_X \otimes [\theta]_\Theta \otimes \mathrm{Tr}_{CR}(\, |x,\varphi\rangle\langle x,\varphi|)_B \\ &= \mathop{\mathbb{E}}_{\theta} \sum_{\substack{x,y,\varphi \\ x_{\iota(\theta,\varphi)}=y_{\iota(\theta,\varphi)}}} \frac{1}{2^{|\theta_J+\varphi|}} [y]_X \otimes [\theta]_\Theta \otimes \mathrm{Tr}_{CR}(\, |x,\varphi\rangle\langle x,\varphi|)_B, \end{aligned} \tag{8.4.23}$$

where $\iota(\theta,\varphi)$ is defined as before. Noting that Bob's register is uncorrelated with part of Alice's register $X_{\iota(\theta,\varphi)^c}$, that gives that Bob's probability of guessing any bit in that register is $\frac{1}{2}$. So, for fixed θ, φ, Bob's probability of guessing X is $\frac{1}{2^{|\iota(\theta,\varphi)^c|}} = \frac{1}{2^{|\theta_J+\varphi|}}$. Since θ_J is uniformly random, Bob's average-case probability of guessing X for fixed φ is,

$$\mathop{\mathbb{E}}_{\theta} \frac{1}{2^{|\theta_J+\varphi|}} = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} \tfrac{1}{2^k} = \left(\tfrac{3}{4}\right)^n. \tag{8.4.24}$$

Since this has no dependence on φ, we see that this is Bob's probability of guessing y, and so the min-entropy is $H_{\min}(X|B)_\sigma \geq -\lg(\frac{3}{4})n$, where we consider Θ as part of Bob's register B. Now we relate this to the smoothed min-entropy of ρ. Since $V \otimes W$ is an isometry, $H_{\min}^{Kn^3\sqrt{\varepsilon}+n\eta}(X|B)_\rho = H_{\min}^{Kn^3\sqrt{\varepsilon}+n\eta}(X|B)_{(V\otimes W)\rho(V\otimes W)^\dagger}$, and σ belongs to a $Kn^3\sqrt{\varepsilon}+n\eta$-ball around $(V \otimes W)\rho(V \otimes W)^\dagger$, so

$$H_{\min}^{Kn^3\sqrt{\varepsilon}+n\eta}(X|B)_\rho \geq H_{\min}(X|B)_\sigma \geq -\lg\left(\tfrac{3}{4}\right)n. \tag{8.4.25}$$

Note that this holds in the same way for Charlie, so he cannot extract any more information that Bob can if he is dishonest. ■

8.4.4 Bit commitment from WSE

In [KWW12], they provide a way to construct an RBC scheme using a weak string erasure scheme and a linear code. We discuss the relationship between the three-party WSE model of the previous section and this commitment construction. The roles of the sender and the

receiver from the WSE scheme are preserved. In particular, with an $(n, \lambda, \varepsilon)$-WSE scheme and an (n, k, d)-linear code, they construct a $\left(\lambda n - (n-k) - d, 2\varepsilon + 2^{-d/2}\right)$-randomised bit string commitment scheme. Using this recipe, our WSE scheme Protocol 8.34 gives a form of bit commitment in a model with two receivers. In this model, Alice is a sender who is required to broadcast, and Bob and Charlie are colluding receivers who are isolated from each other. Similarly to WSE, we only require that Bob be able to read the revealed bit string, rather than both receivers. We call this the *two-receiver model*.

Corollary 8.37. Let $K, N, n, \varepsilon, \eta, \delta$ be constants that satisfy Theorem 8.36, and let $k, d \in \mathbb{N}$ such that there exists an (n, k, d)-linear code. Then, for $\ell = (\lg \frac{4}{3})n - (n-k) - d$ and $\omega = 2Kn^3\sqrt{\varepsilon} + 2n\eta + 2^{-d/2}$, in the two-receiver model, there exists a $(\ell, \omega, \omega, \omega)$-randomised bit string commitment scheme that fails with probability $e^{-2N(\eta\varepsilon-\delta)^2}$.

Using the construction of [KWW12], the correctness and ε-binding of the scheme between Alice and Bob follow immediately from the correctness and security for Bob of WSE. Also, due to the symmetry requirement on security for Alice in three-party WSE, this construction provides ε-hiding when Bob and Charlie are dishonest.

As mentioned before, a construction of [BGKW88] provides classical bit commitment in a model with two senders who may not communicate. We observe that, in contrast, bit commitment is classically impossible in our two-receiver model. The first step of a protocol in our model consists of the preparation of an initial shared state by Bob. If only classical operations are allowed, Bob is just sampling from a probability distribution and sharing the result. In particular, he can make sure that all three parties receive the same classical information. Next, for the remainder of the protocol, Bob and Charlie may not communicate. However, since Alice must communicate by publicly broadcasting, Bob and Charlie receive exactly the same information from her, and may respond to all the same challenges. As such, classically, our model becomes equivalent to the standard two-party model. In particular, bit commitment is impossible. The difference with the two-sender model, where bit commitment does exist classically, arises due to the additional communication restriction we imposed: the receiver of [BGKW88] may share different information with each of the senders, rather than broadcasting publicly.

