Lecture Notes in Secret Sharing

Carles Padró
Nanyang Technological University, Singapore

Version 2. January 4, 2013

Contents

Preface

These are basically the lecture notes for the short course *Applications of Combinatorics to Information-Theoretic Cryptography*, Central European University, Budapest, May-June 2012. With the objective of covering a full course on secret sharing, additional content will be added in subsequent versions of these lecture notes.

Secret sharing, which was independently introduced in 1979 by Shamir [49] and Blakley [6], is one of the most widely studied topics in information-theoretic cryptography. In a secret sharing scheme, a secret value is distributed into shares among a set of participants is such a way that only some qualified coalitions of participants can recover the secret value from their shares. One can think immediately on possible applications of secret sharing. The first one, proposed by the pioneering authors [6, 49], was safe storage of cryptographic keys. Nevertheless, a number of much less obvious applications of secret sharing to different kinds of cryptographic protocols have appeared. Arguably, the most interesting one is secure multiparty computation [5, 11, 12, 14, 29, 30].

Similarly to other topis in cryptography, research in secret sharing has attracted a lot of attention. Shortly after its introduction, difficult open problems appeared, and the attempts to solve them have involved several areas of mathematics. We focus here mainly on the ones involving matroid theory.

Unfortunately, no textbook on secret sharing has appeared yet, but two excellent surveys [1, 54] are available. The reader is referred to [20, 56] for basic textbooks on cryptography. The textbooks on matroid theory by Oxley [44] and by Welsh [57] may be useful too.

Chapter 1

Basics on Matroid Theory and Information Theory

1.1 Introduction

We present here some basic facts on Matroid Theory and Information Theory that will be used in the other chapters. The reader will find more information about these topics in the textbooks [13, 44, 57]. For a set Q, we notate $\mathcal{P}(Q)$ for the power set of Q, that is, the set of all subsets of Q.

1.2 Matroids and Polymatroids

Definition 1.2.1. A *polymatroid* is a pair (Q, f), where Q is a finite set, and f is a map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

1. $f(\emptyset) = 0$.
2. f is *monotone increasing*: if $A \subseteq B \subseteq Q$, then $f(A) \leq f(B)$.
3. f is *submodular*: $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$ for all $A, B \subseteq Q$.

The set Q and the map f are called, respectively, the *ground set* and the *rank function* of the polymatroid. A polymatroid is said to be *integer* if its rank function is integer-valued.

Definition 1.2.2. A *matroid* M is an integer polymatroid (Q, r) such that $r(A) \leq |A|$ for every $A \subseteq Q$. The *independent sets* of M are the subsets $A \subseteq Q$ with $r(A) = |A|$. The sets that are not independent are called *dependent*. A *basis* is a maximal independent set and a *circuit* is a minimal dependent set.

We presented a definition of matroid in terms of the properties of the rank function. The following propositions provide equivalent definitions that are based, respectively, on the properties of the independent sets, the bases, and the circuits. The proofs for these results can be found, for instance, in the textbook by Oxley [44].

Proposition 1.2.3. *Let Q be a finite set and $\mathcal{I} \subseteq \mathcal{P}(Q)$ a family of subsets. Then $\mathcal{I}$ is the family of the independent sets of a matroid with ground set Q if and only if the following properties are satisfied.*

1. $\emptyset \in \mathcal{I}$.

2. *If $F \in \mathcal{I}$ and $F' \subseteq F$, then $F' \in \mathcal{I}$.*

3. *If F_1 and F_2 are in $\mathcal{I}$ and $|F_1| < |F_2|$, then there exists $x \in F_2 - F_1$ such that $F_1 \cup \{x\} \in \mathcal{I}$.*

Moreover, this matroid is unique since its rank function is determined by $r(A) = \max\{|F| : F \in \mathcal{I}, F \subseteq A\}$.

Proposition 1.2.4. *A family $\mathcal{B} \subseteq \mathcal{P}(Q)$ is the family of bases of a matroid with ground set Q if and only if $\mathcal{B}$ is nonempty and the following* exchange condition *is satisfied.*

- *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 $\mathcal{B}$.*

This matroid is unique because the independent sets are determined by the bases.

Proposition 1.2.5. *A family $\mathcal{C} \subseteq \mathcal{P}(Q)$ is the family of circuits of a matroid with ground set Q if and only if the following conditions are satisfied.*

1. *$\emptyset \notin \mathcal{C}$.*

2. *$\mathcal{C}$ is an antichain, that is, $C_1 \not\subseteq C_2$ if $C_1, C_2 \in \mathcal{C}$ and $C_1 \neq C_2$.*

3. *If $C_1, C_2 \in \mathcal{C}$ are different and $x \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ with $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.*

Since the independent sets are determined by the circuits, this matroid is unique.

1.3 Some Operations on Matroids and Polymatroids

Definition 1.3.1. If $\mathcal{S}_1 = (Q, f_1)$ and $\mathcal{S}_2 = (Q, f_2)$ are polymatroids on the same ground set, then $\mathcal{S}_1 + \mathcal{S}_2 = (Q, f_1 + f_2)$ is clearly a polymatroid, which is called the *sum of the polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$*. Moreover, if c is a positive real number, then $c\mathcal{S}_1 = (Q, cf_1)$ is a polymatroid, which is said to be a *multiple of the polymatroid $\mathcal{S}_1$*.

Definition 1.3.2. For a polymatroid $\mathcal{S} = (Q, f)$ and a set $Z \subseteq Q$, the polymatroids $\mathcal{S} \setminus Z = (Q - Z, f_{\setminus Z})$ and $\mathcal{S}/Z = (Q - Z, f_{/Z})$ are defined, respectively, by $f_{\setminus Z}(A) = f(A)$ and $f_{/Z}(A) = f(A \cup Z) - f(Z)$. Every polymatroid that can be obtained from $\mathcal{S}$ by repeatedly applying these operations is called a *minor* of $\mathcal{S}$. Observe that the minors of a matroid are matroids as well.

Proposition 1.3.3. *For a polymatroid $\mathcal{S}$ with ground set Q and disjoint subsets $Z_1, Z_2 \subseteq Q$, the following properties are satisfied.*

1. *$(\mathcal{S} \setminus Z_1) \setminus Z_2 = \mathcal{S} \setminus (Z_1 \cup Z_2)$ and $(\mathcal{S}/Z_1)/Z_2 = \mathcal{S}/(Z_1 \cup Z_2)$.*

2. *$(\mathcal{S} \setminus Z_1)/Z_2 = (\mathcal{S}/Z_2) \setminus Z_1$.*

As a consequence, every minor of $\mathcal{S}$ is of the form $(\mathcal{S} \setminus Z_1)/Z_2$ for some disjoint sets $Z_1, Z_2 \subseteq Q$.

Definition 1.3.4. If $\mathcal{B}$ is the family of bases of a matroid M on a set Q, then

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

is the family of bases of a matroid M^* (Problem 1.2), which is called the *dual matroid of M*.

Proposition 1.3.5. *The following properties hold for a matroid $M = (Q, r)$.*

1. $M^{**} = M$.
2. *The rank function r^* of the dual matroid M^* is given by $r^*(A) = |A| - r(Q) + r(Q - A)$ for every $A \subseteq Q$.*
3. $(M \setminus Z)^* = M^*/Z$ *and* $(M/Z)^* = M^* \setminus Z$ *for every* $Z \subseteq Q$.

1.4 Linear Representations of Matroids and Polymatroids

Let E be a vector space over a field $\mathbb{K}$ and $(V_i)_{i \in Q}$ a tuple of vector subspaces of E. Then the map $f \colon \mathcal{P}(Q) \to \mathbb{Z}$ defined by $f(X) = \dim \sum_{i \in X} V_i$ for every $X \subseteq Q$ is the rank function of an integer polymatroid $\mathcal{Z}$ with ground set Q. Clearly, $\mathcal{Z}$ is a matroid if $\dim V_i \leq 1$ for every $i \in Q$. Matroids and integer polymatroids that can be defined in this way are said to be $\mathbb{K}$-*linearly representable*, or simply $\mathbb{K}$-*linear* or $\mathbb{K}$-*representable*, and the tuple $(V_i)_{i \in Q}$ is called a $\mathbb{K}$-*linear representation* of $\mathcal{Z}$.

Clearly, a $\mathbb{K}$-linear representation of a matroid M can be seen as a tuple $(v_i)_{i \in Q}$ of vectors in E. If a basis of E is given, this representation can be presented as a matrix G over $\mathbb{K}$ with a one-to-one correspondence between the columns of G and the elements in Q. Each column of G contains the components of the corresponding vector v_i. In particular, this matrix can be seen as a generator matrix of a $\mathbb{K}$-linear code C. All generator matrices of a linear code define the same matroid. Nevertheless, a matroid can be $\mathbb{K}$-linearly represented by inequivalent linear codes.

Theorem 1.4.1. *All minors of a $\mathbb{K}$-linear integer polymatroid are $\mathbb{K}$-linear.*

Proof. Let $\mathcal{Z} = (Q, h)$ be a $\mathbb{K}$-linear integer polymatroid and take $Z \subseteq Q$. Consider a tuple $(V_i)_{i \in Q}$ of vector subspaces of a $\mathbb{K}$-vector space E that linearly represents $\mathcal{Z}$ over $\mathbb{K}$. Obviously, $(V_i)_{i \in Q - Z}$ is a $\mathbb{K}$-linear representation of $\mathcal{Z} \setminus Z$. Take $V_Z = \sum_{i \in Z} V_i$ and, for every $i \in Q - Z$, the vector subspace $W_i = (V_i + V_Z)/V_Z$ of E/V_Z. Then $(W_i)_{i \in Q - Z}$ is a $\mathbb{K}$-linear representation of $\mathcal{Z}/Z$. □

Theorem 1.4.2. *If a linear code C linearly represents the matroid M over $\mathbb{K}$, then the dual code $C^\perp$ is a $\mathbb{K}$-linear representation of the dual matroid M^*. Therefore, the dual of a $\mathbb{K}$-linear matroid is $\mathbb{K}$-linear too.*

The multiples of $\mathbb{K}$-linear polymatroids are said to be $\mathbb{K}$-*poly-linear*. Observe that a matroid $M = (Q, r)$ is $\mathbb{K}$-poly-linear if and only if there exists a positive integer c such that the integer polymatroid $cM = (Q, cr)$ is $\mathbb{K}$-linear.

1.5 Shannon Entropy

Definition 1.5.1. Let X be a discrete random variable on a finite set E. The *Shannon entropy* (or simply *entropy*) of X is

$$H(X) = -\sum_{x \in E} \mathrm{p}(x) \log \mathrm{p}(x)$$

where the binary logarithm is considered, and we take $\mathrm{p}(x) \log \mathrm{p}(x) = 0$ if $\mathrm{p}(x) = 0$.

Lemma 1.5.2. ***Jensen's inequality.*** *Let $I \subset \mathbb{R}$ be an interval and $f\colon I \to \mathbb{R}$ a strictly convex function. Then,*

$$f\left(\sum_{i=1}^{k} \lambda_i x_i\right) \leq \sum_{i=1}^{k} \lambda_i f(x_i)$$

for every $x_1, \ldots, x_k \in I$ and $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ with $0 < \lambda_i < 1$ and $\lambda_1 + \cdots + \lambda_k = 1$. The equality holds if and only if $x_1 = \cdots = x_k$.

Proof. Since f is a strictly convex function, for every $x_1, x_2 \in I$, the segment

$$((1-\lambda)x_1 + \lambda x_2, (1-\lambda)f(x_1) + \lambda f(x_2)), \quad 0 \leq \lambda \leq 1$$

lies over the graph of f. That is, $f((1-\lambda)x_1 + \lambda x_2) \leq (1-\lambda)f(x_1) + \lambda f(x_2)$ if $0 \leq \lambda \leq 1$, while the equality holds only if $x_1 = x_2$ or $\lambda = 0, 1$. This proves the lemma for the case $k = 2$. The proof is concluded by induction on k. Consider $x_1, \ldots, x_k$ and $\lambda_1, \ldots, \lambda_k$ in the required conditions. For $i = 1, \ldots, k-1$, take $\mu_i = \lambda_i/(1-\lambda_k)$. Consider as well $y_1 = \sum_{i=1}^{k-1} \mu_i x_i$ and $y_2 = x_k$. Then, by the induction hypothesis,

$$\begin{aligned} f\left(\sum_{i=1}^{k} \lambda_i x_i\right) &= f((1-\lambda_k)y_1 + \lambda_k y_2) \\ &\leq (1-\lambda_k)f(y_1) + \lambda_k f(y_2) \\ &\leq (1-\lambda_k)\sum_{i=1}^{k-1} \mu_i f(x_i) + \lambda_k f(x_k) = \sum_{i=1}^{k} \lambda_i f(x_i). \end{aligned}$$

Clearly, the equality holds if and only if $x_1 = \cdots = x_k$. □

Proposition 1.5.3. *For a discrete random variable X on a set E, the following properties hold.*

- $0 \leq H(X) \leq \log |E|$.
- $H(X) = 0$ *if and only if there exists* $x_0 \in E$ *with* $\mathrm{p}(x_0) = 1$.
- $H(X) = \log |E|$ *if and only if* $\mathrm{p}(x) = 1/|E|$ *for every* $x \in E$.

