A Rank-3 Secret Sharing Scheme over Vector Spaces

Joshua Mulloy

Thesis submitted to the University of Ottawa in partial fulfillment of the requirements for the degree of Master of Science Mathematics and Statistics*

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

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

Abstract

Secret sharing schemes are a tool used to ensure secure distribution of a secret among a group of participants such that only authorized groups can reconstruct the secret. We explore the relationship between secret sharing schemes and matroids, with emphasis placed on matroid-related schemes. Specifically, we focus on the access structures arising from matroids with rank three. We present the projective plane secret sharing scheme, a reformulation of the scheme of Lopes de Souza, now using projective planes instead of LFSR sequences. We show that this scheme is equivalent to the vector space secret sharing scheme of Brickell. Additionally, we show that the induced subhypergraph isomorphism problem is equivalent to the subgraph isomorphism problem, and use this equivalence in a new method to find realizations of access structures by our scheme. Finally, we give some conditions to find the minimal q required for our scheme to realize an access structure in $\mathbb{F}_q$.

Acknowledgements

First, I would like to thank my supervisor, Dr. Lucia Moura, for her invaluable guidance, encouragement, and for fostering my confidence and academic growth. Her mentorship has been instrumental in shaping this work. I would like to extend my sincere thanks to Dr. Paul-Eugène Parent, my former supervisor, for giving me the opportunity to embark on this path. Your belief in me opened the door to countless possibilities.

I am extremely grateful to my parents, Robin and Amanda, whose unwavering support, both emotionally and financially, have made all of this possible. Thank you for always being there for me. I would be remiss in not also mentioning my sister, Jessie, who has forced me to strive to be the best version of myself. Special thanks to Curtis Toupin, whose enthusiasm and belief in my potential convinced me that pursuing a master's degree was not only achievable but also worthwhile.

Lastly, I would like to thank my high school math teacher, Mr. Melville, without whom I would be an engineer right now.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

A secret sharing scheme is a method used by a dealer to distribute a portion of a secret, called a share, among groups of participants such that only authorized sets of participants can reconstruct the secret. For example, suppose there is a bank owner who has a vault that is accessible using a code that changes each day. They employ three managers and four tellers, and want the vault to only be accessible by groups that they feel will keep each other honest. They feel they can trust any two managers, any three tellers, or any manager with any two tellers. Each day, the bank owner would use a secret sharing scheme to distribute parts of the vault code to their employees such that only groups they trust could gain access.

These schemes were introduced in the simplest case by Blakley [6] and Shamir [24], both in 1979. Their secret sharing schemes are referred to as *threshold secret sharing schemes*. In their schemes the sets that can reconstruct the secret are all of the sets with at least a certain number participants t. This scheme was generalized by Brickell [8] in 1990. Brickell's scheme uses vector spaces to distribute the shares to the participants, and so we call it the *vector space secret sharing scheme*. His work was further generalized by Karchmer and Widgerson [14], as well as Beimel [2], using *monotone span programs*.

In 2019, Lopes de Souza introduced a secret sharing scheme based on linear feedback shift register sequences. The scheme uses linear feedback shift registers to construct an orthogonal array, which is then used to assign the shares to the participants. We present a variant of this scheme, called the projective plane secret sharing scheme.

We now give an overview of the structure of this work. In the remainder of Chapter 1 we present the necessary background as follows. In Section 1.2.1 we give an overview of finite fields. We then introduce orthogonal arrays and a method to construct them in Sections 1.2.2 and 1.2.3. Next, we present linear feedback shift register sequences in Section 1.2.4. Finally, we introduce graphs in Section 1.2.5.

In Chapter 2 we present the definition of a secret sharing scheme, as well as the necessary background. We also provide some examples of secret sharing schemes, including three different constructions of the (t, n)-threshold secret sharing scheme and Brickell's construction

of the vector space secret sharing scheme.

In Chapter 3 we give the definitions of matroids, along with some of the connections between matroids and secret sharing schemes. This connection is further explored in Chapter 4 specifically considering rank-3 secret sharing schemes.

In Chapters 5 and 6 we present a proposal for the projective plane secret sharing scheme, an expansion of the scheme from Lopes de Souza. In Chapter 5 we prove that the scheme is perfect, as well as give some examples of the scheme in use. We also prove that the scheme is equivalent to the vector space secret sharing scheme. In Chapter 6 we compare two different methods that can be used to find realizations for the scheme given a finite field $\mathbb{F}_q$, both using hypergraphs. Additionally, in Chapter 6, we give some sufficient conditions for non-existence of a realization for a given access structure and finite field $\mathbb{F}_q$.

1.2 Background

1.2.1 Finite Fields

We begin by giving a short introduction to finite fields based on the book of Lidl and Niederreiter [16]. Finite fields play an important role in secret sharing, often being used as the secret set. We begin by defining groups and rings.

A *group* $(G, \circ)$ is a set G along with a binary operation $\circ$ such that the following properties hold:

1. For any $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$.
2. There is an element $e \in G$, called the identity element, such that for all $a \in G$, $a \circ e = e \circ a = a$.
3. For each $a \in G$, there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

A group is called *abelian* if for all $a, b \in G$, $a \circ b = b \circ a$. We say that a group G with n elements is *cyclic* if there exists an element $g \in G$ such that $\{g^0, g^1, \ldots, g^{n-1}\} = G$. We call this element g a *generator* of the group G. A *ring* $(R, +, \cdot)$ is a set R along with two binary operations $+$ and $\cdot$ such that the following properties hold:

1. R is an abelian group with respect to $+$.
2. For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

If $\cdot$ is commutative and R has an identity element under $\cdot$, then we call R a *commutative ring with identity*. If R is a commutative ring with identity and for all $a, b \in R$ such that $a \cdot b = 0$, either $a = 0$ or $b = 0$, then R is called an *integral domain*. A ring $(R, +, \cdot)$ is called a field if

$(R^\star, \cdot)$, where $R^\star$ is the set R with the additive identity removed, is an abelian group. We call a subset of a ring R or field F that is itself a ring or field under the same operations a *subring* or a *subfield*.

The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all rings, while only $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. Additionally, $\mathbb{Z}_n$ is a field if and only if n is prime [16, Theorem 1.38]. If R is a ring such that there exists a positive integer n with $n \cdot 1 = 0$, where 1 is the mutliplicative identity, then we call the smallest such n the *(positive) characteristic* of R. If R has no positive characteristic then we say it has *characteristic zero*. If the positive integer n is prime, then we say R has *prime characteristic*. A finite field is a field F with a finite number of elements q, called the order. A finite field with q elements is written as $\mathbb{F}_q$. All finite fields have a prime characteristic [16, Corollary 1.45]. We denote the fields constructed from $\mathbb{Z}_p$ as $\mathbb{F}_p$, where p is a prime.

We say that two rings (fields) R and S are isomorphic if there exists a bijection $\phi : R \to S$ that preserves the structure of both of the operations. Specifically, two rings R and S are isomorphic if there exists a bijection $\phi : R \to S$ such that:

1. For all $a, b \in R$, $\phi(a + b) = \phi(a) + \phi(b)$.
2. For all $a, b \in R$, $\phi(ab) = \phi(a)\phi(b)$.
3. If $1_R, 1_S$ are the identity elements under multiplication of R and S, then $\phi(1_R) = 1_S$.

Using a ring R we can construct a new ring by constructing all polynomials with coefficients in R using the $+$ and $\cdot$ operations over R. This ring is called the *polynomial ring*, and is denoted by $R[x]$. For a nonzero polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$ over a ring R with $a_n \neq 0$, we call a_n the *leading coefficient*, a_0 the *independent* or *constant* term, and n the *degree* of f, denoted $\deg(f)$. If a_n is one, then we call $f(x)$ a *monic polynomial*. By convention, we say that the zero polynomial has degree $-\infty$. A *constant polynomial* is a polynomial with degree less than or equal to 0. When we identify the constant polynomials with elements of R then we find R as a subring of $R[x]$. If F is a field, then we call a polynomial f in $F[x]$ *irreducible* over F if the degree of f is positive and if $f = pq$ with $p, q \in F[x]$, then either p or q is a constant polynomial. If $f \in \mathbb{F}_q[x]$, where q is a prime or prime power, and $\deg(f) = m \geq 0$, then $\mathbb{F}_q[x]/(f)$ consists of all polynomials with degree less than m, and has q^m elements. Theorem 1.2.1 tells us when $\mathbb{F}_q[x]/(f)$ is a field.

Theorem 1.2.1 ([16], Theorem 1.61)**.** For a polynomial $f \in F[x]$ over a field F, the ring of polynomials over F modulo f, denoted by $F[x]/(f)$, is a field if and only if f is irreducible over F.

Let K be a field. We have already defined what it means for a set $F \subseteq K$ to be a subfield of K. Namely, when F is itself a field under the same operations as K. In this case we call K an *extension field* or *extension* of F. We call a field that contains no proper subfields a *prime field*. Any finite field of order p, where p is a prime, is a prime field. We call the subfield constructed by taking the intersection of all subfields of F the *prime subfield* of F. The prime subfield of a field is a prime field. If a field K is an extension field of a field F, then we can view K as a vector space over F. The dimension of this vector space

is called the *degree* of K over F and is written as $[K : F]$. If the field K is considered as a vector space over F and is finite-dimensional, then we say K is a *finite extension* of F.

Theorem 1.2.2 ([16], Theorem 1.84)**.** If L is a finite extension of K and M is a finite extension of L, then M is a finite extension of K with

$$[M : K] = [M : L][L : K].$$

Let F and K be fields where F is an extension of K. Then F is a *splitting field* of the polynomial $f \in K[x]$ if f can be written as a product of linear factors in $F[x]$ and if f cannot be written as a product of linear factors in any other subfield of F containing K. The following results are required to show the existence and uniqueness of a finite field with $q = p^n$ elements for every prime p and integer n. We begin with a result that says that finite fields must have prime characteristic.

Theorem 1.2.3 ([16], Theorem 2.2)**.** Let F be a finite field. Then $q = p^n$ where the prime p is the characteristic of F and n is the degree of F over its prime subfield.

Lemma 1.2.4 ([16], Lemma 2.3)**.** If $\mathbb{F}_q$ is a finite field with q elements, then for every $a \in \mathbb{F}_q$, $a^q = a$.

Lemma 1.2.5 ([16], Lemma 2.4)**.** If $\mathbb{F}_q$ is a finite field with q elements and characteristic p, then the polynomial $x^q - x$ factors in $\mathbb{F}_q[x]$ as

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

Additionally, $\mathbb{F}_q$ is a splitting field of $x^q - x$ over $\mathbb{F}_p$.

Combining these results we get the following theorem on the existence and uniqueness of finite fields.

Theorem 1.2.6 ([16], Theorem 2.5)**.** For every prime p and every positive integer n there exists a finite field with p^n elements. Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over $\mathbb{F}_p$.

The uniqueness in this theorem allows us to speak about *the* finite field with q elements. Furthermore, this gives us the following result about subfields of finite fields.

Theorem 1.2.7 ([16], Theorem 2.6)**.** Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Additionally, for every m that is a positive divisor of n, there exists exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Furthermore, the subfield of $\mathbb{F}_{p^n}$ of order p^m, where $m|n$, consists precisely of the roots of $x^{p^m} - x \in \mathbb{F}_p[x]$ in $\mathbb{F}_{p^n}$. The next result is a useful property of the multiplicative groups of finite fields.

Theorem 1.2.8 ([16], Theorem 2.8)**.** The multiplicative group of a finite field $\mathbb{F}_q$, $(\mathbb{F}_q^\star, \cdot)$, is cyclic.

Since these groups are cyclic, we know that they have generators. A generator of the cyclic group $(\mathbb{F}_q^\star, \cdot)$ is called a *primitive* element of $\mathbb{F}_q$. These primitive elements can be used to show that for any finite field $\mathbb{F}_q$ and any positive integer n, there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.

We now introduce a class of irreducible polynomials that is important to us, called the primitive polynomials. Let $\mathbb{F}_q$ be a finite field with characteristic p. We call a polynomial $f \in \mathbb{F}_q[x]$ of degree m *primitive* if it is irreducible and has a primitive element α as a root [13]. Additionally, we can characterize primitive polynomials as the irreducible polynomials $f \in \mathbb{F}_q[x]$ of degree m with the property that $n = q^m - 1$ is the smallest positive integer n such that $f(x)|x^n - 1$.

It is easy for us to represent finite fields with a prime number of elements as we just use $\mathbb{Z}_p$. A more interesting problem is representing fields with a number of elements that is not prime, but is a power of a prime $q = p^m$. There are many ways we can do this, but the main method we will use to represent fields of this form uses root adjunction of irreducible polynomials. To do this we start by picking an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree m. We find a root α of the polynomial f. The elements in $\mathbb{F}_q$ can then be uniquely represented as a polynomial over α in $\mathbb{F}_p$ of degree less than m. For example, suppose we wish to represent $\mathbb{F}_8$ in this way. Then we begin by finding an irreducible polynomial of degree 3 over $\mathbb{F}_2$. One such polynomial is $f(x) = x^3 + x + 1$. Let α be a root of f so that $\alpha^3 + \alpha + 1 = 0$. The eight elements of $\mathbb{F}_8$ are then of the form $a_0 + a_1\alpha + a_2\alpha^2$, where a_0, a_1 and a_2 are elements of $\mathbb{F}_2$. The elements are

$$\{0, 1, \alpha, 1 + \alpha, \alpha^2, 1 + \alpha^2, \alpha + \alpha^2, 1 + \alpha + \alpha^2\}.$$

The operations in the field can then be done using the fact that $\alpha^3 = \alpha + 1$, effectively changing our residue classes from using x to using α in $\mathbb{F}_p[x]/(f)$. Using this method of representing finite fields we can write the elements of a field $\mathbb{F}_{q^m}$ as vectors in $\mathbb{F}_q^m$, where the elements of the vectors represent the coefficients of the polynomials.

1.2.2 Orthogonal Arrays

Next, we define orthogonal arrays, a useful combinatorial design. The following definition comes from Stinson [26].

Definition 1.2.9 (Orthogonal Array, [26])**.** Let t, v, k and λ be positive integers such that $k \geq t \geq 2$. A $\mathrm{OA}_\lambda(N; t, k, v)$ orthogonal array is a pair (X, D) such that the following 3 properties are satisfied:

1. X is a set of v elements called *points*.
2. D is a $N \times k$ array with entries from X, where $N = \lambda v^t$.
3. In any subarray defined by t columns of D, every t-tuple appears exactly λ times as a row.

We call N the size of the array, t the strength of the array, and λ the index. Sometimes when orthogonal arrays have index λ equal to one we drop the subscript, writing $\mathrm{OA}(N; t, k, v)$. We say that an orthogonal array (X, D) is *linear* if $X = \mathbb{F}_q$ for some prime power q and the rows of D form a subspace of the vector space $\mathbb{F}_q^k$. The following theorem from Stinson [26] allows us to construct orthogonal arrays for many different parameters.

Theorem 1.2.10 ([26], Theorem 10.4)**.** Let ℓ and k be positive integers, and let q be a prime power. Let M be an ℓ by k matrix of elements from $\mathbb{F}_q$ such that every set of t columns of M is linearly independent. Define D to be the q^ℓ by k matrix whose rows consist of all the linear combinations of the rows of M. Then $(\mathbb{F}_q, D)$ is an $\mathrm{OA}_{q^{\ell-t}}(q^\ell; t, k, q)$.

A problem that is of interest to us is the problem of finding the largest k such that an $\mathrm{OA}(N; t, k, v)$ exists for fixed values N, t, and v. We denote this maximum by $f(N, v, t)$. The following result from Hedayat, Sloane, and Stufken [1] gives us values for $f(N, v, t)$ when we are constructing an orthogonal array over the elements of a finite field.

Theorem 1.2.11 ([1], Corollary 3.9)**.** Let v be a prime power. Then,

i) $f(v^3, v, 3) = v + 1$, if v is odd, and

ii) $f(v^3, v, 3) = v + 2$, if v is even.

1.2.3 Bush's Construction for Orthogonal Arrays

In 1952, Bush [10] showed that we can construct an $\mathrm{OA}(q^t; t, q + 1, q)$ for any prime power $q > t$. He presents this in the following theorem.

Theorem 1.2.12 ([10])**.** If $q = p^n$ where p is a prime and $q > t$, then we can construct an $\mathrm{OA}(q^t; t, q + 1, q)$.

The construction of the array goes as follows. Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. Consider the polynomials

$$f_i(x) = a_{i_0} + a_{i_1}x + \cdots + a_{i_{t-1}}x^{t-1}$$

where the coefficients range over $\mathbb{F}_q$. There will be q^t of these polynomials as each of the t coefficients has q possible values in the field. For each of the first q columns of the array, we associate to it a distinct element $\alpha \in \mathbb{F}_q$. The ith row of the array is then filled by putting the value $f_i(\alpha)$ in the column associated with α and $a_{i_{t-1}}$ in the final column. An example array constructed using this method is shown in Figure 1.1.

1.2.4 LFSR Sequences

We now introduce another way to construct orthogonal arrays using linear feedback shift register (LFSR) sequences. Let $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1x_1 + c_0$ be a monic polynomial

$f_i(x)$	0	1	2	a_{i_1}
$0+0x$	0	0	0	0
$0+1x$	0	1	2	1
$0+2x$	0	2	1	2
$1+0x$	1	1	1	0
$1+1x$	1	2	0	1
$1+2x$	1	0	2	2
$2+0x$	2	2	2	0
$2+1x$	2	0	1	1
$2+2x$	2	1	0	2

Figure 1.1: Orthogonal array from Bush construction with $q = 3$ and $t = 2$

of degree m in $\mathbb{F}_q[x]$. An LFSR sequence with characteristic polynomial f and initial values $I = (b_0, b_1, \ldots, b_{m-1}) \in \mathbb{F}_q^m$ that are not all zero is a sequence $S(f, I) = (a_0, a_1, a_2, \ldots)$ with elements in $\mathbb{F}_q$ defined by

$$a_i = \begin{cases} b_i, & \text{if } 0 \leq i < m \\ -c_{m-1}a_{i-1} - \cdots - c_0 a_{i-m}, & \text{if } i \geq m \end{cases}.$$

We say that a sequence is *periodic* if there exists a positive integer n such that $a_{n+i} = a_i$ for all $i \geq 0$. We call the smallest such n the *period* of the sequence. The period of an LFSR sequence with a characteristic polynomial of degree m over $\mathbb{F}_q$ divides $q^m - 1$ [16]. An LFSR sequence is an *m-sequence* if the period is $q^m - 1$. The m-sequences are those whose characteristic polynomials are primitive [13]. Let $S(f, I) = (a_i)$ be an LFSR sequence. For any positive integer n, we define $C_i^n(S(f, I)) = (a_i, a_{i+1}, \ldots, a_{i+n-1})$ as the *sub-interval* of $S(f, I)$ that starts at position i and has length n.

Theorem 1.2.13 ([13], Property 5.1)**.** Let f be a primitive polynomial of degree m over $\mathbb{F}_q$ and let $S(f, I)$ be an m-sequence with $I \neq (0, \ldots, 0)$. Then, each nonzero m-tuple of $\mathbb{F}_q^m$ appears exactly once per period as a sub-interval $C_i^m(S(f, I))$ of length m.

Proposition 1.2.14 ([23], Corollary 1)**.** Let f be a primitive polynomial of degree m over $\mathbb{F}_q$, and $I = (b_0, \ldots, b_{m-1})$ be the initial values of the m-sequence $S(f, I) = (a_i)$. Let $k = \frac{q^m-1}{q-1}$. Then $S(f, I)$ has the following properties:

1. For any $i \geq 0$, $C_i^k(S(f, I))$ contains exactly $\frac{q^{m-1}-1}{q-1}$ zeros.
2. For any $i, j \geq 0$, the zeros in $C_i^k(S(f, I))$ and $C_{i+jk}^k(S(f, I))$ appear in the same positions.

We now give two methods for constructing orthogonal arrays using m-sequences. Let q be a prime power and $f \in \mathbb{F}_q[x]$ be a primitive polynomial of degree m with a primitive root α. Let $S(f, I) = (a_i)$ be an m-sequence for initial values $I \neq (0, \ldots, 0)$. We define the

sub-interval array of f using the sub-intervals of $S(f, I)$ with length $k = \frac{q^m-1}{q-1}$ as follows:

$$M(f, I) := \begin{bmatrix} C_0^k(S(f, I)) \\ C_1^k(S(f, I)) \\ \vdots \\ C_{q^m-2}^k(S(f, I)) \\ 0 \dots 0 \end{bmatrix}.$$

The following proposition establishes that the result of this construction is an orthogonal array.

Proposition 1.2.15 ([21], Proposition 2)**.** Let f be a primitive polynomial of degree m over $\mathbb{F}_q$, where q is a prime power. Then $M(f)$ is an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$.

We now define another orthogonal array constructed from m-sequences using the tuple representation of the primitive root α and its powers in the finite field. Since $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$, we can write each power α^j, for $j = 0, \dots, \frac{q^m-1}{q-1} - 1$ as a linear combination of the basis $\{\alpha^0, \dots, \alpha^{m-1}\}$. In other words, we can represent each of these powers α^j as a vector $(c_0, \dots, c_{m-1})$ if $\alpha^j = \sum_{i=0}^{m-1} c_i \alpha^i$. We denote these vectors by $T(\alpha^j)$. We now construct an m by $\frac{q^m-1}{q-1}$ array G_f where its columns are each of the $T(\alpha^j)$:

$$G_f := \left[T(\alpha^0) \quad T(\alpha^1) \quad \dots \quad T(\alpha^{\frac{q^m-1}{q-1}-1}) \right].$$

This matrix G_f has rank m and no two columns are linearly dependent [25]. We refer to this matrix as the *generator matrix* with respect to the primitive polynomial f. We then construct an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$ by taking all linear combinations of the rows of G_f. This new array is denoted by $A(G_f)$. The fact that $A(G_f)$ is an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$ follows Theorem 1.2.10. In addition, we have the following theorem.

Theorem 1.2.16 ([25], Theorem 3.9)**.** The arrays $M(f, I)$ and $A(G_f)$ are identical up to row permutation.

We say that a set of s columns $\{c_{i_1}, \dots, c_{i_s}\}$ of one of these arrays is *covered* if each s-tuple over $\mathbb{F}_q$ appears at least once as a row. We call it uncovered otherwise. The following theorem connects sets of covered columns to linearly dependent sets.

Theorem 1.2.17 ([23], Theorem 2)**.** Let q be a prime power and let f be a primitive polynomial of degree $m \geq 3$ over $\mathbb{F}_q$ with primitive root α. Write $k = \frac{q^m-1}{q-1}$. Let $M(f, I) = [c_0, \dots, c_{k-1}]$ be the sub-interval array of f with initial values I. Then, the following are equivalent:

1. A set of s columns $\{c_{i_1}, \dots, c_{i_s}\}$ is uncovered in $M(f, I)$.
2. The set of vectors $\{T(\alpha^{i_1}), \dots, T(\alpha^{i_s})\}$ is linearly dependent over $\mathbb{F}_q$.

Furthermore, if $s = m$, the following statement is also equivalent to (1) and (2):

3. There is a row r, other than the row of all zeros, such that $r_{i_1} = \dots = r_{i_s} = 0$.

1.2.5 Graphs

We now give an introduction to some graph theory concepts; we follow Bondy and Murty [7]. A *graph* G is an ordered pair $(V(G), E(G))$ where $V(G)$ is a finite set of *vertices*, and $E(G)$ is a multiset of *edges*, where each edge is in $\{\{x, y\} : x, y \in V(G)\}$. If e is an edge of G such that $e = \{u, v\}$ for a pair of vertices u and v, then we say that e *joins* u and v. In this case, we say that u and v are *incident* with e and that u and v are *adjacent*. An edge that joins a vertex to itself is called a *loop*, and if two different edges join the same pair of vertices we call them *parallel*. The *degree* of a vertex v of G is the number of edges incident with v, counting loops twice. A graph with no loops or parallel edges is called *simple* and, in this case, $E(G)$ is a set of edges.

A simple graph G is *complete* if each pair of vertices of G is adjacent. The complete graph with n vertices is denoted by K_n. A graphical representation of the complete graph with 5 vertices is presented in Figure 1.2. If the vertex set of a graph G can be partitioned into two sets X and Y such that each edge has one end in X and the other in Y, then we call G *bipartite* and denote it by $G[X, Y]$. A path of length k is a simple graph with k vertices that can be ordered linearly such that two vertices are adjacent if and only if they are consecutive in the ordering. A cycle of length k is a simple graph with k vertices that can be ordered cyclically such that two vertices are adjacent if and only if they are consecutive in the ordering. A graph F is a *subgraph* of a graph G if $V(F) \subseteq V(G)$ and $E(F) \subseteq E(G)$. We denote that F is a subgraph of G by $F \subseteq G$. Let $V' \subseteq V(G)$. The *subgraph of G induced by V'*, denoted $G[V']$, has vertex set V' and edge set $\{e \in E(G) : e \subseteq V'\}$. We say that a subgraph F of G is *induced* if $F = G[V(F)]$.

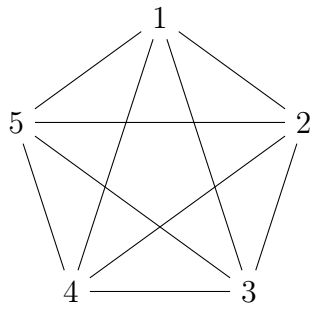


Figure 1.2: Diagram of the graph K_5

A graph G is *connected* if, for every partition of its vertex set into nonempty sets X and Y, there is at least one edge with one end in X and the other in Y. The graph is disconnected otherwise. Two graphs G and H are *disjoint* if they have no common vertex, and *edge-disjoint* if they have no common edge. The union of G and H is the graph $G \cup H$ with vertex set $V(G) \cup V(H)$ and edge set $E(G) \cup E(H)$. When G and H are disjoint we refer to $G \cup H$ as the *disjoint union* of G and H. Because this operation is both associative and commutative, we can extend it to an arbitrary number of graphs. Every graph G can be expressed as a disjoint union of connected graphs. These connected graphs are called the *connected components* of G.

Two simple graphs G and H are *isomorphic* if there exists a bijection φ from $V(G)$ to $V(H)$ which preserves adjacency, that is if $\{u, v\} \in E(G)$ then $\{\varphi(u), \varphi(v)\} \in E(H)$. Such a bijection is referred to as an *isomorphism* between G and H. The problem of verifying if two graphs G and H are isomorphic is referred to as the *graph isomorphism problem*. A related problem, the *subgraph isomorphism problem*, addresses the question of whether, given two graphs G and H, there exists a subgraph of H that is isomorphic to G. We can add a restriction to this problem that the subgraph of H is induced. This variant is called the *induced subgraph isomorphism problem*. There is no known algorithm that solves any of these problems in polynomial time, with the two variants of the subgraph isomorphism problem being known to be NP-complete [11].

A partition of a finite set V is a set of nonempty subsets of V, $\{V_1, \ldots, V_n\}$, such that each element of V is in exactly one of $V_1, \ldots, V_n$. An *ordered partition* is a tuple $\pi = (V_1, \ldots, V_m)$, where $\{V_1, \ldots, V_m\}$ is a partition of a finite set V [15]. When V is the vertex set of a graph, we refer to the sets $V_1, \ldots, V_m$ as the *colour classes* of π. For a vertex v in a graph G, we write $\pi(v)$ for the index of the colour class in which v appears. For this reason, we identify the ordered partition π with the function of $V(G)$ onto $\{1, \ldots, m\}$ defined by $x \to \pi(x)$. A *coloured graph* is a pair (G, π), where G is a graph and π is an ordered partition of $V(G)$. A coloured graph (G, π) is isomorphic to a coloured graph (H, σ) if there exists an isomorphism φ of G onto H such that $\pi(v) = \sigma(\varphi(v))$ for all $v \in V(G)$.

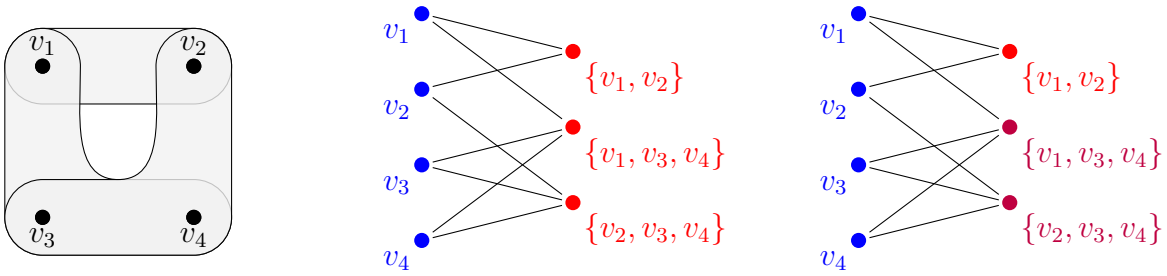
A *hypergraph* $\mathcal{H}$ is a pair of finite sets $(V(\mathcal{H}), E(\mathcal{H}))$, where $V(\mathcal{H})$ is a set of vertices and $E(\mathcal{H})$ is a set of *hyperedges*, where each hyperedge is a set of vertices. We say that two hypergraphs $\mathcal{G}$ and $\mathcal{H}$ are isomorphic if there exists a bijection φ from $V(\mathcal{G})$ to $V(\mathcal{H})$ such that $\{v_1, \ldots, v_\ell\}$ is a hyperedge of $\mathcal{G}$ if and only if $\{\varphi(v_1), \ldots, \varphi(v_\ell)\}$ is a hyperedge of $\mathcal{H}$. We say that a hypergraph $\mathcal{F}$ is a *subhypergraph* of a hypergraph $\mathcal{H}$ if $V(\mathcal{F}) \subseteq V(\mathcal{H})$ and $E(\mathcal{F}) \subseteq E(\mathcal{H})$. Furthermore, we say that a subhypergraph $\mathcal{F}$ of $\mathcal{H}$ is *induced* if $\mathcal{F}$ contains all hyperedges of $\mathcal{H}$ over $V(\mathcal{F})$. The *rank* of a hypergraph $\mathcal{H}$, denoted $r(\mathcal{H})$, is the cardinality of the largest hyperedge in $E(\mathcal{H})$. In other words, $r(H) = \max\{|e| : e \in E(\mathcal{H})\}$.

Let $\mathcal{H}$ be a hypergraph. The *incidence graph* of $\mathcal{H}$, denoted by $\mathrm{IG}(\mathcal{H})$, is a bipartite graph $G[V_1, V_2]$, where $V_1 = V(\mathcal{H})$ and $V_2 = E(\mathcal{H})$ such that for each $v \in V_1$ and $e \in V_2$, $\{v, e\} \in E(G)$ if and only if $v \in e$. The *coloured incidence graph* of $\mathcal{H}$, denoted $\mathrm{IG}^c(\mathcal{H})$, is the coloured graph $(\mathrm{IG}(\mathcal{H}), \pi)$ with $\pi = (V_1, V_2)$. The *size-coloured incidence graph* of $\mathcal{H}$, denoted $\mathrm{IG}^s(\mathcal{H})$, is the coloured graph $(\mathrm{IG}(\mathcal{H}), \pi^+)$ with $\pi^+ = (V_1, V_2^1, \ldots, V_2^n)$ where $V_2^i = \{e \in E(\mathcal{H}) : |e| = i\}$, $1 \leq i \leq n$. An example of a hypergraph $\mathcal{H}$, along with its coloured and size-coloured incidence graphs, is presented in Figure 1.3.