8.5 Everlasting Randomness Expansion

The creation of fresh, trusted, uniform randomness is an important part of many computational and cryptographic tasks. Since quantum mechanics is inherently probabilistic, it

stands to reason that quantum procedures prove useful for this task. A simple demonstration of this can be seen with a one-qubit system. By preparing the qubit in the Hadamard $|+\rangle$ state and then measuring in the computational basis provides a uniformly random bit, without the need to use an input randomness. However, this requires that the quantum system be perfectly trusted.

A major theoretical hurdle in achieving something like this in practice is that it is difficult to characterise the behaviour of an untrusted quantum device: one needs to verify that their source of randomness is truly random and not shared by an eavesdropper. Largely, the methods to bypass this difficulty use a nonlocal game to verify entanglement between two untrusted provers. However, this requires, in particular, that the provers are able to produce entangled states, and keep them from decohering throughout the running time of the protocol. This can be an impractical requirement.

8.5.1 Randomness expansion in the MoE model

In our contribution, we remove the need for long-distance entanglement, and instead make the assumption of a trusted but leaky measurement, as well as a standard computational assumption. We use a construction based on the rigidity of the TFKW game, as given in Theorem 7.14. The protocol consists of two steps: first, Alice samples the output of a pseudorandom generator, allowing her to increase the size of her random string; then, she uses this as the source of randomness to play the TFKW game against computationally-bounded and isolated Bob and Charlie, where the rigidity allows her to extract a string that is uniformly random and unknown to either Bob or Charlie. First, we need to formalise the model we are working in, based on the structure of an MoE game.

Definition 8.38. The *MoE model for randomness expansion* consists of three quantum parties: a trusted verifier Alice, who interacts with two untrusted provers, Bob and Charlie. The model satisfies the following:

- Bob and Charlie are able to prepare a tripartite shared state but then are isolated.
- Alice can make trusted measurements on her register, which are leaky in the sense that Bob and Charlie can learn the measurement bases.

Now, we can define randomness expanders in this model.

Definition 8.39. A $(s(n), \varepsilon)$-*local randomness expander* is a protocol in the MoE model, where, given a uniformly random seed in $S = \mathbb{Z}_2^{s(n)}$, Alice, Bob, and Charlie construct a

quantum state ρ_{YSBC}, where $Y = \mathbb{Z}_2^n$ and S are classical registers that Alice holds and B and C are potentially quantum registers that Bob and Charlie hold, respectively, such that

$$\begin{aligned} \|\rho_{YSB} - \mu_Y \otimes \mu_S \otimes \rho_B\|_{\mathrm{Tr}} &\leq \varepsilon \\ \|\rho_{YSC} - \mu_Y \otimes \mu_S \otimes \rho_C\|_{\mathrm{Tr}} &\leq \varepsilon, \end{aligned} \tag{8.5.1}$$

if Alice does not abort during the execution. As before, we say this scheme *fails with probability* p if these conditions do not hold with probability at most p.

The idea of this definition is that Alice's output needs to be approximately uniformly random in any case, but we can also get the additional guarantee that, as long as Bob and Charlie stay isolated, they cannot hold onto side information that allows them to guess the output. However, we do not constrain their ability to guess the output if they come back together: for example, the register BC could be maximally entangled with Alice's register before she makes her final measurement, without either B or C being maximally entangled on their own.

8.5.2 Computational TFKW game

The main computational tool we will be making use of is the idea of a pseudorandom generator against computationally-bounded adversaries. Pseudorandom generators are functions that take a uniformly random string to a longer string that no QPT algorithm can distinguish from uniform.

Definition 8.40. A family of functions $G_n : \mathbb{Z}_2^{s(n)} \to \mathbb{Z}_2^n$ is a *pseudorandom generator* (PRG) if, for uniform random variables Γ in $\mathbb{Z}_2^{s(n)}$ and Δ in $\mathbb{Z}_2^n$, and for every QPT algorithm $Q : \mathbb{Z}_2^* \to \mathbb{Z}_2$,

$$\Big|\Pr[Q(G_n(\Gamma)) = 1] - \Pr[Q(\Delta) = 1]\Big| \in \mathtt{negl}(n). \tag{8.5.2}$$

The input of G_n is called the *seed* and $s(n)$ is the seed length.

Note that, in our context, the QPT algorithm need only be given classical access to the random variable, since Alice will be simply providing Bob and Charlie with strings sampled from this distribution. As such, that probability of Q outputting 1 takes its usual meaning as the probability measure of $Q^{-1}(\{1\})$.

Because of brute force attacks against G_n, $s(n) \in O(\lg n)$ is a strict lower bound on the seed length. Thus, we cannot hope for exponential randomness expansion with this method, but we can nevertheless expect large polynomial or even superpolynomial expansion. Now we can define a variant of the TFKW game that uses a pseudorandom rather than uniformly random question distribution.

Definition 8.41. Let $G_n : \mathbb{Z}_2^{s(n)} \to \mathbb{Z}_2^n$ be a PRG and let Γ be the uniform random variable on $\mathbb{Z}_2^{s(n)}$. The *computational TFKW game* on n qubits is the MoE game $\mathtt{TFKW}_G^n = \big(\mathbb{Z}_2^n, \mathbb{Z}_2^n, \pi_G, \mathbb{Z}_2^n, \{A^\theta\}\big)$, where $\pi_G(\theta) = \Pr[G_n(\Gamma) = \theta]$, and $A_y^\theta = |y^\theta\rangle\langle y^\theta|$ as for the usual TFKW game.