Proof. Clearly, $H(X) \geq 0$, and $H(X) > 0$ if $0 < \mathrm{p}(x) < 1$ for some $x \in E$. Applying Lemma 1.5.2 to the strictly convex function $f(x) = -\log x$,

$$H(X) = \sum_{x \in E, \mathrm{p}(x) \neq 0} \mathrm{p}(x) \log\left(\frac{1}{\mathrm{p}(x)}\right) \leq \log\left(\sum_{x \in E, \mathrm{p}(x) \neq 0} \frac{\mathrm{p}(x)}{\mathrm{p}(x)}\right) \leq \log |E|$$

and the equality holds if and only if $\mathrm{p}(x) = 1/|E|$ for every $x \in E$. □

If X and Y are two random variables on the sets E and F, respectively, we can consider the entropy of the random variable (X, Y) on the set $E \times F$:

$$H(XY) = -\sum_{(x,y) \in E \times F} \mathrm{p}(x, y) \log \mathrm{p}(x, y).$$

In addition, for every $y \in F$, we can consider the random variable $X|Y = y$ on the set E and its entropy:

$$H(X|Y = y) = -\sum_{x \in E} \mathrm{p}(x|y) \log \mathrm{p}(x|y).$$

The conditional entropy is defined by taking the average of this quantity on the set F.

Definition 1.5.4. Let X and Y be random variables on the sets E and F, respectively. The *conditional entropy of X with respect to Y* is defined as:

$$H(X|Y) = -\sum_{y\in F} \mathrm{p}(y) \left(\sum_{x\in E} \mathrm{p}(x|y) \log \mathrm{p}(x|y) \right).$$

Proposition 1.5.5. *The following properties hold for every two random variables X and Y.*

1. $0 \leq H(X|Y) \leq H(X)$.
2. $H(X|Y) = 0$ *if and only if for every* $y \in F$ *there exists* $x \in E$ *with* $\mathrm{p}(x|y) = 1$.
3. $H(X|Y) = H(X)$ *if and only if the random variables X and Y are independent.*
4. $H(XY) = H(Y) + H(X|Y) = H(X) + H(Y|X)$.

Proof. Clearly, $H(X|Y) \geq 0$. In addition, $H(X|Y) = 0$ if and only if $H(X|Y = y) = -\sum_{x\in E} \mathrm{p}(x|y) \log \mathrm{p}(x|y) = 0$ for every $y \in F$. Observe that the function $f(x) = x \log x$ is strictly convex. Then, by Lemma 1.5.2,

$$\begin{aligned} H(X|Y) &= -\sum_{x\in E} \sum_{y\in F} \mathrm{p}(y)\mathrm{p}(x|y) \log \mathrm{p}(x|y) \\ &\leq -\sum_{x\in E} \left(\sum_{y\in F} \mathrm{p}(y)\mathrm{p}(x|y) \right) \log \left(\sum_{y\in F} \mathrm{p}(y)\mathrm{p}(x|y) \right) \\ &= -\sum_{x\in E} \mathrm{p}(x) \log \mathrm{p}(x) = H(X). \end{aligned}$$

The equality holds if and only if, for every $x \in E$, the value $\mathrm{p}(x|y)$ is constant, that is, $\mathrm{p}(x|y) = \mathrm{p}(x)$ for every $y \in F$. A straightforward calculation proves the fourth property. □

Proposition 1.5.6. *Let X, Y and Z be random variables. Then $H(X|YZ) \leq H(X|Y)$.*

Proof. We proceed in a similar way as in the proof of Proposition 1.5.5.

$$\begin{aligned} H(X|YZ) &= -\sum_{x\in E} \sum_{(y,z)\in F\times G} \mathrm{p}(y,z)\mathrm{p}(x|yz) \log \mathrm{p}(x|yz) \\ &= -\sum_{x\in E} \sum_{y\in F} \mathrm{p}(y) \sum_{z\in G} \mathrm{p}(z|y)\mathrm{p}(x|yz) \log \mathrm{p}(x|yz) \\ &\leq -\sum_{x\in E} \sum_{y\in F} \mathrm{p}(y) \left(\sum_{z\in G} \mathrm{p}(z|y)\mathrm{p}(x|yz) \right) \log \left(\sum_{z\in G} \mathrm{p}(z|y)\mathrm{p}(x|yz) \right) \\ &= -\sum_{x\in E} \sum_{y\in F} \mathrm{p}(y)\mathrm{p}(x|y) \log \mathrm{p}(x|y) = H(X|Y). \end{aligned}$$

□

For a finite set Q, consider a family of random variables $(S_i)_{i\in Q}$, where S_i is defined on a set E_i. For every $A \subseteq Q$, we use S_A to denote the random variable $(S_i)_{i\in A}$ on the set $\prod_{i\in A} E_i$, and $H(S_A)$ will denote its Shannon entropy. Fujishige [27, 28] found out the following connection between Shannon entropy and polymatroids.

Theorem 1.5.7. *Let $(S_i)_{i\in Q}$ be a family of random variables. Consider the mapping $h\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(\emptyset) = 0$ and $h(A) = H(S_A)$ if $\emptyset \neq A \subseteq Q$. Then h is the rank function of a polymatroid with ground set Q.*

Proof. If $A \subseteq B \subseteq Q$, then $h(B) = H(S_B) = H(S_A S_{B-A}) = H(S_A) + H(S_{B-A}|S_A) \geq H(S_A) = h(A)$. Finally, for every two subsets $A, B \subseteq Q$,

$$\begin{aligned} h(A \cup B) &= H(S_A) + H(S_{B-A}|S_A) \\ &\leq H(S_A) + H(S_{B-A}|S_{A\cap B}) \\ &= H(S_A) + H(S_B) - H(S_{A\cap B}) \\ &= h(A) + h(B) - h(A \cap B), \end{aligned}$$

where the inequality is a consequence of Proposition 1.5.6. □

Because of this connection between polymatroids and the Shannon entropy, and by analogy to the conditional entropy, for a polymatroid $\mathcal{S} = (Q, f)$, we write $f(X|Y) = f(X \cup Y) - f(Y)$. Clearly,

$$f(A_1 \cup \cdots \cup A_r) = \sum_{i=1}^{r} f(A_i|A_1 \cup \cdots \cup A_{i-1}) \tag{1.1}$$

for all $A_1, \ldots, A_r \subseteq Q$. Obviously, $f(X|Y) \geq 0$ and submodularity implies that $f(X|Y) \geq f(X|Y \cup Z)$. Moreover, $f(X|Y \cup Z) = f(X|Y)$ if $f(Z|Y) = 0$. Indeed, this is a consequence of the equality $f(Z|Y) + f(X|Y \cup Z) = f(X|Y) + f(Z|X \cup Y)$.

1.6 Entropic Polymatroids

We saw in Section 1.4 that some integer polymatroids admit linear representations, that is, they can be represented by a family of vector subspaces. As a consequence of Theorem 1.5.7, we can use families of discrete random variables to represent polymatroids.

Definition 1.6.1. A polymatroid $\mathcal{S} = (Q, h)$ is said to be *entropic* if there exists a family $(S_i)_{i\in Q}$ of discrete random variables such that $h(A) = H(S_A)$ for every $A \subseteq Q$. A *polyentropic polymatroid* is a multiple of an entropic polymatroid.

In order to prove the main result in this section, Theorem 1.6.2, we need to introduce a special class of families of discrete random variables: the ones defined by linear maps. Consider a finite field $\mathbb{K}$, a family $(E_i)_{i\in Q}$ of $\mathbb{K}$-vector spaces and an injective $\mathbb{K}$-linear map $\pi : E \to \prod_{i\in Q} E_i$ such that the induced linear maps $\pi_i : E \to E_i$ are surjective. By taking the uniform probability distribution on E, these linear maps define, for every $i \in Q$, a random variable S_i on E_i. A family of random variables $(S_i)_{i\in Q}$ that can be defined in this way is said to be $\mathbb{K}$-*linear*. For every $A \subseteq Q$, consider the linear map $\pi_A\colon E \to \prod_{i\in A} E_i$ defined by $\pi_A(x) = (\pi_i(x))_{i\in A}$. Then it is clear that

$$H(S_A) = \operatorname{rank} \pi_A \log |\mathbb{K}| = (\dim E - \dim \ker \pi_A) \log |\mathbb{K}|.$$

For every $i \in Q$, consider $W_i = \ker \pi_i$ and the orthogonal subspace $V_i = W_i^{\perp} \subseteq E^*$. The collection $(V_i)_{i\in Q}$ of subspaces define a $\mathbb{K}$-linear integer polymatroid $\mathcal{Z} = (Q, f)$. For every $A \subseteq Q$,

$$f(A) = \dim \sum_{i\in A} V_i = \dim E - \dim \left(\sum_{i\in A} V_i \right)^{\perp} = \dim E - \dim \bigcap_{i\in A} W_i.$$

Since $\ker \pi_A = \bigcap_{i \in A} \ker \pi_i$,

$$f(A) = \dim E - \dim \ker \pi_A = \frac{H(S_A)}{\log |\mathbb{K}|}.$$

As a consequence of the previous discussion, we obtain the following result.

Theorem 1.6.2. *Let $\mathbb{K}$ be a finite field and $\mathcal{Z} = (Q, f)$ a $\mathbb{K}$-linear integer polymatroid. Take $c = \log |\mathbb{K}|$. Then the polymatroid $\mathcal{S} = (Q, cf)$ is entropic. In particular, every poly-linear polymatroid is poly-entropic.*

1.7 Exercises

1.1. Prove that the sum (Definition 1.3.1) of $\mathbb{K}$-linear polymatroids is $\mathbb{K}$-linear. Prove that the sum of entropic polymatroids is entropic.

1.2. Prove that a nonempty family $\mathcal{B}$ of subsets of a finite set Q is the family of bases of a matroid if and only if the following exchange condition is satisfied.

- 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 $(B_2 - \{y\}) \cup \{x\}$ is in $\mathcal{B}$.

Observe that this exchange condition is slightly different to the one in Proposition 1.2.4. Use this new characterization of families of bases of matroids to prove the statement in Definition 1.3.4.

1.3. Prove Theorem 1.4.2.

1.4. Take $Q = \{1, 2, 3, 4\}$ and the map $f : \mathcal{P}(Q) \to \mathbb{Z}$ defined by:

- $f(\emptyset) = 0$ and $f(\{i\}) = 2$ for every $i \in Q$,
- $f(X) = 3$ for every $X \subseteq Q$ with $|X| = 2$, except for $f(\{1, 4\}) = 4$,
- $f(X) = 4$ for every $X \subseteq Q$ with $|X| \geq 3$.

Prove that f is the rank function of an integer polymatroid $\mathcal{Z}$ on Q. Prove that $\mathcal{Z}$ is not $\mathbb{K}$-linear for any field $\mathbb{K}$.

Chapter 2

Secret Sharing Schemes

2.1 Access Structures

Let P be a finite set. If $\mathcal{F}, \mathcal{A} \subseteq \mathcal{P}(P)$ are families of subsets of P such that $\mathcal{F}$ is monotone decreasing, $\mathcal{A}$ is monotone increasing, and $\mathcal{F} \cap \mathcal{A} = \emptyset$, then the pair $\Gamma = (\mathcal{F}, \mathcal{A})$ is called an *access structure* on P. An access structure with $\mathcal{F} = \emptyset$ or $\mathcal{A} = \emptyset$ is said to be *degenerate*. The sets in $\mathcal{F}$ and the ones in $\mathcal{A}$ are, respectively, the *forbidden* and the *qualified* sets of the access structure Γ. Every access structure is determined by the families $\max \mathcal{F}$ and $\min \mathcal{A}$ of its maximal forbidden sets and minimal qualified sets. An access structure is *connected* if every participant $x \in P$ is in a minimal qualified set and in a minimal non-forbidden set.

As we did before for polymatroids and matroids, we introduce the concepts of dual and minor of an access structure. For a family $\mathcal{H} \subseteq \mathcal{P}(P)$ of subsets of P, we notate

- $\overline{\mathcal{H}} = \mathcal{P}(P) - \mathcal{H} = \{A \subseteq P : A \notin \mathcal{H}\}$, and
- $\mathcal{H}^c = \{A \subseteq P : P - A \in \mathcal{H}\}$.

The *dual of an access structure* $\Gamma = (\mathcal{F}, \mathcal{A})$ on P is the access structure $\Gamma^* = (\mathcal{A}^c, \mathcal{F}^c)$ on the same set. It is clear that the dual of a connected access structure is connected as well. Minors are obtained from two operations on families of subsets of a set. Specifically, for a family $\mathcal{H} \subseteq \mathcal{P}(P)$ and a subset $Z \subseteq P$, we consider

- $\mathcal{H} \setminus Z = \{A \subseteq P - Z : A \in \mathcal{H}\}$, and
- $\mathcal{H}/Z = \{A \subseteq P - Z : A \cup Z \in \mathcal{H}\}$.

For an access structure $\Gamma = (\mathcal{F}, \mathcal{A})$ on P, we consider $\Gamma \setminus Z = (\mathcal{F} \setminus Z, \mathcal{A} \setminus Z)$ and $\Gamma/Z = (\mathcal{F}/Z, \mathcal{A}/Z)$, which are access structures on $P - Z$. Observe that they may be degenerate. Any access structure that is obtained from Γ by repeating these operations is called a *minor of the access structure* Γ. An analogous result to Proposition 1.3.3 applies to access structures, and hence every minor of an access structure Γ is of the form $(\Gamma \setminus Z_1)/Z_2$ for some disjoint sets $Z_1, Z_2 \subseteq P$. Some properties of minors of access structures are given in Problem 2.1.