We show in Proposition 1.2.18 that two hypergraphs are isomorphic if and only if their coloured incidence graphs are.

Proposition 1.2.18. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be hypergraphs. Then, $\mathcal{H}_1$ is isomorphic to $\mathcal{H}_2$ if and only if $\mathrm{IG}^c(\mathcal{H}_1)$ is isomorphic to $\mathrm{IG}^c(\mathcal{H}_2)$.

Proof. Suppose $\mathcal{H}_1 = (V_1, E_1)$ and $\mathcal{H}_2 = (V_2, E_2)$ are hypergraphs with coloured incidence graphs $\mathrm{IG}^c(\mathcal{H}_1) = (\mathrm{IG}(\mathcal{H}_1), \pi_1)$ and $\mathrm{IG}^c(\mathcal{H}_2) = (\mathrm{IG}(\mathcal{H}_2), \pi_2)$, where the colourings are $\pi_1 = (V_1, E_1)$ and $\pi_2 = (V_2, E_2)$.



(a) Hypergraph $\mathcal{H}$

(b) $\mathrm{IG}^c(\mathcal{H})$

(c) $\mathrm{IG}^s(\mathcal{H})$

Figure 1.3: Hypergraph $\mathcal{H}$ with its coloured and size-coloured incidence graphs

($\implies$) Suppose $\varphi : V_1 \to V_2$ is an isomorphism from $\mathcal{H}_1$ to $\mathcal{H}_2$. Then, $\{v_1, \ldots, v_\ell\} \in E_1$ if and only if $\{\varphi(v_1), \ldots, \varphi(v_\ell)\} \in E_2$. Define a $\psi : V_1 \cup E_1 \to V_2 \cup E_2$ such that

$$\begin{cases} \psi(v) = \varphi(v), & v \in V_1 \\ \psi(\{v_1, \ldots, v_\ell\}) = \{\varphi(v_1), \ldots, \varphi(v_\ell)\}, & \{v_1, \ldots, v_\ell\} \in E_1. \end{cases}$$

Since $\{v, e\} \in E(\mathrm{IG}^c(\mathcal{H}_1))$ if and only if $v \in e$, we have that $\psi(v) \in \psi(e)$. So $\{v, e\} \in E(\mathrm{IG}(\mathcal{H}_1))$ if and only if $\{\psi(v), \psi(e)\} \in \mathrm{IG}(\mathcal{H}_2)$, and therefore $\mathrm{IG}(\mathcal{H}_1)$ is isomorphic to $\mathrm{IG}(\mathcal{H}_2)$, and it remains to show that ψ preserves colours. By construction we will have that for any $v \in V_1$, $\pi_1(v) = 1 = \pi_2(\psi(v))$, and for any $e \in E_1$, $\pi_1(e) = 2 = \pi_2(\psi(e))$. So ψ preserves colours, and therefore is an isomorphism between the coloured incidence graphs $\mathrm{IG}^c(\mathcal{H}_1)$ and $\mathrm{IG}^c(\mathcal{H}_2)$.

($\impliedby$) Let $\psi : V_1 \cup E_1 \to V_2 \cup E_2$ be an isomorphism between $\mathrm{IG}^c(\mathcal{H}_1)$ and $\mathrm{IG}^c(\mathcal{H}_2)$. Then, since ψ is an isomorphism of coloured graphs, we have that it maps vertices in V_1 to vertices in V_2 and hyperedges in E_1 to hyperedges in E_2. We claim $\psi|_{V_1}$ is an isomorphism from $\mathcal{H}_1$ to $\mathcal{H}_2$. Since ψ is an isomorphism, we have that

$$\{v, e\} \in E(\mathrm{IG}^c(\mathcal{H}_1)) \iff \{\psi(v), \psi(e)\} \in E(\mathrm{IG}^c(\mathcal{H}_2)).$$

From this we conclude that

$$v \in e \iff \psi(v) \in \psi(e),$$

and so, $\{v_1, \ldots, v_\ell\} \in E_1$ if and only if $\psi(\{v_1, \ldots, v_\ell\}) = \{\psi(v_1), \ldots, \psi(v_\ell)\} \in E_2$. This is the condition required for $\psi|_{V_1}$ to be an isomorphism from $\mathcal{H}_1$ to $\mathcal{H}_2$. ∎

A problem that will be of interest to us is the *subhypergraph isomorphism problem*. Similar to the subgraph isomorphism problem, the subhypergraph isomorphism problem addresses the question of whether a hypergraph $\mathcal{G}$ is isomorphic to a subhypergraph of a hypergraph $\mathcal{H}$. Additionally, we can define the analogue of the induced subgraph isomorphism problem for hypergraphs, the *induced subhypergraph isomorphism problem*. Given two hypergraphs $\mathcal{H}$ and $\mathcal{G}$, the induced subhypergraph isomorphism problem is the problem of finding if there exists an induced subhypergraph of $\mathcal{G}$ that is isomorphic to $\mathcal{H}$. We explore these concepts further in Section 6.2.

Chapter 2

Secret Sharing Schemes

A secret sharing scheme is a method by which a dealer distributes a secret among a group of participants. Each of these participants receives a share which can be used in conjunction with some number of other shares to recover the secret if the set of participants involved is authorized. These schemes play an important role in cryptography, being used as a building block in many applications such as electronic voting, distributed key agreements, and multi-party computation.

2.1 Definitions

In a secret sharing scheme there is a set of participants P, and the power set of P, 2^P, is partitioned into authorized and unauthorized subsets. The set of authorized participants is called the *access structure*. An authorized group of participants should be able to reconstruct the secret, whereas an unauthorized group should not be able to discover any partial information about the secret. We usually denote by $\Gamma \subseteq 2^P$ the set of all authorized sets.

Traditionally, secret sharing schemes use someone called the *dealer* who is a trusted third party that will facilitate the process by receiving the secret, generating shares, and sending the shares to the participants. When a group of participants wants to attempt to reconstruct the secret they send their shares to an entity (possibly the dealer) called the *combiner*. The combiner receives the shares, reconstructs the secret, then shares the secret with the participants if the group is authorized.

In general, for a secret sharing scheme to be used we require the following 2 properties to be satisfied:

- **Correctness:** An authorized group of participants will always be able to reconstruct the secret.
- **Perfect Privacy:** An unauthorized group of participants cannot learn any information about the secret using their shares.

We call a scheme satisfying these properties *perfect*. Additionally, a secret sharing scheme is called *ideal* if each of the shares has the same size as the secret (measured in bits). For instance, if the secret is chosen from a finite field $\mathbb{F}_q$, an ideal scheme requires that each share is also an element of $\mathbb{F}_q$, ensuring that the share size matches the secret size. Beimel shows that this is actually the smallest possible size that the shares can have [3, Lemma 2]. Not all secret sharing schemes are ideal. Ideal schemes are very important, as in any practical implementation of a secret sharing scheme we will want to keep the sizes of shares as small as possible.

A survey from 2011 by Beimel [3] defines secret sharing schemes using distribution schemes and probabilities. A *distribution scheme* is a pair $\Sigma = \langle \Pi, \mu \rangle$ with a domain of secrets K, where μ is a probability distribution on a finite set of random strings R and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where each K_j is the domain of shares for participant p_j. A dealer then distributes a secret $k \in K$ using Σ by sampling a random string $r \in R$ according to μ, then computing $\Pi(k, r) = (s_1, \ldots, s_n)$, the vector of shares, and communicating each of the shares s_j to the participant p_j. We denote by $\Pi(s, r)_A$ the restriction of $\Pi(s, r)$ to the participants in some subset A.

Definition 2.1.1 (Secret Sharing Schemes, [3])**.** Let K be a finite set of secrets, where $|K| \geq 2$. A distribution scheme $\langle \Pi, \mu \rangle$ with domain of secrets K is a *perfect secret sharing scheme* realizing an access structure Γ if it satisfies the correctness and perfect privacy conditions. In secret sharing schemes μ is usually the uniform distribution.

We can view each of these distribution rules as an $(n+1)$-tuple $(k, s_1, \ldots, s_n)$, where k is the secret and s_i is the share of participant i for $i = 1, \ldots, n$. We can then view the distribution scheme as a matrix A containing each of these $(n+1)$-tuples as the rows. To share the secret k we pick a row of A with first entry k uniformly at random and give each participant their corresponding share in the rule. An example of a distribution scheme for a secret sharing scheme realizing the access structure $\Gamma = \{A \subseteq \{p_1, p_2, p_3\} : |A| \geq 2\}$ with four possible secrets is presented in Figure 2.1. The column labeled k corresponds to the value of the secret, and the columns labeled s_1, s_2, and s_3 correspond to the shares of the participants p_1, p_2, and p_3 respectively. In this distribution scheme there are four choices of row for each choice of secret k, therefore, $R = \{r_1, r_2, r_3, r_4\}$ and we have four choices of random strings. This choice is represented in the table in the column R. The mapping Π takes the choice of secret k and row r_i and returns the tuple (s_1, s_2, s_3) in the row corresponding to k labeled by r_i.

Furthermore, when we use distribution schemes to define secret sharing schemes, we can define the correctness and perfect privacy conditions using the probabilities given by the distribution scheme:

- **Correctness:** For any set $B = \{p_{i_1}, \ldots, p_{i_\ell}\} \in \Gamma$ there exists a reconstruction function $\text{RECON}_B : K_{i_1} \times \cdots \times K_{i_\ell} \to K$ such that for every $k \in K$,

$$\Pr[\text{RECON}_B(\Pi(k, r)_B) = k] = 1.$$

R	k	s_1	s_2	s_3
r_1	0	0	0	0
r_2	0	1	2	3
r_3	0	2	3	1
r_4	0	3	1	2
r_1	1	0	3	2
r_2	1	1	1	1
r_3	1	2	0	3
r_4	1	3	2	0

R	k	s_1	s_2	s_3
r_1	2	0	1	3
r_2	2	1	3	0
r_3	2	2	2	2
r_4	2	3	0	1
r_1	3	0	2	1
r_2	3	1	0	2
r_3	3	2	1	0
r_4	3	3	3	3

Figure 2.1: Distribution scheme for a scheme with 4 secrets

- **Perfect Privacy:** For any set $A \notin \Gamma$, any two possible secrets $k_1, k_2 \in K$, and every possible vector of shares $\langle s_j \rangle_{p_j \in A}$:

$$\Pr[\Pi(k_1, r) = \langle s_j \rangle_{p_j \in A}] = \Pr[\Pi(k_2, r) = \langle s_j \rangle_{p_j \in A}].$$

While Beimel's definition requires the scheme to be perfect, it is possible to create secret sharing schemes that do not require the correctness or perfect privacy conditions. Schemes that do not require probability 1 in the correctness condition or do not require that each of the possible secrets have the same probability distributions in the perfect privacy condition are called *statistical secret sharing schemes*, a version of statistical secret sharing using linear block codes is explored in [5].

The *information ratio* of a distribution scheme is

$$\rho = \frac{\max_{1 \leq j \leq n} \log |K_j|}{\log |K|}.$$

Sometimes the reciprocal of ρ is used, this is referred to as the *information rate* of a distribution scheme. These ratios represent the difference in number of bits between the representation of the shares and the secret. A secret sharing scheme is ideal if its information ratio is 1. All of the schemes that we will consider will be perfect, ideal, and linear.

Definition 2.1.2 (Linear Secret Sharing Schemes)**.** Let q be a prime power. A secret sharing scheme is *linear* over a finite field $\mathbb{F}_q$ if the secret is an element of $\mathbb{F}_q$, the random string is a vector over $\mathbb{F}_q$ with each coordinate chosen independently with uniform distribution, and the secret is reconstructed as a linear combination of the shares.

Linear schemes are of note because the computations done to decide the shares and to reconstruct the secret all use linear maps, and are therefore very efficient.

Some of the earliest constructions for secret sharing schemes are the (t, n)-threshold scheme introduced by Shamir [24] and Blakley [6] and the vector space scheme introduced by Brickell [8]. Both of these schemes are perfect, ideal, and linear. Descriptions of these schemes are given in Sections 2.3 and 2.4. A survey by Beimel [3] covers some of the other standard constructions of secret sharing schemes.

One of the smallest access structures that is not realizable by any ideal secret sharing scheme, originally found by Benaloh and Leichter in 1990 [4], has 4 participants and can be represented as a path of length 3. In this example, each of the minimally authorized sets has size two. The vertices represent the participants, labeled a, b, c, d, and each edge represents a minimally authorized set. This graphical representation is given in Figure 2.2. It is shown in [4] that this scheme has an information ratio of at least $\frac{3}{2}$. This structure will be further explored in Chapter 4.

a — b — c — d

Figure 2.2: An access structure that does not admit an ideal secret sharing scheme

Benaloh and Leichter [4] also proposed a general perfect secret sharing scheme for any access structure using monotone formulas. The general scheme is not ideal, so the question of whether a given structure can be realized is usually the question of whether it can be realized by an ideal secret sharing scheme.

2.2 Access Structures

Let $P = \{p_1, \ldots, p_n\}$ be a set of participants. An *access structure* Γ is a collection of non-empty subsets of P, such that a group of participants is authorized if it is in Γ, and unauthorized otherwise. We use access structures to define the authorized and unauthorized sets of secret sharing schemes. Most access structures are *monotone*, meaning that if a set A is authorized then any superset of A is also authorized. Precisely, an access structure Γ is monotone if $A \in \Gamma$ implies $B \in \Gamma$ for all $B \supseteq A$. A monotone access structure is determined by its minimally authorized sets, the smallest sets which are authorized, sometimes referred to as the basis of the access structure. We denote the minimally authorized sets of an access structure Γ by $\min \Gamma$. Similarly, a monotone access structure is determined by its maximal unauthorized sets. All the access structures we consider will be monotone, so we will drop the monotone prefix. When writing the authorized sets in an access structure we sometimes drop the set notation and write $\{a, b, c\}$ as abc when it is clear.

As we are assuming that we wish to share a secret the access structure will not be empty and does not contain every possible group of participants. Additionally, any participant that is authorized on their own can simply be given the secret, so we assume that our access structures contain no singletons. It is possible that there are two participants in an access structure that are indistinguishable. We call two such participants p_1 and p_2 equivalent in an access structure Γ if

1. There is no minimally authorized subset $A \in \min \Gamma$ with $p_1, p_2 \in A$
2. If $B \subseteq P$ and $p_1, p_2 \notin B$, then $B \cup \{p_1\} \in \min \Gamma$ if and only if $B \cup \{p_2\} \in \min \Gamma$.

In practice we combine equivalent participants in a realization of an access structure and give them the same share, so access structures containing equivalent participants are not

considered by us. A participant is called *redundant* if they appear in no minimally authorized sets. Therefore, adding a redundant participant to an unauthorized set will never make it authorized, so we can ignore redundant participants when realizing access structures. A participant is called a *dictator* if every authorized set contains them. We can also ignore dictators when realizing access structures. Suppose d is a dictator in an access structure Γ. We construct a new secret sharing scheme with two participants such that both are required to reconstruct the secret ($(2,2)$-threshold scheme, defined in Section 2.3). In this scheme one of the participants is the dictator d and the other is the group of remaining participants. The dictator is given their share by the dealer, while the remaining participants have their share distributed to them using the original secret sharing scheme but using the access structure $\Gamma\backslash\{d\}$, where the authorized sets of $\Gamma\backslash\{d\}$ are the sets that were authorized in Γ with d removed. Then, any set that would have been authorized in Γ with d included reconstructs their share in the new scheme, which then can be combined with the share of d to reconstruct the secret. Although this method allows us to remove dictators from access structures, it also increases the size of shares required to realize the access structure. For this reason we will often not want to remove dictators to allow the structure to be realized by an ideal secret sharing scheme.

Let Γ be an access structure with participants $P = \{p_1, \ldots, p_n\}$. A *substructure* Γ' of Γ is formed by taking a nonempty subset S of P as its participant set, with minimally authorized sets being the minimally authorized sets of Γ that only include participants in S. Sometimes we denote a substructure by $\Gamma(S)$. We give an example of an access structure along with one of its substructures in Figure 2.3. We use hypergraphs to represent the structure, where a minimally authorized set of size two is represented by an edge connecting the participants, and a minimally authorized set of size three is represented by a hyperedge containing all three participants.

(a) Γ (b) $\Gamma(\{p_1, p_2, p_4, p_5\})$

Figure 2.3: Access structure Γ on participants p_1, p_2, p_3, p_4, p_5, along with $\Gamma(\{p_1, p_2, p_4, p_5\})$

We say that an access structure Γ is *connected* if each participant appears in at least one minimally authorized subset. We note that these connected access structures are the ones that have no redundant participants, as the redundant participants are precisely the participants that would break this condition. The *rank* of an access structure is the size of its largest minimally authorized subset. If Γ_1 and Γ_2 are connected access structures on P_1 and P_2 respectively with $P_1 \cap P_2 = \emptyset$ then we call $\Gamma = \Gamma_1 \sqcup \Gamma_2$ the *disjoint union* of Γ_1 and Γ_2. The minimally authorized subsets of Γ will be $\min(\Gamma_1 \sqcup \Gamma_2) = \min \Gamma_1 \cup \min \Gamma_2$. An access structure Γ is called *strongly connected* if it cannot be decomposed into a disjoint union of

smaller substructures. An access structure is *reduced* if it is strongly connected and contains no equivalent participants. We will mainly be considering reduced access structures.

We present an example of a rank-2 access structure Γ with six participants labeled $\{A, B, C, D, E, F\}$. The minimally authorized sets in this structure are

$$\min \Gamma = \{AB, BC, AC, DE, EF\}.$$

This access structure is connected, but not strongly connected. It is the disjoint union of the structures Γ_1 and Γ_2 where $\min \Gamma_1 = \{AB, BC, AC\}$ and $\min \Gamma_2 = \{DE, EF\}$. It also has two equivalent participants D and F. A graphical representation of the minimally authorized sets of this access structure is presented in Figure 2.4.

Figure 2.4: Access structure with minimally authorized sets
$\min \Gamma = \{AB, BC, AC, DE, EF\}$

The following theorem from Stinson [27] gives us a sufficient condition for when there is no ideal scheme that realizes a rank-2 access structure.

Theorem 2.2.1 ([27], Theorem 13.11)**.** Suppose G is a connected graph that is not complete multipartite. Let $\Gamma(G)$ be the access structure with its minimal authorized sets being the edge set of G. Then any secret sharing scheme realizing $\Gamma(G)$ has information rate $\rho \geq \frac{3}{2}$.

Note that $(2, n)$-threshold access structures, explored in the next section, can be represented as a complete multipartite graph with each part containing one vertex, and it turns out that there are ideal schemes that can realize these access structures. A similar result that is relevant to us from Martí-Farré and Padró [18] that pertains to rank-3 access structures and their $(2, n)$-threshold substructures is presented in Chapter 4.

2.3 Threshold Schemes

One of the most well-known secret sharing schemes is a (t, n)-threshold secret sharing scheme. It was originally presented by Shamir [24] and Blakley [6], both in 1979. In this scheme there is a set of n participants where any subset containing at least t of them is authorized. More precisely a (t, n)-threshold scheme has $\Gamma = \{A \subseteq P : |A| \geq t\}$ as its access structure. Shamir's scheme uses polynomial interpolation over finite fields, Blakley's uses the geometry of hyperplanes. We additionally present a variant of threshold secret sharing which uses orthogonal arrays. The schemes of Shamir and Blakley are always linear. The orthogonal array scheme is sometimes linear depending on the orthogonal array being used. The distribution scheme given in Figure 2.1 realizes the $(2, 3)$-threshold access structure.

2.3.1 Shamir's Threshold Scheme

Given integers $1 \leq t \leq n$, Shamir's scheme considers a finite field $\mathbb{F}_q$ with $q > n$. Suppose we wish to share a secret $k \in \mathbb{F}_q$ using a (t, n)-threshold scheme. The dealer begins by choosing $t-1$ random elements $a_1, \ldots, a_{t-1}$ from $\mathbb{F}_q$ independently with uniform distribution. These random elements along with the secret are the coefficients of a polynomial $F(x) = k + \sum_{i=1}^{t-1} a_i x^i$ of degree $t-1$. The share for participant j is then the pair $(\alpha_j, F(\alpha_j))$, where α_j is a unique non-zero element of $\mathbb{F}_q$. All of these α_j can be posted publicly, with the $F(\alpha_j)$ kept secret. Then, a group of t or more participants can get together and reconstruct the polynomial F using Lagrange interpolation.

Theorem 2.3.1 (Lagrange Interpolation)**.** In every field $\mathbb{F}$, for every t distinct values $x_1, \ldots, x_t$, and for every t values $y_1, \ldots, y_t$, there exists a unique polynomial G of degree at most $t-1$ over $\mathbb{F}$ such that $G(x_j) = y_j$ for $1 \leq j \leq t$.

To see that a group of authorized participants can reconstruct the secret, we first note that any set of shares A of size t or more holds at least t points on the polynomial F. So, by Theorem 2.3.1, there exists a unique polynomial F that passes through these points and the group can reconstruct F using t of these points. They then compute $F(0) = k$ in order to recover the secret. Specifically, a set of participants $A = \{p_{i_1}, \ldots, p_{i_t}\}$ with shares $(\alpha_{i_j}, F(\alpha_{i_j}))$ for $1 \leq j \leq t$, computes the polynomial

$$G(x) = \sum_{\ell=1}^{t} F(\alpha_{i_\ell}) \prod_{1 \leq j \leq t, j \neq \ell} \frac{\alpha_{i_j} - x}{\alpha_{i_j} - \alpha_{i_\ell}}.$$

Then G will be a polynomial over $\mathbb{F}_q$ such that $G(\alpha_{i_\ell}) = F(\alpha_{i_\ell})$ for $1 \leq \ell \leq t$, and so by the uniqueness in the Lagrange interpolation theorem G and F are equal. So the participants have reconstructed F, and are able to compute the secret as $G(0) = F(0) = k$. In particular the participants compute

$$k = G(0) = \sum_{\ell=1}^{t} F(\alpha_{i_\ell}) \prod_{1 \leq j \leq t, j \neq \ell} \frac{\alpha_{i_j}}{\alpha_{i_j} - \alpha_{i_\ell}}.$$

Furthermore, if a set B has $b < t$ participants, then they hold less than t points on F, and so there is a unique polynomial for each other combination of $t-b$ points in $\mathbb{F}_q$. Specifically, if $B = \{p_{i_1}, \ldots, p_{i_{t-1}}\}$ is a set of participants with shares $(\alpha_{i_j}, F(\alpha_{i_j}))$ for $1 \leq j \leq t-1$, then for each $\alpha \in \mathbb{F}$, by Lagrange's interpolation theorem, there is a unique polynomial G_α with degree at most $t-1$ such that such that $G_\alpha(0) = \alpha$ and $G_\alpha(\alpha_{i_\ell}) = F(\alpha_{i_\ell})$ for $1 \leq \ell \leq t-1$. Thus the group of participants B reconstructs a different polynomial for each $\alpha \in \mathbb{F}$, and so they gain no information about what the secret is.

Therefore, we have that this scheme satisfies the correctness and perfect privacy conditions, while the shares and the secret are both in $\mathbb{F}_q$, so it is ideal. So this scheme is perfect and ideal.

2.3.2 Blakley's Threshold Scheme

The Blakley construction [6] for the (t, n)-threshold scheme uses hyperplane geometry over a finite field $\mathbb{F}_q$. Suppose we have a secret $k \in \mathbb{F}_q$ that we wish to share in a (t, n)-threshold scheme. Similar to the Shamir version of the scheme, we require that $1 \leq t \leq n$ and $q > n$. We pick a random point in the t-dimensional affine space with k as its first coordinate and n affine hyperplanes that pass through this point. The n hyperplanes are then given to each of the n participants as their shares. The hyperplane given to participant p_i, $1 \leq i \leq n$, can be viewed as a linear equation of the form

$$a_i^{(1)} x_1 + a_i^{(2)} x_2 + \cdots + a_i^{(t)} x_t = y_i.$$

The dealer publicly posts the values $a_i^{(1)}, \ldots, a_i^{(t)}$ corresponding to each participant. The share given to participant i is the value y_i. If a group of t participants $T = \{p_{i_1}, \ldots, p_{i_t}\}$ wishes to reconstruct the secret they solve the system

$$A_T x = y_T$$

where A_T is a matrix with its jth row being the values $a_{i_j}^{(1)}, \ldots, a_{i_j}^{(t)}$ and y_T is the vector with its jth coordinate being y_{i_j}. The solution to this system will be the point of intersection of all of the hyperplanes, which allows the group to reconstruct the secret as the first coordinate of the solution x. On the other hand, if a group of $t-1$ or fewer participants tries to reconstruct the secret they will solve this system they will not get a point, but a space with dimension greater than zero. For each possible element of $\mathbb{F}_q$, there will be at least one point in this space with that value as its first coordinate. So, the group gets no information about the secret value k and the scheme is perfect. In addition, since both the shares and secret are elements of $\mathbb{F}_q$, the scheme is ideal.

2.3.3 Orthogonal Array Construction

A combinatorial characterization of the (t, n)-threshold scheme uses orthogonal arrays, rather than the more algebraic approach to previous constructions. We follow the presentation of the scheme from Stinson [26]. Recall that an $\mathrm{OA}_\lambda(N; t, k, v)$ is a pair (X, D), where X is a set of v points and D is a v^t by k array over X such that every t-tuple appears exactly λ times as a row in all subarrays defined by t columns of D. We can obtain a (t, n)-threshold scheme from any $\mathrm{OA}_1(N; t, n+1, v)$ (denoted $\mathrm{OA}(N; t, n+1, v)$).

Suppose we have an orthogonal array A, defined on a symbol set X, with columns labeled $1, \ldots, n$ and rows labeled $1, \ldots, v^t$. The secret is chosen as any value in X, giving us v possible secrets to choose from. Each of the n participants is associated to one of the first n columns of the array, leaving the final column to be associated to the secret. For every possible secret $k \in X$ we build a set $R_k = \{r : A(r, n+1) = k\}$, the set of all rows that have that secret k in the final column. If the dealer wants to share a secret k, they find the corresponding set R_k, then choose a row $r \in R_k$ at random. The shares given to the ith participant is the value $s_i = A(r, i)$, for $1 \leq i \leq n$. The array A is posted publicly, along with the column associations of the participants.

If a group of t participants $p_{i_1}, \ldots, p_{i_t}$ wish to reconstruct the secret all they need to do is find the row ℓ of A that has the share $s_{i_j} = A(\ell, i_j)$ for $1 \leq j \leq t$. Because A is an orthogonal array with $\lambda = 1$ this row exists and is unique, so the participants reconstruct the secret as the value $k = A(\ell, n+1)$. If a group of $b < t$ participants $p_{i_1}, \ldots, p_{i_b}$ wish to reconstruct the secret. Then for every possible $l \in X$ in the final column, there are $t - b$ unique rows such that the shares $s_{i_1}, \ldots, s_{i_b}$ along with l appear in the required positions. So the participants cannot conclude anything about the secret, and this scheme is perfect. The secret and the shares are both picked from the set X, so the scheme is ideal. If the chosen orthogonal array is linear, then the resulting scheme is a linear secret sharing scheme.

Stinson showed that if there exists an $\mathrm{OA}(N; t, n+1, v)$ then there exists a (t, n)-threshold scheme ([26], Theorem 11.5). In 1991 it was shown by Martin [20] that if there exists an ideal (t, n)-threshold scheme with v possible secrets, then there exists a *transversal design* $\mathrm{TD}_1(t, n+1, v)$ ([20], Theorem 6.4.3). A transversal design is equivalent to an $\mathrm{OA}(v^t; t, n+1, v)$ ([20], Result 2.1.4), so the existence of an ideal (t, n)-threshold scheme is equivalent to the existence of a linear $\mathrm{OA}(N; t, n+1, v)$. This gives us a useful way to characterize the realizable (t, n)-threshold schemes as many results exist for the existence of orthogonal arrays. For example this tells us that ideal $(1, n)$-threshold schemes exist for all n (although they are not particularly useful), that ideal (n, n)-threshold schemes exist for all $n, q \geq 2$, and that there exists an ideal (t, n)-threshold scheme for all prime powers $q \geq n$ ([20], Lemma 6.4.6-6.4.8). The last of these results follows from the Bush construction, as it allows us to construct an $\mathrm{OA}(q^t; t, n+1, q)$ for any prime power q.

2.3.4 Example

We present an example of the $(2, 4)$-threshold scheme with 5 possible secrets using Shamir's scheme and the orthogonal array construction. Suppose $\{p_1, p_2, p_3, p_4\}$ is a set of participants and we wish to share the secret value 2. We begin with a realization of the $(2, 4)$-threshold using Shamir's scheme and the finite field $\mathbb{F}_5$.

We begin by constructing a polynomial of degree 1 with coefficients in $\mathbb{F}_5$ and independent term 2. We pick the polynomial $F(x) = 3x + 2$. For each participant we pick a unique element $\alpha \in \mathbb{F}_5$ and send them their share $(\alpha, F(\alpha))$, the shares that are distributed are contained in Table 2.1.

p_j	α_j	$f(\alpha_j)$
p_1	1	0
p_2	2	3
p_3	3	1
p_4	4	4

Table 2.1: Shares distributed to participants in Shamir scheme

Suppose p_1 and p_3 wish to reconstruct the secret. They compute

$$k = G(0)$$

$$
\begin{aligned}
&= F(\alpha_1) \cdot \frac{\alpha_3}{\alpha_3 - \alpha_1} + F(\alpha_3) \cdot \frac{\alpha_1}{\alpha_1 - \alpha_3} \\
&= 0 \cdot 4 + 1 \cdot 2 \\
&= 2
\end{aligned}
$$

and have reconstructed the secret. On the other hand, any individual participant cannot conclude anything about the secret as their share is a single point on a line, meaning they cannot conclude what the linear polynomial is in order to find its independent term.