The set of strategies for the computational TFKW game is identical to that for the usual TFKW game, but where we restrict to families of strategies that can be modelled by QPT adversaries. As a warm-up to the main result of this section, we can see that against QPT strategies (shared state and measurements are all QPT), the usual and computational TFKW games behave essentially the same.

Lemma 8.42. Let $n \mapsto \mathtt{S}_n = \big(B_n, C_n, \{(B_n)^\theta\}, \{(C_n)^\theta\}, \rho_n\big)$ be a family of strategies with QPT adversaries. Then, assuming the existence of a PRG $G_n : \mathbb{Z}_2^{s(n)} \to \mathbb{Z}_2^n$, for every $i \in [n]$,

$$\left|\mathfrak{w}^i_{\mathtt{TFKW}^n_G}(\mathtt{S}_n) - \mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}_n)\right| \in \mathtt{negl}(n) \tag{8.5.3}$$

Proof: We will use $\mathtt{S}_n$ to construct a QPT algorithm attempting to distinguish the variable $G_n(\Gamma)$ from uniformly random as follows. To compute $Q(\theta)$, measure the state ρ_n with the POVM $(A^n)^\theta \otimes (B_n)^\theta \otimes (C_n)^\theta$. Output 1 if the measurement result is some (x, x^B, x^C) with $x_i = x_i^B = x_i^C$ and output 0 otherwise. Then, for uniform random variables Γ in $\mathbb{Z}_2^{s(n)}$ and Δ in $\mathbb{Z}_2^n$,

$$\begin{aligned}
&\Big|\Pr[Q(G_n(\Gamma)) = 1] - \Pr[Q(\Delta) = 1]\Big| \\
&= \Bigg| \mathop{\mathbb{E}}_{\theta \leftarrow G_n(\Gamma)} \sum_{y \in \mathbb{Z}_2} \mathrm{Tr}\big[((A^n)^\theta_{y,i} \otimes (B_n)^\theta_{y,i} \otimes (C_n)^\theta_{y,i})\rho_n\big] \\
&\qquad\qquad - \mathop{\mathbb{E}}_{\theta \leftarrow \Delta} \sum_{y \in \mathbb{Z}_2} \mathrm{Tr}\big[((A^n)^\theta_{y,i} \otimes (B_n)^\theta_{y,i} \otimes (C_n)^\theta_{y,i})\rho_n\big] \Bigg| \\
&= \Big|\mathfrak{w}^i_{\mathtt{TFKW}^n_G}(\mathtt{S}_n) - \mathfrak{w}^i_{\mathtt{TFKW}^n}(\mathtt{S}_n)\Big|.
\end{aligned} \tag{8.5.4}$$

We may conclude by noting that the left-hand side is contained in $\texttt{negl}(n)$ by hypothesis. ■

8.5.3 Randomness expansion protocol

We formally present the protocol.

Protocol 8.43 (randomness expansion)**.**

1. Alice samples $(t, u) \in \mathbb{Z}_2^{s(N)+s\left(\left\lceil \lg \binom{N}{n} \right\rceil\right)}$ uniformly at random. She computes $\theta = G_N(t)$ and $J = G_{\left\lceil \lg \binom{N}{n} \right\rceil}(u)$, where she interprets J as a subset of $[N]$ of cardinality n.

2. Bob and Charlie prepare a shared state ρ_{ABC} and then are isolated.

3. Alice measures each of her qubits $i \in [N]$ in basis $\{|0^{\theta_i}\rangle, |1^{\theta_i}\rangle\}$ if $i \notin J$ and in basis $\{|0^i\rangle = |+i\rangle, |1^i\rangle = |-i\rangle\}$ if $i \in J$. This produces a string $y \in \mathbb{Z}_2^N$ that she keeps.

4. Alice sends Bob and Charlie the key θ and J. Bob and Charlie each reply with a guess of y, y^B and y^C respectively.

5. Alice verifies that they win the TFKW game $y_i = y_i^B = y_i^C$ for at least $(\cos^2\left(\frac{\pi}{8}\right) - \delta)N$ of the $i \in [N]\backslash J$, and then, if she accepts, takes y_J to be her output.

The protocol follows a very similar framework to Protocol 8.34, with the main differences being that Alice chooses her questions and test qubits only pseudorandomly, and measures always in the same basis to get her output. This basis is chosen to be mutually unbiased with all of the Breidbart states, and thus gives a uniformly random measurement result for any optimal strategy. Note that Bob and Charlie are able to make the protocol accept and provide randomness without using entanglement simply by preparing the Breidbart state $|\beta\rangle^{\otimes N}$, sending it to Alice, and guessing 0 on all the TFKW game verification rounds.

Also, in this protocol, Alice shares θ and J with Bob and Charlie immediately after she measures, so they have full information about her measurement bases. Thus, it doesn't affect the protocol if that information is leaked.

Theorem 8.44. Let K be the constant from Theorem 7.14, $\varepsilon, \eta, \delta \in (0,1)$ such that $\eta\varepsilon > \delta$, and $N \in \texttt{poly}(n)$. Assuming the existence of a pseudorandom generator, $G_n : \mathbb{Z}_2^{s(n)} \to \mathbb{Z}_2^n$, Protocol 8.43 is a $(s(N) + s(\lg \binom{N}{n}), 2Kn^3\sqrt{\varepsilon} + 2n\eta + \texttt{negl}(n))$-local randomness expander in the MoE model with QPT provers, that fails with probability $e^{-2N(\eta\varepsilon-\delta)^2} + \texttt{negl}(n)$.