The access structures of the form $\Gamma = (\overline{\mathcal{A}}, \mathcal{A})$ are called *perfect*. For perfect access structures, we identify Γ to $\mathcal{A}$. The dual of a perfect access structure is also perfect and $\Gamma^* = \overline{\Gamma^c}$. A perfect access structure is determined by the family $\min \Gamma$ of its minimal qualified subsets. Every minor of a perfect access structure is perfect too.

For $\Gamma = (\mathcal{F}, \mathcal{A})$ and $\Gamma' = (\mathcal{F}', \mathcal{A}')$, access structures on P, we say that Γ' is *stronger than* Γ if $\mathcal{F} \subseteq \mathcal{F}'$ and $\mathcal{A} \subseteq \mathcal{A}'$. In this situation, we write $\Gamma \preceq \Gamma'$. This defines a partial order on the access structures on a set P, and the maximal elements coincide with the perfect access structures. The *minimum gap* of an access structure $\Gamma = (\mathcal{F}, \mathcal{A})$ is defined by

$$g(\Gamma) = \min\{|B - A| \,:\, A \in \mathcal{F}, B \in \mathcal{A}\}.$$

Observe that $g(\Gamma') \leq g(\Gamma)$ if $\Gamma \preceq \Gamma'$. An access structure with minimum gap g that is maximal with this property is called *g-gap-maximal*.

The following definition of an access structure from a polymatroid is well motivated by the definition in Section 2.2 of the access structure of a secret sharing scheme. Consider a polymatroid $\mathcal{S} = (Q, f)$ and a set $P_0 \subseteq Q$ with $f(P_0) > 0$. The access structure $\Gamma_{P_0}(\mathcal{S}) = (\mathcal{F}, \mathcal{A})$ on the set $P = Q - P_0$ is defined by:

- $\mathcal{F} = \{A \subseteq P \,:\, f(P_0|A) = f(P_0)\}$,
- $\mathcal{A} = \{B \subseteq P \,:\, f(P_0|B) = 0\}$.

It is not difficult to check that this is indeed an access structure, that is, that $\mathcal{F}$ is monotone decreasing, $\mathcal{A}$ is monotone increasing, and $\mathcal{F} \cap \mathcal{A} = \emptyset$. The access structure $\Gamma_{P_0}(M)$ is called a *generalized matroid port* if M is a matroid. If, in addition, $P_0 = \{p_0\}$, then $\Gamma_{P_0}(M) = \Gamma_{p_0}(M)$ is said to be a *matroid port* or, more specifically, the *port of the matroid M at the point p_0*. Since the rank function of a matroid $M = (Q, r)$ is integer-valued and $r(\{p_0\}|A) = r(A \cup \{p_0\}) - r(A) \leq r(\{p_0\}) = 1$, we have that $r(\{p_0\}|A) \in \{0, 1\}$ for every $A \subseteq P$. Therefore, matroid ports are perfect access structures. With a slightly different definition, matroid ports were introduced in 1964 by Lehman [36] to solve the Shannon switching game. According to Lehman's definition, which is based on the characterization in Proposition 2.1.1, a matroid port is the family of minimal sets of a matroid port as defined here.

Proposition 2.1.1. *Let M be a matroid and p_0 a point in its ground set Q. Then*

$$\min \Gamma_{p_0}(M) = \{A \subseteq Q - \{p_0\} \,:\, A \cup \{p_0\} \text{ is a circuit of } M\}.$$

Proof. Suppose that $A \cup \{p_0\}$ is a circuit of M. Then A is an independent set while $A \cup \{p_0\}$ is dependent, and hence $r(A \cup \{p_0\}) = r(A)$. Moreover, if $B \subsetneq A$, then $B \cup \{p_0\}$ is independent, and hence $r(B \cup \{p_0\}) = r(B) + 1$. Therefore, A is a minimal set in $\Gamma_{p_0}(M)$.

Assume now that $A \in \min \Gamma_{p_0}(M)$. Observe that $A \cup \{p_0\}$ is a dependent set of M because $r(A \cup \{p_0\}) = r(A)$. Suppose that $A \cup \{p_0\}$ is not a circuit. If A is dependent, then there exists a subset $B \subsetneq A$ with $r(B) = r(A)$. Then $r(B \cup \{p_0\}) \leq r(A \cup \{p_0\}) = r(A) = r(B)$, a contradiction with A being minimal in $\Gamma_{p_0}(M)$. Then A is independent, and there exists $B \subsetneq A$ such that $B \cup \{p_0\}$ is dependent, and hence $B \in \Gamma_{p_0}(M)$, a contradiction again. □

A matroid is said to be *connected* if every two points in the ground set lie in a common circuit. Clearly, all ports of a connected matroid are connected. Moreover, as a consequence of [44, Proposition 4.1.2], a matroid is connected if and only if at least one of its ports is connected. Lehman [36] proved that a connected matroid is determined by the circuits that contain some given point. A proof for this result can be found in [44, Theorem 4.3.2], Therefore, if Γ is a connected matroid port, there exists a unique connected matroid M with $\Gamma = \Gamma_{p_0}(M)$.

We conclude this section by proving that the class of the generalized matroid ports and the class of the matroid ports are minor-closed and duality-closed. This is a consequence of the following proposition, whose proof is left as an exercise.

Proposition 2.1.2. *Let $\mathcal{S}$ be a polymatroid with ground set $Q = P_0 \cup P$ and let $Z \subseteq P$. The following properties hold.*

1. $\Gamma_{P_0}(\mathcal{S} \setminus Z) = \Gamma_{P_0}(\mathcal{S}) \setminus Z$.
2. $\Gamma_{P_0}(\mathcal{S}/Z) = \Gamma_{P_0}(\mathcal{S})/Z$.
3. *If M is a matroid on Q, then* $\Gamma_{P_0}(M^*) = (\Gamma_{P_0}(M))^*$.

2.2 Secret Sharing Schemes

Definition 2.2.1. Let P be a finite set of *participants*, let $p_0 \notin P$ be a special participant, which is usually called *dealer*, and take $Q = P \cup \{p_0\}$. A *secret sharing scheme* Σ on P is a collection $(S_i)_{i \in Q}$ of discrete random variables such that $h(\{p_0\}) > 0$, where $h(A) = H(S_A)$ for every $A \subseteq Q$.

Definition 2.2.2. The *access structure* $\Gamma(\Sigma) = (\mathcal{F}(\Sigma), \mathcal{A}(\Sigma))$ *of a secret sharing scheme* Σ is defined by:

- $\mathcal{F}(\Sigma) = \{A \subseteq P \,:\, h(\{p_0\}|A) = h(\{p_0\})\}$,
- $\mathcal{A}(\Sigma) = \{B \subseteq P \,:\, h(\{p_0\}|B) = 0\}$.

The random variable S_{p_0} corresponds to the *secret value* that is distributed into *shares* among the participants in P according to the random variables $(S_i)_{i \in P}$. The participants in a qualified set $B \in \mathcal{A}(\Sigma)$ can recover the secret value from their shares, while the shares of the participants in a forbidden set $A \in \mathcal{F}(\Sigma)$ do not provide any information at all about the secret value. Observe that a set of participants that is neither qualified nor forbidden can obtain partial information about the secret value. A secret sharing scheme is said to be *perfect* if its access structure is perfect, that is, if every subset of P is either forbidden or qualified. Of course, $\Gamma(\Sigma) = \Gamma_{p_0}(\mathcal{S})$, where $\mathcal{S}$ is the polymatroid (Q, h).

Definition 2.2.3. For a finite field $\mathbb{K}$, a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ is called $\mathbb{K}$-*linear* if it is a $\mathbb{K}$-linear family of random variables (see Section 1.6).

Linear secret sharing schemes were introduced by Simmons [52], Jackson and Martin [33] and Karchmer and Wigderson [35] under other names such as geometric secret sharing schemes or monotone span programs. In a linear secret sharing scheme, the computation of the shares and the recovery of the secret from the shares of a qualified set require only evaluating linear maps and solving linear systems of equations. Therefore, linear schemes are computationally efficient. In addition, most of the proposed constructions to obtain schemes with good information ratio are based on linear secret sharing schemes. Finally, the homomorphic properties of linear schemes make them very useful for many applications of secret sharing such as multiparty computation.

It is useful to describe a secret sharing scheme Σ as a set $E \subseteq \prod_{i \in Q} E_i$ such that every projection $\pi_i \colon E \to E_i$ is surjective, together with some probability distribution on E. Every random choice of a value $x \in E$ provides a *share vector* $(\pi_i(x))_{i \in Q}$, which

contains the secret value $\pi_{p_0}(x) \in E_{p_0}$ and the shares $\pi_i(x) \in E_i$ of the participants in $P = Q - \{p_0\}$. If Σ is $\mathbb{K}$-linear for some finite field $\mathbb{K}$, then every E_i is a $\mathbb{K}$-vector space, E is a vector subspace of $\prod_{i \in Q} E_i$, and the uniform probability distribution is taken on E. Equivalently, a $\mathbb{K}$-linear secret sharing scheme can be seen as an injective $\mathbb{K}$-linear map $\pi\colon E \to \prod_{i \in Q} E_i$ such that the induced maps $\pi_i\colon E \to E_i$ are surjective.

The *information ratio* $\sigma(\Sigma)$ of a secret sharing scheme Σ is defined as the ratio between the maximum length of the shares and the length of the secret value. That is,

$$\sigma(\Sigma) = \frac{\max_{i \in P} h(\{i\})}{h(\{p_0\})}.$$

The *average information ratio* $\widetilde{\sigma}(\Sigma)$ is defined by

$$\widetilde{\sigma}(\Sigma) = \frac{1}{|P|} \sum_{i \in P} \frac{h(\{i\})}{h(\{p_0\})}.$$

Obviously, $\widetilde{\sigma}(\Sigma) \leq \sigma(\Sigma)$. If Σ is a linear secret sharing scheme, then

$$\sigma(\Sigma) = \frac{\max_{i \in P} \dim E_i}{\dim E_{p_0}} \quad \text{and} \quad \widetilde{\sigma}(\Sigma) = \frac{1}{|P|} \sum_{i \in P} \frac{\dim E_i}{\dim E_{p_0}}.$$

The information ratio of a secret sharing scheme is lower bounded by the inverse of the minimum gap of its access structure.

Proposition 2.2.4. *If Σ is a secret sharing scheme with access structure Γ, then $\sigma(\Sigma) \geq 1/g(\Gamma)$.*

Proof. Consider $A \in \mathcal{F}$ and $B \in \mathcal{A}$ such that $A \subseteq B$. Then

$$h(A) + h(\{p_0\}) = h(A \cup \{p_0\}) \leq h(B \cup \{p_0\}) = h(B) \leq h(A) + h(B - A),$$

and hence

$$h(\{p_0\}) \leq h(B - A) \leq \sum_{y \in B - A} h(\{y\}) \leq |B - A| \max_{x \in P} h(\{x\}) \tag{2.1}$$

which clearly concludes the proof. □

In particular, $\sigma(\Sigma) \geq 1$ if Σ is a perfect secret sharing scheme. If, in addition, the access structure of Σ is connected, then $h(\{i\}) \geq h(\{p_0\})$ for every participant $i \in P$. This can be proved with a similar argument as in the previous proof. This fact motivated the following definition: a perfect secret sharing scheme is called *ideal* if every share has the same length as the secret. Observe that the only perfect secret sharing schemes with information ratio $\sigma(\Sigma) = 1$ are the ideal ones.

2.3 Threshold Secret Sharing Schemes

A *threshold access structure* is of the form $\Gamma = (\mathcal{F}, \mathcal{A})$ with $\mathcal{F} = \{A \subseteq P\,;\, |A| \leq t - g\}$ and $\mathcal{A} = \{A \subseteq P\,;\, |A| \geq t\}$ for some integers $1 \leq g \leq t \leq |P|$. If $g = 1$, such an access structure is perfect, and it is called the (t, n)-*threshold access structure*, where n is the number of participants.

We present first an example of a perfect secret sharing scheme for the (n, n)-threshold access structure. Let $(G, +)$ be a non-trivial finite commutative group. Consider the set

$E \subseteq G^Q$ formed by the tuples $(s_i)_{i\in Q}$ with $\sum_{i\in Q} s_i = 0$ and take the uniform probability distribution on it. Clearly, this defines an ideal perfect secret sharing scheme in which the set P is the only qualified set.

In Shamir's [49] seminal paper on secret sharing, a method to construct an ideal perfect secret sharing scheme for every (t, n)-threshold access structure is presented. The schemes that are obtained by this method are linear. Given integers $1 \leq t \leq n$, consider a finite field $\mathbb{K}$ with at least $n + 1$ elements and the $\mathbb{K}$-vector space $E = \mathbb{K}_{t-1}[x]$ of the polynomials over $\mathbb{K}$ with degree at most $t - 1$, and take $E_i = \mathbb{K}$ for every $i \in Q$. Given a tuple $(x_i)_{i\in Q}$ of different elements in $\mathbb{K}$, the linear map $\pi\colon E \to \prod_{i\in Q} E_i = \mathbb{K}^Q$ defined by $\pi(f) = (f(x_i))_{i\in Q}$ for every $f \in E$ provides an ideal perfect secret sharing scheme for the (t, n)-threshold access structure. This fact is a straightforward consequence of the following well known basic fact about polynomials.