Next we give a realization of this scheme using orthogonal arrays. We start with an orthogonal array of size 25 and strength 2 with symbol set $X = \{0, 1, 2, 3, 4\}$ and 5 rows built using Bush's construction. This array is shared publicly so that all the participants have access to it. In order to share the secret $k = 2$ we randomly pick one of the rows of the orthogonal array containing 2 in the final column, the chosen column is bolded in Figure 2.5. The shares given to the participants are $s_1 = 0$, $s_2 = 3$, $s_3 = 1$, and $s_4 = 4$.

$$
\begin{array}{ccccc}
p_1 & p_2 & p_3 & p_4 & k \\
\left[\begin{array}{ccccc}
0 & 0 & 0 & 0 & 0 \\
1 & 2 & 3 & 4 & 0 \\
2 & 4 & 1 & 3 & 0 \\
3 & 1 & 4 & 2 & 0 \\
4 & 3 & 2 & 1 & 0 \\
0 & 4 & 3 & 2 & 1 \\
1 & 1 & 1 & 1 & 1 \\
2 & 3 & 4 & 0 & 1 \\
3 & 0 & 2 & 4 & 1 \\
4 & 2 & 0 & 3 & 1 \\
\mathbf{0} & \mathbf{3} & \mathbf{1} & \mathbf{4} & \mathbf{2} \\
1 & 0 & 4 & 3 & 2 \\
2 & 2 & 2 & 2 & 2 \\
3 & 4 & 0 & 1 & 2 \\
4 & 1 & 3 & 0 & 2 \\
0 & 2 & 4 & 1 & 3 \\
1 & 4 & 2 & 0 & 3 \\
2 & 1 & 0 & 4 & 3 \\
3 & 3 & 3 & 3 & 3 \\
4 & 0 & 1 & 2 & 3 \\
0 & 1 & 2 & 3 & 4 \\
1 & 3 & 0 & 2 & 4 \\
2 & 0 & 3 & 1 & 4 \\
3 & 2 & 1 & 0 & 4 \\
4 & 4 & 4 & 4 & 4
\end{array}\right]
\end{array}
$$

Figure 2.5: OA$(25; 2, 5, 5)$ used for $(2, 4)$-threshold scheme

Suppose p_2 and p_4 wish to reconstruct the secret. They look in the orthogonal array

and find the row that has 3 in the second column and 4 in the fourth column. The only row having these two values in these positions is the randomly chosen one, which is presented in bold. They reconstruct the secret 2 as the value in the fifth column of this row. On the other hand, if p_2 tried to reconstruct the secret on their own they would find five different places where the value in the second column is 3, one for each possible secret. So p_2 alone gains no information about the secret.

These two examples illustrate a connection between Shamir's scheme and the orthogonal array scheme when the arrays are constructed using Bush's construction. When using this construction we get an array where each row corresponds to a different polynomial of degree t. Since each of the first q columns receives a distinct element of $\mathbb{F}_q$ in Shamir's scheme and the secret is the independent variable of the polynomial, each of the rows of the array corresponds to a possible setup for the Shamir scheme. Thus, when we construct an orthogonal array in this way, the random choice of row made in the Stinson orthogonal array scheme is equivalent to the choice of polynomial in the Shamir interpolation scheme.

2.4 Vector Space Secret Sharing Schemes

After the introduction of the (t, n)-threshold scheme by Shamir and Blakley, Brickell developed a generalized form of the scheme that uses vector spaces [8]. It is also a perfect and ideal secret sharing scheme.

Brickell's scheme also uses a finite field $\mathbb{F}_q$. The secret a_0 is an element of $\mathbb{F}_q$ and with the secret the dealer picks a vector $a = (a_0, a_1, \ldots, a_t)$ for some t, where each $a_j \in \mathbb{F}_q$ for $1 \leq j \leq t$. For each participant p_i the dealer picks a distinct $(t+1)$-dimensional vector v_i over $\mathbb{F}_q$, then makes all these vectors public. The shares given to the participants are $s_i = v_i \cdot a$. The following proposition from Brickell describes the authorized and unauthorized sets.

Proposition 2.4.1 (Vector Space Authorized Sets, [8])**.** Let $P = \{p_{i_1}, \ldots, p_{i_k}\}$ be a set of participants.

1. The participants in P can determine the secret a_0 if the subspace $\langle v_{i_1}, \ldots, v_{i_k}\rangle$ contains e_1, the unit vector with a 1 in the first position and zeros everywhere else.

2. The participants in P cannot determine any information about the secret a_0 if the subspace $\langle v_{i_1}, \ldots, v_{i_k}\rangle$ does not contain e_1.

Proof. Suppose we have a group of participants $\{p_{i_1}, \ldots, p_{i_k}\}$ with shares $s_{i_1}, \ldots, s_{i_k}$ that is authorized, so $e_1 \in \langle v_{i_1}, \ldots, v_{i_k}\rangle$. Let M be the matrix with $v_{i_1}, \ldots, v_{i_k}$ as its rows, and let w be the vector such that $wM = e_1$. Then, $wMa = e_1 a = a_0$ and since $Ma = (s_{i_1}, \ldots, s_{i_k})$, the participants can reconstruct the secret by computing $w \cdot (s_{i_1}, \ldots, s_{i_k}) = a_0$.

Conversely, suppose $\{p_{i_1}, \ldots, p_{i_k}\}$ is a group of participants with shares $s_{i_1}, \ldots, s_{i_k}$ that is not authorized, so $e_1 \notin \langle v_{i_1}, \ldots, v_{i_k}\rangle$. Again we construct the matrix M with rows $v_{i_1}, \ldots, v_{i_k}$. Let $w_0, \ldots, w_t$ be the column vectors of M. Then $w_0 \in \langle w_1, \ldots, w_t\rangle$, as otherwise we would be able to find a vector $d \in \mathbb{F}_q^{t+1}$ such that $d \cdot w_0 = 1$ and $d \cdot w_i = 0$ for $1 \leq i \leq t$, giving

us that $dM = e_1$. The only information that the participants know about the secret is that $Ma = s$, but since $w_0 \in \langle w_1, \ldots, w_t \rangle$ we can find a vector $b \in \mathbb{F}_q^{t+1}$ such that $Mb = 0$ and $b_0 \neq 0$, and thus they can only conclude that $s = Ma = M(a + \alpha b)$ where α is any element of $\mathbb{F}_q$. As a consequence, given some $c_0 \in \mathbb{F}_q$, they can find a vector $c = (c_0, \ldots, c_t) \in \mathbb{F}_q^{t+1}$ such that $Mc = s$, and cannot learn any information about the value of the secret. ∎

If an access structure is realizable by this scheme then we call it a *vector space access structure*. This scheme requires that the dealer finds sets of vectors that match with the requirements of the access structure, a task that is not trivial and could be impossible depending on the parameters. Additionally, this scheme can be further generalized by allowing a vector to be assigned to more than one participant, called *monotone span programs*.

Karchmer and Widgerson [14] showed that the existence of a monotone span program implies the existence of a linear secret sharing scheme. Later, it was proved by Beimel [2] that the existence of a linear secret sharing scheme implies the existence of a monotone span program. So the two structures are equivalent and, similarly to the case with threshold schemes and orthogonal arrays, we are able to use the lower bounds on the sizes of monotone span programs to get lower bounds on the information ratio of linear secret sharing schemes.

Chapter 3

Matroids

Matroids are structures that generalize the concept of linear dependence. They are mainly used to represent structures arising from linear algebra and graph theory. There are many different ways to define matroids. We give the standard definition, then present some properties of matroids. We then connect matroids to access structures using matroid ports. Our main reference for this chapter is Oxley [22].

3.1 Definitions

Definition 3.1.1 (Matroids, [22])**.** A *matroid* is a pair $(Q, \mathcal{I})$ where Q is a finite set and $\mathcal{I}$ is a collection of subsets of Q with the following three properties:

1. $\emptyset \in \mathcal{I}$,
2. If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$, and
3. If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists $x \in I_2 - I_1$ such that $I_1 \cup \{x\} \in \mathcal{I}$.

Here we call the second and third conditions the *hereditary* and *independence augmentation* properties, respectively. We view the elements of $\mathcal{I}$ as the *independent sets* of the *ground set* Q. Any subset of Q that is not in $\mathcal{I}$ is called *dependent*.

One of the fundamental examples of matroids arises from matrices. Let Q be the set of column labels of an $m \times n$ matrix A over a field $\mathbb{F}$, and let $\mathcal{I}$ be the set of subsets X of Q for which the multiset of columns labeled by X is a set and is linearly independent in the vector space over $\mathbb{F}$ of dimension m, $V(m, \mathbb{F})$. Then $M = (Q, \mathcal{I})$ is a matroid. The resulting matroid M is called the *vector matroid* of A. We denote by $M[A]$ the matroid obtained in this way from the matrix A. Two vector matroids over $\mathbb{F}_4$ on the ground set $Q = \{1, 2, 3, 4\}$ are presented in Figure 3.1.

A minimal dependent set of a matroid M is called a *circuit* of M. The circuits of a matroid M are determined entirely by the independent sets $\mathcal{I}(M)$ of the matroid, and

$$\begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \omega \end{bmatrix} \end{array} \qquad \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \omega+1 \end{bmatrix} \end{array}$$

Figure 3.1: Vector matroids over $\mathbb{F}_4$ on ground set $Q = \{1, 2, 3, 4\}$

similarly the independent sets can be determined by the circuits $\mathcal{C}(M)$. This is done by just defining the independent sets as the subsets of Q that do not contain any circuits of M. Because of this we can build matroids entirely using their circuits, rather than their independent sets. The following proposition gives conditions for a set C to be the collection of circuits of a matroid M on a set Q.

Proposition 3.1.2 ([22], Corollary 1.1.5)**.** Let $\mathcal{C}$ be a set of subsets of a set Q. Then $\mathcal{C}$ is the collection of circuits of a matroid on Q if and only if the following conditions are satisfied:

- $\emptyset \in \mathcal{C}$,
- $C_1 \not\subseteq C_2$ if $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$, and
- If $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$, and $x \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) - \{x\}$

Using the circuits we can quickly define matroids on the edge sets of graphs. To do this we use the edge sets of the cycles of the graph as the circuits of a matroid on the edge set. The resulting matroid is called the *cycle matroid* of the graph, denoted by $M(G)$ for a graph G. The independent sets of this matroid are the sets of edges that do not contain a cycle. Similarly to graph theory, we have a concept of connectedness for matroids. A matroid is *connected* if for every pair $p, q \in Q$, there is a circuit C with $p, q \in C$. An element of Q is a *loop* if it is a single element circuit of M. If p and q are elements of a matroid such that $\{p, q\}$ is a circuit, then we call p and q *parallel* in M. A *parallel class* of M is a maximal subset $X \subseteq Q$ such that X contains no loops and any two distinct elements of X are parallel. We call a parallel class trivial if it contains a single element. A matroid is *simple* if it contains no loops and no non-trivial parallel classes.

We present an example of a graph G that represents a cycle matroid $M(G)$ in Figure 3.2. The elements of $M(G)$ are the edges $e_1, e_2, e_3, e_4, e_5, e_6, e_7$ and the circuits are the sets $\{e_1\}$, $\{e_2, e_3, e_4\}$, $\{e_5, e_6\}$, $\{e_5, e_7\}$, and $\{e_6, e_7\}$. We see that e_1 forms a single element circuit and each of e_5, e_6, and e_7 are parallel with each other. Hence, we have that e_1 is a loop of $M(G)$ and $\{e_5, e_6, e_7\}$ is a non-trivial parallel class of $M(G)$. All other elements of $M(G)$ form trivial parallel classes as a singleton.

We call a maximally independent set of a matroid M a *base* or *basis* of M. For a matroid $M = (Q, \mathcal{I})$ a family $\mathcal{B} \subseteq \mathcal{I}$ is the family of bases, sometimes denoted $\mathcal{B}(M)$, if and only if $\mathcal{B}$ is nonempty and the following condition is satisfied:

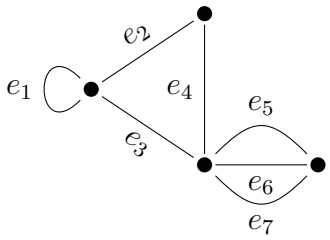


Figure 3.2: Graph G whose cycle matroid contains a loop and a non-trivial parallel class

- For every $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, there exists $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\}$ is in $\mathcal{B}$.

All of the bases of a matroid have the same size ([22], Lemma 1.2.1). Like with the collection of circuits, a matroid M is uniquely determined by its family of bases. Bases of matroids are very similar to those of vector spaces. We can use the collection of bases of a matroid M to define the *dual* M^* of M. Suppose $M = (Q, \mathcal{I})$ is a matroid with family of bases $\mathcal{B}$ and let

$$\mathcal{B}^* = \{Q - B : B \in \mathcal{B}\}.$$

Then B^* is the family of bases of a matroid M^*, called the dual of M ([22], Theorem 2.1.1). The dual of the dual of a matroid M, $(M^*)^*$, is M itself. For a matroid M on the ground set Q, another characterization of loops are the elements of Q that belong to no basis. Elements of Q that are loops in the dual of M are called *coloops*. These are the elements that belong to every basis, and thus are the elements that belong to no circuits.

It is possible for two matroids to have the same structure, but be labeled differently. We call such matroids *isomorphic*. Two matroids $M_1 = (Q_1, \mathcal{I}_1)$ and $M_2 = (Q_2, \mathcal{I}_2)$ are isomorphic, written $M_1 \cong M_2$, if there exists a bijection $\psi : Q_1 \to Q_2$ such that for all $I \subseteq Q_1$, $I \in \mathcal{I}_1$ if and only if $\psi(I) \in \mathcal{I}_2$. If a matroid M is isomorphic to the cycle matroid of a graph, then we call M graphic. Another collection of matroids defined from isomorphisms are the *representable* matroids. These are the matroids that are isomorphic to vector matroids. These matroids have strong connections to ideal secret sharing schemes and are introduced in Section 3.4.

3.2 Rank Functions

Suppose $M = (Q, \mathcal{I})$ is a matroid and $X \subseteq Q$. We define the restriction of M to X as the matroid $M|X = (X, \mathcal{I}|X)$ where $\mathcal{I}|X = \{I \subseteq X : I \in \mathcal{I}\}$. Sometimes this matroid is referred to as the deletion of $Q - X$ from M. The circuits of this matroid are the circuits of M that are entirely contained in X. As all of the bases of $M|X$ have the same cardinality, we define a function r from the power set of Q to the nonnegative integers, called the *rank function*, as $r(X) = |B|$, where B is a base of $M|X$. The rank of a matroid M, written $r(M)$, is the size of any basis of M. The following proposition gives conditions for when a function is a rank function.

Proposition 3.2.1 ([22], Corollary 1.3.4)**.** Let Q be a set. A function $r : P(Q) \to \mathbb{Z}^+ \cup \{0\}$ is the rank function of a matroid M if and only if r has the following three properties:

- If $X \subseteq Q$, then $0 \leq r(X) \leq r(M)$,
- If $X \subseteq Y \subseteq Q$, then $r(X) \leq r(Y)$, and
- If $X, Y \subseteq Q$, then
$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

The independent sets, bases, and circuits of a matroid M can all be characterized in terms of rank functions.

Proposition 3.2.2 ([22], Proposition 1.3.5)**.** Let $M = (Q, \mathcal{I})$ be a matroid with rank function r and $X \subseteq Q$. Then

- $X \in \mathcal{I}$ if and only if $r(X) = |X|$,
- $X \in \mathcal{B}(M)$ if and only if $|X| = r(X) = r(M)$, and
- $X \in \mathcal{C}(M)$ if and only if $X \neq \emptyset$ and, for all $x \in X$, $r(X - x) = |X| - 1 = r(X)$.

As the independent sets of a matroid are entirely determined by the rank function, we usually represent matroids as $M = (Q, r)$ instead of $M = (Q, \mathcal{I})$, where Q is the ground set and r is the rank function. A subset $X \subseteq Q$ is a *flat* of the matroid $M = (Q, r)$ if $r(X \cup \{p\}) > r(X)$ for all $p \notin X$. The *closure* of X is the flat $\mathrm{cl}(X) = \{p \in Q : r(X \cup \{p\}) = r(X)\}$. This closure operation has the property that each subset of Q has the same rank as its closure.

An interesting class of matroids for secret sharing are the *uniform matroids*. Given integers k, n such that $1 \leq k < n$ the uniform matroid $U_{k,n} = (Q, r)$ has ground set Q of size n and rank function $r(A) = \min\{|A|, k\}$. The circuits of these matroids are the subsets $C \subseteq Q$ such that $|C| = k + 1$. The rank of the uniform matroid $U_{k,n}$ is k for all $n > k$. The bases of the uniform matroid $U_{k,n}$ are all of the k element subsets of Q. Hence, the collection of bases of the dual of $U_{k,n}$ consists of all of the $n - m$ subsets of Q. So, $U^*_{k,n} = U_{n-k,n}$. The two matroids presented in Figure 3.1 are matrix representations of $U_{2,4}$.

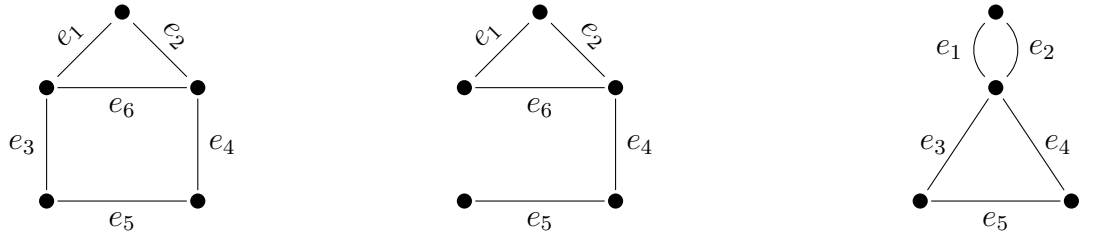
3.3 Minors

Continuing down the path of generalizing concepts from linear algebra and graph theory to matroids, we generalize the concept of graph minors. Let $M = (Q, r)$ be a matroid. Given a subset T of Q, we define the matroid $M \backslash T$ to be the *deletion* of T from M. This matroid has ground set $Q \setminus T$ and its independent sets are those that were independent in M and are contained in $Q \setminus T$. We now define an analogue of edge contraction in graphs for matroids.

Let $M = (Q, r)$ be a matroid and let T be a subset of Q. Then the contraction of T from M, M/T, is given by

$$M/T = (M^*\backslash T)^*.$$

Then, M/T is a matroid on the ground set $Q\backslash T$. In Figure 3.3 give a graph G that represents a matroid $M(G)$, as well as examples of the deletion and contraction operations in $M(G)$.



(a) $M(G)$ (b) $M(G)\backslash\{e_3\}$ (c) $M(G)/\{e_6\}$

Figure 3.3: Graph $M(G)$, along with $M(G)\backslash\{e_3\}$ and $G/\{e_6\}$

In order to use the deletion and contraction operations to define minors, we first need to see that they commute with each other and themselves.

Proposition 3.3.1 ([22], Proposition 3.1.25)**.** Let $M = (Q, r)$ be a matroid, and let T_1 and T_2 be disjoint subsets of Q. Then

1. $(M\backslash T_1)\backslash T_2 = (M\backslash T_2)\backslash T_1 = M\backslash(T_1 \cup T_2)$,
2. $(M/T_1)/T_2 = (M/T_2)/T_1 = M/(T_1 \cup T_2)$, and
3. $(M\backslash T_1)/T_2 = (M/T_2)\backslash T_1$.

When there is no confusion, we drop the parentheses in these expressions. From the final result we can write any sequence of contractions and deletions as $M\backslash X/Y$ for disjoint sets X and Y. For a matroid M, we call substructures of this form *minors* of M. Note that we allow X and Y to be empty in the definition of a minor. In the case where $X \cup Y$ is nonempty we call $M\backslash X/Y$ a *proper minor* of M. An example of a proper minor is given in Figure 3.4 using the graph G from Figure 3.3. Additionally, the matroids (b) and (c) from Figure 3.3 are proper minors. If $\mathcal{N}$ is a set of matroids, we call N_1 an $\mathcal{N}$-minor of M if N_1 is a minor of M that is isomorphic to some N in $\mathcal{N}$. If $\mathcal{N} = \{N\}$, then we call N_1 an N-minor of M.

There are some classes of matroids who have the property that when you take a minor of a member of the class, the result is also from that class. We call such classes *closed under minors* or *minor-closed*. Two classes that are minor-closed that we have already seen are the graphic and the uniform matroids. Another class with this property that is relevant for secret sharing are the representable matroids.

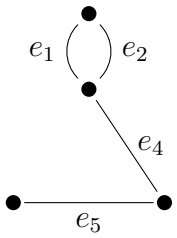


Figure 3.4: $M(G)\backslash\{e_3\}/\{e_6\}$

3.4 Representable Matroids

One of the most important characteristics that a matroid can have for us is being *representable*.

Definition 3.4.1 (Representable Matroids)**.** Let $M = (Q, r)$ be a matroid with n elements. Then, M is $\mathbb{F}$-*linearly representable* ($\mathbb{F}$-*representable* or just *representable*) if M is isomorphic to the vector matroid of an $m \times n$ matrix A over a field $\mathbb{F}$ with $m \geq r(M)$. The matrix A is referred to as an $\mathbb{F}$-*representation* of M.

The isomorphism here gives us a natural map ψ_A from Q to the vector space over $\mathbb{F}$ with dimension m, $V(m, \mathbb{F})$. We call this map a *coordinatization* of M. These coordinatizations will have the property that for all $X \subseteq Q$, $r_M(X) = \dim\langle\psi(X)\rangle$. In a coordinatization of M, an element is mapped to the zero vector if and only if it is a loop in M. Furthermore, a pair of elements are mapped to nonzero scalar multiples in $V(m, \mathbb{F})$ if and only if they are parallel in M [22].

Suppose $\psi : Q \to V(m, \mathbb{F})$ is a coordinatization of a simple matroid $M = (Q, r)$. Then ψ is one-to-one, $\psi(Q)$ will not contain the zero vector, and $\psi(Q)$ contains at most one element of any 1-dimensional subspace of $V(m, \mathbb{F})$. This matroid M will be the matroid associated to the projective geometry $\mathrm{PG}(m-1, \mathbb{F})$, defined in the next section.

3.4.1 Projective Geometries

We now define a projective geometry associated with a vector space V, based on the definition from Oxley [22]. Let V be a vector space over a field $\mathbb{F}$. The *projective geometry* associated with V consists of a set of *points*, *lines*, and an *incidence relation* between the points and lines. The points and lines are the 1-dimensional and 2-dimensional subspaces of V, and the incidence is determined by set inclusion. The construction of $\mathrm{PG}(V)$ from the vector space V is equivalent to the construction of a simple matroid from a non-simple matroid M by deleting the loops and deleting all but one element of each of the parallel classes. To see this, we construct $\mathrm{PG}(V)$ by removing the zero vector of V, then deleting all but one element of each 1-dimensional subspace of V. This deletion is usually done following some pattern, for example taking the element whose first nonzero element is one in each 1-dimensional subspace of $V(m, \mathbb{F})$. The projective geometry $\mathrm{PG}(V)$ has the following properties [22]:

1. Every two distinct points, a and b, are on exactly one line ab.
2. Every line contains at least three points.
3. Suppose a, b, c, d are four distinct points, with no three of them lying on the same line, then if ab intersects cd, ac must intersect bd.

We write (P, L, ι) to represent projective geometries, sometimes called projective spaces. Here, P and L are sets of points and lines, and ι is an incidence relation such that the above properties hold. Because of the first two properties we can view lines as subsets of points, allowing ι to be expressed using set notation. A *subspace* of a projective geometry is a set P_1 of P such that for every pair of distinct points a and b, P_1 contains all points on the line ab. Examples of subspaces are $\emptyset$, P itself, all singletons, and all the lines. A *hyperplane* is a subspace of P that is not properly contained in any subspace except P itself. The subspaces of a projective geometry can be partially ordered by set inclusion. This gives us a way to define the dimension of a subspace. The *dimension* of a subspace P_1 is the maximum length of a chain from $\emptyset$ to P_1 in this partial ordering.

If V is a vector space of dimension $n+1$ over a field $\mathbb{F}$, then $\mathrm{PG}(V)$ has dimension n and we denote it by $\mathrm{PG}(n, \mathbb{F})$. If $\mathbb{F}_q$ is a finite field with q elements, then we denote the projective geometry by $\mathrm{PG}(n, q)$ instead of $\mathrm{PG}(n, \mathbb{F}_q)$. If a projective geometry has dimension two, then we call it a *projective plane*. Projective planes are of note to us as they give rise to rank-3 representable matroids. The following theorem from Oxley connects projective geometries and representable matroids.

Theorem 3.4.2 ([22], Theorem 6.1.3)**.** Let M be a simple matroid with rank r and $\mathbb{F}$ a field. The following statements are equivalent:

1. M is $\mathbb{F}$-representable.
2. $\mathrm{PG}(r-1, \mathbb{F})$ has a finite subset T such that $M \cong \mathrm{PG}(r-1, \mathbb{F})|T$.
3. For some $m \geq r$, there is a finite subset S of $\mathrm{PG}(m-1, \mathbb{F})$ such that $M \cong \mathrm{PG}(m-1, \mathbb{F})|S$.

From this result we can see that every simple $\mathbb{F}$-representable matroid with rank r can be obtained from $\mathrm{PG}(r-1, \mathbb{F})$ by deleting elements.

For a finite field $\mathbb{F}_q$ with q elements, the projective geometry $\mathrm{PG}(r-1, q)$ has $\frac{q^r-1}{q-1}$ points. This is because the projective geometry is formed from the vector space $V = (r, \mathbb{F}_q)$ by removing the zero vector, then deleting all but one of the $q-1$ elements in each 1-dimensional subspace. The following result follows from the previous theorem and this fact.

Proposition 3.4.3 ([22], Corollary 6.1.7)**.** A simple matroid M with rank r and ground set Q that is representable over $\mathbb{F}_q$ has at most $\frac{q^r-1}{q-1}$ elements. Moreover, if $|Q| = \frac{q^r-1}{q-1}$ then $M \cong \mathrm{PG}(r-1, q)$.

In subsequent chapters, we will be interested in some other characteristics of projective planes. In particular, the projective plane $\mathrm{PG}(2, q)$ consists of q^2+q+1 points and lines, where each line contains $q+1$ points, and each point lies on $q+1$ lines [22].

3.4.2 Equivalent Representations

When dealing with representable matroids it is possible to find different matrix representations of a matroid. It then becomes important for us to be able to distinguish whether these different representations are actually different. The following operations from Oxley [22] applied to a matrix A over a field $\mathbb{F}$ will not change the associated matroid $M[A]$.

(i) Interchange two rows.

(ii) Multiply a row by a nonzero element of $\mathbb{F}$.

(iii) Replace a row with the sum of that row and another.

(iv) Add or remove a zero row.

(v) Interchange two rows.

(vi) Multiply a column by a nonzero element of $\mathbb{F}$.

(vii) Replace each entry in A with its image under an automorphism of $\mathbb{F}$.

The first six of these come directly from matrix operations. The last is a property of fields. We say that matrices A_1 and A_2 are *equivalent representations* of M if A_2 can be obtained from A_1 using these seven operations. Furthermore, we call A_1 and A_2 *projectively equivalent* if A_2 can be obtained from A_1 using the first six of these operations. Matrices that are not projectively equivalent are called projectively inequivalent. The two matroids in Figure 3.1 are equivalent representations, but are not projectively equivalent as they use the automorphism mapping ω to $\omega + 1$. Figure 3.5 shows six inequivalent representations of $U_{3,5}$ [22].

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}\qquad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}\qquad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}\qquad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix}\qquad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 4 \end{bmatrix}$$

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}\qquad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}\qquad \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 1 & 2 \end{bmatrix}\qquad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 2 \end{bmatrix}\qquad \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

Figure 3.5: Inequivalent representations of $U_{3,5}$

3.4.3 Fano Plane Matroid

Two representable matroids that we will see come up again later in the context of secret sharing are the Fano and non-Fano matroids, F_7 and F_7^-.

The Fano matroid, F_7, is the matroid on the ground set $Q = \{1, 2, 3, 4, 5, 6, 7\}$ with family of bases

$$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{3, 4, 7\}, \{3, 5, 6\}, \{2, 4, 6\}, \{2, 5, 7\}\}.$$

The non-Fano matroid, F_7^-, is the matroid that results from removing $\{3, 5, 6\}$ from $\mathcal{B}$. We can represent the Fano matroid graphically, representing the elements as points and the bases as lines between the points. A graphical representation of F_7 and F_7^- is presented in Figure 3.6.

(a) F_7 (b) F_7^-

Figure 3.6: The Fano and non-Fano matroids

The matrix A in Figure 3.7 is a representation of either F_7 or F_7^-, depending on the choice of field $\mathbb{F}$. If the characteristic of $\mathbb{F}$ is two, then it is a representation of F_7 and if the characteristic of $\mathbb{F}$ is not two, then it is a representation of F_7^-. The fact that A is a

$$A = \begin{array}{c} \begin{matrix} 1 & 2 & 7 & 5 & 6 & 3 & 4 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Figure 3.7: Representation of F_7 and F_7^-

representation of F_7 or F_7^- depending on the characteristic of the field $\mathbb{F}$ follows from the following lemma. The proof of this lemma comes from considering the possible circuits of F_7 and F_7^-.

Lemma 3.4.4 ([22], Lemma 6.4.4)**.** Let A be the matrix from Figure 3.7 viewed over a field $\mathbb{F}$. If the characteristic of $\mathbb{F}$ is two, then $M[A] = F_7$, while if the characteristic of $\mathbb{F}$ is not two, then $M[A] = F_7^-$.

The following proposition generalizes this result to all possible representations of F_7 and F_7^-.

Proposition 3.4.5 ([22], Proposition 6.4.8)**.** Let $\mathbb{F}$ be a field. Then

1. F_7 is $\mathbb{F}$-representable if and only if the characteristic of $\mathbb{F}$ is two; and
2. F_7^- is $\mathbb{F}$-representable if and only if the characteristic of $\mathbb{F}$ is not two

The Fano and non-Fano matroids will come up again when considering the access structures that are realizable using our secret sharing scheme in Chapter 5.

Chapter 4

Matroid Ports and Access Structures

4.1 Matroid Ports

In order to connect access structures and secret sharing to matroids we use a new structure based on matroids, called *matroid ports*.

Definition 4.1.1 (Matroid Ports)**.** For a matroid $M = (Q, r)$ and a point p_0 in the ground set Q of M, the *port* of M at p_0 is the family of subsets of $P = Q \setminus \{p_0\}$ defined by

$$M_{p_0} = \{A \subseteq P : A \cup \{p_0\} \text{ is a circuit of } M\}.$$

Matroid ports were first used in the context of secret sharing by Brickell and Davenport [9]. They showed that an access structure is a matroid port if it is ideal. Additionally, they showed that if an access structure is the port of a representable matroid, then the access structure is realizable by Brickell's vector space secret sharing scheme. This idea was further developed by Martí-Farré and Padró [18], with them showing that access structures that are not matroid ports can only be realized by secret-sharing schemes with an information ratio that is at least 1.5.

Given a matroid $M = (Q, r)$ and a point $p_0 \in Q$. On the set $P = Q \setminus \{p_0\}$ we define the access structure

$$\Gamma_{p_0} = \{A \subseteq P : r(A \cup \{p_0\}) = r(A)\}.$$

A subset $A \subseteq P$ is minimally qualified in Γ_{p_0} if and only if $A \cup \{p_0\}$ is a circuit of M. So, the collection of minimally qualified sets in Γ_{p_0} is the matroid port M_{p_0}. Because of this, by an abuse of notation, we call access structures of this form matroid ports as well. The (t, n)-threshold scheme is a port of the uniform matroid $U_{t,n+1}$. We give an example of the $(2, 3)$-threshold access structure as a port of $U_{2,4}$ in Figure 4.1 using the representations from Figure 3.1. If a connected access structure Γ is a matroid port, then we can find a unique connected matroid M such that $\Gamma = \Gamma_{p_0}(M)$ for some p_0 [18]. We observe that for a matroid $M = (Q, r)$ and an element $p_0 \in Q$, $\text{rank}(\Gamma_{p_0}(M)) \leq r(M)$.