The scenario in Example 7.15 allows us to take $N = n^{27}$, so provided that $s(n) \in o(n^{1/27})$ is possible, this yields randomness expansion.

Proof: Write $b = \lceil \lg \binom{N}{n} \rceil$. Let U be the random variable representing the number of rounds Bob and Charlie win, let V be the random variable representing the number of rounds they would have won if Alice chose J uniformly at random (among the subsets of $[N]$ with cardinality n), and let W be the number of rounds they would have won if Alice chose both J and θ uniformly at random.

Take $Q(\theta, J)$ to be the QPT algorithm computed by running steps 2-5 of the randomness expansion protocol, and outputting 1 if Alice accepts the verification of the TFKW games, and 0 otherwise. Then, taking $\Gamma_1, \Gamma_2, \Delta_1, \Delta_2$ to be random variables in $\mathbb{Z}_2^{s(N)}$, $\mathbb{Z}_2^{s(b)}$, $\mathbb{Z}_2^N$, and $\mathbb{Z}_2^b$, respectively, we know that

$$\begin{aligned} &\Pr[Q(G_N(\Gamma_1), G_b(\Gamma_2)) = 1] = \Pr\big[U \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big], \\ &\Pr[Q(G_N(\Gamma_1), \Delta_2) = 1] = \Pr\big[V \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big], \text{ and} \\ &\Pr[Q(\Delta_1, \Delta_2) = 1] = \Pr\big[W \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big], \end{aligned} \tag{8.5.5}$$

giving

$$\begin{aligned} &\Big|\Pr\big[U \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big] - \Pr\big[W \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big]\Big| \\ &\quad\leq \Big|\Pr\big[U \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big] - \Pr\big[V \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big]\Big| \\ &\qquad + \Big|\Pr\big[V \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big] - \Pr\big[W \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big]\Big| \\ &\quad\in \texttt{negl}(b) + \texttt{negl}(N) \subseteq \texttt{negl}(n), \end{aligned} \tag{8.5.6}$$

as $N \in \texttt{poly}(n)$ and $b \in O(n \lg n)$. Now, using Lemma 7.13 as in Theorem 8.36, if less than $(1-\eta)N$ of the rounds have winning probability greater than $\cos^2(\frac{\pi}{8}) - \varepsilon$, then

$$\Pr\big[W \geq (\cos^2(\tfrac{\pi}{8}) - \delta)N\big] \leq e^{-2N(\eta\varepsilon-\delta)^2}. \tag{8.5.7}$$

By the above, then

$$\Pr\big[U \geq (\cos^2\big(\tfrac{\pi}{8}\big) - \delta)N\big] \in e^{-2N(\eta\varepsilon-\delta)^2} + \texttt{negl}(n). \tag{8.5.8}$$

So, other than with negligible failure probability, at least $(1-\eta)N$ of the rounds have winning probability greater than $\cos^2\big(\frac{\pi}{8}\big) - \varepsilon$.

If we select n rounds uniformly at random, each of the rounds has probability $1-\eta$ of winning with probability greater than $\cos^2\big(\frac{\pi}{8}\big) - \varepsilon$. Of course, the rounds are actually selected pseudorandomly: we claim that Bob and Charlie have a negligible probability of distinguishing the two cases. Let $E \subseteq [N]$ be the set of rounds that win with probability greater than $\cos^2\big(\frac{\pi}{8}\big) - \varepsilon$, and write $J = \{j_1(J), \ldots, j_n(J)\}$, where $j_1(J) < \ldots < j_n(J)$. Then, as Bob and Charlie's strategy is QPT, it is possible, for each $i \in [n]$, by using their strategy to play TFKW a polynomial number of times, to get a QPT algorithm that, on input J, outputs whether $j_i(J) \in E$ correctly with $1 - \texttt{negl}(n)$ probability. Thus, using pseudorandomness, we know

$$|\Pr[j_i(G_b(\Gamma_2)) \in E] - \Pr[j_i(\Delta_2) \in E]| \in \texttt{negl}(n). \tag{8.5.9}$$

As $\Pr[j_i(\Delta_2) \in E] \geq 1-\eta$, each of the rounds chosen pseudorandomly has probability at least $1 - \eta - \texttt{negl}(n)$ of having winning probability greater than $\cos^2\big(\frac{\pi}{8}\big) - \varepsilon$. So, by Theorem 7.14 there exists a constant $K \geq 0$, isometries $V : \mathcal{H}_B \to \mathcal{H}_{B'}$ and $W : \mathcal{H}_C \to \mathcal{H}_{C'}$, an auxiliary register R, and a state $|\phi\rangle = \sum_{x,\varphi\in\mathbb{Z}_2^n} \mathfrak{G}^{\otimes n}|x^\varphi\rangle \otimes |x,\varphi\rangle_{BCR}$ where the $|x,\varphi\rangle_{BCR} \in \mathcal{H}_{B'C'R}$ have orthogonal support on both B' and C' such that

$$\mathop{\mathbb{E}}_{J\leftarrow G_b(\Gamma_2)} \big\|(V\otimes W)\rho_{A_JBC}(V\otimes W)^\dagger - \mathrm{Tr}_R(\,|\phi\rangle\langle\phi|)\big\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta + \texttt{negl}(n). \tag{8.5.10}$$