Lemma 2.3.1. *For every $A \subseteq Q$ with $|A| = t$ and for every tuple $(s_i)_{i\in A} \in \mathbb{K}^A$, there exists a unique polynomial $f \in \mathbb{K}_{t-1}[x]$ such that $f(x_i) = s_i$ for every $i \in A$.*

Observe that the secret value can be efficiently computed from the shares of a qualified set by using, for instance, Lagrange interpolation. Efficient computation of the shares and efficient secret reconstruction are common to all linear secret sharing schemes.

We present in the following two variants of Shamir's threshold scheme. The first one, which was presented in his seminal paper [49], may be useful for hierarchical organizations. The second one has a non-perfect threshold access structure.

Perfect access structures that reflect the existence of a hierarchy among the participants can be obtained by assigning a positive integer, called *weight*, to every participant. A set is qualified if and only if the weight sum of its participants attain a certain threshold. It is easy to obtain a secret sharing scheme for such an access structure. One has to consider a threshold secret sharing scheme and give to every participant as many shares as its weight. Nevertheless, the scheme obtained in this way is not ideal.

In the other variant of Shamir's threshold scheme we discuss here, $g+n$ different values $(y_1, \ldots, y_g, (x_i)_{i\in P})$ in $\mathbb{K}$ are taken. In addition, we consider $E_{p_0} = \mathbb{K}^g$ and $\pi_{p_0}(f) = (f(y_1), \ldots, f(y_g))$ for every $f \in E$. As before, $\pi_i(f) = f(x_i)$ if $i \in P$. A non-perfect secret sharing scheme is obtained in this way. The forbidden sets are those with at most $t - g$ participants, while the ones with at least t participants are qualified. Observe that the information ratio of this scheme attains the bound in Proposition 2.2.4.

2.4 Secret Sharing Schemes from Linear Codes

Brickell [9] proposed a method, based on linear algebra, to construct ideal perfect secret sharing schemes for some non-threshold access structures. The schemes that are obtained by this method are the ones in the family that is defined next.

Definition 2.4.1. A $\mathbb{K}$-linear secret sharing scheme Σ in which $E_i = \mathbb{K}$ for every $i \in Q$ is called a $\mathbb{K}$-*vector space secret sharing scheme*.

That is, in a $\mathbb{K}$-vector space secret sharing scheme, the linear maps $\pi_i\colon E \to E_i$ are nonzero linear forms. Moreover, for every collection $(\pi_i)_{i\in Q}$ of nonzero linear forms on a $\mathbb{K}$-vector space E and for every choice of a distinguished participant $p_0 \in Q$, a $\mathbb{K}$-vector space secret sharing scheme on $P = Q - \{p_0\}$ is obtained. Such schemes are perfect and ideal. A set $A \subseteq P$ is qualified if and only if the linear form $\pi_{p_0} \in E^*$ is a linear combination of

the linear forms $(\pi_i)_{i\in A}$. Observe that Shamir's threshold scheme is a particular case of such a scheme. Specifically, the one given by the linear forms $\pi_i = (1, x_i, \ldots, x_i^{t-1})$.

Let Σ be a $\mathbb{K}$-vector space secret sharing scheme and let $\mathcal{S} = (Q, h)$ be its associated polymatroid. Given a basis of the space E, consider the matrix G such that $\pi(x) = xG$ for every $x \in E$, that is, every column of G correspond to a linear form π_i. Then G can be seen as the generator matrix of a $\mathbb{K}$-linear code $C \subseteq \mathbb{K}^Q$ with length $n+1$, where $|Q| = n+1$. Every codeword $(s_i)_{i\in Q}$ corresponds to a share vector of the secret sharing scheme. One of the entries of the codeword (the one given by the choice of the distinguished participant p_0) corresponds to the secret value and the other entries are the shares to be distributed among the participants. As we saw in Section 1.4, the code C defines a $\mathbb{K}$-linear matroid $M = (Q, r)$. Moreover, if $\mathcal{S} = (Q, h)$ is the polymatroid associated to Σ, then $h = \log|\mathbb{K}| \cdot r$, and hence the access structure of Σ is the matroid port $\Gamma_{p_0}(M)$. Conversely, if a matroid M is $\mathbb{K}$-linear, a $\mathbb{K}$-vector space secret sharing scheme can be obtained for every one of its ports. This is summarized in the next proposition.

Theorem 2.4.2. *A perfect access structure admits a $\mathbb{K}$-vector space secret sharing scheme if and only if it is a port of some $\mathbb{K}$-linear matroid.*

In particular, Shamir's (t, n)-threshold schemes coincide with the $\mathbb{K}$-vector space secret sharing schemes that are obtained from Reed-Solomon codes. The (t, n)-threshold access structure is a port of the *uniform matroid* $U_{t,n+1}$, whose bases are precisely the sets with t elements from a ground set with $n+1$ elements. The uniform matroid $U_{t,n+1}$ is $\mathbb{K}$-linear for every field with at least n elements.

There exist vector space secret sharing schemes whose access structures are not threshold. For instance, for a finite field $\mathbb{K}$ with characteristic greater than 3, consider the $\mathbb{K}$-linear code C with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 3 \end{pmatrix}$$

By identifying the columns of G with the elements in $Q = \{0, 1, \ldots, 5\}$, and assuming that the first column corresponds to the dealer $p_0 = 0$, this code defines a $\mathbb{K}$-vector space secret sharing scheme in which the minimal qualified sets are $\{1, 2\}$, $\{3, 4\}$, $\{1, 3, 5\}$, $\{1, 4, 5\}$, $\{2, 3, 5\}$ and $\{2, 4, 5\}$. If we take instead $p_0 = 6$, a $\mathbb{K}$-vector space secret sharing scheme is obtained for the access structure whose minimal qualified sets are all 3-subsets of $\{0, 1, 2, 3, 4\}$ except $\{0, 1, 2\}$ and $\{0, 3, 4\}$.

In a similar way as we did with Shamir's threshold scheme, we can extend vector space secret sharing schemes to a more general class of schemes that are not perfect in general.

Definition 2.4.3. A $\mathbb{K}$-linear secret sharing scheme Σ in which $E_i = \mathbb{K}$ for every $i \in P$ is called a *generalized $\mathbb{K}$-vector space secret sharing scheme*.

That is, in a generalized $\mathbb{K}$-vector space secret sharing scheme the secret value can be a vector instead of an element in the field $\mathbb{K}$. The shares of the participants are, as before, elements in the field $\mathbb{K}$. Therefore, these schemes are not perfect in general. In this case, the matrix G is a generator matrix of a linear code C with length $n + g$, where $g = \dim E_{p_0}$. The secret corresponds to the first g entries of a codeword, and the other entries give the shares of the participants. The access structures of those schemes are also related to matroids.

Theorem 2.4.4. *An access structure admits a generalized $\mathbb{K}$-vector space secret sharing scheme if and only if it is a generalized port of some $\mathbb{K}$-linear matroid.*

2.5 A Secret Sharing Scheme for Every Access Structure

The aim of this section is to discuss two constructions, which were presented in [4, 32] providing secret sharing schemes for every perfect access structure. In both constructions the (n, n)-threshold secret sharing scheme described at the beginning of Section 2.3 is used. The second construction is based on the following obvious fact.

Lemma 2.5.1. *Let Γ be a perfect access structure on a set P. Then a subset $A \subseteq P$ is in Γ if and only if $A \cap B \neq \emptyset$ for every B in the dual access structure Γ^*.*

Let Γ be a perfect access structure on a set P, and let $(G, +)$ be a non-trivial finite commutative group. We present next two secret sharing schemes, Σ_1 and Σ_2, with set of secret values G and access structure Γ. For Σ_1, given a secret value $s \in G$, for every $A \in \min \Gamma$ values $(s_{A,i})_{i \in A}$ with $s_{A,i} \in G$ and $s = \sum_{i \in A} s_{A,i}$ are randomly selected. For every $i \in P$, take $M_i = \{A \in \min \Gamma \, : \, i \in A\}$. The share corresponding to participant i is the tuple $(s_{A,i})_{A \in M_i} \in G^{M_i}$. The scheme Σ_2 is obtained by taking at random a tuple $(s_B)_{B \in \min \Gamma^*}$ with $s_B \in G$ and $\sum_{B \in \min \Gamma^*} s_B = s$, the secret value. The share for $i \in P$ is $(s_B)_{B \in M_i^*} \in G^{M_i^*}$, where $M_i^* = \{B \in \min \Gamma^* \, : \, i \in B\}$.

Every perfect access structure Γ on a set P can be described by the monotone boolean function $\xi_\Gamma \colon \{0,1\}^P \to \{0,1\}$ defined by $\xi_\Gamma(\mathbf{x}) = 1$ if and only if $\mathbf{x}$ is the characteristic vector of a set in Γ. The following two formulas can be used to describe this function.

$$\xi_\Gamma((x_i)_{i \in P}) = \bigvee_{A \in \min \Gamma} \left(\bigwedge_{i \in A} x_i \right) \quad \text{and} \quad \xi_\Gamma((x_i)_{i \in P}) = \bigwedge_{B \in \min \Gamma^*} \left(\bigvee_{i \in B} x_i \right).$$

The schemes Σ_1 and Σ_2 can be obtained, respectively, from the first and the second formula by replacing the $\wedge$ gates by (n, n)-threshold schemes and the $\vee$ gates by $(1, n)$-threshold schemes.

These general constructions provide highly inefficient secret sharing schemes because the length of the shares is too large. Clearly, the information ratios of those schemes are $\sigma(\Sigma_1) = \max_{i \in P} |M_i|$ and $\sigma(\Sigma_2) = \max_{i \in P} |M_i^*|$. Both values grow exponentially with the number of participants.

These constructions can be easily adapted to non-perfect access structures (Exercise 2.4). If G is a finite field, linear secret sharing schemes are obtained. Summarizing, the following result has been proved in this section.

Theorem 2.5.2. *Consider an access structure Γ and an integer $q > 2$. Then there exists a secret sharing scheme with $|E_{p_0}| = q$ and access structure Γ. If q is a prime power, then there exists an $\mathbb{F}_q$-linear secret sharing scheme with access structure Γ and $E_{p_0} = \mathbb{F}_q$.*

2.6 Linear Secret Sharing Schemes: Access Structure

We saw in Section 2.2 that every secret sharing scheme Σ defines a polymatroid $\mathcal{S} = (Q, h)$ and that the access structure of Σ is $\Gamma = \Gamma_{p_0}(\mathcal{S})$. In this section, we analyze some properties of this polymatroid in the case that Σ is linear, and we present a description of its access structure.

Consider a linear map $\pi : E \to \prod_{i \in Q} E_i$ defining a $\mathbb{K}$-linear secret sharing scheme $\Sigma = (S_i)_{i \in Q}$, and let $\mathcal{S} = (Q, h)$ be the associated polymatroid, which is given by $h(A) = H(S_A)$ for every $A \subseteq Q$. As we saw in Section 1.6,

$$h(A) = \operatorname{rank} \pi_A \log |\mathbb{K}| = (\dim E - \dim \ker \pi_A) \log |\mathbb{K}|$$

for every $A \subseteq Q$, where $\pi_A \colon E \to \prod_{i\in A} E_i$ is defined by $\pi_A(x) = (\pi_i(x))_{i\in A}$. Therefore, the polymatroid $\mathcal{Z} = (Q, f)$ with $f = (\log|\mathbb{K}|)^{-1}h$ is integer. Obviously, the access structure of Σ is $\Gamma = (\mathcal{F}, \mathcal{A}) = \Gamma_{p_0}(\mathcal{S}) = \Gamma_{p_0}(\mathcal{Z})$. Moreover, $\mathcal{Z}$ is $\mathbb{K}$-linear. Indeed, if $W_i = \ker \pi_i \subseteq E$ and $V_i = W_i^{\perp} \subseteq E^*$, then the subspaces $(V_i)_{i\in Q}$ are a $\mathbb{K}$-linear representation of $\mathcal{Z}$, as it was proved in Section 1.6. Therefore, a set $A \subseteq P$ is in $\mathcal{F}$ if and only if

$$\dim\left(V_{p_0} + \sum_{i\in A} V_i\right) = f(A \cup \{p_0\}) = f(A) + f(\{p_0\}) = \dim V_{p_0} + \dim \sum_{i\in A} V_i.$$

On the other hand, $A \in \mathcal{A}$ if and only if

$$\dim\left(V_{p_0} + \sum_{i\in A} V_i\right) = f(A \cup \{p_0\}) = f(A) = \dim \sum_{i\in A} V_i.$$

That is, the access structure $\Gamma = (\mathcal{F}, \mathcal{A})$ of Σ is given by:

- $\mathcal{F} = \{A \subseteq P \,:\, V_{p_0} \cap \left(\sum_{i\in A} V_i\right) = \{0\}\}$,
- $\mathcal{A} = \{A \subseteq P \,:\, V_{p_0} \subseteq \sum_{i\in A} V_i\}$.

By duality, we obtain a description of the access structure of Σ in terms of the subspaces $W_i = \ker \pi_i$:

- $\mathcal{F} = \{A \subseteq P \,:\, W_{p_0} + \left(\bigcap_{i\in A} W_i\right) = E\}$,
- $\mathcal{A} = \{A \subseteq P \,:\, \bigcap_{i\in A} W_i \subseteq W_{p_0}\}$.