The access structures which can be constructed as matroid ports are called *matroid related*. Every ideal access structure is matroid related, but not every matroid related access

$$\begin{array}{c} \begin{matrix} p_0 & p_1 & p_2 & p_3 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \omega \end{bmatrix} \end{array} \qquad \begin{array}{c} \begin{matrix} p_0 & p_1 & p_2 & p_3 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \omega+1 \end{bmatrix} \end{array}$$

Figure 4.1: $(2,3)$-threshold scheme as a port of $U_{2,4}$ using two representation over $\mathbb{F}_4$

structure is ideal [19]. An example of an access structure that is matroid related but is not ideal is presented in Section 4.4. We call matroids that are obtained from ideal secret sharing schemes *ideal secret sharing representable* or *iss-representable*. We present a hierarchy of the different types of access structures that we have defined in Figure 4.2.

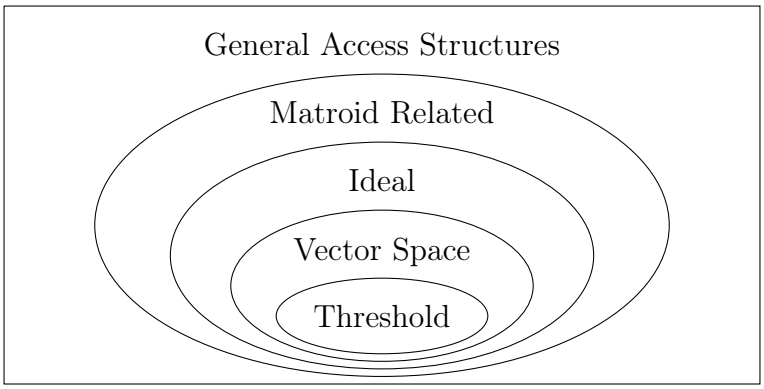


Figure 4.2: Hierarchy of access structures types

4.2 Matroid Operations and Access Structures

Earlier we defined the deletion operation, $M\backslash T$, for a matroid $M = (Q, r)$ and subset $T \subseteq Q$. We can define a similar operation for access structures with the property that $\Gamma_{p_0}(M\backslash T) = \Gamma_{p_0}(M)\backslash T$ [18]. For an access structure Γ on a set of participants P, we define the deletion of $T \subseteq P$ from Γ as $\Gamma\backslash T = \{A \subset P - T : A \in \Gamma\}$. Similarly, we can define analogue of matroid contraction for access structures. For an access structure Γ on a set of participants P, we define the contraction of $T \subseteq P$ in Γ as $\Gamma/T = \{A \subseteq P - T : A \cup T \in \Gamma\}$. Additionally, for access structures Γ_1 and Γ_2 on disjoint sets of participants P_1 and P_2, and a participant $p \in P_1$, we define the *composed access structure* $\Gamma = \Gamma_1[\Gamma_2, p]$ on the set of participants $P = P_1 \cup P_2$ as the access structure with qualified sets $A \subseteq P$ such that $A \cap P_1 \in \Gamma_1$, or $A \cap P_2 \in \Gamma_2$ and $(A \cap P_1) \cup \{p\} \in \Gamma_1$ [18]. Additionally, we define $\Gamma_1[\Gamma_2, \hat{p}] = \Gamma_1[\Gamma_2, p]\backslash\{p\}$. These two variants of composed access structures are connected to matroids through the parallel connection and 2-sum operations.

Martí-Farré and Padró [18] define the *parallel connection* and *2-sum* operations as follows. Let $M_1 = (Q_1, r_1)$ and $M_2 = (Q_2, r_2)$ be connected matroids and suppose that

$Q_1 \cap Q_2 = \{p\}$. The parallel connection of M_1 and M_2 with base point p is the matroid $M = M_1 \oplus_p M_2$ with ground set $Q = Q_1 \cup Q_2$ with rank function

$$r(A) = r_1(A \cap Q_1) + r_2(A \cap Q_2) - \delta$$

where $\delta = 1$ if $r_i(A \cap Q_i) = r_i((A \cap Q_i) \cup \{p\})$ for $i = 1, 2$ and $\delta = 0$ otherwise. The 2-sum of the matroids with base point p is $M_1 \widehat{\oplus}_p M_2 = (M_1 \oplus_p M_2) \setminus p$. Oxley [22, Chapter 7] shows that the parallel connection and 2-sum of two connected matroids is connected, and that the parallel connection and 2-sum of two $\mathbb{F}$-representable matroids are also $\mathbb{F}$-representable.

The following proposition from Martí-Farré and Padró [18] establishes the relationships between these operations and access structures that are ports of matroids.

Proposition 4.2.1 ([18], Proposition 2.1)**.** Let M_1 and M_2 be matroids on ground sets Q_1 and Q_2, where $Q_1 \cap Q_2 = \{p\}$. Then

- $\Gamma_p(M_1 \oplus_p M_2) = \Gamma_p(M_1) \sqcup \Gamma_p(M_2)$, and
- If $\Gamma_1 = \Gamma_{p_0}$ where $p_0 \in Q_1 - \{p\}$ and $\Gamma_2 = \Gamma_p(M_2)$, then $\Gamma_{p_0}(M_1 \oplus_p M_2) = \Gamma_1[\Gamma_2; p]$ and $\Gamma_{p_0}(M_1 \widehat{\oplus}_p M_2) = \Gamma_1[\Gamma_2; \hat{p}]$.

The next proposition, also from Martí-Farré and Padró [18], gives us a way to construct access structures that are ports of matroids by composing smaller structures. This result follows from Proposition 4.2.1.

Proposition 4.2.2 ([18], Proposition 2.2)**.** Let Γ_1 and Γ_2 be access structures. Then $\Gamma_1 \sqcup \Gamma_2$, $\Gamma_1[\Gamma_2; p]$, and $\Gamma_1[\Gamma_2; \hat{p}]$ are matroid ports if and only if Γ_1 and Γ_2 are matroid ports.

Propositions 4.2.1 and 4.2.2 allow us to analyze components of an access structure rather than the whole structure.

4.3 Ideal Schemes with rank at most 3

We now explore the reduced access structures with rank 3. These are the access structures whose minimally authorized sets have at most three participants. Martí-Farré and Padró [18] give conditions for when these access structures exist. These access structures will arise from matroids with rank at least 3. We split the possible matroids into two parts; those that arise from matroids with rank greater than 3, and those that arise from matroids with rank 3.

4.3.1 Matroids with Rank Greater than Three

We present four matroids with rank greater than three. We then present Theorem 4.3.1 from Martí-Farré and Padró [18]. This theorem classifies all of the rank-3 access structures

that are matroid ports of matroids with rank at least 4. We start by looking at the access structure where the minimally authorized sets are the lines of the Fano plane.

Let $P = \{1, 2, \ldots, 7\}$ be a set of seven participants. Let $\Gamma(F)$ be the access structure defined on this set of participants with minimal authorized sets being the lines of the Fano plane. Then

$$\min \Gamma(F) = \{\{1,2,3\},\{1,4,5\},\{1,6,7\},\{3,4,7\},\{3,5,6\},\{2,4,6\},\{2,5,7\}\}.$$

Next, we define the access structure $\Gamma(F^-) = \Gamma(F)\backslash\{6\}$ on the set of participants $P^- = P - \{6\}$. The minimally authorized sets of $\Gamma(F^-)$ are

$$\min \Gamma(F^-) = \{\{1,2,3\},\{1,4,5\},\{3,4,7\},\{2,5,7\}\}.$$

Let $Q = P \cup \{8\}$ be the set of column labels for the matroid M_1 corresponding to the following matrix from Martí-Farré and Padró [18]:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array}$$
$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Then $\Gamma(F) = \Gamma_8(M_1)$ and $\Gamma(F^-) = \Gamma_8(M_2)$ where $M_2 = M_1\backslash\{6\}$. The ranks of M_1 and M_2 are both 4. The above matrix appears in Chapter 6 of Oxley's book *Matroid Theory* [22] as a representation of $\mathrm{AG}(3,2)$, where $\mathrm{AG}(3,2)$ is the result of deleting the points of one of the hyperplanes of $\mathrm{PG}(3,2)$. This matroid is representable over any finite field $\mathbb{F}_q$ of characteristic 2 [22]. Removing the sixth column, to obtain M_2, we get a matroid that is representable over any finite field $\mathbb{F}_q$. So both of these access structures are ideal and are realizable by Brickell's vector space secret sharing scheme, with $\Gamma(F)$ using a finite field of characteristic 2 and $\Gamma(F^-)$ using any finite field.

The next two matroids from Martí-Farré and Padró [18] that we consider are both defined on the set $Q = Q_0 \cup Q_1 \cup \cdots \cup Q_\ell$, where $\ell \geq 2$, $|Q_i| \geq 3$, and $Q_i \cap Q_j = \{p\}$ for $i \neq j$. We denote $n_i = |Q_i|$. First, we consider the matroid M with ground set Q as

$$M = U_{2,n_0} \oplus_p U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell},$$

where $U_{k,n}$ is the uniform matroid with ground set Q of size n and rank function $r(A) = \min\{|A|, k\}$. By Proposition 4.2.1, for each $p \in Q_0 - \{p_0\}$, the access structure $\Gamma_{p_0}(M)$ is of the form $\Gamma_{p_0}(M) = \Gamma_1[\Gamma_2; p]$, where $\Gamma_1 = \Gamma_{p_0}(U_{2,n_0})$ and $\Gamma_2 = \Gamma_p(U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell})$. So, Γ_1 is a $(2, n_0 - 1)$-threshold access structure and Γ_2 is of the form $\Gamma_2 = \Delta_1 \sqcup \cdots \sqcup \Delta_\ell$, where each Δ_i is a $(2, n_i - 1)$-threshold access structure. The minimally qualified sets of $\Gamma_{p_0}(M)$ are

- the subsets of Q_0 that contain two participants, and

- the subsets X of Q of the form $X = \{a, b, c\}$ where $a \in Q_0 - \{p, p_0\}$ and $b, c \in Q_i - \{p\}$ for some i, $1 \leq i \leq \ell$.

This access structure clearly has rank 3 and is reduced. The matroid M has a minimum rank of 4, which could possibly be larger depending on the choice of ℓ and number of elements in each of the Q_i. Additionally, this matroid is representable over any finite field $\mathbb{F}_q$ with $q \geq \max\{n_0, n_1, \ldots, n_\ell\}$. The final access structure we consider will be the result of deleting p from $\Gamma_{p_0}(M)$. This access structure is of the form

$$\Gamma_{p_0}(M)\backslash\{p\} = \Gamma_{p_0}(M\backslash\{p\}) = \Gamma_{p_0}(U_{2,n_0}\widehat{\oplus}_p(U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell})).$$

The matroid $U_{2,n_0}\widehat{\oplus}_p(U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell})$ also has rank 4 or greater and is representable over any finite field $\mathbb{F}_q$ with $q \geq \max\{n_0, n_1, \ldots, n_\ell\}$. As both of these access structures are ports of representable matroids, they are both ideal and are realizable by Brickell's vector space secret sharing scheme over $\mathbb{F}_q$ with $q \geq \max\{n_0, n_1, \ldots, n_\ell\}$.

The following theorem from Martí-Farré and Padró uses these four matroids and access structures to classify all of the rank 3 access structures that arise as ports of matroids with rank at least 4.

Theorem 4.3.1 ([18], Theorem 3.1)**.** Let M be a matroid with $r(M) \geq 4$. Then $\Gamma = \Gamma_{p_0}(M)$ is a reduced access structure of rank-3 if and only if one of the following statements holds:

1. $M \cong U_{2,n_0}\widehat{\oplus}_p(U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell})$, for $\ell \geq 2$ and $n_i \geq 3$, $i = 0, 1, \ldots, \ell$.
2. $M \cong U_{2,n_0} \oplus_p U_{2,n_1} \oplus_p \cdots \oplus_p U_{2,n_\ell}$, for $\ell \geq 2$ and $n_i \geq 3$, $i = 0, 1, \ldots, \ell$ and $p_0 \neq p$.
3. $M \cong M_1$ and $\Gamma \cong \Gamma(F)$.
4. $M \cong M_2$ and $\Gamma \cong \Gamma(F^-)$.

Additionally, since each of these access structures are ports of representable matroids, we know that if a reduced access structure with rank 3 is the port of a matroid with rank 4 or greater, then it is realizable by a vector space secret sharing scheme.

4.3.2 Matroids with Rank Three

In order to characterize the reduced access structures with rank 3 that arise as ports of matroids with rank 3, Martí-Farré and Padró [18] first define sets $\mathcal{D}_1(\Gamma)$ and $\mathcal{D}_2(\Gamma)$ for an access structure Γ. For an access structure Γ on a set of participants P, they define $\mathcal{D}_1(\Gamma)$ to be the family of all maximally unqualified subsets of Γ, and they define $\mathcal{D}_2(\Gamma)$ to be the family of maximal subsets $X \subseteq P$ such that $\Gamma(X)$ is the $(2, |X|)$-threshold access structure.

We give two example access structures and their corresponding sets $\mathcal{D}_1$ and $\mathcal{D}_2$. The first access structure Γ_1 is represented graphically as:

a — b — c — d

Its minimally qualified sets are $\{a,b\},\{b,c\}$ and $\{c,d\}$. For this access structure, $\mathcal{D}_1(\Gamma_1) = \{\{a,c\},\{b,d\},\{a,d\}\}$ and $\mathcal{D}_2(\Gamma_1) = \{\{a,b\},\{b,c\},\{c,d\}\}$. The second access structure Γ_2 that we consider has 5 participants labeled $1,2,3,4,5$ and its minimally qualified sets are

$$\min\Gamma_2 = \{\{1,2\},\{1,3\},\{2,3\},\{2,4,5\},\{3,4,5\}\}.$$

For this access structure, $\mathcal{D}_1(\Gamma_2) = \{\{1,4,5\},\{2,4\},\{2,5\},\{3,4\},\{3,5\}\}$ and $\mathcal{D}_2(\Gamma_2) = \{\{1,2,3\}\}$.

For an access structure Γ, if X_1 is in $\mathcal{D}_1(\Gamma)$ and X_2 is in $\mathcal{D}_2(\Gamma)$, then they intersect in at most one point. This is due to the fact that any subset of size 2 or more in $\mathcal{D}_2$ is authorized in the access structure, and thus cannot be in a set in $\mathcal{D}_1$. The following theorem from Martí-Farré and Padró considers when X_1 and X_2 are in the same family $\mathcal{D}_1$ or $\mathcal{D}_2$. This theorem characterizes the access structures with rank 3 that are ports of matroids with rank 3.

Theorem 4.3.2 ([18], Theorem 3.3)**.** Let Γ be a reduced access structure with rank 3. Then Γ is the port of a matroid with rank 3 if and only if $|X_1 \cap X_2| \leq 1$ for $X_1, X_2 \in \mathcal{D}_1$, $X_1 \neq X_2$, and $|X_1 \cap X_2| = 0$ for $X_1, X_2 \in \mathcal{D}_2$, $X_1 \neq X_2$.

The access structures that meet the conditions of Theorem 4.3.2 are not necessarily ideal. However, if the access structure is the port of a representable matroid, then the access structure can be realized by Brickell's vector space secret sharing scheme.

4.4 Examples of Rank-3 Access Structures

Applying Theorem 4.3.2 to the previous two examples Γ_1 and Γ_2, where

$$\min\Gamma_1 = \{\{a,b\},\{b,c\},\{c,d\}\}$$

and

$$\min\Gamma_2 = \{\{1,2\},\{1,3\},\{2,3\},\{2,4,5\},\{3,4,5\}\}.$$

We saw that $\mathcal{D}_2(\Gamma_1) = \{\{a,b\},\{b,c\},\{c,d\}\}$, and thus Γ_1 is not the port of a matroid with rank 3, as all of these sets intersect in one place with at least one of the others. Additionally, Γ_1 is not one of the structures that is the port of a matroid with rank 4, so this access structure is not ideal. On the other hand $\mathcal{D}_1(\Gamma_2) = \{\{1,4,5\},\{2,4\},\{2,5\},\{3,4\},\{3,5\}\}$ and $\mathcal{D}_2(\Gamma_2) = \{\{1,2,3\}\}$. These two sets meet the conditions in Theorem 4.3.2, so this scheme is the port of a rank 3 matroid M. Furthermore, the matroid M is representable with an $\mathbb{F}_3$-representation being

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 2 & 2 & 1 \\ 0 & 1 & 1 & 2 & 1 & 0 \end{bmatrix}.$$

So Γ_2 is realizable by a vector space access structure over $\mathbb{F}_3$, and is therefore ideal. By Theorem 5.4.2 that we prove in Chapter 5, Γ_2 is ideal in any field of characteristic three.

We now consider a case where an access structure is the port of a rank-3 matroid, but is not ideal. Let P be a set of participants and $A_1, \ldots, A_s$ be disjoint subsets of P of size 2. We can then define an access structure Γ_3 whose authorized sets are all of these sets $A_1, \ldots, A_s$, as well as any set of 3 or more participants. Then $\mathcal{D}_1(\Gamma_3) = \{X \subseteq P : |X| = 2\} - \{A_1, \ldots, A_s\}$ and $\mathcal{D}_2(\Gamma_3) = \{A_1, \ldots, A_s\}$. This access structure meets the conditions of Theorem 4.3.2, so Γ_3 is the port of a matroid with rank 3. One such access structure results from considering the non-Desargues matroid, presented in [19]. This rank-3 matroid is not representable and any secret sharing scheme realizing it has an information ratio of at least $\frac{4}{3}$, so it is not ideal [19].

Next, we consider a rank-3 access structure that is realizable by an ideal secret sharing scheme, but is not the port of a representable matroid. Let Γ_4 be the access structure on a set of nine participants $P = \{p_1, \ldots, p_9\}$. The minimally qualified subsets of Γ_4 are all of the subsets of P with 3 participants, except for the sets $\{p_1, p_2, p_3\}$, $\{p_1, p_5, p_7\}$, $\{p_1, p_6, p_8\}$, $\{p_2, p_4, p_7\}$, $\{p_2, p_6, p_9\}$, $\{p_3, p_4, p_8\}$, $\{p_3, p_5, p_9\}$, and $\{p_4, p_5, p_6\}$. Then $\mathcal{D}_1(\Gamma_4)$ is the set with these eight excluded sets, and $\mathcal{D}_2(\Gamma_4) = \emptyset$. This access structure is referred to as the non-Pappus access structure [18]. It meets the conditions of Theorem 4.3.2, so it is the port of a matroid with rank 3. Martí-Farré and Padró [17] showed that while Γ_4 is ideal, it is not the port of a representable matroid and so it cannot be realized by a vector space secret sharing scheme for any finite field $\mathbb{F}_q$.

The last example access structure we consider, Γ_5, is defined on a set of five participants, labeled $p_1, \ldots, p_5$. The minimally qualified subsets of Γ_5 are

$$\min \Gamma_5 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3, p_5\}\}.$$

We see that $\mathcal{D}_1(\Gamma_5) = \{\{p_1, p_3\}, \{p_2, p_4, p_5\}, \{p_1, p_4, p_5\}, \{p_2, p_3, p_5\}\}$ and therefore this access structure does not meet the conditions of Theorem 4.3.2, as $\{p_2, p_3, p_5\} \cap \{p_2, p_4, p_5\} = \{p_2, p_5\}$. So it is not the port of a matroid with rank 3. However, if we make $\{p_2, p_4, p_5\}$ authorized, then the structure does meet the conditions of Theorem 4.3.2, so this new access structure, call it Γ_6, is the port of a matroid with rank 3. Furthermore, the resulting matroid is representable over any finite field with characteristic 2, using the following representation:

$$\begin{matrix} 0 & 1 & 2 & 3 & 4 & 5 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

So Γ_6 is realizable using a vector space access structure over any finite field of characteristic 2.

Chapter 5

Projective Plane Secret Sharing

We now present a secret sharing scheme for access structures with rank 3. This scheme uses projective planes to construct an orthogonal array. The access structures that this scheme realizes are precisely those that are ports of representable matroids, so it is equivalent to Brickell's vector space scheme for access structures with rank 3. This scheme was originally defined by Lopes de Souza in [12] using linear feedback shift register (LFSR) sequences. An exploration of using LFSR sequences to construct $\mathrm{PG}(2, q)$, as well as analysis of its benefits, is included in Section 5.5.

5.1 The Scheme

Let Γ be an access structure on a set of n participants P and let q be an integer such that $q^2 + q \geq n$. We define a secret sharing scheme that utilizes $\mathrm{PG}(2, q)$ to construct a 3 by $q^2 + q + 1$ array, which we then extend to a q^3 by $q^2 + q + 1$ array. Recall that $\mathrm{PG}(2, q)$ consists of $\frac{q^3-1}{q-1} = q^2 + q + 1$ non-zero vectors in $\mathbb{F}_q^3$, where no two of the vectors are linearly independent.

Suppose we have constructed $\mathrm{PG}(2, q)$ with the vectors $v_0, \ldots, v_{q^2+q}$. We begin by constructing a 3 by q^2+q+1 array $V(v_0, \ldots, v_{q^2+q})$ where each column is one of the points of $\mathrm{PG}(2, q)$. We then extend $V(v_0, \ldots, v_{q^2+q})$ to an array $A(v_0, \ldots, v_{q^2+q})$ by taking all possible linear combinations of the rows of $V(v_0, \ldots, v_{q^2+q})$. Due to the symmetry of $\mathrm{PG}(2, q)$, the choice of vectors, as well as the order that they are placed in the array $V(v_0, \ldots, v_{q^2+q})$ will not affect the secret sharing scheme. For this reason we denote $V(v_0, \ldots, v_{q^2+q})$ by $V_{\mathrm{PG}(2,q)}$ and $A(v_0, \ldots, v_{q^2+q})$ by $A_{\mathrm{PG}(2,q)}$, writing the specific ordering used when it is necessary. The scheme works similarly to Brickell's vector space scheme, where we assign columns of $A_{\mathrm{PG}(2,q)}$ to participants based on the linear dependence properties of the corresponding vector in $V_{\mathrm{PG}(2,q)}$ with the other column vectors in $V_{\mathrm{PG}(2,q)}$. We give two examples of these matrices in Figure 5.1, one using $\mathrm{PG}(2, 2)$, and one using $\mathrm{PG}(2, 3)$. In both of these matrices the submatrix $V_{\mathrm{PG}(2,q)}$ is given in bold. By Theorem 1.2.10, with $\ell = 3$ and $n = q^2 + q + 1$, we have that $A_{\mathrm{PG}(2,q)}$ is an $\mathrm{OA}_q(q^3; 2, q^2 + q + 1, q)$ with $\mathbb{F}_q$ as its symbol set. So in any two columns of $A_{\mathrm{PG}(2,q)}$, each 2-tuple appears exactly q times.

$$\begin{bmatrix}
\mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\
\mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\
\mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(a) $A_{\mathrm{PG}(2,2)}$

$$\begin{bmatrix}
\mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{0} & \mathbf{2} \\
\mathbf{0} & \mathbf{0} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{0} & \mathbf{2} & \mathbf{2} \\
\mathbf{0} & \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{0} & \mathbf{2} & \mathbf{2} & \mathbf{0} \\
2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 \\
1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 \\
1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 \\
1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 \\
2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 \\
1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\
0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 \\
2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 \\
0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 \\
2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 \\
2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 \\
2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 \\
2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 \\
1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 \\
2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 \\
1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(b) $A_{\mathrm{PG}(2,3)}$

Figure 5.1: Matrices constructed from $\mathrm{PG}(2,2)$ and $\mathrm{PG}(2,3)$.

In order to share a secret $k \in \mathbb{F}_q$, the dealer first chooses a row r of the array $A_{\mathrm{PG}(2,q)}$ containing k in the first column at random. We view the vector v_0 as the vector associated to the secret, which we denote c_0. The participants are each allocated vectors $v_{p_1}, \ldots, v_{p_n}$. We denote the vector associated to participant p_i by c_i. The dealer publicly shares the columns vectors $c_1, \ldots, c_n$ associated to each participant and gives each participant i the value in their corresponding column of r as their share s_i. In order to avoid confusion related to the use of subscripts we denote these vectors and their components by $c_i = (c_i^{(1)}, c_i^{(2)}, c_i^{(3)})$. To reconstruct the secret, a group of participants $p_1, \ldots, p_\ell$ with shares $s_1, \ldots, s_\ell$, solves the system

$$v_1 c_1 + \cdots + v_\ell c_\ell = c_0,$$

for variables $v_1, \ldots, v_\ell$. We show in Section 5.3 that the solution to this system exists if and only if the group of participants is authorized. If the solution exists then they compute the value of the secret as

$$k = \sum_{i=1}^{\ell} s_i v_i.$$

Otherwise, they will not be able to conclude anything about the value of the secret.

When assigning the participants to columns, we need to assign them such that the solution to the above system of equations exists if and only if the group of participants is authorized. The following definition gives us the requirements for a set of participants to be minimally authorized.

Definition 5.1.1. Let $v_0, v_1, \ldots, v_{q^2+q}$ be the column vectors resulting from taking the first three rows of the array $A_{\mathrm{PG}(2,q)}$ constructed from $\mathrm{PG}(2,q)$. Let Γ be an access structure with participants $p_1, \ldots, p_n$. We say that Γ is *realizable* by the projective plane secret sharing scheme with domain of secret $\mathbb{F}_q$ if there exists an injective function $\varphi : \{p_1, \ldots, p_n\} \to \{v_1, \ldots, v_{q^2+q}\}$ such that the following properties are met:

- $\{p_i, p_j\} \in \min \Gamma$ if and only if $\{v_0, \varphi(p_i), \varphi(p_j)\}$ is a linearly dependent set.
- $\{p_i, p_j, p_k\} \in \min \Gamma$ if and only if $\{\varphi(p_i), \varphi(p_j), \varphi(p_k)\}$ is a linearly independent set and no pair of $\{p_i, p_j, p_k\}$ is minimally authorized.

For simplicity, refer to φ as an *allocation* of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$. When we do this we write c_i for $\varphi(p_i)$ and c_0 for v_0. Note that in Definition 5.1.1 the minimally authorized sets coincide exactly with the sets of participants whose columns become circuits of the matroid associated to $\mathrm{PG}(2,q)$ when c_0 is added to them. From Definition 5.1.1 we get the following result about which sets are authorized in the secret sharing scheme.

Proposition 5.1.2. Let Γ be an access structure that is realizable by the projective plane secret sharing scheme with participant set $P = \{p_1, \ldots, p_n\}$. A set $A \subseteq P$ is authorized if and only if one (or both) of the following hold:

- A contains a set $\{p_i, p_j\}$ such that $\{c_0, c_i, c_j\}$ is a linearly dependent set, or

- A contains a set $\{p_i, p_j, p_k\}$ such that $\{c_i, c_j, c_k\}$ is a linearly independent set.

Proof. Follows from Definition 5.1.1 and the fact that Γ is a monotone access structure. ∎

It is clear from Definition 5.1.1 that a set of participants of size two that is not minimally authorized must correspond to a pair of columns that form a linearly independent set with the column associated to the secret. In Theorem 5.1.3 we give the analogous result for sets of participants of size three.

Theorem 5.1.3. Let Γ be an access structure with no equivalent participants that is realizable by the projective plane secret sharing scheme. If $\{p_i, p_j, p_k\} \notin \min \Gamma$, then:

1. $\{c_i, c_j, c_k\}$ is a linearly dependent set if all or none of $\{p_i, p_j\}$, $\{p_i, p_k\}$, and $\{p_j, p_k\}$ are minimally authorized in Γ.

2. $\{c_i, c_j, c_k\}$ is a linearly independent set otherwise.

Proof.

(1) Suppose $\{p_i, p_j, p_k\} \notin \min \Gamma$. We consider two cases:
Case 1: All of $\{p_i, p_j\}, \{p_i, p_k\}$, and $\{p_j, p_k\}$ are minimally authorized.
Suppose $\{p_i, p_j\}, \{p_i, p_k\}, \{p_j, p_k\} \in \min \Gamma$. Then, the sets

$$\{c_0, c_i, c_j\}, \{c_0, c_i, c_k\}, \{c_0, c_j, c_k\}$$

are all linearly dependent. So, the vectors c_0, c_i, c_j, c_k are colinear in $\mathrm{PG}(2, q)$. Thus, each triple of them is linearly dependent, so $\{c_i, c_j, c_k\}$ is a linearly dependent set.

Case 2: None of $\{p_i, p_j\}, \{p_i, p_k\}$, or $\{p_j, p_k\}$ are minimally authorized.
Since none of $\{p_i, p_j\}, \{p_i, p_k\}$, or $\{p_j, p_k\}$ are minimally authorized, by Definition 5.1.1, if $\{c_i, c_j, c_k\}$ was a linearly independent set we would have that $\{p_i, p_j, p_k\}$ is minimally authorized, a contradiction. So $\{c_i, c_j, c_k\}$ is a linearly dependent set.

(2) Suppose $\{p_i, p_j, p_k\} \notin \min \Gamma$. We consider two cases:
Case 1: Exactly one of $\{p_i, p_j\}, \{p_i, p_k\}$, or $\{p_j, p_k\}$ is minimally authorized.
Without loss of generality, suppose $\{p_i, p_j\}$ is minimally authorized. Then $\{c_0, c_i, c_k\}$, and $\{c_0, c_j, c_k\}$ are linearly independent sets and $\{c_0, c_i, c_j\}$ is a linearly dependent set. Since $\{c_0, c_i, c_j\}$ is linearly dependent, we can write

$$c_i = ac_0 + bc_j$$

for nonzero integers a and b. For the sake of contradiction, suppose $\{c_i, c_j, c_k\}$ is a linearly dependent set. Then,

$$c_i = xc_j + yc_k$$

for nonzero integers x and y. Combining these, we get that

$$\begin{aligned} ac_0 + bc_j &= xc_j + yc_k \\ 0 &= (x - b)c_j + yc_k - ac_0. \end{aligned}$$

Since a, b, x, y are nonzero, $x - b$ must also be nonzero, as otherwise the pair of vectors $\{c_0, c_k\}$ would be linearly dependent, which is not allowed by the construction of $\mathrm{PG}(2, q)$. Therefore, $\{c_0, c_j, c_k\}$ is a linearly dependent set, a contradiction. So $\{c_i, c_j, c_k\}$ is a linearly independent set.