Let $\sigma_{A_JBC} = \mathrm{Tr}_R(\,|\phi\rangle\langle\phi|)$. If Alice measures her register in the basis $\{|y^i\rangle | y \in \mathbb{Z}_2^n\}$, she gets

$$\begin{aligned}\sigma_{YB} &= \sum_{y,x,\varphi\in\mathbb{Z}_2^n} \big|\,\langle y^i|\mathfrak{G}^{\otimes n}|x^\varphi\rangle\big|^2 [y]_Y \otimes \mathrm{Tr}_{CR}(\,|x,\varphi\rangle\langle x,\varphi|)_B \\ &= \sum_{y,x,\varphi\in\mathbb{Z}_2^n} \frac{1}{2^n}[y]_Y \otimes \mathrm{Tr}_{CR}(\,|x,\varphi\rangle\langle x,\varphi|)_B = \mu_Y \otimes \sigma_B.\end{aligned} \tag{8.5.11}$$

So, following the protocol, Alice measures A_J of ρ in this basis, giving

$$\mathop{\mathbb{E}}_{J\leftarrow G_b(\Gamma_2)} \|V\rho_{Y_JB}V^\dagger - \mu_Y \otimes \sigma_B\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta + \mathtt{negl}(n). \tag{8.5.12}$$

Acting with the trace non-increasing channel $\rho \mapsto V^\dagger \rho V$,

$$\mathop{\mathbb{E}}_{J\leftarrow G_b(\Gamma_2)} \|\rho_{Y_JB} - \mu_Y \otimes V^\dagger\sigma_B V\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta + \mathtt{negl}(n), \tag{8.5.13}$$

where in particular,

$$\mathop{\mathbb{E}}_{J\leftarrow G_b(\Gamma_2)} \|\rho_B - V^\dagger\sigma_B V\|_{\mathrm{Tr}} \leq Kn^3\sqrt{\varepsilon} + n\eta + \mathtt{negl}(n), \tag{8.5.14}$$

so, using the triangle inequality,

$$\mathop{\mathbb{E}}_{J\leftarrow G_b(\Gamma_2)} \|\rho_{Y_JB} - \mu_Y \otimes \rho_B\|_{\mathrm{Tr}} \leq 2Kn^3\sqrt{\varepsilon} + 2n\eta + \mathtt{negl}(n). \tag{8.5.15}$$

Let S be a classical register holding the seed, and let $I = G_b(S)$ be the register that holds J. Then,

$$\begin{aligned}
\|\rho_{YSB} - \mu_Y \otimes \mu_S \otimes \rho_B\|_{\mathrm{Tr}} &\leq \Big\| \mathop{\mathbb{E}}_{t\in\mathbb{Z}_2^{s(b)}} [t]_S \otimes [G_b(t)]_I \otimes \Big(\rho_{Y_{G_b(t)}B} - \mu_Y \otimes \rho_B\Big)\Big\|_{\mathrm{Tr}} \\
&= \mathop{\mathbb{E}}_{t\in\mathbb{Z}_2^{s(b)}} \Big\|\rho_{Y_{G_b(t)}B} - \mu_Y \otimes \rho_B\Big\|_{\mathrm{Tr}} \\
&\leq 2Kn^3\sqrt{\varepsilon} + 2n\eta + \mathtt{negl}(n)
\end{aligned} \tag{8.5.16}$$

The same proof holds for ρ_{YSC}. ■

Chapter 9

Conclusion

We have formally discussed the setting of uncloneability games, and studied properties of some interesting examples. We have proven winning probability bounds on new families of NC games, showing a conjecture of [CLLZ21], and demonstrated the first example of rigidity for MoE games. We also found applications of these results to a variety of cryptographic problems. There are, however, still many important questions left over. We ask a selection here.

Does uncloneable encryption exist in the plain model? This is a question first asked in [BL20] and that remains open. We give a construction of uncloneable encryption in the plain model, but where the decryption requires interaction. Is there a way to remove the interaction?

Are there other interesting uncloneability games that satisfy a rigidity property? Perhaps it is possible to find other rigidity results for XNL games. For example, the coset state games we have studied might also satisfy a similar rigidity property to the TFKW game. However, a major hurdle to showing this is that our upper bound on the winning probability is not tight. More generally, are there rigidity results for NC games as well as MoE games? This might require different techniques: as an example, the exact rigidity of the TFKW game is easily adapted to the NC version, but the robust rigidity isn't, as it does not give a strong bound on the natural distance of channels, the diamond norm.

Are there other applications of rigidity of MoE games? Rigidity, as it was already known for nonlocal games, has various important applications. With this in mind, there might be a similar range of possible applications for MoE rigidity.

Bibliography

[AB09] S. Arora and B. Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[AC12] S. Aaronson and P. Christiano. Quantum money from hidden subspaces. In *44th Annual ACM Symposium on Theory of Computing—STOC 2012*, pages 41–60, 2012.
DOI: 10.1145/2213977.2213983.

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical review letters*, 49(25): 1804, 1982.
DOI: 10.1103/PhysRevLett.49.1804.

[AK21] P. Ananth and F. Kaleoglu. Unclonable encryption, revisited. In *18th Theory of Cryptography Conference—TCC 2021*, pages 299–329, 2021.
DOI: 10.1007/978-3-030-90459-3_11.