2.7 Matrix Representation and Duality

Given bases of E and every E_i, one can consider the matrix G of the linear map $\pi : E \to \prod_{i\in Q} E_i$. Take $k = \dim E$ and $k_i = \dim E_i$. If we assume that $Q = \{0, 1, \ldots, n\}$ and $p_0 = 0$, the matrix G is of the form $G = (G_0|G_1|\cdots|G_n)$, where G_i is the $k \times k_i$ matrix of the linear map $\pi_i : E \to E_i$ (which means $\pi(x) = xG$). The columns of this matrix are linear forms on E, that is, vectors in E^*, and the columns of G_i span the subspace V_i for every $i \in Q$.

Moreover, G is the generator matrix of a $\mathbb{K}$-linear code C with dimension k and length $N = \sum_{i\in Q} k_i$. Therefore, we can consider the $\mathbb{K}$-linear matroid $M = (\widehat{Q}, r)$ defined by the code C. The ground set $\widehat{Q}$ of M in in one-to-one correspondence with the columns of G, and hence it is a disjoint union $\widehat{Q} = \bigcup_{i\in Q} \widehat{Q}_i$, where $|\widehat{Q}_i| = k_i$. The integer polymatroid $\mathcal{Z} = (Q, f)$ defined by the subspaces $(V_i)_{i\in Q}$ can be determined from M because $f(A) = r(\bigcup_{i\in A} \widehat{Q}_i)$ for every $A \subseteq Q$.

The dual code $C^{\perp}$ of C has a generator matrix of the form $H = (H_0|H_1|\cdots|H_n)$, which is the transpose of a parity-check matrix of C. Each submatrix H_i has as many columns as G_i. The code $C^{\perp}$ defines a linear secret sharing scheme Σ^* on the same set of participants as Σ. This scheme is called the *dual linear secret sharing scheme* of Σ. By Theorem 1.3.4, the code $C^{\perp}$ is a $\mathbb{K}$-linear representation of the matroid $M^* = (\widehat{Q}, r^*)$, the dual of M. In particular, the access structure of Σ^* is $\Gamma_{p_0}(\mathcal{Z}^*)$, where $\mathcal{Z}^* = (Q, f^*)$ is the polymatroid defined by

$$f^*(A) = r^*\left(\bigcup_{i\in A} \widehat{Q}_i\right) = \left|\bigcup_{i\in A} \widehat{Q}_i\right| - r(\widehat{Q}) + r\left(\bigcup_{i\in Q-A} \widehat{Q}_i\right) = \sum_{i\in A} k_i - k + f(Q - A)$$

for every $A \subseteq Q$. We have used here the formula for r^* in Proposition 1.3.5.

Theorem 2.7.1. *Let Σ be a $\mathbb{K}$-linear secret sharing scheme with non-degenerate access structure $\Gamma = (\mathcal{F}, \mathcal{A})$. Then the dual linear secret sharing scheme Σ^* has access structure $\Gamma^* = (\mathcal{A}^c, \mathcal{F}^c)$.*

Proof. As we saw before, the access structure of Σ^* is equal to $\Gamma_{p_0}(\mathcal{Z}^*) = (\mathcal{F}', \mathcal{A}')$. Observe that

- $f^*(A \cup \{p_0\}) = k_0 + \sum_{i \in A} k_i - k + f(P - A)$,
- $f^*(A) = \sum_{i \in A} k_i - k + f(Q - A)$, and
- $f^*(\{p_0\}) = k_0 - k + f(P) = k_0$ (since Γ is not degenerate, $f(P) = f(Q)$).

A set $A \subseteq P$ is in $\mathcal{F}'$ if and only if $f^*(A \cup \{p_0\}) = f^*(A) + f^*(\{p_0\})$, which is equivalent to $f(P - A) = f(Q - A) = f((P - A) \cup \{p_0\})$, and hence equivalent to $P - A \in \mathcal{A}$. Finally, $A \in \mathcal{A}'$ if and only if $f^*(A \cup \{p_0\}) = f^*(A)$, which is equivalent to $f((P - A) \cup \{p_0\}) = f(P - A) + k_0$, and hence equivalent to $P - A \in \mathcal{F}$. □

2.8 An Example of a Linear Secret Sharing Scheme

We present in this section an example of a perfect linear secret sharing scheme. Differently to the ones in the family introduced in Section 2.4, it is not ideal.

Take $Q = \{0, 1, 2, 3, 4\}$ and $p_0 = 0$. Consider as well a finite field $\mathbb{K}$ and the $\mathbb{K}$-vector spaces $E = \mathbb{K}^6$ and $(E_i)_{i \in Q}$, where $E_0 = E_1 = E_4 = \mathbb{K}^2$ and $E_2 = E_3 = \mathbb{K}^3$. Let Σ by the linear secret sharing scheme on P defined by the linear map $\pi : E \to \prod_{i \in Q} E_i$ given by the matrix

$$G = \left(\begin{array}{cc|cc|ccc|ccc|cc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right).$$

Consider as before, for every $i \in Q$, the vector subspace $V_i \subseteq E^*$ spanned by the columns of G corresponding to i. One can check that $V_0 \subseteq V_i + V_j$ if $\{i, j\}$ is one of the subsets $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$ or $A_3 = \{3, 4\}$, and that $V_0 \cap (V_i + V_j) = \{0\}$ if $\{i, j\}$ is any other 2-subset of $\{1, 2, 3, 4\}$. As a consequence of that, the secret sharing scheme we have defined from the linear mappings π_i is perfect and A_1, A_2, A_3 are the minimal qualified subsets in its access structure. The information ratio of this scheme is equal to $3/2$. We will prove in the following chapters that there does not exist any ideal scheme for that access structure and that the proposed scheme has optimal information ratio among all schemes for that structure.

2.9 Exercises

2.1. Prove the following properties about minors and duals of access structures. For an access structure Γ on a set P and $Z \subseteq P$,

1. $\Gamma^{**} = \Gamma$, and

2. $(\Gamma \setminus Z)^* = \Gamma^*/Z$ and $(\Gamma/Z)^* = \Gamma^* \setminus Z$.

2.2. Prove Proposition 2.1.2.

2.3. Let n be a prime power and t an integer with $1 \leq t \leq n$. By modifying Shamir's threshold scheme, present a $\mathbb{K}$-vector space secret sharing scheme for the (t, n)-threshold access structure in which $|\mathbb{K}| = n$. Recall that in the description of Shamir's threshold scheme in Section 2.3 we required that $|\mathbb{K}| \geq n + 1$.

2.4. Complete the proof of Theorem 2.5.2. Specifically, by adapting the previous general constructions for the perfect case, prove that every (maybe non-perfect) access structure admits a linear secret sharing scheme.

2.5. On the set $P = \{1, 2, 3, 4\}$, consider the perfect access structure Γ whose minimal qualified subsets are $\{1, 2\}$, $\{2, 3\}$, and $\{3, 4\}$. Prove that Γ is not a matroid port. Describe the two secret sharing schemes for Γ that are obtained by applying the constructions in Section 2.5.

2.6. Prove that the two general constructions of linear secret sharing schemes described in Section 2.5 are dual of each other.

Chapter 3

Optimization of Secret Sharing Schemes

3.1 Parameters to Be Optimized

Some optimization problems for secret sharing schemes with general (non-threshold) access structure are considered in this chapter. Even though such problems could be considered in the general case, they have been studied almost exclusively for perfect secret sharing schemes. Because of that, only the perfect case is considered in this chapter.

By Theorem 2.5.2 there exists a secret sharing scheme for every perfect access structure and for every size of the set of values of the secret. A constructive proof was given, but it provides very inefficient schemes. A natural question appearing at this point is to determine the most efficient efficient scheme for every given access structure.

Among all possible ways to measure the efficiency of a secret sharing scheme, the length of the shares, generally in relation to the length of the secret value, has been the most widely considered. More specifically, we define in the following the parameters whose optimization has attracted most of the attention.

Definition 3.1.1. The *optimal information ratio* $\sigma(\Gamma)$ *of a perfect access structure* Γ is the infimum of the information ratios of all secret sharing schemes for Γ. The *optimal average information ratio* $\widetilde{\sigma}(\Gamma)$ is defined analogously. If we restrict to linear secret sharing schemes, we have the parameters $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$, the infimum of the information ratios and, respectively, average information ratios of all linear secret sharing schemes for Γ.

Obviously, $1 \leq \sigma(\Gamma) \leq \lambda(\Gamma)$ and $1 \leq \widetilde{\sigma}(\Gamma) \leq \widetilde{\lambda}(\Gamma)$ for every perfect access structure Γ. Determining the values of these parameters has appeared to be a very difficult open problem. They are unknown even for very simple access structures. Moreover, there is a huge gap between the best known general upper and lower bounds on the asymptotic behavior of those parameters.

For a polymatroid $\mathcal{S} = (Q, f)$ and $p_0 \in Q$, we notate

$$\sigma_{p_0}(\mathcal{S}) = \frac{\max\{f(\{i\}) \,:\, i \in Q - \{p_0\}\}}{f(\{p_0\})} \quad \text{and} \quad \widetilde{\sigma}_{p_0}(\mathcal{S}) = \frac{1}{|Q|-1} \sum_{i \in Q - \{p_0\}} \frac{f(\{i\})}{f(\{p_0\})}.$$

Observe that $\Gamma_{p_0}(\mathcal{S}') = \Gamma_{p_0}(\mathcal{S})$ if $\mathcal{S}'$ is a multiple of $\mathcal{S}$. Therefore, for every perfect access structure Γ,

$$\sigma(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-entropic polymatroid with } \Gamma = \Gamma_{p_0}(\mathcal{S})\}$$

and

$$\lambda(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a poly-linear polymatroid with } \Gamma = \Gamma_{p_0}(\mathcal{S})\}.$$

Similar expressions hold for $\widetilde{\sigma}(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$. We introduce a new parameter:

$$\kappa(\Gamma) = \inf\{\sigma_{p_0}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a polymatroid with } \Gamma = \Gamma_{p_0}(\mathcal{S})\},$$

and $\widetilde{\kappa}(\Gamma)$ is defined analogously. Observe that $1 \leq \kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$ and $1 \leq \widetilde{\kappa}(\Gamma) \leq \widetilde{\sigma}(\Gamma) \leq \widetilde{\lambda}(\Gamma)$ for every perfect access structure Γ.

Theorem 3.1.2. *If Γ' is a minor of Γ, then $\kappa(\Gamma') \leq \kappa(\Gamma)$, $\sigma(\Gamma') \leq \sigma(\Gamma)$, and $\lambda(\Gamma') \leq \lambda(\Gamma)$. The same applies to the parameters related to the optimal average information ratio.*

Proof. The statements about the parameters κ and λ are a consequence of Proposition 2.1.2 and Theorem 1.4.1. Let $\Sigma = (S_i)_{i\in Q}$ be a secret sharing scheme for Γ and $Z \subseteq P$. Then $\Sigma \setminus Z = (S_i)_{i\in Q-Z}$ is obviously a secret sharing scheme for $\Gamma \setminus Z$. Consider a tuple $s_Z = (s_j)_{j\in Z}$ such that $S_Z = (S_j)_{j\in Z} = s_Z$ with nonzero probability. Then $\Sigma/Z = (S_i|S_Z = s_Z)_{i\in Q-Z}$ is clearly a secret sharing scheme for Γ/Z. Finally, observe that both $\sigma(\Sigma \setminus Z)$ and $\sigma(\Sigma/Z)$ are at most $\sigma(\Sigma)$. The same proof applies for the parameters related to the average information rate. □

It is not difficult to check that $\sigma(\Sigma) = \sigma(\Sigma^*)$ and $\widetilde{\sigma}(\Sigma) = \widetilde{\sigma}(\Sigma^*)$ if Σ is a linear secret sharing scheme and Σ^* is its dual. By combining this with Theorem 2.7.1, the next result is deduced.

Theorem 3.1.3. *If Γ is a perfect access structure, then $\lambda(\Gamma) = \lambda(\Gamma^*)$ and $\widetilde{\lambda}(\Gamma) = \widetilde{\lambda}(\Gamma^*)$.*

We prove in Theorem 3.3.8 that this also applies to the parameter κ. Nevertheless, it is not known if there is any connection between the optimal (average) information ratio of an access structure and that of its dual.

3.2 Upper Bounds

Every construction of a secret sharing scheme for Γ provides upper bounds on those parameters. Unfortunately, no general construction is known providing bounds that are asymptotically better than the ones given by the constructions in Section 2.5. So the best known general upper bounds on $\sigma(\Gamma)$ are exponential on the number of participants.

Nevertheless, several construction methods have been proposed that provide better upper bounds for several particular families of access structures. Most of these constructions give linear secret sharing schemes, and hence upper bounds on $\lambda(\Gamma)$. These methods are based on decomposing the given access structures into substructures that admit ideal secret sharing schemes schemes, and combine them to obtain a scheme for the given structure. By using a small example, we describe in the following a simple decomposition method, which was used, for instance, in [8]. Subsequently, we present a more sophisticated and effective construction: the so-called *λ-decomposition method* due to Stinson [55].