Case 2: Exactly two of $\{p_i, p_j\}, \{p_i, p_k\}$, or $\{p_j, p_k\}$ are minimally authorized.
Without loss of generality, suppose that $\{p_i, p_j\}, \{p_i, p_k\} \in \min \Gamma$ and $\{p_j, p_k\} \notin \min \Gamma$. Then $\{p_i, p_j\}, \{p_i, p_k\}$ are in different sets in $\mathcal{D}_2(\Gamma)$ that intersect in the participant p_i, contradicting Theorem 4.3.2. So we cannot have that exactly two of $\{p_i, p_j\}, \{p_i, p_k\}$, or $\{p_j, p_k\}$ are minimally authorized.

∎

Proofs that this scheme meets the correctness and perfect privacy conditions are included in Section 5.3. Similarly to the orthogonal array construction for threshold schemes, the entire array $A_{\mathrm{PG}(2,q)}$ can be posted publicly. Additionally, if the number of participants n is less than $q^2 + q$, the columns of $A_{\mathrm{PG}(2,q)}$ that are not associated with any participant or the secret can be discarded. In this case, the resulting array is an $\mathrm{OA}_q(q^3; 2, n + 1, q)$. We now show that the projective plane secret sharing scheme is equivalent to Brickell's vector space scheme over a vector space with dimension three.

Theorem 5.1.4. Suppose Γ is an access structure with no equivalent participants. Then, Γ is realizable by Brickell's vector space secret sharing scheme over $\mathbb{F}_q^3$ if and only if Γ is realizable by the projective plane secret sharing scheme using $\mathrm{PG}(2, q)$.

Proof. ($\Longrightarrow$) Let Γ be an access structure with no equivalent participants that is realizable by Brickell's vector space secret sharing scheme over $\mathbb{F}_q$ with dimension three. Suppose $s \in \mathbb{F}_q$ is the secret we wish to share. Then we have a vector $a = (s, a_1, a_2)$ and vectors $v_i \in \mathbb{F}_q^3$ for each participant p_i, such that the vectors meet the conditions of Proposition 2.4.1 for Γ. Note that since we assume that no participant is authorized on their own, none of the vectors v_i are a scalar multiple of a.

Proposition 2.4.1 says that the authorized sets are the sets of participants $\{p_{i_1}, \ldots, p_{i_k}\}$ such that $\langle v_{i_1}, \ldots, v_{i_k} \rangle$ contains e_1, and thus we have that the minimally authorized sets of Γ have size two or three. If a minimally authorized set of participants $\{p_{i_1}, p_{i_2}\}$ has size two, then we must have that $\{e_1, v_{i_1}, v_{i_2}\}$ is a linearly dependent set. On the other hand, if $p_{i_1}, p_{i_2}, p_{i_3}$ are a minimally authorized group of participants, then we must have that $e_1 \in \langle v_{i_1}, v_{i_2}, v_{i_3} \rangle$, but e_1 is not in the span of any pair in $\{v_{i_1}, v_{i_2}, v_{i_3}\}$. So $\{v_{i_1}, v_{i_2}, v_{i_3}\}$ must be a linearly independent set.

We then have that the vectors $v_1, \ldots, v_n$ meet the conditions of Definition 5.1.1 for the minimally qualified sets of Γ, and thus we can construct a realization of Γ using the projective plane secret sharing scheme with these vectors as the columns allocated to the participants and e_1 as the column associated to the secret.

($\Longleftarrow$) Let Γ be an access structure with no equivalent participants that is realizable by the projective plane secret sharing scheme using $\mathrm{PG}(2, q)$. Without loss of generality, suppose that the column vector associated to the secret is e_1 and let $c_1, \ldots, c_n$ be the column

vectors associated to the participants $p_1, \ldots, p_n$. This is possible due to the symmetry of $\mathrm{PG}(2, q)$. Then, by Definition 5.1.1, there exists an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$ such that

i) $\{p_{i_1}, p_{i_2}\} \in \min \Gamma$ if and only if $\{e_1, c_{i_1}, c_{i_2}\}$ is a linearly dependent set, and

ii) $\{p_{i_1}, p_{i_2}, p_{i_3}\} \in \min \Gamma$ if and only if $\{c_{i_1}, c_{i_2}, c_{i_3}\}$ is a linearly independent set and no pair of $p_{i_1}, p_{i_2}, p_{i_3}$ is minimally authorized.

Therefore, if a set of two participants $\{p_{i_1}, p_{i_2}\}$ is minimally authorized, we will have that $e_1 \in \langle c_{i_1}, c_{i_2} \rangle$. If a set of three participants $\{p_{i_1}, p_{i_2}, p_{i_3}\}$ is minimally authorized, then e_1 is not in the span of the vectors associated to any pair of $p_{i_1}, p_{i_2}, p_{i_3}$. Since the vectors are in $\mathbb{F}_q^3$, we have that $\{e_1, c_{i_1}, c_{i_2}, c_{i_3}\}$ is a linearly dependent set, and so $e_1 \in \langle c_{i_1}, c_{i_2}, c_{i_3} \rangle$. Additionally, if a set $\{p_{i_1}, \ldots, p_{i_\ell}\}$ of participants is not authorized, then $e_1 \notin \langle c_{i_1}, \ldots, c_{i_\ell} \rangle$, as if e_1 was in this span there would need be a set of two or three participants in $\{p_{i_1}, \ldots, p_{i_\ell}\}$ that is minimally authorized.

So, choosing the vectors $v_1, \ldots, v_n$ to be the columns $c_1, \ldots, c_n$ from the realization using $\mathrm{PG}(2, q)$, we have a set of vectors such that the conditions of Proposition 2.4.1 are met for the access structure Γ, so the access structure is realizable by Brickell's vector space scheme. ∎

5.2 Some Realizable Structures

We now present two access structures realizable by the projective plane secret sharing scheme. The first access structure Γ_1 that we consider has minimally qualified sets

$$\min \Gamma_1 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_5, p_6\}, \{p_1, p_3, p_5\}, \{p_1, p_4, p_6\}, \{p_2, p_3, p_6\}, \{p_2, p_4, p_5\}\}.$$

Based on the minimally qualified sets, we get that the sets $\{c_0, c_1, c_2\}$, $\{c_0, c_3, c_4\}$, and $\{c_0, c_5, c_6\}$ must be linearly dependent, while the sets $\{c_1, c_3, c_5\}$,$\{c_1, c_4, c_6\}$,$\{c_2, c_3, c_6\}$, and $\{c_2, c_4, c_5\}$ must be linearly independent. Additionally, the other sets of columns associated to 3 participants that are not authorized must all be dependent. There are therefore seven sets of three columns that are dependent, which are $\{c_0, c_1, c_2\}$, $\{c_0, c_3, c_4\}$, $\{c_0, c_5, c_6\}$, $\{c_1, c_3, c_6\}$, $\{c_1, c_4, c_5\}$, $\{c_2, c_3, c_5\}$, and $\{c_2, c_4, c_6\}$. These are precisely the circuits of the Fano plane matroid, so this scheme is only realizable if q is a power of 2.

Suppose we wish to share the secret 1 in a domain of secrets with two elements. To do this we use $\mathrm{PG}(2, 2)$. The array $A_{\mathrm{PG}(2,2)}$, as well as the column associations for participants and the shares that are distributed is given in Figure 5.2. Additionally, the randomly chosen row with a 1 in its first column is given in bold in $A_{\mathrm{PG}(2,2)}$.

Suppose the authorized set of participants $\{p_1, p_2, p_3\}$ wishes to reconstruct the secret. They solve the following system for the unknown variables v_1, v_2, v_3:

$$0 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3 = 1$$

$$A_{\mathrm{PG}(2,2)} \simeq \begin{array}{c} \begin{matrix} p_0 & p_1 & p_6 & p_2 & p_3 & p_4 & p_5 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

P	c_{p_i}	s_{p_i}
p_1	$(0,0,1)$	1
p_2	$(1,0,1)$	0
p_3	$(0,1,1)$	0
p_4	$(1,1,1)$	1
p_5	$(1,1,0)$	0
p_6	$(0,1,0)$	1

Figure 5.2: Projective plane scheme for Γ_1

$$0 \cdot v_1 + 0 \cdot v_2 + 1 \cdot v_3 = 0$$
$$1 \cdot v_1 + 1 \cdot v_2 + 1 \cdot v_3 = 0.$$

The unique solution to this system is $(v_1, v_2, v_3) = (1, 1, 0)$. The participants reconstruct the secret as

$$k = 1 \cdot s_{p_1} + 0 \cdot s_{p_2} + 0 \cdot s_{p_3} = 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 0 = 1.$$

On the other hand, suppose the unauthorized group of participants $\{p_1, p_3, p_6\}$ attempts to reconstruct the secret. They attempt to solve the following system for the unknown variables v_1, v_2, v_3:

$$0 \cdot v_1 + 0 \cdot v_3 + 0 \cdot v_6 = 1$$
$$0 \cdot v_1 + 1 \cdot v_3 + 1 \cdot v_6 = 0$$
$$1 \cdot v_1 + 1 \cdot v_3 + 0 \cdot v_6 = 0.$$

This system has no solutions and therefore the participants are not able to reconstruct the secret as a linear combination of their shares.

The second access structure Γ_2 that we realize with our scheme has minimally qualified sets

$$\min \Gamma_2 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_2, p_4, p_5\}\}.$$

Suppose we wish to share the secret 2 in a domain of secrets with three elements. To do this, we use $\mathrm{PG}(2,3)$, and assign five of the twelve possible columns to the participants. In Figure 5.3 we present the array $A_{\mathrm{PG}(2,3)}$, the allocation of participants to columns, and the shares that are distributed. A randomly chosen row with a 2 in the first column is again presented in bold. Note that in this case, we only need to publish and store the columns of the array $A_{\mathrm{PG}(2,3)}$ that are allocated to the secret or a participant.

Suppose that the authorized group of participants $\{p_1, p_3, p_4, p_5\}$ wishes to reconstruct the secret. They solve the following system for the unknown variables v_1, v_3, v_4, v_5:

$$1 \cdot v_1 + 2 \cdot v_3 + 0 \cdot v_4 + 2 \cdot v_5 = 1$$
$$1 \cdot v_1 + 0 \cdot v_3 + 0 \cdot v_4 + 2 \cdot v_5 = 0$$

$$A_{\mathrm{PG}(2,3)} \simeq \begin{array}{c} \begin{array}{cccccccccccccc} p_0 & p_4 & p_2 & & & p_1 & & & & & p_3 & & p_5 \end{array} \\ \left[\begin{array}{cccccccccccccc} 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 \\ 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 \\ 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 \\ 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\ 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 \\ 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 \\ 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 \\ 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 \\ 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 \\ 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 \\ \mathbf{2} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{1} & \mathbf{0} & \mathbf{2} & \mathbf{0} & \mathbf{2} & \mathbf{2} & \mathbf{0} & \mathbf{0} \\ 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 \\ 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \end{array}$$

P	c_{p_i}	s_{p_i}
p_1	$(1,1,2)$	1
p_2	$(0,2,1)$	1
p_3	$(2,0,2)$	2
p_4	$(0,0,2)$	1
p_5	$(2,2,0)$	0

Figure 5.3: Projective plane scheme for Γ_2

$$2 \cdot v_1 + 2 \cdot v_3 + 2 \cdot v_4 + 0 \cdot v_5 = 0.$$

Solving this system we find that (v_1, v_3, v_4, v_5) is either $(0,2,1,0)$, $(1,2,0,1)$, or $(2,2,2,2)$. In all of these cases, we find that the participants reconstruct the secret by computing

$$k = v_1 \cdot s_{p_1} + v_3 \cdot s_{p_3} + v_4 \cdot s_{p_4} + v_5 \cdot s_{p_5} = v_1 + 2v_3 + v_4 = 2.$$

Similarly to the previous example, any group of unauthorized participants will find an unsolvable system. For example, if the group of participants $\{p_1, p_4, p_5\}$ attempted to reconstruct the secret, they would attempt to solve the following system for v_1, v_2, v_3:

$$1 \cdot v_1 + 0 \cdot v_4 + 2 \cdot v_5 = 1$$

$$1 \cdot v_1 + 0 \cdot v_4 + 2 \cdot v_5 = 0$$
$$2 \cdot v_1 + 2 \cdot v_4 + 0 \cdot v_5 = 0$$

This system clearly has no solutions, so they would not be able to solve for the value of the secret.

5.3 Proof that this Scheme is Perfect

We now show that this scheme is perfect. First, we show that a pair of authorized participants is capable of reconstructing the secret.

Proposition 5.3.1. Let Γ be an access structure realizable by the projective plane secret sharing scheme, $\{p_{i_1}, p_{i_2}\}$ be a subset of participants such that $\{p_{i_1}, p_{i_2}\} \in \min \Gamma$, c_0 be the column associated to the secret k, (c_{i_1}, s_{i_1}) be the column and share of participant i_1, and (c_{i_2}, s_{i_2}) be the column and share of participant i_2. Then the following system has a unique solution v_{i_1}, v_{i_2}.

$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2}$$

Moreover, the secret can be reconstructed as $k = v_{i_1} s_{i_1} + v_{i_2} s_{i_2}$.

Proof. Suppose that $\{p_{i_1}, p_{i_2}\} \in \min \Gamma$. Then the set of columns $\{c_0, c_{i_1}, c_{i_2}\}$ is linearly dependent, so we can find $w_0, w_1, w_2 \in \mathbb{F}_q$ such that not all of w_0, w_1 or w_2 are zero and

$$w_0 c_0 = w_1 c_{i_1} + w_2 c_{i_2}. \tag{5.3.1}$$

Additionally, since no two rows are linearly dependent, none of w_0, w_1 or w_2 are zero, as otherwise there would exist a pair of columns that were linearly dependent. Multiplying Equation 5.3.1 by w_0^{-1} and writing $v_{i_1} = w_0^{-1} w_1$ and $v_{i_2} = w_0^{-1} w_2$ we get

$$c_0 = w_0^{-1} w_1 c_{i_1} + w_0^{-1} w_2 c_{i_2}$$
$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2}.$$

So we have that v_1, v_2 is a solution to the system. Let $x, y, z \in \mathbb{F}_q$ be the linear combinations of the rows of $V_{\mathrm{PG}(2,q)}$ that represent the chosen row with the secret in the first column. Then $k = x c_0^{(1)} + y c_0^{(2)} + z c_0^{(3)}$. Since

$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2},$$

we can write

$$\begin{aligned} k &= x(v_{i_1} c_{i_1}^{(1)} + v_{i_2} c_{i_2}^{(1)}) + y(v_{i_1} c_{i_1}^{(2)} + v_{i_2} c_{i_2}^{(2)}) + z(v_{i_1} c_{i_1}^{(3)} + v_{i_2} c_{i_2}^{(3)}) \\ &= v_{i_1}(x c_{i_1}^{(1)} + y c_{i_1}^{(2)} + z c_{i_1}^{(3)}) + v_{i_2}(x c_{i_2}^{(1)} + y c_{i_2}^{(2)} + z c_{i_2}^{(3)}) \\ &= v_{i_1} s_{i_1} + v_{i_2} s_{i_2}. \end{aligned}$$

So we have that the secret k is reconstructed as $k = v_{i_1} s_{i_1} + v_{i_2} s_{i_2}$. ∎

We now prove a similar result for minimally authorized sets of size three.

Proposition 5.3.2. Let Γ be an access structure realizable by the projective plane secret sharing scheme, $\{p_{i_1}, p_{i_2}, p_{i_3}\}$ be a subset of participants such that $\{p_{i_1}, p_{i_2}, p_{i_3}\} \in \min \Gamma$, c_0 be the column associated to the secret k, (c_{i_1}, w_{i_1}) be the column and share of participant i_1, (c_{i_2}, s_{i_2}) be the column and share of participant i_2, and (c_{i_3}, s_{i_3}) be the column and share of participant i_3. Then the following system has a unique solution $v_{i_1}, v_{i_2}, v_{i_3}$.

$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2} + v_{i_3} c_{i_3}$$

Moreover, the secret can be reconstructed as $k = v_{i_1} s_{i_1} + v_{i_2} s_{i_2} + v_{i_3} s_{i_3}$.

Proof. Suppose that $\{p_{i_1}, p_{i_2}, p_{i_3}\} \in \min \Gamma$. Then the following sets of columns are all linearly independent: $\{c_{i_1}, c_{i_2}, c_{i_3}\}$, $\{c_0, c_{i_1}, c_{i_2}\}$, $\{c_0, c_{i_1}, c_{i_3}\}$, and $\{c_0, c_{i_2}, c_{i_3}\}$. So, no combination of two or three of $c_0, c_{i_1}, c_{i_2}, c_{i_3}$ are linearly dependent. Since we are working in a space of dimension 3, the set $\{c_0, c_{i_1}, c_{i_2}, c_{i_3}\}$ is linearly dependent, so we can find $w_0, w_1, w_2, w_3 \in \mathbb{F}_q$ that are not all zero such that

$$w_0 c_0 = w_1 c_{i_1} + w_2 c_{i_2} + w_3 c_{i_3}.$$

Additionally, since no pair or triple of $c_0, c_{i_1}, c_{i_2}, c_{i_3}$ is linearly dependent, we must have that none of w_0, w_1, w_2, w_3 are zero. Writing $v_{i_1} = w_0^{-1} w_1$, $v_{i_2} = w_0^{-1} w_2$, and $v_{i_3} = w_0^{-1} w_3$, we get that

$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2} + v_{i_3} c_{i_3}.$$

So, $v_{i_1}, v_{i_2}, v_{i_3}$ is a solution to the system of equations. Let $x, y, z \in \mathbb{F}_q$ be integers such that when r_1, r_2, r_3 are the first three rows of $A_{\mathrm{PG}(2,q)}$, $xr_1 + yr_2 + zr_3$ is the chosen row with the secret in the first column. Then $k = xc_0^{(1)} + yc_0^{(2)} + zc_0^{(3)}$ and since

$$c_0 = v_{i_1} c_{i_1} + v_{i_2} c_{i_2} + v_{i_3} c_{i_3}$$

we can write

$$\begin{aligned} k &= x(v_{i_1} c_{i_1}^{(1)} + v_{i_2} c_{i_2}^{(1)} + v_{i_3} c_{i_3}^{(1)}) + y(v_{i_1} c_{i_1}^{(2)} + v_{i_2} c_{i_2}^{(2)} + v_{i_3} c_{i_3}^{(2)}) + z(v_{i_1} c_{i_1}^{(3)} + v_{i_2} c_{i_2}^{(3)} + v_{i_3} c_{i_3}^{(3)}) \\ &= v_{i_1}(xc_{i_1}^{(1)} + yc_{i_1}^{(2)} + zc_{i_1}^{(3)}) + v_{i_2}(xc_{i_2}^{(1)} + yc_{i_2}^{(2)} + zc_{i_2}^{(3)}) + v_{i_3}(xc_{i_3}^{(1)} + yc_{i_3}^{(2)} + zc_{i_3}^{(3)}) \\ &= v_{i_1} s_{i_1} + v_{i_2} s_{i_2} + v_{i_3} s_{i_3}. \end{aligned}$$

So we have that the secret k is reconstructed as $k = v_{i_1} s_{i_1} + v_{i_2} s_{i_2} + v_{i_3} s_{i_3}$. ∎

We now combine these to get a result for authorized sets of any size.

Proposition 5.3.3. Let Γ be an access structure realizable by the projective plane secret sharing scheme and let $\{p_{i_1}, \ldots, p_{i_\ell}\}$ be an authorized set of participants. Then any solution to the system of equations

$$c_0 = v_{i_1} c_{i_1} + \cdots + v_{i_\ell} c_{i_\ell}$$

allows the correct reconstruction of the secret as $k = v_{i_1} s_{i_1} + \cdots + v_{i_\ell} s_{i_\ell}$.

Proof. Since $\{p_{i_1}, \ldots, p_{i_\ell}\}$ is an authorized set it contains a subset S such that $|S| = 2$ or 3. By Propositions 5.3.1 and 5.3.2 there is at least one solution $v_{i_1}, \ldots, v_{i_\ell}$ to the system of equations

$$c_0 = v_{i_1}c_{i_1} + \cdots + v_{i_\ell}c_{i_\ell}.$$

Let $x, y, z \in \mathbb{F}_q$ be integers such that when r_1, r_2, r_3 are the first three rows of $A_{\mathrm{PG}(2,q)}$, $xr_1 + yr_2 + zr_3$ is the chosen row with the secret in the first column. Then using these solutions to the system of equations we get that

$$\begin{aligned} k &= x(v_{i_1}c_{i_1}^{(1)} + \cdots + v_{i_\ell}c_{i_\ell}^{(1)}) + y(v_{i_1}c_{i_1}^{(2)} + \cdots + v_{i_\ell}c_{i_\ell}^{(2)}) + z(v_{i_1}c_{i_1}^{(3)} + \cdots + v_{i_\ell}c_{i_\ell}^{(3)}) \\ &= v_{i_1}(xc_{i_1}^{(1)} + yc_{i_1}^{(2)} + zc_{i_1}^{(3)}) + \cdots + v_{i_\ell}(xc_{i_\ell}^{(1)} + yc_{i_\ell}^{(2)} + zc_{i_\ell}^{(3)}) \\ &= v_{i_1}s_{i_1} + \cdots + v_{i_\ell}s_{i_\ell}. \end{aligned}$$

So the participants are able to reconstruct the secret as $k = v_{i_1}s_{i_1} + \cdots + v_{i_\ell}s_{i_\ell}$. ∎

Next, we show that an unauthorized group of participants is not able to learn anything about the secret. To do this we first show that a group of unauthorized participants is not able to find a solution to the system of equations.

Proposition 5.3.4. Let Γ be an access structure realizable by the projective plane secret sharing scheme and let $\{p_{i_1}, \ldots, p_{i_\ell}\}$ be an unauthorized set of participants with columns and shares $\{(c_{i_1}, s_{i_1}), \ldots, \{(c_{i_\ell}, s_{i_\ell})\}\}$. Then the system of equations

$$c_0 = v_{i_1}c_{i_1} + \cdots + v_{i_\ell}c_{i_\ell}$$

has no solutions $v_1, \ldots, v_\ell$.

Proof. We begin by writing our system of equations as an augmented matrix:

$$\left[\begin{array}{cccc|c} c_{i_1}^{(1)} & c_{i_2}^{(1)} & \cdots & c_{i_\ell}^{(1)} & c_0^{(1)} \\ c_{i_1}^{(2)} & c_{i_2}^{(2)} & \cdots & c_{i_\ell}^{(2)} & c_0^{(2)} \\ c_{i_1}^{(3)} & c_{i_2}^{(3)} & \cdots & c_{i_\ell}^{(3)} & c_0^{(3)} \end{array}\right]$$

Since the set of participants is unauthorized, for every set of three different participants $p_{i_a}, p_{i_b}, p_{i_c}$, we have that the set of columns $\{c_{i_a}, c_{i_b}, c_{i_c}\}$ is linearly dependent while the sets of columns $\{c_0, c_{i_a}, c_{i_b}\}$, $\{c_0, c_{i_a}, c_{i_c}\}$, and $\{c_0, c_{i_b}, c_{i_c}\}$ are all linearly independent. So any three columns of coefficient matrix are linearly dependent, however any two rows of the coefficient matrix, along with the last row of the augmented matrix, are linearly independent. So, the original matrix has rank 3 while the augmented matrix has rank 2. Therefore, this system of equations has no solutions. ∎

Next we show that an unauthorized group is unable to get any information about the secret from their shares. The proof of this result follows the proof of a similar result from Lopes de Souza [12].

Proposition 5.3.5 ([12], Theorem 5.2.5)**.** Let $S = \{p_{i_1}, \ldots, p_{i_\ell}\}$ be an unauthorized group of participants in an access structure Γ with columns and shares $\{(c_{i_1}, s_{i_1}), \ldots, \{(c_{i_\ell}, s_{i_\ell})\}\}$ and let $A_{r,i}$ represent the value in row r of the column associated to participant i in $A_{\mathrm{PG}(2,q)}$. Let $R = \{1, \ldots, q^3\}$ represent the rows of $A_{\mathrm{PG}(2,q)}$, labeled in order. Then for any $s_0 \in \mathbb{F}_q$,

$$\frac{|\{r \in R : (A_{r,0}, A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_0, s_{i_1}, \ldots, s_{i_\ell})\}|}{|\{r \in R : (A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_{i_1}, \ldots, s_{i_\ell})\}|} = \frac{1}{q}.$$

Proof. Let n be the number of participants in Γ. As $A_{\mathrm{PG}(2,q)}$ is an $\mathrm{OA}_q(q^3; 2, n+1, q)$, in any two columns of $A_{\mathrm{PG}(2,q)}$ each 2-tuple appears exactly q times. So, for two distinct participants i and j and any two values $a, b \in \mathbb{F}_q$,

$$|\{r \in R : (A_{r,i}, A_{r,j}) = (a, b)\}| = q.$$

Additionally, since there are q^3 columns and q values, with each column containing the same quantity of each value, we have that for any participant i and any value $b \in \mathbb{F}_q$,

$$|\{r \in R : (A_{r,i}) = (b)\}| = q^2.$$

Let $\bar{s} \in \mathbb{F}_q$ be a possible value for the secret. We consider two cases, when $|S| = 1$ and when $|S| \geq 2$.

Case 1: $|S| = 1$. Since our only participant's share is $s_{i_1} \in \mathbb{F}_q$ and $\bar{s} \in \mathbb{F}_q$, we have that

$$\frac{|\{r \in R : (A_{r,0}, A_{r,i_1}) = (s_0, s_{i_1})\}|}{|\{r \in R : (A_{r,i_1}) = (s_{i_1})\}|} = \frac{q}{q^2} = \frac{1}{q}.$$

So the participant is not able to conclude any information about $\bar{s}$.

Case 2: $|S| \geq 2$. Since S is unauthorized, by Proposition 5.1.2, for any three participants $i, j, k \in \{i_1, \ldots, i_\ell\}$ the set $\{c_i, c_j, c_k\}$ is linearly dependent. Furthermore, by construction, for any two participants $i, j \in \{i_1, \ldots, i_\ell\}$ the set $\{c_i, c_j\}$ is linearly independent. So,

$$\{r \in R : (A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_{i_1}, \ldots, s_{i_\ell})\} = \{r \in R : (A_{r,i_1}, A_{r,i_2}) = (s_{i_1}, s_{i_2})\}.$$

On the other hand, by Proposition 5.1.2, for any two participants $i, j \in \{i_1, \ldots, i_\ell\}$ the set $\{c_0, c_i, c_j\}$ is linearly independent. So,

$$\begin{aligned}&\{r \in R : (A_{r,0}, A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_0, s_{i_1}, \ldots, s_{i_\ell})\} \\ &= \{r \in R : (A_{r,0}, A_{r,i_1}, A_{r,i_2}) = (s_0, s_{i_1}, s_{i_2})\}.\end{aligned}$$

Since $\{c_0, c_{i_1}, c_{i_2}\}$ is a linearly independent set, each 2-tuple of elements of $\mathbb{F}_q$ appears q times in the columns c_{i_1} and c_{i_2}, once for each element of $\mathbb{F}_q$ in the column c_0. Therefore, there will be only one row where this happens. Combining these two results, we get that

$$\frac{|\{r \in R : (A_{r,0}, A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_0, s_{i_1}, \ldots, s_{i_\ell})\}|}{|\{r \in R : (A_{r,i_1}, \ldots, A_{r,i_\ell}) = (s_{i_1}, \ldots, s_{i_\ell})\}|}$$

$$= \frac{|\{r \in R : (A_{r,0}, A_{r,i_1}, A_{r,i_2}) = (s_0, s_{i_1}, s_{i_2})\}|}{|\{r \in R : (A_{r,i_1}, A_{r,i_2}) = (s_{i_1}, s_{i_2})\}|}$$
$$= \frac{1}{q}.$$

So the group of participants is not able to conclude any information about $\bar{s}$. ∎

Proposition 5.3.5, along with Proposition 5.3.4, give us the perfect privacy condition, while Proposition 5.3.3 gives us the correctness condition. So our scheme is perfect.

5.4 Extension of the Domain of the Secret

In this scheme we sometimes want to have a large domain of secrets in our realization of an access structure Γ. However, finding column allocations is significantly more difficult as the size of the domain of secrets increases (see Section 6.3). It is possible in this case that we are able to find a realization of the scheme for a smaller size of domain of secrets q. We now show that we can extend this realization to one in a domain of secrets of size q^m.

Let Γ be an access structure that is realizable over a finite field $\mathbb{F}_q$. Suppose that we have a realization of the scheme with $C = \{c_0, c_1, \ldots, c_n\}$ being the set of vectors associated to the secret and each of the participants $p_1, \ldots, p_n$. We construct a $(n+1) \times 3$ subarray of $V_{\mathrm{PG}(2,q)}$ only taking the columns associated to the secret and the participants. We then construct a subarray of $A_{\mathrm{PG}(2,q^m)}$ by taking the $(q^m)^3$ linear combinations of the rows of our subarray of $V_{\mathrm{PG}(2,q)}$ using the elements of the extension field $\mathbb{F}_{q^m}$, by embedding the elements of $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$. Proposition 5.4.1 shows that the linear dependence properties of three vectors in $\mathbb{F}_q^3$ are preserved when we extend $\mathbb{F}_q$ to $\mathbb{F}_{q^m}$, so we have that the same allocation of participants from the realization over $\mathbb{F}_q$ in the new subarray of $A_{\mathrm{PG}(2,q^m)}$ will be a realization over $\mathbb{F}_{q^m}$.

Proposition 5.4.1. Let $\mathbb{F}_q$ be a finite field with $u = (u_0, u_1, u_2)$, $v = (v_0, v_1, v_2)$, and $w = (w_0, w_1, w_2)$ being vectors in $\mathbb{F}_q^3$. Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$, with elements of $\mathbb{F}_{q^m}$ written as polynomials modulo an irreducible polynomial f of degree m over $\mathbb{F}_q$. Define an injection ϕ from $\mathbb{F}_q$ to $\mathbb{F}_{q^m}$ such that $\phi(z) = z + 0x + \cdots + 0x^{m-1}$. Denote

$$\phi\begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \phi(z_0) \\ \phi(z_1) \\ \phi(z_2) \end{pmatrix} = \begin{pmatrix} z_0 + 0x + \cdots + 0x^{m-1} \\ z_1 + 0x + \cdots + 0x^{m-1} \\ z_2 + 0x + \cdots + 0x^{m-1} \end{pmatrix}.$$

Then, the set $\{u, v, w\}$ is linearly independent if and only if the set $\{\phi(u), \phi(v), \phi(w)\}$ is linearly independent in $\mathbb{F}_{q^m}^3$.

Proof. Let u, v, w and ϕ be defined as above.