[AM16] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature*, 540: 213–219, 2016.
DOI: 10.1038/nature20119.

[AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *41st Annual Symposium on Foundations of Computer Science—FOCS 2000*, pages 547–553, 2000.
DOI: 10.1109/SFCS.2000.892142.

[Ash02] R. B. Ash. *Abstract Algebra: the basic graduate year*. 2002. Available at https://faculty.math.illinois.edu/~r-ash/Algebra.html.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBCS01] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology—CRYPTO 1991*, pages 351–366, 2001.
DOI: 10.1007/3-540-46766-1_29.

[BC21] A. Broadbent and E. Culf. Rigidity for monogamy-of-entanglement games, 2021.
DOI: 10.48550/ARXIV.2111.08081.

[BC22] A. Broadbent and E. Culf. Uncloneable cryptographic primitives with interaction, 2022. Manuscript in preparation.

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2): 156–189, 1988.
DOI: 10.1016/0022-0000(88)90005-0.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics 1*, pages 195–200, 1964.
Online: http://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf.

[BGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Widgerson. Multi-prover interactive proofs: how to remove intractability assumptions. In *20th Annual ACM Symposium on Theory of Computing—STOC 1988*, pages 113–131, 1988.
DOI: 10.1145/62212.62223.

[BJ00] B. Brandsen and C. Joachain. *Quantum Mechanics*. Pearson, Harlow, 2nd ed. edition, 2000.

[BL20] A. Broadbent and S. Lord. Uncloneable quantum encryption via oracles. In *15th Conference on the Theory of Quantum Computation, Communication*

and Cryptography—TQC 2020, pages 4:1 – 4:22, 2020.
DOI: 10.4230/LIPIcs.TQC.2020.4.

[BO08] N. P. Brown and N. Ozawa. *C*-algebras and finite-dimensional approximations*. Graduate studies in mathematics, v. 88. American Mathematical Society, Providence, R.I, 2008.

[Boh13] N. Bohr. On the Constitutions of Atoms and Molecules. Pt. I. *Philosophical Magazine*, 26: 1–25, 1913.
DOI: 10.1080/14786441308634955.

[Bor26] M. Born. Zur Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik*, 37(12): 863–867, 1926.
DOI: 10.1007/BF01397477.

[BR03] P. O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67(4): 042317, 2003.
DOI: 10.1103/PhysRevA.67.042317.

[BS16] A. Broadbent and C. Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1): 351–382, 2016.
DOI: 10.1007/s10623-015-0157-4.

[CGH04] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. *Journal of the ACM*, 51(4): 557–594, 2004.
DOI: 10.1145/1008731.1008734.

[Cha87] D. Chaum. Demonstrating that a public predicate can be satisfied without revealing any information about how. In *Advances in Cryptology—CRYPTO 1986*, page 195–199, 1987.

[CHSH69] J. F. Clauser, M. A. Horne., A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15): 880–884, 1969.
DOI: 10.1103/PhysRevLett.23.880.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Physical Review A*, 61(5): 052306, 200.
DOI: 10.1103/PhysRevA.61.052306.

[CLLZ21] A. Coladangelo, J. Liu, Q. Liu, and M. Zhandry. Hidden cosets and applications to unclonable cryptography. In *Advances in Cryptology—CRYPTO 2021*, pages 556–584, 2021.
DOI: 10.1007/978-3-030-84242-0_20.

[CMMN20] D. Cui, A. Mehta, H. Mousavi, and S. S. Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4: 346, 2020.
DOI: 10.22331/q-2020-10-21-346.

[Col06] R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, UK, 2006.
arXiv: 0911.3814.

[Col17] A. Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information & Computation*, 17(9-10): 831–865, 2017.
DOI: 10.5555/3179561.3179567.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *Advances in Cryptology—CRYPTO 1987*, pages 350–354, 1988.
DOI: 10.1007/3-540-48184-2_30.

[Cré11] C. Crépeau. *Commitment*, pages 224–227. Springer US, Boston, MA, 2011.
DOI: 10.1007/978-1-4419-5906-5_239. Available at http://crypto.cs.mcgill.ca/~crepeau/PDF/Commit.pdf.

[CSST11] C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Two provers in isolation. In *Advances in Cryptology—ASIACRYPT 2011*, pages 407–430, 2011.
DOI: 10.1007/978-3-642-25385-0_22.

[CV22] E. Culf and T. Vidick. A monogamy-of-entanglement game for subspace coset states. *Quantum*, 6: 791, 2022.
DOI: 10.22331/q-2022-09-01-791.

[CW05] M. Christandl and S. Wehner. Quantum anonymous transmissions. In *Advances in Cryptology—ASIACRYPT 2005*, pages 217–235, 2005.
DOI: 10.1007/11593447_12.

[CY14] M. Coudron and H. Yuen. Infinite randomness expansion with a constant number of devices. In *46th Annual ACM Symposium on Theory of Computing—STOC 2014*, page 427–436, 2014.
DOI: 10.1145/2591796.2591873.

[de 23] L. de Broglie. Waves and Quanta. *Nature*, 112(2815): 540, 1923.
DOI: 10.1038/112540a0.

[Deu83] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.*, 50: 631–633, 1983.
DOI: 10.1103/PhysRevLett.50.631.

[DFSS08] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6): 1865–1890, 2008.
DOI: 10.1137/060651343.