Consider the perfect access structure Γ on the set $P = \{1, 2, 3, 4\}$ whose minimal qualified sets are $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$ and $A_3 = \{3, 4\}$. A linear secret sharing scheme for this access structure with information ratio equal to $3/2$ was presented in Section 2.8. Consider the access structures Γ_1 with $\min\Gamma_1 = \{A_1, A_2\}$ and Γ_2 with $\min\Gamma_2 = \{A_3\}$. Observe that $\Gamma_1 \cup \Gamma_2 = \Gamma$ and, because of that, we say that these structures form a

decomposition of Γ. Both Γ_1 and Γ_2 admit a $\mathbb{K}$-vector space secret sharing scheme for every finite field $\mathbb{K}$. Indeed, a scheme Σ_1 for Γ_1 is obtained by randomly splitting the secret value $s = s_1 + s_2$. Participants 1 and 3 receive the share s_1 and participant 2 receive the share s_2. A scheme Σ_2 for Γ_2 is obtained by taking another random split $s = t_1 + t_2$ and giving the share t_1 to participant 3 and the share t_2 to participant 4. Now we combine the schemes Σ_1 and Σ_2 into a scheme Σ. Specifically, a secret value $s \in \mathbb{K}$ is distributed according to the two schemes Σ_1 and Σ_2. If a participant is involved in both schemes, its share will be an element in $\mathbb{K}^2$. That is, the participants in P receive the shares: $S_1 = s_1 \in \mathbb{K}$, $S_2 = s_2 \in \mathbb{K}$, $S_3 = (s_1, t_1) \in \mathbb{K}^2$, and $S_4 = t_2 \in \mathbb{K}$. We have obtained in this way a linear secret sharing scheme for Γ with information ratio equal to 2.

We can improve this value of the information ratio by considering two decompositions of Γ instead of one. In addition to Γ_1, Γ_2, we consider the access structures Γ_1' with $\min\Gamma_1' = \{A_1\}$ and Γ_2' with $\min\Gamma_2' = \{A_2, A_3\}$. By symmetrically using the decomposition $\Gamma = \Gamma_1' \cup \Gamma_2'$, we obtain a linear secret sharing scheme Σ' for Γ in which participant 3 receives a share in $\mathbb{K}^2$ while the secret and the other shares are taken from $\mathbb{K}$. Finally, we combine the two schemes obtained from those two decompositions: given a secret value $(s, s') \in \mathbb{K}^2$, we compute shares for s according to Σ and shares for s' according to Σ'. In this way, the shares for participants 1 and 4 are elements in $\mathbb{K}^2$, while the shares for participants 2 and 3 are taken from $\mathbb{K}^3$. Since the secret value is an element in $\mathbb{K}^2$, we have obtained a $\mathbb{K}$-linear secret sharing scheme for Γ with information ratio equal to $3/2$. Actually, this is the same scheme as the one we presented in Section 2.8.

That access structure is a member of the family of structures defined from graphs, for which the optimization problems we are considering here have been widely studied. Given a graph G, we define the perfect access structure $\Gamma = \Gamma[G]$, whose participants and minimal qualified sets are, respectively, the vertices and edges of G. Take $\Gamma = \Gamma[G]$, where G is a cycle of even length. The minimal qualified sets $\min\Gamma = \{A_1, \ldots, A_{2n}\}$ coincide with the edges of G. For every $i = 1, \ldots, 2n$, consider the access structure Γ_i with $\min\Gamma_i = \{A_i, A_{i+1}\}$, where the sum in the subindex is in $\mathbb{Z}_{2n}$. We have two decompositions of Γ, namely $\{\Gamma_{2i} : i = 1, \ldots, n\}$ and $\{\Gamma_{2i-1} : i = 1, \ldots, n\}$. By using these decompositions in the same way as before, we obtain a linear secret sharing scheme Σ for Γ with information ratio equal to $3/2$.

A scheme with the same information ratio cannot be obtained for the cycles with odd length by applying the same technique. Nevertheless, this can be attained by using the decomposition method proposed by Stinson [55]. The following construction applies to a cycle with arbitrary length n. Consider the same structures Γ_i, where $i = 1, \ldots, n$, as before. Let $\mathbb{K}$ be a field with $|\mathbb{K}| \geq n$ and take n different values $x_1, \ldots, x_n \in \mathbb{K}$. Every one of the access structures Γ_i admits a $\mathbb{K}$-vector space secret sharing scheme Σ_i. The secret value is a pair $(s_1, s_2) \in \mathbb{K}^2$. A random polynomial f with degree at most one such that $f(x_1) = s_1$ and $f(x_2) = s_2$ is taken. Fore every $i = 1, \ldots, n$, the value s_i is distributed into shares according to the scheme Σ_i, which involves only the participants in $A_i \cup A_{i+1}$. Therefore, every participant receives three elements in $\mathbb{K}$ as its share, and hence the information ratio of the scheme is equal to $3/2$. Since every minimal qualified subset $A_i \in \min\Gamma$ appears in the substructures Γ_{i-1} and Γ_i, the participants in A_i can recover the values $s_{i-1} = f(x_{i-1})$ and $s_i = f(x_i)$, and hence they can recover the polynomial f and the secret value. On the other hand, the shares of the participants in an unqualified subset do not provide any information about the values $s_1, \ldots, s_n$.

In general, the λ-decomposition method by Stinson is based on the following result.

Proposition 3.2.1. *For a perfect access structure Γ, consider substructures $(\Gamma_1, \ldots, \Gamma_m)$*

with $\Gamma = \bigcup_{i=1}^{m} \Gamma_i$. *For every* $i = 1, \ldots, m$, *consider the set* $P_i \subseteq P$ *of participants that appear in some minimal qualified subset of the substructure* Γ_i, *and, for every* $x \in P$, *consider* $w(x) = |\{i : x \in P_i\}|$ *and take* $w = \max_{x \in P} w(x)$. *For every minimal qualified subset* $A \in \min \Gamma$, *consider* $\gamma(A) = |\{i : A \in \Gamma_i\}|$ *and take* $\gamma = \min_{A \in \min \Gamma} \gamma(A)$. *Assume that there exists a finite field* $\mathbb{K}$ *with* $|\mathbb{K}| \geq m$ *such that all substructures* Γ_i *are* $\mathbb{K}$*-vector space access structures. Then, there exists for the access structure* Γ *a* $\mathbb{K}$*-linear secret sharing scheme with set of secrets* $E_0 = \mathbb{K}^\gamma$ *whose complexity is equal to* w/γ.

Proof. Take m different values $x_1, \ldots, x_m \in \mathbb{K}$. Given a secret value $(s_1, \ldots, s_\gamma) \in E_0$, take a random polynomial f with degree at most $\gamma - 1$ such that $f(x_i) = s_i$ for every $i = 1, \ldots, \gamma$. For every $i = 1, \ldots, m$, the value $s_i f(x_i)$ is distributed among the participants in P_i according to a $\mathbb{K}$-vector space secret sharing scheme Σ_i with access structure Γ_i. Clearly, every participant receives at most w elements in $\mathbb{K}$ as its share. Every minimal qualified set can recover γ of the values $(s_1, \ldots, s_m)$, and hence the polynomial f. An unqualified subset does not obtain any information about the secret value. □

3.3 Lower Bounds

Most of the lower bounds that have been obtained for $\sigma(\Gamma)$ are in fact lower bounds on $\kappa(\Gamma)$. We prove in the following that both $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be computed by solving a linear programming problem. The rank function of a polymatroid $\mathcal{S} = (Q, f)$ is a vector in $\mathbb{R}^{\mathcal{P}(Q)}$, and $\kappa(\Gamma)$ can be obtained as the solution of the following linear programming problem.

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & \mathcal{S} = (Q, f) \text{ is a polymatroid} \\ & f(\{p_0\}) = 1 \\ & \Gamma = \Gamma_{p_0}(\mathcal{S}) \\ & v \geq f(\{i\}) \text{ for every } i \in Q \end{array}$$

Analogously, the solution of the following linear programming problem determines $\widetilde{\kappa}(\Gamma)$.

$$\begin{array}{ll} \text{Minimize} & \sum_{i \in P} f(\{i\}) \\ \text{subject to} & \mathcal{S} = (Q, f) \text{ is a polymatroid} \\ & f(\{p_0\}) = 1 \\ & \Gamma = \Gamma_{p_0}(\mathcal{S}) \end{array}$$

Because of that, the infimum in the definition of those parameters is in fact a minimum and both of them are rational numbers. Nevertheless, this does not mean that the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$ can be efficiently computed. Observe that both the number of variables and of constraints are exponential on the number of participants.

Since not all polymatroids are poly-entropic, we may expect that $\kappa(\Gamma) < \sigma(\Gamma)$ in general. Nevertheless not many examples have been found of access structures in which the equality does not hold. Nevertheless, Theorem 3.3.2, which was proved by Csirmaz [16], implies that the lower bounds on $\sigma(\Gamma)$ that are obtained by finding lower bounds on $\kappa(\Gamma)$ are at most linear on the number of participants. Even though we do not have a proof for that, this seems to imply that those lower bounds are not very good. We need the following technical result, which was also proved by Csirmaz [16].

Proposition 3.3.1. *Let* Γ *be a perfect access structure on a set* P *and let* $\mathcal{S}' = (P, f)$ *be a polymatroid with ground set* P. *The polymatroid* $\mathcal{S}'$ *can be extended to a polymatroid*

$\mathcal{S} = (Q, f)$ with $f(\{p_0\}) = 1$ such that $\mathcal{S} \setminus \{p_0\} = \mathcal{S}'$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$ if and only if the following conditions are satisfied.

1. *If $A \subseteq B \subseteq P$ are such that $A \notin \Gamma$ and $B \in \Gamma$, then $f(A) \leq f(B) - 1$.*
2. *If $A, B \in \Gamma$ and $A \cap B \notin \Gamma$, then $f(A \cup B) + f(A \cap B) \leq f(A) + f(B) - 1$.*

Theorem 3.3.2. *If Γ is an access structure on a set of n participants, then $\kappa(\Gamma) \leq n$.*

Proof. For a set P with $|P| = n$, consider the polymatroid $\mathcal{S}' = (P, f)$ defined by $f(X) = n + (n-1) + \cdots + (n-(k-1))$ if $|X| = k$. This polymatroid satisfies the conditions in Proposition 3.3.1 for every access structure Γ. □

Anyway, the polymatroid technique, that is, finding lower bounds on $\kappa(\Gamma)$, has proved to be very useful when studying some particular families of access structures. In some cases the obtained lower bounds are tight or, at least, close to the best known upper bounds. As an example of the kind of results that are obtained by using this technique, we present the *independent sequence method*, which was introduced in [7] and was improved in [45]. Let Γ be an access structure on a set of participants P. Consider $A \subseteq P$ and an increasing sequence of subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$. We say that $(B_1, \ldots, B_m \,|\, A)$ is an *independent sequence* in Γ with *length* m and *size* s if $|A| = s$ and, for every $i = 1, \ldots, m$, there exists $X_i \subseteq A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ if $i \geq 2$. The independent sequence method is based on Theorem 3.3.4. We notice that this result was not stated in [7, 45] in terms of polymatroids, but in terms of the entropy function.

Lemma 3.3.3. *Let Γ be an access structure on the set P and let $\mathcal{S} = (Q, f)$ be a polymatroid such that $f(\{p_0\}) = 1$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. Then, for every $A, B \subseteq P$,*

- *$f(A|B) = 1 + f(A|B \cup \{p_0\})$ if $B \notin \Gamma$ and $A \cup B \in \Gamma$, and*
- *$f(A|B) = f(A|B \cup \{p_0\})$ if $B \in \Gamma$.*

Proof. The equality $f(A|B) + f(\{p_0\}|A \cup B) = f(\{p_0\}|B) + f(A|B \cup \{p_0\})$ proves both statements. □

Theorem 3.3.4 ([7, 45])**.** *Let Γ be an access structure on the set P and let $\mathcal{S} = (Q, f)$ be a polymatroid such that $f(\{p_0\}) = 1$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \,|\, A)$ with length m and size s, then $f(A) \geq m$, and consequently $\kappa(\Gamma) \geq m/s$.*

Proof. We prove first that $f(A) - f(A|B_m) \geq m - 1$ by induction on m. This is obviously true if $m = 1$. Suppose that $m \geq 2$ and take $b_m = B_m - B_{m-1}$. By Lemma 3.3.3,

$$\begin{aligned} f(A|B_{m-1}) - f(A|B_m) &= f(b_m|B_{m-1}) - f(b_m|A \cup B_{m-1}) \\ &\geq f(b_m|X_m \cup B_{m-1}) - f(b_m|A \cup B_{m-1}) \\ &= 1 + f(b_m|X_m \cup B_{m-1} \cup \{p_0\}) - f(b_m|A \cup B_{m-1} \cup \{p_0\}) \\ &\geq 1. \end{aligned}$$

By induction hypothesis,

$$f(A) - f(A|B_m) = f(A) - f(A|B_{m-1}) + (A|B_{m-1}) - f(A|B_m) \geq m - 1.$$

Therefore, $f(A) \geq m$ because $f(A|B_m) \geq 1$ by Lemma 3.3.3. Finally, since $\sum_{i \in A} f(\{i\}) \geq f(A) \geq m$, there must exist $i \in A$ with $f(\{i\}) \geq m/|A| = m/s$. Since this holds for every polymatroid $\mathcal{S} = (Q, f)$ with $f(\{p_0\}) = 1$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$, it is clear that $\kappa(\Gamma) \geq m/s$. □

By using this and other techniques, Csirmaz [16] was able to find a family of access structures which contains, for every positive integer n, an access structure Γ_n on n participants such that $\kappa(\Gamma_n) \geq n/\log n$. This is the best known lower bound on the asymptotic behavior of the optimal information ratio.

In the following we prove another positive result about the polymatroid technique. Namely, we prove in Theorem 3.3.8 that the bounds that are obtained by this technique for an access structure apply also to its dual.