($\implies$) Suppose $\{u, v, w\}$ is a linearly independent set. Then, there are no non-zero solutions a, b, c over $\mathbb{F}_q$ to

$$au + bv + cw = 0. \tag{5.4.1}$$

Suppose that a', b', c' is a solution to

$$a'\phi(u) + b'\phi(v) + c'\phi(w) = 0$$

over $\mathbb{F}_{q^m}$. Since we are writing the elements of $\mathbb{F}_{q^m}$ as polynomials, we can write a' as $a'_0 + a'_1 x + \cdots + a_{m-1}x^{m-1}$, where $a'_i \in \mathbb{F}_q$ for $i = 0, \ldots, m-1$, and we can write b' and c' in similar forms. Multiplying a', b', and c' through the vectors and considering each term x^i individually, we get the following:

$$\begin{aligned} 0 &= a'_0 u + b'_0 v + c'_0 w \\ 0x &= a'_1 ux + b'_1 vx + c'_1 wx \\ &\vdots \\ 0x^{m-1} &= a'_{m-1} ux^{m-1} + b'_{m-1} vx^{m-1} + c'_{m-1} wx^{m-1}. \end{aligned}$$

Just considering the coefficients in each of these, we get the following equations over $\mathbb{F}_q$:

$$\begin{aligned} 0 &= a'_0 u + b'_0 v + c'_0 w \\ 0 &= a'_1 u + b'_1 v + c'_1 w \\ &\vdots \\ 0 &= a'_{m-1} u + b'_{m-1} v + c'_{m-1} w. \end{aligned}$$

In each of these cases a solution $a'_i, b'_i, c'_i \in \mathbb{F}_q$ is a solution to Equation 5.4.1. So, $a'_i = b'_i = c'_i = 0$ for $i = 0, \ldots, m-1$ and, therefore, a', b', and c' are all the zero polynomial in $\mathbb{F}_{q^m}$. Therefore, any solution to

$$a'\phi(u) + b'\phi(v) + c'\phi(w) = 0 \tag{5.4.2}$$

is nonzero and the set $\{\phi(u), \phi(v), \phi(w)\}$ is linearly independent.

($\Longleftarrow$) Suppose $\{\phi(u), \phi(v), \phi(w)\}$ is a linearly independent set. Then, there are no non-zero solutions a', b', c' to

$$a'\phi(u) + b'\phi(v) + c'\phi(w) = 0$$

over $\mathbb{F}_{q^m}$. Writing these as polynomials and considering just the coefficients we get that

$$\begin{aligned} 0 &= a'_0 u + b'_0 v + c'_0 w \\ 0 &= a'_1 u + b'_1 v + c'_1 w \\ &\vdots \\ 0 &= a'_{m-1} u + b'_{m-1} v + c'_{m-1} w. \end{aligned}$$

Since there are no non-zero solutions a', b', c' to Equation 5.4.2, we have that there exists no non-zero solutions to any of these equations over $\mathbb{F}_q$. Therefore, there is no non-zero solution $a, b, c \in \mathbb{F}_q$ to

$$au + bv + cw = 0.$$

So, $\{u, v, w\}$ is a linearly independent set. ∎

We now connect Proposition 5.4.1 to the projective plane secret sharing scheme in Theorem 5.4.2.

Theorem 5.4.2. Let Γ be an access structure that is realizable by the projective plane secret sharing scheme over a finite field $\mathbb{F}_q$. Then, Γ is realizable by the projective plane secret sharing scheme over $\mathbb{F}_{q^m}$ for any integer $m > 1$.

Proof. Let Γ be an access structure with n participants $p_1, \ldots, p_n$ that is realizable by the projective plane secret sharing scheme over $\mathbb{F}_q$ for some prime power q. Then there exists an allocation of $p_1, \ldots, p_n$ to the vectors of $\mathrm{PG}(2, q)$ meeting the linear dependence conditions of Definition 5.1.1.

Let $m > 1$ be an integer. We construct $\mathrm{PG}(2, q^m)$ by choosing our vectors to represent the 1-dimensional subspaces such that those that we used before in $\mathrm{PG}(2, q)$ are used again. Then, by Proposition 5.4.1, we have that the same allocation of participants to columns in $\mathrm{PG}(2, q^m)$ will meet the conditions of Definition 5.1.1, so Γ is realizable by the projective plane secret sharing scheme over $\mathbb{F}_{q^m}$. ∎

We now present an example of this process using our previous example whose authorized sets gave rise to the dependent sets of the Fano plane. Let Γ be the access structure with

$$\min \Gamma = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_5, p_6\}, \{p_1, p_3, p_5\}, \{p_1, p_4, p_6\}, \{p_2, p_3, p_6\}, \{p_2, p_4, p_5\}\}.$$

Earlier we found a realization of this scheme over $\mathbb{F}_2$ as presented in Figure 5.4

P	Column	c_{p_i}
p_0	1	$(1, 0, 0)$
p_1	2	$(0, 0, 1)$
p_2	4	$(1, 0, 1)$
p_3	5	$(0, 1, 1)$
p_4	6	$(1, 1, 1)$
p_5	7	$(1, 1, 0)$
p_6	3	$(0, 1, 0)$

Figure 5.4: Column allocations over $\mathbb{F}_2$

Suppose we wish to extend this realization to $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$. We begin by building our array $V_{\mathrm{PG}(2,2)}$ as

$$V_{\mathrm{PG}(2,q)} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

We then extend this to a subarray of $A_{\mathrm{PG}(2,4)}$ by taking all linear combinations of the rows of $V_{\mathrm{PG}(2,2)}$ over $\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$ where α is a root of the polynomial $x^2 + x + 1$. The subarray of $A_{\mathrm{PG}(2,4)}$ is presented in Figure 5.5. Due to Proposition 5.4.1, we can allocate each participant to the same column as before to realize the scheme over $\mathbb{F}_4$.

$$
\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & \alpha & 0 & \alpha & \alpha & \alpha & 0 \\
0 & \alpha+1 & 0 & \alpha+1 & \alpha+1 & \alpha+1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & \alpha & 1 & \alpha & \alpha+1 & \alpha+1 & 1 \\
0 & \alpha+1 & 1 & \alpha+1 & \alpha & \alpha & 1 \\
0 & 0 & \alpha & 0 & \alpha & \alpha & \alpha \\
0 & 1 & \alpha & 1 & \alpha+1 & \alpha+1 & \alpha \\
0 & \alpha & \alpha & \alpha & 0 & 0 & \alpha \\
0 & \alpha+1 & \alpha & \alpha+1 & 1 & 1 & \alpha \\
0 & 0 & \alpha+1 & 0 & \alpha+1 & \alpha+1 & \alpha+1 \\
0 & 1 & \alpha+1 & 1 & \alpha & \alpha & \alpha+1 \\
0 & \alpha & \alpha+1 & \alpha & 1 & 1 & \alpha+1 \\
0 & \alpha+1 & \alpha+1 & \alpha+1 & 0 & 0 & \alpha+1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & \alpha & 0 & \alpha+1 & \alpha & \alpha+1 & 1 \\
1 & \alpha+1 & 0 & \alpha & \alpha+1 & \alpha & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & \alpha & 1 & \alpha+1 & \alpha+1 & \alpha & 0 \\
1 & \alpha+1 & 1 & \alpha & \alpha & \alpha+1 & 0 \\
1 & 0 & \alpha & 1 & \alpha & \alpha+1 & \alpha+1 \\
1 & 1 & \alpha & 0 & \alpha+1 & \alpha & \alpha+1 \\
1 & \alpha & \alpha & \alpha+1 & 0 & 1 & \alpha+1 \\
1 & \alpha+1 & \alpha & \alpha & 1 & 0 & \alpha+1 \\
1 & 0 & \alpha+1 & 1 & \alpha+1 & \alpha & \alpha \\
1 & 1 & \alpha+1 & 0 & \alpha & \alpha+1 & \alpha \\
1 & \alpha & \alpha+1 & \alpha+1 & 1 & 0 & \alpha \\
1 & \alpha+1 & \alpha+1 & \alpha & 0 & 1 & \alpha \\
\alpha & 0 & 0 & \alpha & 0 & \alpha & \alpha \\
\alpha & 1 & 0 & \alpha+1 & 1 & \alpha+1 & \alpha \\
\alpha & \alpha & 0 & 0 & \alpha & 0 & \alpha \\
\alpha & \alpha+1 & 0 & 1 & \alpha+1 & 1 & \alpha \\
\alpha & 0 & 1 & \alpha & 1 & \alpha+1 & \alpha+1 \\
\alpha & 1 & 1 & \alpha+1 & 0 & \alpha & \alpha+1 \\
\alpha & \alpha & 1 & 0 & \alpha+1 & 1 & \alpha+1 \\
\alpha & \alpha+1 & 1 & 1 & \alpha & 0 & \alpha+1 \\
\alpha & 0 & \alpha & \alpha & \alpha & 0 & 0 \\
\alpha & 1 & \alpha & \alpha+1 & \alpha+1 & 1 & 0 \\
\alpha & \alpha & \alpha & 0 & 0 & \alpha & 0 \\
\alpha & \alpha+1 & \alpha & 1 & 1 & \alpha+1 & 0 \\
\alpha & 0 & \alpha+1 & \alpha & \alpha+1 & 1 & 1 \\
\alpha & 1 & \alpha+1 & \alpha+1 & \alpha & 0 & 1 \\
\alpha & \alpha & \alpha+1 & 0 & 1 & \alpha+1 & 1 \\
\alpha & \alpha+1 & \alpha+1 & 1 & 0 & \alpha & 1 \\
\alpha+1 & 0 & 0 & \alpha+1 & 0 & \alpha+1 & \alpha+1 \\
\alpha+1 & 1 & 0 & \alpha & 1 & \alpha & \alpha+1 \\
\alpha+1 & \alpha & 0 & 1 & \alpha & 1 & \alpha+1 \\
\alpha+1 & \alpha+1 & 0 & 0 & \alpha+1 & 0 & \alpha+1 \\
\alpha+1 & 0 & 1 & \alpha+1 & 1 & \alpha & \alpha \\
\alpha+1 & 1 & 1 & \alpha & 0 & \alpha+1 & \alpha \\
\alpha+1 & \alpha & 1 & 1 & \alpha+1 & 0 & \alpha \\
\alpha+1 & \alpha+1 & 1 & 0 & \alpha & 1 & \alpha \\
\alpha+1 & 0 & \alpha & \alpha+1 & \alpha & 1 & 1 \\
\alpha+1 & 1 & \alpha & \alpha & \alpha+1 & 0 & 1 \\
\alpha+1 & \alpha & \alpha & 1 & 0 & \alpha+1 & 1 \\
\alpha+1 & \alpha+1 & \alpha & 0 & 1 & \alpha & 1 \\
\alpha+1 & 0 & \alpha+1 & \alpha+1 & \alpha+1 & 0 & 0 \\
\alpha+1 & 1 & \alpha+1 & \alpha & \alpha & 1 & 0 \\
\alpha+1 & \alpha & \alpha+1 & 1 & 1 & \alpha & 0 \\
\alpha+1 & \alpha+1 & \alpha+1 & 0 & 0 & \alpha+1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
$$

Figure 5.5: Subarray of $A_{\mathrm{PG}(2,4)}$ over $\mathbb{F}_4$

5.5 LFSR Generation

We now present a method to generate the array $A_{\mathrm{PG}(2,q)}$ for this scheme using m-sequences. Suppose we wish to share a secret in a domain of size q, where q is a prime power. Let f be an irreducible monic polynomial of degree 3 and let $I \in \mathbb{F}_q^3$ be a vector of initial values. We construct our array $A_{\mathrm{PG}(2,q)}$ using the sub-interval array of the m-sequence $S(f, I)$. Proposition 5.5.1 gives us that each row of the array can be written as a linear combination of the first three rows, allowing us to use it in our scheme. We note that, due to Theorem 1.2.16, we could also use the matrix $A(G_f)$ corresponding to $S(f, I)$.

Proposition 5.5.1. Let $S(f, I) = (a_i)$ be an m-sequence with primitive polynomial f and initial values I. Then, for all $r \geq 0$ we can find $x_0, x_1, x_2 \in \mathbb{F}_q$ such that for all i,

$$a_{i+r} = x_0 a_i + x_1 a_{i+1} + x_2 a_{i+2}.$$

Proof. We use induction on r. If $r = 0$, then we set $x_0 = 1$, $x_1 = 0$, and $x_2 = 0$ and equality holds. We do similarly for $r = 1$ and $r = 2$, setting $x_1 = 1$ or $x_2 = 1$ with the others being set to 0.

Let n be an integer. Suppose that for all $r \leq n$ there exists $x_0, x_1, x_2 \in \mathbb{F}_q$ such that for all i,

$$a_{i+r} = x_0 a_i + x_1 a_{i+1} + x_2 a_{i+2}.$$

We show that there is $x_0', x_1', x_2' \in \mathbb{F}_q$ such that for all i,

$$a_{i+r+1} = x_0' a_i + x_1' a_{i+1} + x_2' a_{i+2}.$$

By the definition of LFSR sequences,

$$a_{i+r+1} = -c_0 a_{i+r} - c_1 a_{i+r-1} - c_2 a_{i+r-2}.$$

By our induction hypothesis, there exists $y_0, y_1, y_2, z_0, z_1, z_2, w_0, w_1, w_2 \in \mathbb{F}_q$ such that

$$\begin{aligned} a_{i+r} &= y_0 a_i + y_1 a_{i+1} + y_2 a_{i+2} \\ a_{i+r-1} &= z_0 a_i + z_1 a_{i+1} + z_2 a_{i+2} \\ a_{i+r-2} &= w_0 a_i + w_1 a_{i+1} + w_2 a_{i+2}. \end{aligned}$$

Substituting these into the definition of the LFSR sequence at a_{i+r+1} then grouping similar terms, we get that

$$a_{i+r+1} = -(c_2 y_0 + c_1 z_0 + c_0 w_0) a_i - (c_2 y_1 + c_1 z_1 + c_0 w_1) a_{i+1} - (c_2 y_2 + c_1 z_2 + c_0 w_2) a_{i+2}.$$

Setting

$$\begin{aligned} x_0' &= -(c_2 y_0 + c_1 z_0 + c_0 w_0) \\ x_1' &= -(c_2 y_1 + c_1 z_1 + c_0 w_1) \\ x_2' &= -(c_2 y_2 + c_1 z_2 + c_0 w_2) \end{aligned}$$

we get that $a_{i+r+1} = x_0' a_i + x_1' a_{i+1} + x_2' a_{i+2}$. ∎

There are two main advantages of using m-sequences to form our array $A_{\mathrm{PG}(2,q)}$. Usually, when we are using this scheme, the dealer needs to store and share all of the vectors in $V_{\mathrm{PG}(2,q)}$ in order to generate the array $A_{\mathrm{PG}(2,q)}$. When using the sub-interval array of an m-sequence, we instead only need to store the primitive polynomial f and the initial values I. These savings become significantly more pronounced as q increases, although there is a tradeoff due to it being difficult to find primitive polynomials for large q. Additionally, by Theorem 1.2.17, the indices in which zeros appear in each row correspond to the indices of the columns which form linearly dependent sets of size three. This allows us to quickly see which pairs of participants could possibly be authorized, as we can find the indices of the pairs of zeros in rows that have a zero in the column associated to the secret.

An example of an array resulting from an m-sequence is given in Figure 5.6. In this example, the m-sequence $S(f, I)$ over $\mathbb{F}_3$ is used, where f is the primitive polynomial $x^3 + x^2+2x+1$ and the initial values I are $(1, 0, 2)$. If we used this array in practice, we would only need to store and share the polynomial f and the initial values I, and we can immediately see that the following pairs of columns are dependent with the column associated with the secret (the first column), and thus they can be associated to a pair of participants that are minimally authorized:

$$\{c_2, c_5\}, \{c_2, c_6\}, \{c_5, c_6\}, \{c_3, c_4\}, \{c_3, c_{11}\}, \{c_4, c_{11}\},$$
$$\{c_1, c_8\}, \{c_1, c_{10}\}, \{c_8, c_{10}\}, \{c_7, c_9\}, \{c_7, c_{12}\}, \{c_9, c_{12}\}.$$

This can possibly reduce the size of the space that we are required to search when we are trying to find an allocation of the participants of an access structure to the columns of the array. However, we do not explore this as a method in this work.

$$\begin{bmatrix}
1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\
0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 \\
2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 \\
0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 \\
2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 \\
2 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
2 & 2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 \\
2 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 \\
2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 \\
1 & 2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 \\
2 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 \\
1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 \\
1 & 0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 \\
0 & 0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 \\
0 & 2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 \\
2 & 1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 \\
1 & 1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 \\
1 & 1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 \\
1 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 \\
2 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 2 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

Figure 5.6: Example array $A_{\mathrm{PG}(2,3)}$ from the m-sequence $S(x^3 + x^2 + 2x + 1, (1, 0, 2))$

Chapter 6

Finding Realizations

In this chapter, we consider some possible methods to find if a realization exists for a particular finite field, in addition to some conditions on the size of field required for a given access structure. In Sections 6.1 and 6.2, we give some different methods to find realizations which use hypergraphs and their incidence graphs. In Section 6.3, we give run time analysis of our implementations of these different methods. In Section 6.4, we give some possible methods to identify which access structures are not realizable, as well as which finite fields, if any, a given access structure might be realizable in. Finally, in Section 6.5, we list all access structures with four, five, and six participants that are realizable by the projective plane secret sharing scheme.

All of the algorithms in this chapter were implemented in the programming language Python using the Galois library to manage operations over finite fields and the NetworkX library to manage graphs. All python code we used is posted online at `https://github.com/mulloyj/mulloyj_masters`.

6.1 Using Hypergraphs

Recall from Section 1.2.5 that hypergraphs are a generalization of graphs allowing edges to contain any number of vertices. We begin by presenting an algorithm for finding an allocation of the participants of an access structure to the columns of the array $A_{\mathrm{PG}(2,q)}$ for some q. To do this, we create two hypergraphs, hypergraph $\mathcal{H}_\Gamma$ corresponding to the access structure, and hypergraph $\mathcal{A}_q$ corresponding to $A_{\mathrm{PG}(2,q)}$. We then identify if there exists an isomorphism mapping $\mathcal{H}_\Gamma$ to an induced subhypergraph of $\mathcal{A}_q$. The corresponding induced subhypergraph isomorphism is then used to assign the participants to columns of $A_{\mathrm{PG}(2,q)}$. We present two algorithms, one that constructs hypergraphs from the access structure itself and one that constructs hypergraphs from the required linear independence properties of the access structure. The method using linear independence is based on the work of Lopes de Souza [12], while the method based on the access structure is first proposed here.

6.1.1 Hypergraphs from the Access Structure

We begin by defining a method to construct a hypergraph $\mathcal{J}(\Gamma)$ from an arbitrary access structure Γ.

Definition 6.1.1. Let Γ be an access structure. We construct a hypergraph $\mathcal{J}(\Gamma)$ associated to Γ with vertex set $\{p_1, \ldots, p_n\}$, and such that $\{p_{i_1}, \ldots, p_{i_\ell}\}$ in $E(\mathcal{J}(\Gamma))$ if and only if $\{p_{i_1}, \ldots, p_{i_\ell}\}$ is a minimally authorized set in Γ.

An example hypergraph associated to the access structure Γ_1 with minimally authorized sets $\min \Gamma_1 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_2, p_4, p_5\}\}$ is presented in Figure 6.1.

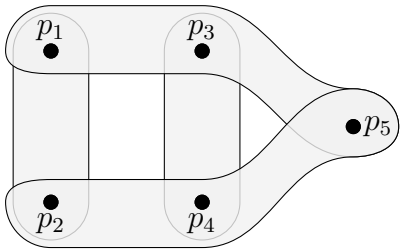


Figure 6.1: Hypergraph $\mathcal{J}(\Gamma_1)$

Next, we show how we can construct an access structure $\Gamma_{\mathbb{F}_q}$ from $\mathrm{PG}(2, q)$. Considering the first column c_0 of $A_{\mathrm{PG}(2,q)}$ to be the column associated with the secret and the remaining $q^2 + q$ columns to be the participants, we define the minimally authorized sets to be the sets of columns that meet the conditions given in Definition 5.1.1. So, a pair of participants is minimally authorized in $\Gamma_{\mathbb{F}_q}$ if their corresponding columns are linearly dependent with c_0 and a triple of participants is minimally authorized in $\Gamma_{\mathbb{F}_q}$ if their corresponding columns are linearly independent and no pair of them is minimally authorized. In the case of $q = 2$ with the same ordering of columns as given in Figure 5.2, we get an access structure $\Gamma_{\mathbb{F}_2}$ with six participants $c_1, \ldots, c_6$ and minimally authorized sets

$$\min \Gamma_{\mathbb{F}_2} = \{\{c_1, c_3\}, \{c_2, c_6\}, \{c_4, c_5\}, \{c_1, c_2, c_5\}, \{c_1, c_4, c_6\}, \{c_2, c_3, c_4\}, \{c_3, c_5, c_6\}\}.$$

Proposition 6.1.2 shows that an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$ that meets the conditions of Definition 5.1.1 corresponds to an induced subhypergraph isomorphism from $\mathcal{J}(\Gamma)$ to $\mathcal{J}(\Gamma_{\mathbb{F}_q})$.

Proposition 6.1.2. Let Γ be an access structure, and let $\mathbb{F}_q$ be a finite field. Suppose $\mathcal{H}_\Gamma = \mathcal{J}(\Gamma)$ and $\mathcal{A}_q = \mathcal{J}(\Gamma_{\mathbb{F}_q})$ are the hypergraphs obtained from Γ and $\Gamma_{\mathbb{F}_q}$ using Definition 6.1.1. Then, an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$ which meets the conditions of Definition 5.1.1 exists if and only if $\mathcal{H}_\Gamma$ is isomorphic to an induced subhypergraph of $\mathcal{A}_q$.

Proof. Suppose $\varphi : \{p_1, \ldots, p_n\} \to \{c_1, \ldots, c_{q^2+q}\}$ is an injective function. Then the result follows from the following chain of equivalences:

φ corresponds to an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$ which meets the conditions of Definition 5.1.1.

$$\Updownarrow$$

φ maps the participants of the minimally qualified sets of Γ to columns of $A_{\mathrm{PG}(2,q)}$ such that a set $\{p_i, p_j\}$ is minimally authorized if and only if $\{c_0, \varphi(p_i), \varphi(p_j)\}$ is a linearly dependent set and a set $\{p_i, p_j, p_k\}$ is minimally authorized if and only if $\{\varphi(p_i), \varphi(p_j), \varphi(p_k)\}$ is linearly independent and no pair from among them is minimally authorized. (These conditions correspond to $\{c_i, c_j\}$ and $\{c_i, c_j, c_k\}$ being minimally authorized in $\Gamma_{\mathbb{F}_q}$.)

$$\Updownarrow$$

The image of φ corresponds to a copy of Γ as a substructure of the access structure $\Gamma_{\mathbb{F}_q}$.

$$\Updownarrow$$

φ is an isomorphism between $\mathcal{H}_\Gamma$ and an induced subhypergraph of $\mathcal{A}_q$.

∎

6.1.2 Hypergraphs from Linear Independence

The second method we use to associate the access structure to a hypergraph uses the required linear dependence properties of the columns to be associated to the participants from Γ using Definition 5.1.1. Define the hypergraph $\mathcal{R}(\Gamma)$ with its vertex set being the set of participants $p_1, \ldots, p_n$, as well as an additional dealer participant p_0, with hyperedges $\{p_{i_1}, p_{i_2}, p_{i_3}\}$ if and only if the columns corresponding to $p_{i_1}, p_{i_2}, p_{i_3}$ are linearly independent by Definition 5.1.1. This is a change to the method of Lopes de Souza [12], where all hyperedges of size two were included to indicate that columns corresponding to pairs of participants are linearly independent. We show in 6.1.3 that this change does not effect the ability of the method to find allocations of participants to columns. For example, the access structure Γ_2 with four participants and minimally authorized sets $\min \Gamma_2 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}\}$ corresponds to the hypergraph $\mathcal{R}(\Gamma)$ with vertex set $V = \{p_0, p_1, p_2, p_3, p_4\}$ and hyperedges

$$E = \{\{p_0, p_1, p_3\}, \{p_0, p_1, p_4\}, \{p_0, p_2, p_3\}, \{p_0, p_2, p_4\}, \{p_0, p_3, p_4\}, \{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}\}.$$

The hyperedges in E correspond to sets of participants whose vectors must be linearly independent.

Next, we construct the hypergraph $\mathcal{R}(A_{\mathrm{PG}(2,q)})$ from $A_{\mathrm{PG}(2,q)}$ in a similar way. The vertex set of $\mathcal{R}(A_{\mathrm{PG}(2,q)})$ is the set of columns of $V_{\mathrm{PG}(2,q)}$, $\{c_0, \ldots, c_{q^2+q}\}$ and a hyperedge $\{c_{i_1}, c_{i_2}, c_{i_3}\}$ exists if and only if $\{c_{i_1}, c_{i_2}, c_{i_3}\}$ is a linearly independent set in $A_{\mathrm{PG}(2,q)}$. We now give the analogue of Proposition 6.1.2 using the linear independence method.

Proposition 6.1.3. Let Γ be an access structure and $\mathbb{F}_q$ be a finite field. Suppose $\mathcal{H}_\Gamma = \mathcal{R}(\Gamma)$ and $\mathcal{A}_q = \mathcal{R}(A_{\mathrm{PG}(2,q)})$ are the hypergraphs obtained from Γ and $A_{\mathrm{PG}(2,q)}$ using the linear independence method. Then, an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$ exists if and only if $\mathcal{H}_\Gamma$ is isomorphic to an induced subhypergraph of $\mathcal{A}_q$ by a mapping that sends $p_0 \in V(\mathcal{H}_\Gamma)$ to $c_0 \in V(\mathcal{A}_q)$.

Proof. Suppose $\varphi : \{p_0, p_1, \ldots, p_n\} \to \{v_0, c_1, \ldots, c_{q^2+q}\}$ is an injective function. Then the result follows from the following chain of equivalences:

φ corresponds to an allocation of the participants of Γ to the columns of $A_{\mathrm{PG}(2,q)}$.

$$\Updownarrow$$

φ maps the participants of Γ to columns of $A_{\mathrm{PG}(2,q)}$ that meet the conditions of Definition 5.1.1.

$$\Updownarrow$$

Minimally qualified sets of the form $\{p_i, p_j\}$ are mapped to columns sets of columns $\{\varphi(p_i), \varphi(p_j)\}$ of $A_{\mathrm{PG}(2,q)}$ which form a linearly dependent set with c_0 and minimally qualified sets of the form $\{p_i, p_j, p_k\}$ are mapped to sets of columns $\{\varphi(p_i), \varphi(p_j), \varphi(p_k)\}$ of $A_{\mathrm{PG}(2,q)}$ which form a linearly independent set of size three. (These conditions correspond to $\{c_i, c_j\}$ and $\{c_i, c_j, c_k\}$ being minimally authorized in $\Gamma_{\mathbb{F}_q}$.)

$$\Updownarrow$$

The image of φ corresponds to columns of $A_{\mathrm{PG}(2,q)}$ that have the same linear dependence and linear independence requirements as Γ.

$$\Updownarrow$$

φ is an isomorphism between $\mathcal{H}_\Gamma$ and an induced subhypergraph of $\mathcal{A}_q$.

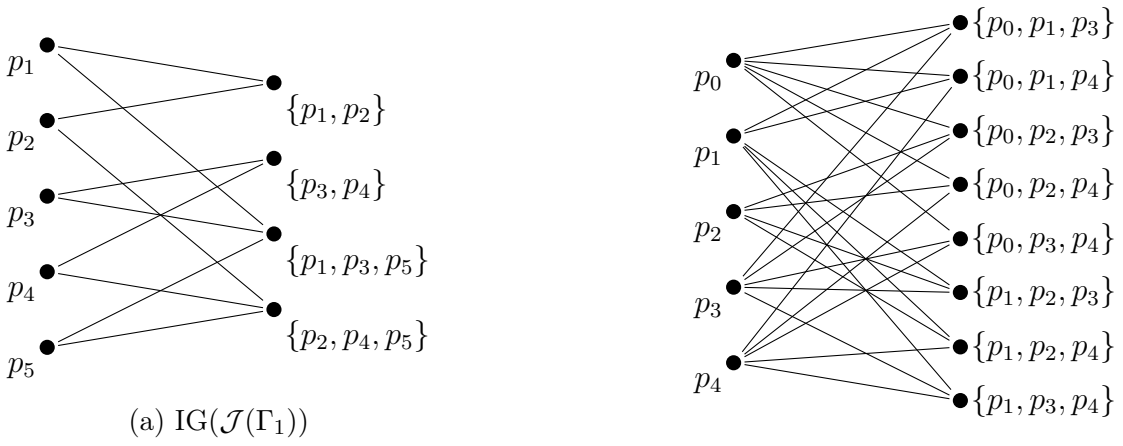
∎

6.2 Converting Subhypergraph Isomorphism

Since software to solve the subgraph isomorphism problem is more readily available than its hypergraph counterpart, we convert our hypergraphs into their incidence graphs, then use those to find our subgraph isomorphisms. The incidence graphs for the hypergraphs resulting from the access structures Γ_1 and Γ_2 from the previous two sections are given in Figure 6.2.

Recall from Section 1.2.5 that the size-coloured incidence graph of a hypergraph $\mathcal{H}$, $\mathrm{IG}^s(\mathcal{H})$, is the coloured graph $(\mathrm{IG}(\mathcal{H}), \pi^+)$ with $\pi^+ = (V_1, V_2^1, \ldots, V_2^n)$ where $V_2^i = \{e \in E(\mathcal{H}) : |e| = i\}$, $1 \leq i \leq n$. In order to convert the subgraph isomorphism problem to the subhypergraph isomorphism problem, we need to use the size-coloured incidence graph. The reason for this is that we need a way to force the isomorphism to map vertices corresponding to hyperedges to those of the same size. We show that we can use subgraph isomorphism to solve the subhypergraph isomorphism problem in Proposition 6.2.1.

Proposition 6.2.1. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be hypergraphs. Then, $\mathcal{H}_1$ is isomorphic to a subhypergraph $\mathcal{H}_2'$ of $\mathcal{H}_2$ if and only if $\mathrm{IG}^s(\mathcal{H}_1)$ is isomorphic to a subgraph G of $\mathrm{IG}^s(\mathcal{H}_2)$.



(a) $\mathrm{IG}(\mathcal{J}(\Gamma_1))$

(b) $\mathrm{IG}(\mathcal{R}(\Gamma_2))$

Figure 6.2: Incidence graphs for $\mathcal{J}(\Gamma_1)$ and $\mathcal{R}(\Gamma_2)$

Proof. Suppose $\mathcal{H}_1 = (V_1, E_1)$ and $\mathcal{H}_2 = (V_2, E_2)$ are hypergraphs with ranks $r(\mathcal{H}_1)$ and $r(\mathcal{H}_2)$. Let $r = \max\{r(\mathcal{H}_1), r(\mathcal{H}_2)\}$. Let $\mathrm{IG}^s(\mathcal{H}_1) = (\mathrm{IG}(\mathcal{H}_1), \pi_1)$ and $\mathrm{IG}^s(\mathcal{H}_2) = (\mathrm{IG}(\mathcal{H}_2), \pi_2)$ be the size-coloured incidence graphs of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively, with colourings $\pi_1 = (V_1, E_1^1, \ldots, E_1^r)$ and $\pi_2 = (V_2, E_2^1, \ldots, E_2^r)$, where some colour classes are possibly empty.