[DG28] C. J. Davisson and L. H. Germer. Reflection of Electrons by a Crystal of Nickel. *Proceedings of the National Academy of Science*, 14(4): 317–322, 1928.
DOI: 10.1073/pnas.14.4.317.

[Die82] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6): 271–272, 1982.
DOI: 10.1016/0375-9601(82)90084-6.

[Die18] R. Diestel. *Graph theory*. Springer, 2018.
DOI: 10.1007/978-3-662-53622-3.

[DMS00] P. Dumais, D. Mayers, and L. Salvail. Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation. In *Advances in Cryptology—EUROCRYPT 2000*, pages 300–315, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.
DOI: 10.1007/3-540-45539-6_21.

[DPVR12] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):

915–940, 2012.
DOI: 10.1137/100813683.

[Ein05] A. Einstein. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*, 322(6): 132–148, 1905.
DOI: 10.1002/andp.19053220607.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6): 661–663, 1991.
DOI: 10.1103/PhysRevLett.67.661.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review Letters*, 47(10): 777–780, 1935.
DOI: 10.1103/physrev.47.777.

[FH14] J. Franck and G. Hertz. Über zusammenstöße zwischen elektronen und den molekülen des quecksilberdampfes und die ionisierungsspannung desselben. *Verh. D. Phys. Ges.*, 16: 457–467, 1914.

[GH17] W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups. *Sbornik: Mathematics*, 208(12): 1784–1817, 2017.
DOI: 10.1070/sm8872.

[Gle57] A. Gleason. Measures on the Closed Subspaces of a Hilbert Space. *Indiana Univ. Math. J.*, 6: 885–893, 1957.

[Got03] D. Gottesman. Uncloneable encryption. *Quantum Information & Computation*, 3(6): 581–602, 2003.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:

682–686, 2015.
DOI: 10.1038/nature15759.

[Hei27] W. Heisenberg. Schwankungserscheinungen und quantenmechanik. *Zeitschrift für Physik*, 40(7): 501–506, 1927.
DOI: 10.1007/BF01440827.

[Her82] N. Herbert. FLASH —– A superluminal communicator based upon a new kind of quantum measurement. *Foundations of Physics*, 12(12): 1171–1179, 1982.
DOI: 10.1007/BF00729622.

[Hir57] I. I. Hirschman. A note on entropy. *American Journal of Mathematics*, 79(1): 152–156, 1957.
Online: http://www.jstor.org/stable/2372390.

[HMN+21] J. W. Helton, H. Mousavi, S. S. Nezhadi, V. I. Paulsen, and T. B. Russell. Synchronous values of games, 2021.
DOI: 10.48550/ARXIV.2109.14741.

[Hoe63] W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, 58(301): 13–30, 1963.
DOI: 10.1080/01621459.1963.10500830.

[JMRW16] N. Johnston, R. Mittal, V. Russo, and J. Watrous. Extended non-local games and monogamy-of-entanglement games. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 472(2189): 20160003, 2016.
DOI: 10.1098/rspa.2016.0003.

[JNV+21] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. $\mathsf{MIP}^* = \mathsf{RE}$. *Communications of the ACM*, 64(11): 131–138, 2021.
DOI: 10.1145/3485628.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *20th Annual ACM Symposium on Theory of Computing—STOC 1988*, pages 20–31, 1988.
DOI: 10.1145/62212.62215.

[KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[KT08] R. T. König and B. M. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2): 749–762, 2008.
DOI: 10.1109/TIT.2007.913245.

[KT22] S. Kundu and E. Y. Z. Tan. Device-independent uncloneable encryption, 2022.
DOI: 10.48550/ARXIV.2210.01058.

[KWW12] R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3): 1962–1984, 2012.
DOI: 10.1109/TIT.2011.2177772.

[LC97] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17): 3410–3413, 1997.
DOI: 10.1103/PhysRevLett.78.3410.

[LC99] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410): 2050–2056, 1999.
DOI: 10.1126/science.283.5410.2050.

[May96] D. Mayers. The trouble with quantum bit commitment, 1996.
arXiv: quant-ph/9603015.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17): 3414–3417, 1997.
DOI: 10.1103/PhysRevLett.78.3414.

[MNP21] L. Mančinska, T. G. Nielsen, and J. Prakash. Glued magic games self-test maximally entangled states, 2021. Available at https://arxiv.org/abs/2105.10658.

[MR22] T. Metger and R. Renner. Security of quantum key distribution from generalised entropy accumulation, 2022.
DOI: 10.48550/ARXIV.2203.04993.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes: Volume 1*. North-Holland mathematical library ; v. 16. North-Holland Pub. Co., Amsterdam, 1977.

[MU88] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12): 1103–1106, 1988.
DOI: 10.1103/PhysRevLett.60.1103.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4(4): 273–286, 2004.
Online: http://dl.acm.org/citation.cfm?id=2011827.2011830.

[MYS12] M. McKague, T. H. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Physics A*, 45(45): 455304, 2012.
DOI: 10.1088/1751-8113/45/45/455304.

[Nao91] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4: 151–158, 1991.
DOI: 10.1007/BF00196774.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition, 2010.

[NV17] A. Natarajan and T. Vidick. A quantum linearity test for robustly verifying entanglement. In *49th Annual ACM Symposium on Theory of Computing—STOC 2017*, pages 1003–1015, 2017.
DOI: 10.1145/3055399.3055468.