There exist several inequivalent ways to define the dual of a polymatroid [57] and we have to choose the suitable one to prove our result. Specifically, if $\mathcal{S} = (Q, f)$ is a polymatroid, we consider the *dual polymatroid* $\mathcal{S}^* = (Q, f^*)$, where $f^*\colon \mathcal{P}(Q) \to \mathbb{R}$ is defined by

$$f^*(X) = \sum_{x \in X} f(\{x\}) - f(Q) + f(Q - X).$$

Clearly, if $M = (Q, r)$ is a matroid with $r(\{x\}) = 1$ for every $x \in Q$, then the dual matroid of M coincides with the dual polymatroid. We prove in the next lemma that $\mathcal{S}^*$ is actually a polymatroid, and we describe in Lemma 3.3.6 the relation between the dual of a polymatroid and the dual of the associated access structure.

Lemma 3.3.5. *$\mathcal{S}^* = (Q, f^*)$ is a polymatroid.*

Proof. Obviously, $f^*(\emptyset) = 0$. Take a subset $X \subseteq Q$ and a point $y \notin X$. Since $f(\{y\}) + f(Q-(X\cup\{y\})) \geq f(Q-X)$, we get that $f^*(X\cup\{y\}) \geq f^*(X)$. Therefore, f^* is monotone increasing. Finally, consider two arbitrary subsets $X, Y \subseteq Q$. Then from the definition of f^* and the submodularity of f,

$$f^*(X) + f^*(Y) - f^*(X \cup Y) - f^*(X \cap Y) =$$

$$= f(Q - X) + f(Q - Y) - f(Q - (X \cup Y)) - f(Q - (X \cap Y)) \geq 0.$$

This proves that f^* is submodular. □

Lemma 3.3.6. *Let Γ be an non-degenerate perfect access structure and let $\mathcal{S} = (Q, f)$ be a polymatroid such that $f(\{p_0\}) = 1$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. Then $\mathcal{S}^* = (Q, f^*)$ satisfies that $f^*(\{p_0\}) = 1$ and $\Gamma^* = \Gamma_{p_0}(\mathcal{S}^*)$.*

Proof. Since Γ is non-degenerate, $f(P) = f(Q)$, and hence $h^*(\{p_0\}) = 1$. For every $X \subseteq P$,

$$f^*(X \cup \{p_0\}) = f(\{p_0\}) + \sum_{x \in X} f(\{x\}) - f(Q) + f(P - X).$$

If $X \in \Gamma^*$, then $P - X \notin \Gamma$ and $f(P - X) = f(Q - X) - 1$, which implies that

$$f^*(X \cup \{p_0\}) = f^*(X).$$

Finally, $f^*(X\cup\{p_0\}) = f^*(X)+1$ if $X \notin \Gamma^*$ because in this case $f(P-X) = f(Q-X)$. □

To be precise, the polymatroid $\mathcal{S}^*$ is properly a dual of $\mathcal{S}$, in the sense that $\mathcal{S}^{**} = \mathcal{S}$, if and only if $f(Q-\{x\}) = f(Q)$ for every $x \in Q$. The polymatroids satisfying this property will be said to be *normalized*. In addition, we need some technical results that are given in the next lemma, whose proof is an easy exercise.

Lemma 3.3.7. *Let $\mathcal{S} = (Q, f)$ be a polymatroid. Then the following properties hold.*

1. *The polymatroid $\mathcal{S}^* = (Q, f^*)$ is normalized.*

2. *$f^{**}(X) \leq f(X)$ for every $X \subseteq Q$.*

3. *$\mathcal{S}$ is normalized if and only if $\mathcal{S}^{**} = \mathcal{S}$.*

4. *If $\mathcal{S}$ is normalized, then $f^*(\{x\}) = f(\{x\})$ for every $x \in Q$, and hence $\sigma_{p_0}(\mathcal{S}^*) = \sigma_{p_0}(\mathcal{S})$.*

Theorem 3.3.8. *If Γ is a non-degenerate perfect access structure, then $\kappa(\Gamma) = \kappa(\Gamma^*)$ and $\widetilde{\kappa}(\Gamma) = \widetilde{\kappa}(\Gamma^*)$.*

Proof. Let $\mathcal{S} = (Q, f)$ be a polymatroid such that $f(\{p_0\}) = 1$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$. From the fact that $\Gamma^{**} = \Gamma$ and Lemma 3.3.6, we have that $\Gamma^* = \Gamma_{p_0}(\mathcal{S}^*)$ and $\Gamma = \Gamma_{p_0}(\mathcal{S}^{**})$ $\mathcal{S}^*$ and $\mathcal{S}^{**}$ are, Observe that $\sigma_{p_0}(\mathcal{S}^{**}) \leq \sigma_{p_0}(\mathcal{S})$ by Lemma 3.3.7, (2). In addition, since $\mathcal{S}^*$ is normalized, we have that $\sigma_{p_0}(\mathcal{S}^*) = \sigma_{p_0}(\mathcal{S}^{**})$ by Lemma 3.3.7, (4). Therefore, for every access structure Γ and for every $\mathcal{S}$ with $\Gamma = \Gamma_{p_0}(\mathcal{S})$, exists a polymatroid $\mathcal{S}^*$ with $\Gamma^* = \Gamma_{p_0}(\mathcal{S}^*)$ such that $\sigma_{p_0}(\mathcal{S}^*) \leq \sigma_{p_0}(\mathcal{S})$, and hence $\kappa(\Gamma^*) \leq \kappa(\Gamma)$. Dually, $\kappa(\Gamma^*) \leq \kappa(\Gamma^{**})$. The same argument can be used to prove that $\widetilde{\kappa}(\Gamma) = \widetilde{\kappa}(\Gamma^*)$. □

3.4 The Problem Is Solved for Some Access Structures

We present here some examples of access structures for which we can find the exact value of their optimal information ratio. In addition to the few access structures that are discussed here, one can find in the literature many more cases in which the problem has been solved. For instance, most of the access structures on at most five participants [34], most of the access structures defined by graphs with at most six vertices [22] and, most remarkably, all access structures defined by trees [19].

On the set $P_4 = \{1, 2, 3, 4\}$, Consider the access structures Γ_1 and Γ_2 with $\min \Gamma_1 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ and $\min \Gamma_2 = \min \Gamma_1 \cup \{\{2, 4\}\}$. The dual access structure Γ_1^* is isomorphic to Γ_1, while $\min \Gamma_2^* = \{\{2, 3\}, \{2, 4\}, \{1, 3, 4\}\}$. We presented in Section 3.2 a linear secret sharing scheme for Γ_1 with information ratio equal to $3/2$. A similar construction can be done for Γ_2. Therefore, $\sigma(\Gamma_j) \leq \lambda(\Gamma_j) \leq 3/2$ for $j = 1, 2$ and, by Theorem 3.1.3, $\sigma(\Gamma_2^*) \leq \lambda(\Gamma_2^*) = \lambda(\Gamma_2) \leq 3/2$. On the other hand, by taking $B_1 = \emptyset$, $B_2 = \{1\}$, and $B_3 = \{1, 4\}$ with $X_1 = \{2, 3\}$, $X_2 = \{2\}$, and $X_3 = \{3\}$, we obtain an independent sequence with length $m = 3$ and size $s = 2$ that applies to both Γ_1 and Γ_2. Hence, by Theorem 3.3.4, $\kappa(\Gamma_j) \geq 3/2$ if $j = 1, 2$ and $\kappa(\Gamma_2^*) \geq 3/2$ by Theorem 3.3.8. Therefore, we have been able to determine the optimal information ratios of the access structures Γ_1, Γ_2 and Γ_2^*, which are all equal to $3/2$.

Consider now, for every $k \geq 3$, the access structure Γ_k on the set $P = \{x_0, x_1, \ldots, x_k\}$ whose minimal qualified sets are $\{x_1, \ldots, x_k\}$ and all pairs $\{x_0, x_i\}$. We prove in the following that $\sigma(\Gamma_k) = 2 - 1/(k-1)$.

Proposition 3.4.1. *$\kappa(\Gamma_k) \geq 2 - 1/(k-1)$ for every $k \geq 3$.*

Proof. Let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(\{p_0\}) = 1$ and $\Gamma_k = \Gamma_{p_0}(\mathcal{S})$. Take $B_1 = \emptyset$, and $B_2 = \{x_{k-1}\}$, and $B_j = \{x_{k-j+2}, \ldots, x_k\}$ for every $j = 3, \ldots, k$. In addition, take $X_1 = \{x_0, x_1\}$, and $X_2 = \{x_0\}$, and $X_j = \{x_1, \ldots, x_{k-j+1}\}$ for every $j = 3, \ldots, k$. It

is easy to check that $(B_1, \ldots, B_{k+1} \mid A)$, where $A = \{x_0, x_1, \ldots, x_{k-2}\}$, is an independent sequence, and hence $f(A) \geq k$ by Theorem 3.3.4. In addition,

$$f(A) = f(\{x_0\}) + \sum_{j=1}^{k-2} f(\{x_j\}|\{x_0, \ldots, x_{j-1}\}) \leq f(\{x_0\}) + f(\{x_1\}) + \sum_{j=2}^{k-2} f(\{x_j\}|\{x_0, x_1\}).$$

By Lemma 3.3.3,

$$f(\{x_j\}|\{x_0\}) - f(\{x_j\}|\{x_0, x_1\}) = 1 + f(\{x_j\}|\{x_0, p_0\}) - f(\{x_j\}|\{x_0, x_1, p_0\}) \geq 1,$$

and hence $f(\{x_j\}|\{x_0, x_1\}) \leq f(\{x_j\}|\{x_0\}) - 1 \leq f(\{x_j\}) - 1$ for every $j = 2, \ldots, k-2$. Therefore, $f(A) \leq k - 3 + \sum_{j=0}^{k-2} f(\{x_j\})$, and hence $\sum_{j=0}^{k-2} f(\{x_j\}) \geq 2k - 3$. This implies that $f(\{x_j\}) \geq (2k-3)/(k-1)$ for some $j = 0, \ldots, k-2$. □

Proposition 3.4.2. *For every $k \geq 3$ and for every finite field $\mathbb{K}$ with at least 3 elements, there exists a $\mathbb{K}$-linear secret sharing scheme Σ with access structure Γ_k, set of secret values $\mathbb{K}^{k-1}$, and information ratio equal to $2 - 1/(k-1)$.*

Proof. We begin by constructing two $\mathbb{K}$-linear secret sharing schemes for Γ_k. Consider $E = \mathbb{K}^{k+1}$, and $E_{p_0} = E_{x_0} = \mathbb{K}$, and $E_{x_j} = \mathbb{K}^2$ for every $j = 1, \ldots, k$. Consider, for $x \in Q = P \cup \{p_0\}$, the linear maps $\pi_x \colon E \to E_x$ determined by

- $\pi_{p_0}(s, a, b_1, \ldots, b_{k-1}) = s$,
- $\pi_{x_0}(s, a, b_1, \ldots, b_{k-1}) = a$
- $\pi_{x_j}(s, a, b_1, \ldots, b_{k-1}) = (s - a, b_j)$ for $j = 1, \ldots, k-1$, and
- $\pi_{x_k}(s, a, b_1, \ldots, b_{k-1}) = (s - a, s + b_1 + \cdots + b_{k-1})$.

These maps define a $\mathbb{K}$-linear secret sharing scheme Σ_1 with access structure Γ_k. Consider now $F = \mathbb{K}^k$, and $F_{p_0} = \mathbb{K}$, and $F_{x_0} = \mathbb{K}^{k-1}$, and $F_{x_j} = \mathbb{K}$ for every $j = 1, \ldots, k$. Consider, for $x \in Q = P \cup \{p_0\}$, the linear mappings $\tau_x \colon F \to F_x$ determined by

- $\tau_{p_0}(s, c_1, \ldots, c_{k-1}) = s$,
- $\tau_{x_0}(s, c_1, \ldots, c_{k-1}) = (c_1, \ldots, c_{k-1})$,
- $\tau_{x_1}(s, c_1, \ldots, c_{k-1}) = \lambda s - c_1$, where $\lambda \in \mathbb{K} - \{0, 1-k\}$,
- $\tau_{x_j}(s, c_1, \ldots, c_{k-1}) = s - c_j$ for $j = 2, \ldots, k-1$, and
- $\tau_{x_k}(s, c_1, \ldots, c_{k-1}) = s + c_1 + \cdots + c_{k-1}$.

The access structure of the $\mathbb{K}$-linear secret sharing scheme Σ_2 defined by these mappings is again Γ_k.

By combining $k-2$ copies of the scheme Σ_1 with the scheme Σ_2, we obtain a $\mathbb{K}$-linear secret sharing scheme for Γ_k with set of secrets $\mathbb{K}^{k-1}$ and information ratio equal to $(2k-3)/(k-1)$. □

3.5 Exercises

3.1. Explain how to construct a linear secret sharing scheme with information ratio equal to 3/2 for the perfect access structure Γ on the set $P = \{1, 2, 3, 4\}$ whose minimal qualified sets are $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$, $A_3 = \{3, 4\}$, and $A_4 = \{2, 4\}$.

Chapter 4

Ideal Secret Sharing Schemes

4.1 Brickell-Davenport Theorem

We introduced in Section 2.4 a family of ideal perfect secret sharing schemes whose access structures coincide with the ports of the linear matroids. A natural question arising at this point is to find out if there are other access structures that admit an ideal secret sharing scheme or, more generally, to try to determine what access structures admit an ideal secret sharing scheme. A perfect access structure is called *ideal* if it admits an ideal secret sharing scheme.