($\implies$) Suppose $\varphi : V_1 \to V_2$ is an isomorphism mapping $\mathcal{H}_1$ to a subhypergraph $\mathcal{H}_2' = (V_2', E_2')$ of $\mathcal{H}_2$. Define $\psi : V_1 \cup E_1 \to V_2' \cup E_2'$ such that

$$\begin{cases} \psi(v) = \varphi(v), & v \in V_1 \\ \psi(\{v_1, \ldots, v_\ell\}) = \{\varphi(v_1), \ldots, \varphi(v_\ell)\}, & \{v_1, \ldots, v_\ell\} \in E_1. \end{cases}$$

Since $\{v, e\} \in E(\mathrm{IG}^s(\mathcal{H}_1))$ if and only if $v \in e$, we have that $\psi(v) \in \psi(e)$. So $\{v, e\} \in E(\mathrm{IG}(\mathcal{H}_1))$ if and only if $\{\psi(v), \psi(e)\} \in \mathrm{IG}(\mathcal{H}_2)$, and thereforee $\mathrm{IG}(\mathcal{H}_1)$ is isomorphic to $\mathrm{IG}(\mathcal{H}_2)$. By construction, we have that for $e \in E_1^i$, $\pi_1(e) = \pi_2(\psi(e))$, as ψ maps sets of size i in E_1 to sets of size i in E_2'. So ψ is an isomorphism from $\mathrm{IG}^s(\mathcal{H}_1)$ to a subgraph of $\mathrm{IG}^s(\mathcal{H}_2)[V_2' \cup E_2']$.

($\impliedby$) Suppose $\psi : V_1 \cup E_1 \to V_2 \cup E_2$ is an isomorphism from $\mathrm{IG}^s(\mathcal{H}_1)$ to a subgraph (G, π_2') of $\mathrm{IG}^s(\mathcal{H}_2)$, where π_2' is the same colouring as π_2 restricted to the vertices of G. Then for $e \in E_1^i$, we have that

$$\pi_1(e) = \pi_2(\psi(e))$$

and so ψ maps sets of size i in E_1 to sets of size i in E_2'. Since ψ is an isomorphism, we have that

$$\{v, e\} \in E(\mathrm{IG}^c(\mathcal{H}_1)) \iff \{\psi(v), \psi(e)\} \in E(G),$$

and from this we conclude that

$$v \in e \iff \psi(v) \in \psi(e).$$

Combining these results, we have that $\{v_1, \ldots, v_\ell\} \in E_1$ if and only if $\psi(\{v_1, \ldots, v_\ell\}) = \{\psi(v_1), \ldots, \psi(v_\ell)\} \in E_2'$. This is the condition for $\mathcal{H}_1$ to be isomorphic to the subhypergraph $\mathcal{H}_2' = (V_2', E_2')$ of $\mathcal{H}_2$. ∎

We now define the *size-coloured complete incidence graph* which we will use to compute induced subhypergraph isomorphisms. Let $\mathcal{H} = (V, E)$ be a hypergraph with rank r and size-coloured incidence graph $\mathrm{IG}^s(\mathcal{H})$, where $\mathrm{IG}^s(\mathcal{H})$ is coloured by $\pi = (V, E^1, \ldots, E^r)$. Define the set $V' = V \cup \binom{V}{1} \cup \cdots \cup \binom{V}{r}$, as well as sets $F^i = \{e \notin E(\mathcal{H}) : |e| = i\}$ for $i = 1, \ldots, r$. Let $\pi' = (V, E^1, \ldots, E^r, F^1, \ldots, F^r)$. The size-coloured complete incidence graph of $\mathcal{H}$, denoted $\mathrm{IG}^+(\mathcal{H})$ is the coloured bipartite graph $(G[V, \binom{V}{1} \cup \cdots \cup \binom{V}{r}], \pi')$, such that for $v \in V$ and $e \in \binom{V}{1} \cup \cdots \cup \binom{V}{r}$, $\{v, e\} \in E(\mathrm{IG}^+(\mathcal{H}))$ if and only if $v \in e$. We show in Proposition 6.2.2 that we can use the size-coloured complete incidence graph to convert induced subhypergraph isomorphisms into subgraph isomorphisms.

Proposition 6.2.2. Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be hypergraphs. Then, $\mathcal{H}_1$ is isomorphic to an induced subhypergraph of $\mathcal{H}_2$ if and only if $\mathrm{IG}^+(\mathcal{H}_1)$ is isomorphic to a subgraph of $\mathrm{IG}^+(\mathcal{H}_2)$.

Proof. Suppose $\mathcal{H}_1 = (V_1, E_1)$ and $\mathcal{H}_2 = (V_2, E_2)$ are hypergraphs with induced incidence graphs $\mathrm{IG}^+(\mathcal{H}_1)$ and $\mathrm{IG}^+(\mathcal{H}_2)$, which are coloured by $\pi_1' = (V_1, E_1^1, \ldots, E_1^k, F_1^1, \ldots, F_1^k)$ and $\pi_2' = (V_2, E_2^1, \ldots, E_2^n, F_2^1, \ldots, F_2^n)$.

($\implies$) Suppose φ is an isomorphism from $\mathcal{H}_1$ to an induced subhypergraph $\mathcal{H}_2' = (V_2', E_2')$ of $\mathcal{H}_2$. Since $\mathcal{H}_2'$ is an induced subhypergraph, we have that it contains all of the edges of $\mathcal{H}_2$ over the vertices in V_2'. Define $\psi : V_1 \cup E_1 \to V_2' \cup E_2'$ such that

$$\begin{cases} \psi(v) = \varphi(v), & v \in V_1 \\ \psi(\{v_1, \ldots, v_\ell\}) = \{\varphi(v_1), \ldots, \varphi(v_\ell)\}, & \{v_1, \ldots, v_\ell\} \in E_1 \cup F_1. \end{cases}$$

By the construction of the induced incidence graph, we have that

$$\{v_1, \ldots, v_\ell\} \notin E_1 \iff \{v_1, \ldots, v_\ell\} \in F_1^\ell.$$

Since φ is an isomorphism from $\mathcal{H}_1$ to $\mathcal{H}_2'$ and $\mathcal{H}_2'$ is an induced subgraph of $\mathcal{H}_2$, we additionally have that

$$\{v_1, \ldots, v_\ell\} \notin E_1 \iff \{\varphi(v_1), \ldots, \varphi(v_\ell)\} \notin E_2' \iff \{\varphi(v_1), \ldots, \varphi(v_\ell)\} \in F_2^\ell.$$

Combining these results we see that

$$\{v_1, \ldots, v_\ell\} \in F_1^\ell \iff \psi(\{v_1, \ldots, v_\ell\}) = \{\varphi(v_1), \ldots, \varphi(v_\ell)\} \in F_2^\ell,$$

so ψ will preserve colours and for any i, $f \in F_1^i$, and $v \in f$,

$$\{v, f\} \in E(\mathrm{IG}^+(\mathcal{H}_1)) \iff \{\psi(v), \psi(f)\} \in E(\mathrm{IG}^+(\mathcal{H}_2')).$$

By the same argument as was used in Proposition 6.2.1, for any i, $e \in E_1^i$, and $v \in e$,

$$\{v, e\} \in E(\mathrm{IG}^+(\mathcal{H}_1)) \iff \{\psi(v), \psi(e)\} \in E(\mathrm{IG}^+(\mathcal{H}_2')).$$

So ψ is an isomorphism from $\mathrm{IG}^+(\mathcal{H}_1)$ to the, not necessarily induced, subgraph $\mathrm{IG}^+(\mathcal{H}_2')$ of $\mathrm{IG}^+(\mathcal{H}_2)$.

($\Longleftarrow$) Suppose ψ is an isomorphism from $\mathrm{IG}^+(\mathcal{H}_1)$ to a subgraph (G, π_2') of $\mathrm{IG}^+(\mathcal{H}_2)$, where π_2' is the same colouring as π_2 restricted to the vertices of G. We claim that $\mathcal{H}_1$ is isomorphic to the induced subhypergraph $\mathcal{H}_2[V(G)]$ of $\mathcal{H}_2$.

Since ψ is an ismorphism of coloured graphs, we have that for $\pi_1'(f) = \pi_2'(\phi(f))$ for all $f \in F_1$. So we have that $f \in F_1^i$ is mapped to $\psi(f) \in F_2^i$. In other words, $f \notin E_1$ if and only if $\psi(f) \notin E_2'$. But, since $\mathrm{IG}^+(\mathcal{H}_1)$ contains all of the possible hyperedges of $\mathcal{H}_1$, G must as well, so we have that $f \notin E_1$ if and only if $\psi(f) \notin E_2$. The fact that $\mathcal{H}_2[V(G)]$ is an induced subhypergraph of $\mathcal{H}_2$ that is isomorphic to $\mathcal{H}_1$ follows from this result and the same argument as was used in Proposition 6.2.1. ∎

We now present two procedures to find allocations of participants to columns of $A_{\mathrm{PG}(2,q)}$; one using the size-coloured incidence graph, and one using the size-coloured complete incidence graph. To compute subgraph isomorphisms we use the "subgraph_is_isomorphic" method of the "GraphMatcher" class in the Python library networkX.

6.2.1 Hybrid Procedure to find a Realization

The first procedure we consider uses the size-coloured incidence graphs to find candidate subgraph isomorphisms, which are then verified to see if they result in an induced subhypergraph. For this reason we refer to this procedure as the *hybrid procedure*.

If we are using the access structure construction of our hypergraphs, then we decide whether an allocation exists in $A_{\mathrm{PG(2,q)}}$ by computing whether $\mathcal{J}(\Gamma)$ is isomorphic to an induced subhypergraph of $\mathcal{J}(\Gamma_{\mathbb{F}_q})$. We do this in the hybrid method by looping through all subgraphs of $\mathrm{IG}^s(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$ which are isomorphic to $\mathrm{IG}^s(\mathcal{J}(\Gamma))$ until we find one which has the property that all of the sets of participants of size two or three that are supposed to be unauthorized in Γ remain unauthorized under the mapping into $\Gamma_{\mathbb{F}_q}$. The graph $\mathrm{IG}^s(\mathcal{J}(\Gamma_1))$ for our previous example is given in Figure 6.3, with the participants coloured red, the authorized sets of size two coloured green, and the authorized sets of size three coloured blue.

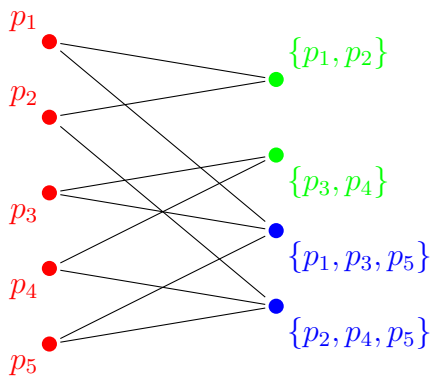


Figure 6.3: Final graph $\mathrm{IG}^s(\mathcal{J}(\Gamma))$ used to find mapping of participants to columns for Γ_1 with the hybrid method

If we are using the linear independence construction of our hypergraphs, then we compute whether an allocation exists in $A_{\mathrm{PG}(2,\mathrm{q})}$ by computing whether $\mathcal{R}(\Gamma)$ is isomorphic to an induced subhypergraph of $\mathcal{R}(A_{\mathrm{PG}(2,\mathrm{q})})$. We do this in the hybrid method by looping through all subgraphs of $\mathrm{IG}^s(\mathcal{R}(A_{\mathrm{PG}(2,\mathrm{q})}))$ which are isomorphic to $\mathrm{IG}^s(\mathcal{R}(\Gamma))$ until we find one (if it exists) that has the property that all of the sets of three columns which are linearly dependent by Definition 5.1.1 remain dependent when mapping into $A_{\mathrm{PG}(2,\mathrm{q})}$. When using the linear independence, we additionally include the requirement that the vertex p_0 in $\mathcal{R}(\Gamma)$ is mapped to the vertex c_0 in $\mathcal{R}(A_{\mathrm{PG}(2,\mathrm{q})})$ in order to have the first column always be allocated to the dealer. We do this by adding an extra colour class to each of $\mathcal{R}(\Gamma)$ and $\mathcal{R}(A_{\mathrm{PG}(2,q)})$ that contains only the vertex p_0 or c_0, respectively. The graph $\mathrm{IG}^s(\mathcal{R}(\Gamma_2))$ for our previous example is given in Figure 6.4 with p_0 coloured purple, the participants coloured red, and the linearly independent sets coloured blue.

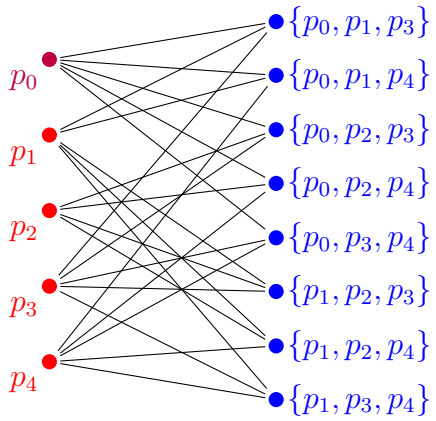


Figure 6.4: Final graph $\mathrm{IG}^s(\mathcal{R}(\Gamma))$ used to find mapping of participants to columns for Γ_2 with the hybrid method

In summary, the **hybrid procedure** to find if a realization exists for some choice of $\mathbb{F}_q$ is as follows:

1. Construct the hypergraph $\mathcal{H}_\Gamma$, where $\mathcal{H}_\Gamma = \mathcal{J}(\Gamma)$ if we are using the access structure or $\mathcal{H}_\Gamma = \mathcal{R}(\Gamma)$ if we are using the linear independence.
2. Construct the hypergraph $\mathcal{A}_q$, where $\mathcal{A}_q = \mathcal{J}(\Gamma_{\mathbb{F}_q})$ if we are using the access structure or $\mathcal{A}_q = \mathcal{R}(A_{\mathrm{PG}(2,q)})$ if we are using the linear independence.
3. Generate the size-coloured incidence graphs $\mathrm{IG}^s(\mathcal{H}_\Gamma)$ and $\mathrm{IG}^s(\mathcal{A}_q)$.
4. Loop through all isomorphisms φ from $\mathrm{IG}^s(\mathcal{H}_\Gamma)$ to a subgraph of $\mathrm{IG}^s(\mathcal{A}_q)$
   (a) If such an isomorphism φ exists, verify if it corresponds to an induced subhypergraph. If it does, return it as the allocation of participants to columns of $A_{\mathrm{PG}(2,q)}$. Otherwise, continue looping.
   (b) If no such isomorphism to a subgraph exists, return that there is no mapping.

6.2.2 Graph Procedure to find a Realization

The second procedure we consider uses the size-coloured complete incidence graphs to find induced subhypergraph isomorphisms. Since any subgraph isomorphism that we find using this procedure will not need an additional verification step at the end of the procedure, as was required in the hybrid variant, we simply refer to this method as the *graph procedure*.

If we are using the access structure construction of our hypergraphs, then we use the size-coloured complete incidence graphs $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ and $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$. By Proposition 6.2.2, $\mathcal{J}(\Gamma)$ is isomorphic to an induced subhypergraph of $\mathcal{J}(\Gamma_{\mathbb{F}_q})$ if and only if $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ is isomorphic to a subgraph of $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$. We can simplify the requirements of this mapping in the following three rules:

1. Participants in $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ are mapped to columns in $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$.
2. Authorized sets of size i in $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ are mapped to authorized sets of size i in $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$, where $i = 2, 3$.
3. Unauthorized sets of size i in $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ are mapped to unauthorized sets of size i in $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$, where $i = 2, 3$.

Due to the nature of these requirements, we can simplify the size-coloured complete incidence graphs $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ and $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$. We do this by removing any authorized sets of size three which are included as vertices in the incidence graphs that are not minimally authorized, as the minimally qualified pair which makes the triple authorized already encodes the required information in the graph. The variant of $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ that we use is exemplified in Figure 6.5 with the participants coloured red, the minimally authorized sets of size two coloured green, the minimally authorized sets of size three coloured blue, the unauthorized sets of size two coloured orange, and the unauthorized sets of size three coloured purple.

If we are using the access structure construction of our hypergraphs, then we use the size-coloured complete incidence graphs $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ and $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$. By Proposition 6.2.2, $\mathcal{J}(\Gamma)$ is isomorphic to an induced subhypergraph of $\mathcal{J}(\Gamma_{\mathbb{F}_q})$ if and only if $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ is isomorphic to a subgraph of $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_q}))$.

If we are using the linear independence construction for our hypergraphs, then we use the size-coloured complete incidence graphs $\mathrm{IG}^+(\mathcal{R}(\Gamma))$ and $\mathrm{IG}^+\mathcal{R}(A_{\mathrm{PG}(2,q)})$. By Proposition 6.2.2, $\mathcal{R}(\Gamma)$ is isomorphic to an induced subhypergraph of $\mathcal{R}(A_{\mathrm{PG}(2,q)})$ if and only if $\mathrm{IG}^+(\mathcal{R}(\Gamma))$ is isomorphic to a subgraph of $\mathrm{IG}^+(\mathcal{R}(A_{\mathrm{PG}(2,q)}))$. Unlike in the case where the graphs were constructed using the access structure, we can not simplify our graph as we need the information of whether each triple of columns is linearly independent or linearly dependent. However, we do add the requirement that p_0 in $\mathcal{R}(\Gamma)$ is mapped to c_0 in $\mathcal{R}(A_{\mathrm{PG}(2,q)})$ by colouring them differently from the other participants. The variant of $\mathrm{IG}^+(\mathcal{J}(\Gamma))$ that we use is exemplified in Figure 6.6 with the participants coloured red, the authorized sets of size two coloured green, the authorized sets of size three coloured blue, the unauthorized sets of size two coloured orange, and the unauthorized sets of size three coloured purple.

In summary, the **graph procedure** to find if a realization exists for some choice of $\mathbb{F}_q$ is as follows:

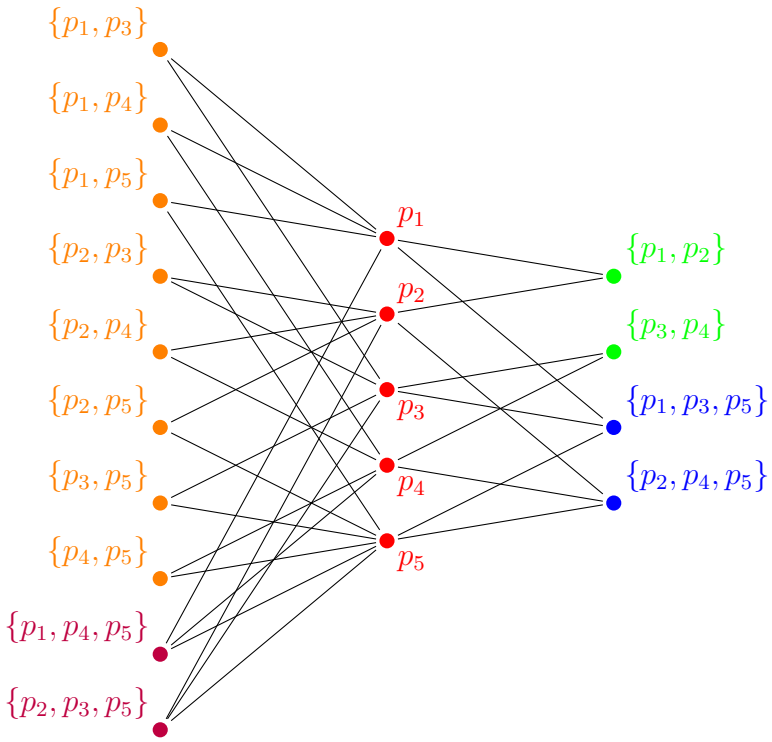


Figure 6.5: Graph for Γ_1 with the minimally authorized sets and all unauthorized sets of size two or three

1. Construct the hypergraph $\mathcal{H}_\Gamma$, where $\mathcal{H}_\Gamma = \mathcal{J}(\Gamma)$ if we are using the access structure or $\mathcal{H}_\Gamma = \mathcal{R}(\Gamma)$ if we are using the linear independence.
2. Construct the hypergraph $\mathcal{A}_q$, where $\mathcal{A}_q = \mathcal{J}(\Gamma_{\mathbb{F}_q})$ if we are using the access structure or $\mathcal{A}_q = \mathcal{R}(A_{\mathrm{PG}(2,q)})$ if we are using the linear independence.
3. Generate the size-coloured complete incidence graphs $\mathrm{IG}^+(\mathcal{H}_\Gamma)$ and $\mathrm{IG}^+(\mathcal{A}_q)$, with the simplifications explained in this section.
4. Find if there exists an isomorphism φ from $\mathrm{IG}^+(\mathcal{H}_\Gamma)$ to a subgraph of $\mathrm{IG}^+(\mathcal{A}_q)$.
   (a) If such an isomorphism φ exists, return it as the allocation of participants to columns of $A_{\mathrm{PG}(2,q)}$.
   (b) If no such isomorphism exists, return that there is no mapping.

6.3 Comparing the Hypergraph Construction Methods

We now compare the access structure and linear independence methods to construct our graphs for four small access structures. We begin with the access structure Γ_1 on five participants, which has minimally qualified sets

$$\min \Gamma_1 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_2, p_4, p_5\}, \{p_1, p_4, p_5\}\}.$$

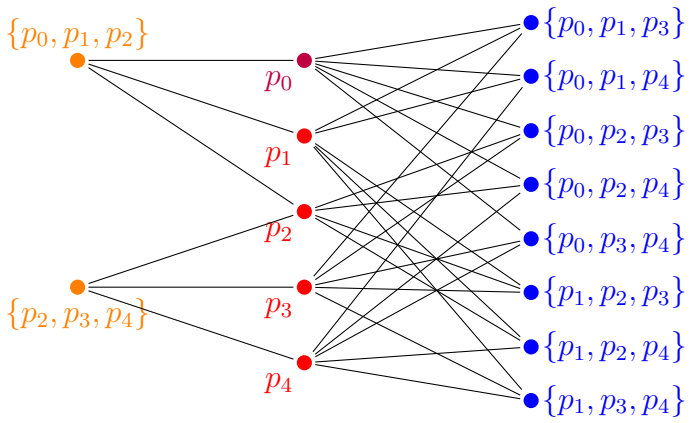


Figure 6.6: Graph for Γ_2 with its requisite linearly dependent and linearly independent sets

Next, we consider Γ_2 also with five participants, which is similar to Γ_1. The minimally qualified sets of Γ_2 are the same as those of Γ_1 with the addition of $\{p_2, p_3, p_5\}$. So,

$$\min \Gamma_2 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_2, p_4, p_5\}, \{p_1, p_4, p_5\}, \{p_2, p_3, p_5\}\}.$$

We then consider two different access structures that give rise to larger graphs, again both with five participants. The first of these is Γ_3 which has minimally qualified sets

$$\min \Gamma_3 = \{\{p_1, p_2\}, \{p_1, p_3\}, \{p_2, p_3\}, \{p_1, p_4, p_5\}, \{p_2, p_4, p_5\}, \{p_3, p_4, p_5\}\}.$$

Finally, we consider Γ_4 whose minimally qualified sets are those of the $(3, 5)$-threshold access structure with $\{p_3, p_4, p_5\}$ removed. So,

$$\begin{aligned}\min \Gamma_4 = \{&\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_5\}, \{p_1, p_3, p_4\}, \{p_1, p_3, p_5\},\\ &\{p_1, p_4, p_5\}, \{p_2, p_3, p_4\}, \{p_2, p_3, p_5\}, \{p_2, p_4, p_5\}\}.\end{aligned}$$

We compare the running time of our methods for these structures in Table 6.1 and Table 6.2. In Table 6.1 we use the graph method to check for isomorphism and in Table 6.2 we use the hybrid method. In both of these tables, the first column (Γ) and second column (q) correspond to an access structure and a possible choice of q to realize that access structure. The next two columns (AS Setup, AS Realization) contain the CPU time required by the implementation to construct the hypergraphs and then to find if a subgraph isomorphism exists for the method using the access structure, respectively. The following two columns (LI Setup, LI Realization) contain the same information for the linear independence method. The final column (S/F) is 'success' if a realization exists for that choice of q with the access structure, and is 'fail' if one does not. In both of these tables, a runtime of 0ns is included if the program ran quicker than our implementation in Python was capable of measuring.

In Table 6.1 we see that the CPU time spent setting up the graphs is about the same regardless of whether the graphs were constructed from the access structures or linear independence. Additionally, we see that in all cases the access structure method identifies if a realization exists, and finds one if it does, quicker than the linear independence method.

Γ	q	AS Setup	AS Realization	LI Setup	LI Realization	S/F
Γ_1	2	1.33s	0ns	1.44s	281ms	fail
Γ_1	3	2.38s	0ns	2.11s	734ms	success
Γ_2	2	1.56s	15.6ms	1.45s	266ms	fail
Γ_2	3	1.86s	3.11s	2.06s	3m 2s	fail
Γ_2	4	2.8s	31.2ms	2.67s	406ms	success
Γ_3	2	1.64s	0ns	1.34s	156ms	fail
Γ_3	3	1.75s	1.16s	1.91s	2m 17s	fail
Γ_3	4	2.81s	15.6ms	2.55s	4.77s	success
Γ_4	2	1.45s	31.2ms	1.53s	109ms	fail
Γ_4	3	2.08s	3.69s	2.06s	1m 56s	fail
Γ_4	4	2.83s	12m 25s	2.48s	3h 16m 38s	fail
Γ_4	5	6.52s	141ms	5.28s	594ms	success

Table 6.1: Runtime of graph method

The most pronounced of these differences is when considering $q = 4$ with Γ_4. In this case, the access structure method identifies that a realization does not exist in 12 minutes 25 seconds, whereas the linear independence method requires 3 hours 16 minutes 38 seconds to identify the same thing, an improvement of about 94%. When we use the Γ_4 as our access structure with $q = 4$ and construct the graphs using the access structure method, we have that $\mathrm{IG}^+(\mathcal{J}(\Gamma_4))$ has 25 vertices and 50 edges, and $\mathrm{IG}^+(\mathcal{J}(\Gamma_{\mathbb{F}_4}))$ has 850 vertices and 2300 edges. On the other hand, constructing the graphs using the linear independence method results in a graph $\mathrm{IG}^+(\mathcal{R}(\Gamma_4))$ with 26 vertices and 60 edges, and a graph $\mathrm{IG}^+(\mathcal{R}(A_{\mathrm{PG}(2,4)}))$ with 1351 vertices and 3990 edges. Sizes of graphs for all cases are given in Table 6.3. This difference in sizes is likely what leads to the difference in runtimes. We now consider the same access structures using the hybrid method in Table 6.2.

Γ	q	AS Setup	AS Realization	LI Setup	LI Realization	S/F
Γ_1	2	672ms	0ns	719ms	234ms	fail
Γ_1	3	953ms	0ns	641ms	562ms	success
Γ_2	2	719ms	0ns	938ms	234ms	fail
Γ_2	3	1.8s	31.2ms	953ms	2m 34s	fail
Γ_2	4	1.02s	15.6ms	1000ms	344ms	success
Γ_3	2	719ms	0ns	797ms	156ms	fail
Γ_3	3	672ms	672ms	797ms	1m 49s	fail
Γ_3	4	1000ms	0ns	1030ms	4.31s	success
Γ_4	2	781ms	0ns	672ms	109ms	fail
Γ_4	3	781ms	2.11s	859ms	1m 46s	fail
Γ_4	4	1080ms	7m 35s	922ms	2h 55m 12s	fail
Γ_4	5	1560ms	109ms	1920ms	656ms	success

Table 6.2: Runtime of hybrid method

In Table 6.2 we see similar results to those of Table 6.1. Again, we see that the setup times are comparable in all cases. Additionally, the access structure method uses less computational resources to find if a realization exists than the linear independence method in all tested cases. This difference is again largest in the case where $q = 4$ with the access structure Γ_4. In this case, the access structure method identifies that no realization exits in 7 minutes 35 seconds, whereas the linear independence method requires 2 hours 55 minutes 12 seconds, an improvement of about 96%. We can see the reason for this difference in the sizes of the graphs. When we use the access structure method with Γ_4 and $q = 4$, the graph $\mathrm{IG}^s(\mathcal{J}(\Gamma_4))$ has 14 vertices and 27 edges and the graph $\mathrm{IG}^s(\mathcal{J}(\Gamma_{\mathbb{F}_4}))$ has 530 vertices and 1500 edges. On the other hand, when we use the linear independence method, the graph $\mathrm{IG}^s(\mathcal{R}(\Gamma_4))$ has 25 vertices and 57 edges and the graph $\mathrm{IG}^s(\mathcal{R}(A_{\mathrm{PG}(2,4)}))$ has 1141 vertices and 3360 edges.

6.3.1 Conclusions from Experiments

We now compare the runtimes of the hybrid and graph methods using the data from Tables 6.1 and 6.2. We see that the hybrid method takes the same amount of time or is quicker than the graph method in all cases except for the case where $q = 5$ with Γ_4. The differences in runtimes however is much less than the difference between the different methods used to construct the graphs. We see that creating the graphs using the access structure with the hybrid method is the quickest, followed by creating the graphs with the access structure and using the graph method. We found that the slowest method is when we form the graphs using the linear independence properties and use the graph method.

The most likely reason for this discrepancy is the size of the graphs used. We present the different sizes of graphs from the methods in Table 6.3. In this table, the first column represents the access structure being considered, which is then followed by the number of vertices and edges in the corresponding graphs when using the access structure with the hybrid method (Hybrid AS), the linear independence method with the hybrid method (Hybrid LI), the access structure with the graph method (Graph AS), and the linear independence method with the graph method (Graph LI). We see that forming the graphs using the access structure results in a smaller graph, irrespective of if we are using the hybrid or graph method.

We see in Table 6.3 that the quickest methods are those that use smaller graphs. We see that the sizes of the graphs are not the same between Γ_1, Γ_2, Γ_3, and Γ_4 when using either construction with the hybrid method or when using the access structure construction with the graph method. However, we see that when we use the linear independence construction with the graph method, the graph always has the same number of vertices and edges. This happens because the number of participants is consistent between the four access structures, and the linear dependence method with the graph method includes every participant and all triples of participants.

From these results it would seem that using the access structures to construct our hypergraphs is quicker regardless of whether the graph or hybrid method is used. This construction keeps the size of the graphs small, with the hybrid method being slightly faster

	Hybrid AS		Hybrid LI		Graph AS		Graph LI	
Γ	Vertices	Edges	Vertices	Edges	Vertices	Edges	Vertices	Edges
Γ_1	10	13	23	51	19	32	26	60
Γ_2	11	16	24	54	19	32	26	60
Γ_3	11	15	22	48	18	29	26	60
Γ_4	14	27	25	57	25	50	26	60
$\Gamma_{\mathbb{F}_2}$	13	18	35	84	29	54	42	105
$\Gamma_{\mathbb{F}_3}$	96	240	247	702	186	456	299	858
$\Gamma_{\mathbb{F}_4}$	530	1500	1141	3360	850	2300	1351	3990
$\Gamma_{\mathbb{F}_5}$	2090	6120	3906	11625	2965	8370	4526	13485
$\Gamma_{\mathbb{F}_7}$	16688	49728	26125	78204	20804	60704	29317	87780

Table 6.3: Graph size comparison between methods

in our experiments. Due to computational resources available to us, we were not able to do these experiments with larger structures. It is therefore possible that when the structure becomes larger, the graph method eclipses the hybrid method as the quicker of the two methods, as it is simply looking directly for the induced isomorphism, rather than checking each isomorphism candidate to verify if it is induced.