[Oza13] N. Ozawa. About the Connes Embedding Conjecture—Algebraic approaches—, 2013. Available at https://arxiv.org/abs/1212.1700.

[Par70] J. L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1): 23–33, 1970.
DOI: 10.1007/BF00708652.

[Pau02] V. I. Paulsen. *Completely bounded maps and operator algebras*. Cambridge studies in advanced mathematics ; 78. Cambridge University Press, Cambridge ;, 2002.

[Per03] A. Peres. How the no-cloning theorem got its name. *Fortschritte der Physik: Progress of Physics*, 51(4-5): 458–461, 2003.
DOI: 10.1002/prop.200310062.

[Pla01] M. Planck. Über das Gesetz der Energieverteilung im Normalspectrum. *Annalen der Physik*, 309(3): 553–563, 1901.
DOI: 10.1002/andp.19013090310.

[Pre92] O. Pretzel. *Error-correcting codes and finite fields*. Oxford applied mathematics and computing science series. Clarendon Press, Oxford, 1992.

[Rén70] A. Rényi. *Probability Theory*. North-Holland Series in Applied Mathematics and Mechanics, V.10. Amsterdam, North-Holland Pub. Co., 1970.

[Ren05] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 06(01): 1–127, 2005.
DOI: 10.1142/S0219749908003256.

[RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496: 456–460, 2013.
DOI: 10.1038/nature12035.

[Sch26] E. Schrödinger. Quantisierung als eigenwertproblem. *Annalen der Physik*, 384(4): 361–376, 1926.
DOI: 10.1002/andp.19263840404.

[Ser77] J.-P. Serre. *Linear representations of finite groups.* Graduate texts in mathematics ; 042. Springer-Verlag, New York, 1977.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4): 656–715, 1949.

[SML10] D. Stebila, M. Mosca, and N. Lütkenhaus. The case for quantum key distribution. In *Quantum Communication and Quantum Networking*, volume 36,

pages 283–296, 2010.
DOI: 10.1007/978-3-642-11731-2_35.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2): 441–444, 2000.
DOI: 10.1103/physrevlett.85.441.

[SW08] V. B. Scholz and R. F. Werner. Tsirelson's Problem, 2008.
DOI: 10.48550/arXiv.0812.4305.

[SZB+21] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill. Device-independent randomness expansion with entangled photons. *Nature Physics*, 17: 452–456, 2021.
DOI: 10.1038/s41567-020-01153-4.

[Ter04] B. M. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48(1): 71–78, 2004.
DOI: 10.1147/rd.481.0071.

[TFKW13] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10): 103002, 2013.
DOI: 10.1088/1367-2630/15/10/103002.

[TL17] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1: 14, 2017.
DOI: 10.22331/q-2017-07-14-14.

[Tom16] M. Tomamichel. *Quantum Information Processing with Finite Resources Mathematical Foundations*. SpringerBriefs in Mathematical Physics, 5. Springer International Publishing, Cham, 2016.

[Tre01] L. Trevisan. Extractors and Pseudorandom Generators. *Journal of the ACM*, 48(4): 860–879, 2001.
DOI: 10.1145/502090.502099.

[Tsi80] B. Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2): 93–100, 1980.
DOI: 10.1007/bf00417500.

[Tsi93] B. S. Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronic Journal Supplement*, 8: 329–345, 1993.

[Unr10] D. Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology—EUROCRYPT 2010*, pages 486–505, 2010.
DOI: 10.1007/978-3-642-13190-5_25.

[Unr13] D. Unruh. Everlasting multi-party computation. In *Advances in Cryptology—CRYPTO 2013*, pages 380–397, 2013.
DOI: 10.1007/978-3-642-40084-1_22.

[Vid18] T. Vidick. Expository note based on [NV17], 2018.
Online: http://users.cms.caltech.edu/~vidick/notes/pauli_braiding_1.pdf.

[VV12] U. V. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *44th Annual ACM Symposium on Theory of Computing—STOC 2012*, pages 61–76, 2012.
DOI: 10.1145/2213977.2213984.

[VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113(14): 140501, 2014.
DOI: 10.1103/PhysRevLett.113.140501.

[VZ21] T. Vidick and T. Zhang. Classical proofs of quantum knowledge. In *Advances in Cryptology—EUROCRYPT 2021*, pages 630–660, 2021.
DOI: 10.1007/978-3-030-77886-6_22.

[Wat18] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 1st edition, 2018.

[WC81] M. N. Wegman and J. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3): 265–279, 1981.
DOI: 10.1016/0022-0000(81)90033-7.

[Wei03] S. H. Weintraub. *Representation theory of finite groups : algebra and arithmetic*. Graduate studies in mathematics, v. 59. American Mathematical Society, Providence, R.I, 2003.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1): 78–88, 1983. DOI: 10.1145/1008908.1008920.

[WW10] S. Wehner and A. Winter. Entropic uncertainty relations- a survey. *New Journal of Physics*, 12(2): 025009, 2010. DOI: 10.1088/1367-2630/12/2/025009.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299: 802–803, 1982. DOI: 10.1038/299802a0.

[YXTZ14] Y.-G. Yang, P. Xu, J. Tian, and H. Zhang. Quantum oblivious transfer with an untrusted third party. *Optik*, 125(18): 5409–5413, 2014. DOI: 10.1016/j.ijleo.2014.06.023.