6.4 Unrealizable Access Structures

It is possible that a realization does not exist for any choice of q for a given access structure. This happens due to the matroids not being representable over a vector space of dimension three. In this case, we will not be able to identify when to stop using our subhypergraph isomorphism algorithm, as we could just keep trying different values of q. In this section, we explore methods to find if an access structure is not realizable.

6.4.1 Failing $\mathcal{D}_1$ and $\mathcal{D}_2$ Conditions

Suppose Γ is an access structure that we would like to know whether it may be realizable for any q. Recall from Section 4.3.2, that $\mathcal{D}_1(\Gamma)$ is the family of all maximally unqualified subsets of Γ, while $\mathcal{D}_2(\Gamma)$ is the family of maximal subsets X of Γ such that X is a $(2, |X|)$-threshold access structure. By Theorem 4.3.2, if $\mathcal{D}_1(\Gamma)$ contains two sets that intersect in more than one element, or $\mathcal{D}_2(\Gamma)$ contains two sets that intersect, then Γ is not the port of a any matroid with rank-3, and thus it is not realizable by the projective plane secret sharing scheme.

We begin by considering the $\mathcal{D}_1$ condition. Given an access structure Γ with n participants, we believe the problem of verifying if Γ meets the $\mathcal{D}_1$ condition to be quite hard to solve. This is due to the inconsistent nature of the sizes of the subsets in $\mathcal{D}_1$. Even though there are very strict conditions on the sizes of the minimally qualified sets of Γ, the subsets

in $\mathcal{D}_1$ can have any size from 1 to $n-1$. Because of this, it seems that we need to traverse a large portion of the power set of the set of participants in order to find the largest sets that are unauthorized. A visualization of this process for the access structure $\Gamma_{\mathcal{D}_1}$ with minimally qualified sets

$$\min \Gamma_{\mathcal{D}_1} = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_5\}, \{p_1, p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_1, p_4, p_5\}\}$$

is presented in Figure 6.7. In order to simplify the picture, we represent sets of participants by concatenating the indices of their participants. For example, we use 12 to represent the set $\{p_1, p_2\}$. In this graph, each level represents a subset S_i of the power set of $\{1, \ldots, n\}$, such that each set has i participants in it. An edge connects two sets if the lower is a subset of the higher. This is the Hasse diagram of the power set, partially ordered by set inclusion. We have included the access structure $\Gamma_{\mathcal{D}_1}$, with the authorized sets being green, and the unauthorized being red. The minimally authorized sets and the maximally unauthorized sets are underlined in the graph.

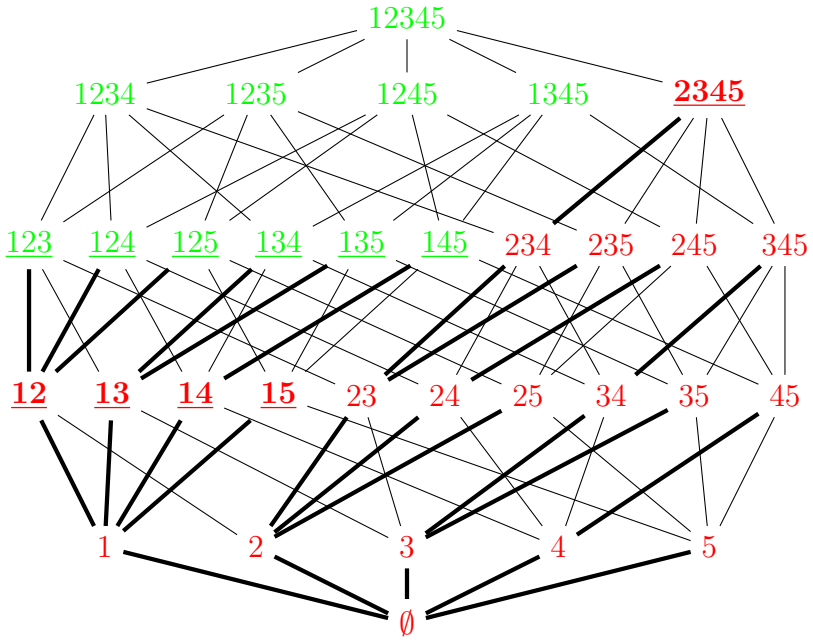


Figure 6.7: Visualization of the access structure $\Gamma_{\mathcal{D}_1}$ with $\mathcal{D}_1(\Gamma_{\mathcal{D}_1})$

In Algorithm 1 we give a backtracking algorithm that computes $\mathcal{D}_1(\Gamma)$ for any access structure Γ. The computational complexity of this algorithm is exponential, although it is more efficient than using brute force. The algorithm computes $\mathcal{D}_1(\Gamma)$ recursively, starting from $\emptyset$ and progressing through the graph. The backtracking tree root is the empty set. The children of a set in the backtracking tree are their supersets obtained by adding a larger element than its largest element. In Figure 6.7 the edges of the backtracking tree are marked in bold. Each time we reach a new set in the graph, we verify whether any of its children that have not already been checked are unauthorized. If any are unauthorized, then we continue on that path. Once we reach a node whose children are all authorized, we verify if any of its supersets that are not children are also authorized, returning that node as a set in $\mathcal{D}_1$ if all of them are.

Algorithm 1 find$\mathcal{D}_1$ Pseudocode

Input: Access structure Γ with participants labelled $1, \ldots, p$, empty array A
Output: Computes $\mathcal{D}_1(\Gamma)$, the set of maximally unqualified sets

```
1: function FIND𝒟1(Γ, 𝒟1, A)
2:     n ← p, max ← max A, ok ← true
3:     for x ∈ {max+1, ..., n} do      ▷ Children are supersets with a new largest element
4:         if A + [x] is not authorized in Γ then
5:             find𝒟1(Γ, A + [x])
6:             ok ← false                          ▷ A is unqualified but not maximally
7:         end if
8:     end for
9:     if ok == true then                                  ▷ If all kids are authorized
10:        for x ∈ {1, ..., max −1} \ A do      ▷ Check if another superset is unauthorized
11:            if A + [x] is not authorized in Γ then
12:                return
13:            end if
14:        end for
15:        𝒟1 ← 𝒟1 ∪ {A}                          ▷ If here, all supersets are authorized
16:    end if
17:    return
18: end function
```

On the other hand, we give a procedure that checks the $\mathcal{D}_2$ condition quickly using connected components of graphs. Given an access structure Γ, we begin by constructing a graph $G_{\mathcal{D}_2}(\Gamma)$ from the minimally authorized sets of size two. The vertices of $G_{\mathcal{D}_2}(\Gamma)$ are all of the participants that are part of at least one minimally authorized set of size two. There exists an edge between two participants if and only if they belong to a minimally authorized set of size two. The following proposition connects $G_{\mathcal{D}_2}(\Gamma)$ to the $\mathcal{D}_2$ condition.

Proposition 6.4.1. Let Γ be an access structure. Then, Γ meets the $\mathcal{D}_2$ condition if and only if the connected components of $G_{\mathcal{D}_2}(\Gamma)$ are all complete graphs.

Proof. ($\Longrightarrow$) Suppose that Γ meets the $\mathcal{D}_2$ condition. Then, for any two sets $X_1, X_2 \in \mathcal{D}_2(\Gamma)$, $X_1 \cap X_2 = \emptyset$. Since each subset $X \in \mathcal{D}_2(\Gamma)$ corresponds to a $(2, |X|)$-threshold scheme, as the subgraph induced by each X, $G_{\mathcal{D}_2}(\Gamma)[X]$ is complete. Each pair of sets $X, Y \in \mathcal{D}_2$ are disjoint, so we have that $G_{\mathcal{D}_2}(\Gamma)[X]$ and $G_{\mathcal{D}_2}(\Gamma)[Y]$ are different connected components of $G_{\mathcal{D}_2}(\Gamma)$. Finally, each edge of $G_{\mathcal{D}_2}(\Gamma)[X]$ lies entirely in one $X \in \mathcal{D}_2(\Gamma)$, so the connected components are all complete.

($\Longleftarrow$) Suppose the connected components of $G_{\mathcal{D}_2}(\Gamma)$ are all complete. Since each of the connected components are complete, each of the vertices in a connected component are adjacent to all other vertices in that component. Each of them are a set in $\mathcal{D}_2(\Gamma)$ and, since each connected components is disconnected from each other connected component, there does not exist $X_1, X_2 \in \mathcal{D}_2(\Gamma)$ such that $|X_1 \cap X_2| > 0$. So, Γ meets the $\mathcal{D}_2$ condition. ∎

In order to verify this condition on $G_{\mathcal{D}_2}(\Gamma)$ for an access structure Γ, we compute the connected components of $G_{\mathcal{D}_2}(\Gamma)$ using depth-first search (DFS). We give the pseudocode for this procedure in Algorithm 2. The algorithm computes the connected components of $G_{\mathcal{D}_2}(\Gamma)$ tracking the number of vertices in each connected component, as well as the number of edges that are traversed. We know that a complete graph with n vertices has $\frac{n(n-1)}{2}$ edges and since each edge is traversed twice, once in each direction, in DFS we check that the half the number of edges traversed is $\frac{n(n-1)}{2}$. If any of them are not complete we return that the access structure fails the $\mathcal{D}_2$ condition, otherwise return that it passes the condition. By Proposition 6.4.1, if we ever find a connected component that is not complete we return that Γ fails the $\mathcal{D}_2$ condition. Since DFS is known to run in $O(n+m)$ time, where n is the number of participants appearing in at least one minimally qualified set and m is the number of minimally qualified sets of size two, and the check to verify if the connected components are complete is also done in $O(n+m)$ time, this algorithm will run in polynomial time. So, this is a practical check that we can run before trying to find a realization of an access structure.

6.4.2 Lower bounds on q from Threshold Substructures

As we saw in Section 4.4, it is possible that an access structure meets the $\mathcal{D}_1$ and $\mathcal{D}_2$ conditions but is not ideal, and thus not realizable by the projective plane secret sharing scheme. In these cases, it is useful to have some conditions on the minimum size of q that allows us to realize certain access structures. For an access structure Γ, we introduce $\mathcal{D}_3(\Gamma)$, the equivalent of $\mathcal{D}_2(\Gamma)$ but with $(3,k)$-threshold substructures. To be precisee, $\mathcal{D}_3(\Gamma)$ is family of maximal subsets $X \subseteq P$ such that $\Gamma(X)$ is the $(3,|X|)$-threshold access structure. We now use $\mathcal{D}_2(\Gamma)$ and $\mathcal{D}_3(\Gamma)$ to find some conditions on the possible q that can be used to realize Γ. First, we give Theorem 6.4.2 where we connect the size of the largest substructure in $\mathcal{D}_2(\Gamma)$ to the possible choices of q that we could make.

Theorem 6.4.2. Let Γ be an access structure and let q be a prime power such that there exists a realization of Γ using $\mathrm{PG}(2,q)$ with the projective plane secret sharing scheme. Then $q \geq \max |S_i|_{S_i \in \mathcal{D}_2(\Gamma)}$.

Proof. Suppose Γ is an access structure that is realizable using the projective plane secret sharing scheme with $\mathrm{PG}(2,q)$ for a prime power q. Let $X \in \mathcal{D}_2(\Gamma)$, i.e. X is a set of participants of a $(2,|X|)$-threshold substructure. Then c_0 and the columns $c_1, c_2, \ldots, c_{|X|}$ corresponding to X are a subspace of $\mathbb{F}_q^3$ of dimension 2. In other words, $c_0, c_1, \ldots, c_{|X|}$ must be contained in a line of $\mathrm{PG}(2,q)$. Since each line has $q+1$ points , $|X| \leq q$. As this is true for every $X \in \mathcal{D}_2(\Gamma)$, the result follows. ∎

Next, we connect the number of substructures in T_2 to the possible choices of q that we could make.

Theorem 6.4.3. Let Γ be an access structure and let q be a prime power such that there exists a realization of Γ using $\mathrm{PG}(2,q)$ with the projective plane secret sharing scheme. Then $|\mathcal{D}_2(\Gamma)| \leq q+1$.

Algorithm 2 check$\mathcal{D}_2$ Pseudocode

Input: Graph $G_{\mathcal{D}_2}(\Gamma)$
Output: Whether or not Γ passes the $\mathcal{D}_2$ condition

```
1: function CHECKD2(G_D2(Γ))
2:     visited ← array of n 0s
3:     for node in G_D2(Γ).nodes do
4:         if visited[node] == 0 then
5:             n ← 0
6:             edgeCount ← 0
7:             Initialize an empty stack
8:             stack.push(node)
9:             while stack is not empty do
10:                current ← stack.pop()
11:                if visited[current] == 0 then
12:                    visited[current] ← 1
13:                    n = n + 1
14:                    for neighbour in G_D2(Γ).neighbours(current) do
15:                        edgeCount = edgeCount + 1
16:                        if visited[neighbour] == 0 then
17:                            stack.push(neighbour)
18:                        end if
19:                    end for
20:                end if
21:            end while
22:            expectedEdges ← n(n−1)/2
23:            if expectedEdges ≠ edgeCount/2 then
24:                return False
25:            end if
26:        end if
27:    end for
28:    return True
29: end function
```

Proof. Suppose Γ is an access structure that is realizable using the projective plane secret sharing scheme with $\mathrm{PG}(2, q)$ for a prime power q. Each set in $\mathcal{D}_2(\Gamma)$ corresponds to a different line of $\mathrm{PG}(2, q)$, with all of them intersecting at the point corresponding to the dealer. Since each point in $\mathrm{PG}(2, q)$ has $q + 1$ lines passing through it, we must have that $|\mathcal{D}_2(\Gamma)| \leq q + 1$. ∎

Finally, we now present Theorem 6.4.4 which connects the size of the largest set in T_3 to the possible choices of q that we could make.

Theorem 6.4.4. Let Γ be an access structure and q be a prime power such that there exists a realization of Γ using $\mathrm{PG}(2, q)$ with the projective plane secret sharing scheme. Let $t_3 = \max |S_i|_{S_i \in \mathcal{D}_3(\Gamma)}$. Then,

i) $q \geq t_3$ if q is odd, and

ii) $q \geq t_3 - 1$ if q is even.

Proof. Suppose Γ is an access structure that is realizable over $\mathbb{F}_q$. For any subset $S \in \mathcal{D}_3(\Gamma)$, by Definition 5.1.1, any triple of the vectors corresponding to the participants S form a linearly independent set. Additionally, any pair of the vectors corresponding to the participants of S along with the vector corresponding to the secret will also form a linearly independent set. Let $A(S)$ be the subarray of $A_{\mathrm{PG}(2,q)}$ with only the columns associated to the participants of S and the dealer. Then, by Theorem 1.2.10, $A(S)$ is an $\mathrm{OA}(q^3; 3, |S| + 1, q)$.

Let t_3 be the largest value such that a $(3, t_3)$-threshold substructure exists in Γ. We now obtain a lower bound on the possible choices of q based on whether an $\mathrm{OA}(q^3; 3, t_3 + 1, q)$ exists. To do this we consider two cases, when q is odd and when q is even.

Case 1: q is odd. Since q is odd, by Theorem 1.2.11, we have that

$$f(q^3, q, 3) = q + 1$$

is an upper bound on the number of columns our orthogonal array must have. So, $q + 1 \geq t_3 + 1$, and thus $q \geq t_3$.

Case 2: q is even. Since q is even, by Theorem 1.2.11, we have that

$$f(q^3, q, 3) = q + 2$$

is an upper bound on the number of columns our orthogonal array must have. So, $q + 2 \geq t_3 + 1$, and thus $q \geq t_3 - 1$. ∎

6.5 Realizable Access Structures from 2-threshold Substructures

The following tables list the access structures that meet the $\mathcal{D}_1$ and $\mathcal{D}_2$ conditions with four, five and six participants. All of these lists contain the possible access structures up to relabeling of participant indices. Additionally, in the tables we include the smallest q for which a realization exists of the access structure. By Theorem 5.4.2 these values represent an infinite family of choices of fields which realize the access structure, $\mathbb{F}_{q^k}$ for all k. We note that we do not list the realizable access structures with less than four participants as they are trivial.

In order to do this we define $T_2(\gamma)$ as the family of all minimally authorized sets of Γ with size two and $T_3(\Gamma)$ as the family of all minimally qualified sets of Γ with size three.

The lists are generated by first finding all possible substructures that could exist in T_2 for a certain number of participants n, then finding all the sets of size three that can be included. We do this by using a program that finds all the possible T_2 substructures, then for each of these finds the minimal number of sets in T_3 that allow the new access structure

to meet the $\mathcal{D}_1$ condition. The remaining access structures (the ones without the minimal number of sets in T_3) are then found by hand.

In the tables, each row represents an access structure Γ that meets $\mathcal{D}_1$ and $\mathcal{D}_2$ conditions, split into the sets in $T_2(\Gamma)$ and $T_3(\Gamma)$. The column labeled q represents the smallest finite field $\mathbb{F}_q$ for which a realization has been found. Again, we use the concatenation of the indices of the participants to represent each of the minimally qualified sets.

We begin with Table 6.4, which contains the realizable access structures with four participants. In addition to the T_2 and T_3 substructures, we also give the set $\mathcal{D}_1$ for each of the access structures. To construct these access structures we start with all of the possible two threshold substructures. We can find these decompositions of the structure into two threshold substructures by looking at the different integer partitions of the total number of participants n. In the case of four participants, this leaves us with the possible partitions

$$\begin{aligned}&4,\\&3+1,\\&2+2,\\&2+1+1, \text{ and}\\&1+1+1+1.\end{aligned}$$

In each of these the integers represent the size of a possible set in $\mathcal{D}_2$, since parts of size one can be ignored as a 2-threshold substructure cannot have only one participant. We note that if an access structure has n participants, then it cannot contain an $(2, n-1)$-threshold substructure, as otherwise there would be a participant that is not part of any minimally authorized set. So the possible 2-threshold substructures, up to isomorphism, are $\{12, 13, 14, 23, 24, 34\}$, $\{12, 34\}$, $\{12\}$, and $\emptyset$. The possible sets in $T_3(\Gamma)$ are then added such that the access structure meets the $\mathcal{D}_1$ condition.

$T_2(\Gamma)$	$T_3(\Gamma)$	q	$\mathcal{D}_1(\Gamma)$
$12, 34$		2	$13, 14, 23, 24$
12	134	2	$13, 14, 234$
12	$134, 234$	3	$13, 14, 23, 24, 34$
$12, 13, 14, 23, 24, 34$		4	$1, 2, 3, 4$
	$123, 124, 134$	3	$12, 13, 14, 234$
	$123, 124, 134, 234$	4	$12, 13, 14, 23, 24, 34$

Table 6.4: All realizable structures with 4 participants

Next, we give the table with all realizable structures with five participants in Table 6.5. In the case of five participants, we have the following partitions:

$$\begin{aligned}&5,\\&4+1,\\&3+2,\\&3+1+1,\end{aligned}$$

$$2+2+1,$$
$$2+1+1+1, \text{ and}$$
$$1+1+1+1+1.$$

After removing the partition with a four threshold, we get that the possible T_2 substructures, up to isomorphism, with five participants are $\{12,13,14,15,23,24,25,34,35,45\}$, $\{12,13,23,45\}$, $\{12,13,23\}$, $\{12,34\}$, $\{12\}$, and $\emptyset$.

$T_2(\Gamma)$	$T_3(\Gamma)$	q
$12,34$	$135,245$	2
$12,34$	$135,245,145$	3
$12,34$	$135,245,145,235$	4
12	$134,135,145$	3
12	$134,135,145,234,235,245$	3
12	$134,135,145,234,235,245,345$	4
$12,13,23,45$		3
$12,13,23$	$145,245$	3
$12,13,23$	$145,245,345$	4
$12,13,14,15,23,24,25,34,35,45$		5
	$123,124,125,134,135,145$	4
	$123,124,125,134,135,235,245,345$	4
	$123,124,125,134,135,145,234,235,245$	5
	$123,124,125,134,135,145,234,235,245,345$	4

Table 6.5: All realizable structures with 5 participants

In Table 6.5 we see an interesting pattern in the structures which have no T_2 substructures. The structures of note are Γ_1 with minimally qualified sets

$$\min\Gamma_1 = \{123,124,125,134,135,145,234,235,245\}$$

and Γ_2 with minimally qualified sets

$$\min\Gamma_2 = \{123,124,125,134,135,145,234,235,245,345\}.$$

We see in the table that, although the minimally qualified sets of Γ_1 are contained in those of Γ_2, the first value of q for which Γ_1 is realizable is $q=5$, whereas Γ_2 is realizable with $q=4$. This is happening because of the underlying dependence structures required to realize both structures. In Γ_2, we have the $(3,5)$-threshold access structure, and so all triples of vectors in the realization form linearly independent sets. By Theorem 6.4.4, a realization exists if an $\mathrm{OA}(4^3;3,6,4)$ exists, which one does. On the other hand, Γ_1 is not a threshold access structure, in it each of the triples of vectors in the realization are linearly independent sets except for those corresponding to the set of participants $\{p_3,p_4,p_5\}$, which must be linearly dependent. This difference results in the underlying structure requiring a larger value of q for the structure to be realized.

The last table we give is Table 6.6 with all of the realizable structures with six participants, up to isomorphism. The possible partitions of the six participants are:

$$
\begin{aligned}
&6,\\
&5+1,\\
&4+2,\\
&4+1+1,\\
&3+3,\\
&3+2+1,\\
&3+1+1+1,\\
&2+2+2,\\
&2+2+1+1,\\
&2+1+1+1+1, \text{ and}\\
&1+1+1+1+1+1.
\end{aligned}
$$

After ignoring the threshold with five participants, we get the possible T_2 substructures listed in Table 6.6.

$T_2(\Gamma)$	$T_3(\Gamma)$	q
$12, 34, 56$	$135, 146, 236, 245$	2
$12, 34, 56$	$135, 136, 146, 236, 245$	3
$12, 34, 56$	$135, 136, 145, 146, 236, 245$	4
$12, 34, 56$	$135, 136, 145, 146, 235, 236, 245$	5
$12, 34, 56$	$135, 136, 145, 146, 235, 236, 245, 246$	4
$12, 34$	$135, 146, 236, 245, 156, 256, 356, 456$	3
$12, 34$	$135, 136, 146, 236, 245, 156, 256, 356, 456$	4
$12, 34$	$135, 136, 145, 146, 236, 245, 156, 256, 356, 456$	5
$12, 34$	$135, 136, 145, 146, 235, 236, 245, 156, 256, 356, 456$	5
$12, 34$	$135, 136, 145, 146, 235, 236, 245, 246, 156, 256, 356, 456$	5
12	$134, 135, 136, 145, 146, 156$	4
12	$134, 136, 145, 156, 234, 235, 246, 256, 345, 346, 356, 456$	4
12	$134, 135, 136, 145, 156, 234, 235, 246, 256, 345, 346, 356, 456$	5
12	$134, 135, 136, 145, 146, 156, 234, 235, 246, 256, 345, 346, 356, 456$	4
12	$134, 135, 136, 145, 146, 156, 234, 235, 236, 246, 256, 345, 346, 356, 456$	5
12	$134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256, 345, 346, 356, 456$	7
$12, 13, 23, 45$	$146, 256, 156, 246, 346$	4
$12, 13, 23, 45$	$146, 256, 156, 246, 346, 356$	5
$12, 13, 23, 45, 46, 56$		3
$12, 13, 23$	$145, 146, 156, 245, 246, 256$	3
$12, 13, 23$	$145, 146, 246, 256, 345, 356, 456$	3
$12, 13, 23$	$145, 146, 156, 246, 256, 345, 356, 456$	4
$12, 13, 23$	$145, 146, 156, 245, 246, 256, 345, 356, 456$	5
$12, 13, 23$	$145, 146, 156, 245, 246, 256, 345, 346, 356, 456$	7
$12, 13, 14, 23, 24, 34, 56$		5
$12, 13, 14, 23, 24, 34$	$156, 256, 356$	5
$12, 13, 14, 23, 24, 34$	$156, 256, 356, 456$	5
$12, 13, 14, 15, 16, 23, 24, 25, 26, 34, 35, 36, 45, 46, 56$		7
	$123, 124, 125, 126, 134, 135, 136, 145, 146, 156$	5
	$123, 124, 125, 126, 134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256$	7
	$124, 125, 126, 134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256, 345, 346, 356$	7
	$123, 124, 125, 126, 134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256, 345, 346, 356$	7
	$123, 124, 125, 126, 134, 135, 136, 145, 146, 156, 234, 235, 236, 245, 246, 256, 345, 346, 356, 456$	7

Table 6.6: All realizable structures with 6 participants

Chapter 7

Conclusion

In this work, we proposed the projective plane secret sharing scheme based on the LFSR secret sharing scheme of Lopes de Souza [12]. Specifically, we reformulated the scheme using matroids in order to simplify the construction. We provided four methods that can be used to find if a realization exists for a certain access structure and choice of q. These methods were based on two methods to construct the hypergraphs, one from the access structure and one from linear independence, and two methods to compute induced subhypergraph isomorphisms, the hybrid method which keeps the size of the graphs small but requires additional checks and the graph method which uses larger graphs but does not require the additional checks. It appears that subgraph isomorphisms obtained from the method of [12] may not correspond to induced hypergraphs. We fix this by introducing the additional checks or using the size-coloured complete incidence graph.

In Chapter 5, we showed that, when using a vector space of dimension three, this scheme is equivalent to the vector space secret sharing scheme of Brickell, and that it is ideal. Additionally, we proved that realizations of access structures using this scheme could be extended from a finite field $\mathbb{F}_q$ to any extension field $\mathbb{F}_{q^k}$, a result which mirrors previous results pertaining to threshold schemes, although the conditions of threshold schemes allow any larger q to be used once a realization is found.

In Chapter 6, we gave a method for converting induced subhypergraph isomorphism into subgraph isomorphism, as well as providing some conditions on potential choices of q that can be used for general access structures. Additionally, we provided algorithms that compute whether an access structure passes the $\mathcal{D}_1$ and $\mathcal{D}_2$ conditions. Finally, we gave a complete list of all access structures which are realizable by the projective plane secret sharing scheme with $n \leq 6$ participants, along with the smallest value of q which realizes them.

We recommend that future research focuses on the following areas:

- **Conditions on q:** We have given some conditions for which q can be used to realize an access structure given its 2-threshold and 3-threshold substructures. A possible question that arises is whether there exist other conditions on the size of finite field required to realize a given access structure.

- **Algorithm for $\mathcal{D}_1$:** We gave an inefficient algorithm to compute $\mathcal{D}_1$ for a given access structure. This algorithm could possibly be improved, likely by verifying the condition while computing $\mathcal{D}_1(\Gamma)$, rather than computing the entirety of $\mathcal{D}_1$ before checking if the condition is met. It could also possibly be done using a connection to packing designs.

- **Algorithm for finding all realizable structures with n participants:** We gave the tables of realizable structures for $n \leq 6$. In finding these, we used a combination of a computer and trial and error. It is likely that there exists an algorithm which computes all the realizable structures with an arbitrary choice n of participants. Possible by a connection to packing designs.

- **Extending the scheme to higher dimesnions:** We have limited ourselves to projective planes in this work and this restriction is the reason why our minimally qualified sets all have size two or three. We believe that exploring the possible extensions of this scheme to higher dimensions could lead to the scheme being generalized to realize any vector space access structure. While we did not explore it in this work, we believe that the scheme will remain perfect when expanding to projective geometries with more dimensions, through the connection from Definition 5.1.1 to the circuits of matroids.

Bibliography

[1] John Stufken A. S. Hedayat, N. J. A. Sloane. *Orthogonal Arrays: Theory and Applications*. Springer Series in Statistics. Springer New York, 1999.

[2] Amos Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Technion, 1996.

[3] Amos Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[4] Josh Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology*, pages 27–35. Springer New York, 1990.

[5] Michael Bertilsson and Ingemar Ingemarsson. A construction of practical secret sharing schemes using linear block codes. In *Advances in Cryptology*, pages 67–79. Springer Berlin Heidelberg, 1993.

[6] G. R. Blakley. Safeguarding cryptographic keys. *International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318, 1979.

[7] A. Bondy and U.S.R. Murty. *Graph Theory*. Graduate Texts in Mathematics. Springer London, 2011.

[8] Ernest F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology — EUROCRYPT '89*, pages 468–475. Springer Berlin Heidelberg, 1990.

[9] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4:123–134, 1991.

[10] K. A. Bush. Orthogonal arrays of index unity. *The Annals of Mathematical Statistics*, 23(3):426 – 434, 1952.

[11] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158, New York, NY, USA, 1971. Association for Computing Machinery.

[12] Rick Lopes de Souza. *Secret sharing schemes with hidden sets and a new secret sharing scheme based on linear feedback shift register sequences*. PhD thesis, Universidade Federal de Santa Catarina, 2019.

[13] S.W. Golomb and G. Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[14] M. Karchmer and A. Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pages 102–111, 1993.

[15] P. Kaski and P.R.J. Östergård. *Classification Algorithms for Codes and Designs*. Algorithms and Computation in Mathematics. Springer Berlin Heidelberg, 2006.

[16] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[17] Jaume Martí-Farré and Carles Padró. Secret sharing schemes on sparse homogeneous access structures with rank three. *The Electronic Journal of Combinatorics*, 11, 10 2004.

[18] Jaume Martí-Farré and Carles Padró. Ideal secret sharing schemes whose minimal qualified subsets have at most three participants. In *Security and Cryptography for Networks*, pages 201–215. Springer Berlin Heidelberg, 2006.

[19] Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. In *Theory of Cryptography*, pages 273–290. Springer Berlin Heidelberg, 2007.

[20] Keith Martin. *Discrete Structures in the Theory of Secret Sharing*. PhD thesis, University of London, 1991.

[21] Lucia Moura, Gary L. Mullen, and Daniel Panario. Finite field constructions of combinatorial arrays. *Designs, Codes, and Cryptography*, 78(1):197–219, 2016.

[22] James Oxley. *Matroid Theory*. Oxford University Press, 02 2011.

[23] Sebastian Raaphorst, Lucia Moura, and Brett Stevens. A construction for strength-3 covering arrays from linear feedback shift register sequences. *Designs, Codes and Cryptography*, 73, 2014.

[24] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[25] Kianoosh Shokri and Lucia Moura. New families of strength-3 covering arrays using linear feedback shift register sequences. *To appear in Journal of Combinatorial Designs*, 2024.

[26] Douglas Stinson. *Combinatorial Designs: Constructions and Analysis*. Springer, New York, 2004.

[27] Douglas Stinson. *Cryptography Theory And Practice*. Discrete Mathematics and Its Applications. CRC-Press, 3rd edition, 2006.