Brickell and Davenport [10] generalized Theorem 2.4.2 by proving that every ideal secret sharing scheme (linear or not) defines a matroid M with ground set $Q = P \cup \{p_0\}$ such that the access structure of the scheme is the matroid port $\Gamma_{p_0}(M)$. We present here a combinatorial version of that result.

Lemma 4.1.1. *Let Γ be a perfect access structure and let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(\{p_0\}) = 1$ and $\Gamma_{p_0}(\mathcal{S}) = \Gamma$. If $C \notin \Gamma$ and $C \cup \{x\} \in \Gamma$, then $f(\{x\}|C) = 1$ and $f(\{x\}|C \cup \{p_0\}) = 0$.*

Proof. Use $f(C)+f(\{p_0\}|C)+f(\{x\}|C\cup\{p_0\}) = f(B)+f(\{p_0\}|B)$, where $B = C\cup\{x\}$. □

Theorem 4.1.2. *Let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(\{p_0\}) = 1$ such that the access structure $\Gamma_{p_0}(\mathcal{S})$ is perfect and connected. If $f(\{x\}) = 1$ for every $x \in Q$, then $\mathcal{S}$ is a matroid.*

Proof. Since $f(A \cup \{p_0\}) - f(A) \in \{0, 1\}$, we only have to prove that $f(A) \in \mathbb{Z}$ for every $A \subseteq P$. Suppose that f is not integer-valued and take $A \subseteq P$, minimal with $f(A) \notin \mathbb{Z}$. Then $m < f(A) < m + 1$ for some integer m. Clearly, $f(A - \{x\}) = m$ and $0 < f(\{x\}|A - \{x\}) < 1$ for every $x \in A$.

Suppose that $A \in \Gamma$. By Lemma 4.1.1, $A-\{x\} \in \Gamma$ for every $x \in A$. Let B be a minimal qualified set with $B \subseteq A$, and take $x \in B$ and $C = B-\{x\}$. Then $f(\{x\}|C\cup\{p_0\}) = 0$ and, since $A-\{x\}$ is qualified, $f(\{x\}|A-\{x\}) = f(\{x\}|(A-\{x\})\cup\{p_0\}) = 0$, a contradiction.

Suppose now that $A \notin \Gamma$ and consider $B \subseteq P$, minimal with $B \notin \Gamma$ and $A \cup B \in \Gamma$. There exists such a set because Γ is connected. By Lemma 4.1.1, $f(\{y\}|(A\cup B)-\{y\}) = 1$ for every $y \in B$, and hence $f(A \cup B) = f(A) + |B|$. Since $f(\{x\}|(A \cup B) - \{x\}) \leq f(\{x\}|A - \{x\}) < 1$ for every $x \in A$, we have by Lemma 4.1.1 that $(A \cup B) - \{x\} \in \mathcal{A}$ for every $x \in A$. This implies that $f((A \cup B) - \{x\}) = f(A - \{x\}) + |B|$. Consider now a minimal qualified subset C such that $B \subseteq C \subseteq A \cup B$ and take $x \in A \cap C$ and the

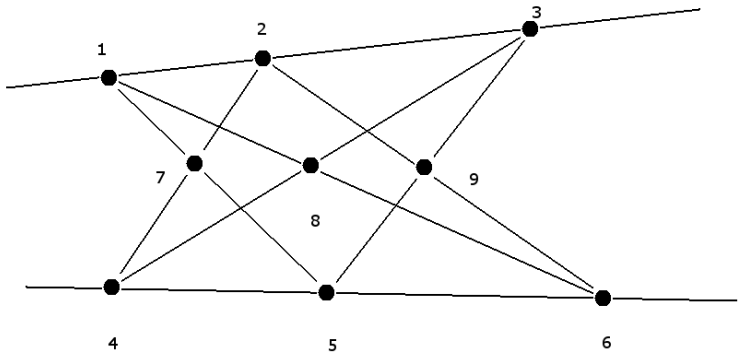

Figure 4.1: The non-Pappus matroid

subsets $C' = C - \{x\}$ and $A' = (A \cup B) - \{x\}$. Then $f(\{x\}|C' \cup \{p_0\}) = 0$, and hence $f(\{x\}|A') = f(\{x\}|A' \cup \{p_0\}) = 0$. Therefore, $f(A \cup B) = f(A') + f(\{x\}|A') = f(A')$, which implies that $f(A) = f(A - \{x\})$, a contradiction. □

In particular, Theorem 4.1.2 implies that Γ is a matroid port if and only if $\kappa(\Gamma) = 1$. Another consequence of Theorem 4.1.2 is that the symmetry property that was proved in Section 2.4 for vector space secret sharing schemes applies to every ideal secret sharing scheme. Namely, if a collection $(S_i)_{i \in Q}$ of random variables defines an ideal secret sharing scheme on $Q - \{p_0\}$ for some $p_0 \in Q$, then it defines as well an ideal secret sharing scheme on $Q - \{p\}$ for every $p \in Q$.

4.2 Two Counterexamples and Two Open Problems

Observe that Theorem 2.4.2 provides a sufficient condition for an access structure to be ideal. Namely, the ports of linear matroids are ideal access structures. As a consequence of Theorem 4.1.2, an access structure is ideal if and only if it is a port of some poly-entropic matroid. In particular, being a matroid port is a necessary condition for an access structure to be ideal. Seymour [48] showed that the necessary condition is not sufficient by proving that the ports of the Vámos matroid are not ideal access structures. On the other hand, Simonis and Ashikhmin [53] proved that the sufficient condition is not necessary because the non-Pappus matroid is not linearly representable but each of its ports admit an ideal secret sharing scheme.

The ground set of the *Vámos matroid* is $Q = \{1, \ldots, 8\}$ and its bases are all subsets with 4 elements except $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{3,4,5,6\}$, $\{3,4,7,8\}$, and $\{5,6,7,8\}$. Observe that, by identifying the pairs $\{1,2\}$, $\{3,4\}$, $\{5,6\}$, and $\{7,8\}$ we obtain from the Vámos matroid the integer polymatroid defined in Exercise 1.4. Since this polymatroid is not linear over any field, the same applies to the Vámos matroid. Moreover, by using the information inequality given by Zhang and Yeung [58], which is discussed in Chapter 5, it can be easily proved that the Vámos matroid is not poly-entropic. Seymour [48] presented a direct combinatorial proof of this fact. Bounds on the optimal information ratio of the ports of the Vámos matroid are given in Chapter 5.

The matroid on 9 points that is geometrically represented in Figure 4.1 is called the *non-Pappus* matroid. That is, it is a matroid with rank 3 in which all 2-sets are independent and a set with three points is dependent if and only if these points are collinear. For instance, $\{2,4,7\}$ is a dependent set while $\{1,2,8\}$ and $\{7,8,9\}$ are independent. This matroid is not linearly representable over any field. Otherwise, Figure 4.1 would correspond to a configuration of points and lines on a projective plane over some field, and hence the three central points $(7,8,9)$ should be collinear by Pappus Theorem, a contradiction. Nevertheless, Simonis and Ashikhmin [53] proved that the non-Pappus matroid is $\mathbb{F}_3$-poly-linear. Specifically, the following matrix provides an $\mathbb{F}_3$-linear representation of the polymatroid $2M$, where M is the non-Pappus matroid.

$$G = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc|cc} 1&0&1&0&0&0&1&0&0&0&1&0&1&0&1&0&0&0 \\ 0&1&0&1&0&0&0&1&0&0&0&1&0&1&0&1&0&0 \\ 0&0&0&0&0&0&1&0&1&0&2&1&0&1&1&0&1&0 \\ 0&0&0&0&0&0&0&2&0&1&2&0&1&2&0&2&0&1 \\ 0&0&1&0&1&0&0&1&0&0&0&1&0&0&1&1&1&0 \\ 0&0&0&1&0&1&2&1&0&0&2&1&0&0&1&0&0&1 \end{array}\right).$$

Therefore, the non-Pappus matroid is poly-entropic by Theorem 1.6.2, and hence every one of its ports admits an ideal secret sharing scheme. Actually, the matrix G provides an $\mathbb{F}_3$-linear ideal secret sharing scheme for every port of the non-Pappus matroid.

Several classes of matroids and matroid ports have appeared here. Each class contains the preceding ones.

1. The first one is the class of the linear matroids, whose ports are the vector space access structures.

2. The poly-linear matroids form the second class. Their ports are precisely those access structures that admit a linear ideal secret sharing scheme.

3. The class of the poly-entropic matroids and their ports, the ideal access structures.

4. Finally, the class of all matroids and the class of all matroid ports.

The Vámos matroid is not poly-entropic, while the non-Pappus matroid is poly-linear but it is not linear. The existence of poly-entropic matroids that are not poly-linear remains an open question. All those classes are minor-closed, and all but the third one are duality-closed. It is unknown whether the dual of a poly-entropic matroid is poly-entropic.

4.3 Ideal Access Structures Defined by Graphs

For a graph $G = (V, E)$, we consider the access structure $\Gamma[G]$ in which the participants are identified to the vertices of G and the edges correspond to the minimal qualified subsets. In this section, we determine which graph access structures admit an ideal secret sharing scheme. Observe that it is enough to solve this question for connected graphs, because a graph access structure $\Gamma[G]$ admits an ideal secret sharing scheme if and only if this is the case for every connected component of G. Moreover, we can assume that G is not trivial, that is, it has at least two vertices.

We begin by identifying in Proposition 4.3.1 the graph access structures that are matroid ports. Then we prove in Proposition 4.3.2 that all those matroid ports admit a

vector space secret sharing scheme. In a *complete multipartite graph*, the set of vertices is partitioned into several parts and two vertices are adjacent if and only if they belong to different parts.

Proposition 4.3.1. *Let G be a connected graph. Then the access structure $\Gamma[G]$ is a matroid port if and only if G is a complete multipartite graph.*

Proof. Let $G = (V, E)$ be a complete multipartite graph. Take $Q = V \cup \{p_0\}$ and the family $\mathcal{B} \subseteq \mathcal{P}(Q)$ formed by the edges of G and the sets of the form $\{p_0, x\}$ with $x \in V$. Clearly, $\mathcal{B}$ is the family of bases of a matroid M with ground set Q. Moreover, $\Gamma[G] = \Gamma_{p_0}(M)$.

We prove now the converse. Let $G = (V, E)$ be a connected graph and suppose that $\Gamma[G] = \Gamma_{p_0}(M)$ for some matroid $M = (Q, r)$ with $Q = V \cup \{p_0\}$.

We affirm that the matroid M has rank 2, that is, $r(Q) = 2$. This can be proved by induction on n, the number of vertices. If $n = 2$, then $Q = \{p_0, x, y\}$ and $\{x, y\}$ is the only qualified set. Clearly, $\{x, p_0\}$ is independent but Q is dependent, and hence $r(Q) = 2$. Suppose that $n > 2$. Take a vertex $x \in V$ such that the subgraph G' of G induced by $V - \{x\}$ is connected (such a vertex always exist). Then $\Gamma[G'] = \Gamma[G] \setminus \{x\}$, and hence $\Gamma[G'] = \Gamma_{p_0}(M \setminus \{x\})$ by Proposition 2.1.2. By the induction hypothesis, the matroid $M \setminus \{x\}$ has rank 2, and hence $r(Q - \{x\}) = 2$. Let $y \in V - \{x\}$ be a neighbor of x. Then $r(\{p_0, y\}) = r(\{p_0, x, y\}) = 2$. Finally, $r(Q) + r(\{p_0, y\}) \leq r(Q - \{x\}) + r(\{p_0, x, y\})$, and hence $r(Q) = 2$.

Consider the binary relation on V defined by $x \sim y$ if and only if $x = y$ or $\{x, y\}$ is a dependent set of M. It is not difficult to check that this is an equivalence relation, which induces a partition $V = V_1 \cup \cdots \cup V_s$. Observe that a subset $\{x, y\} \subseteq V$ is in $\Gamma_{p_0}(M)$ if and only if $\{x, y\}$ is a basis of M, that is, if and only $x \in V_i$ and $y \in V_j$ with $i \neq j$. Therefore, G is a complete multipartite graph. □

Proposition 4.3.2. *If G is a complete multipartite graph, then the access structure $\Gamma[G]$ admits a vector space secret sharing scheme.*

Proof. Let $G = (V, E)$ be a complete multipartite graph for the partition $V = V_1 \cup \cdots \cup V_s$ of the set of vertices. Consider a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq s$ and a $\mathbb{K}$-vector space secret sharing scheme Σ for the $(2, s)$-threshold access structure on the set of participants $\{V_1, \ldots, V_s\}$ Finally, consider a secret sharing scheme on the set V in which all participants in V_i receive the share corresponding to V_i according to the scheme Σ. Clearly, this is a $\mathbb{K}$-vector space secret sharing scheme for the access structure $\Gamma[G]$. □

Propositions 4.3.1 and 4.3.2 provide a characterization of the ideal access structures defined by graphs. This characterization and an additional result are given in Theorem 4.3.4.

Lemma 4.3.3. *Let G be a connected graph. If G is not a complete multipartite graph, then there exists an induced subgraph of G on four vertices which is isomorphic to one of the graphs in Figure 4.2.*

Proof. A graph G is a complete multipartite graph if and only if every connected component of its complementary graph G' is a complete graph. Let G be a connected graph that is not a complete multipartite graph and let G' be its complement. If there exist two vertices x, y of G at distance 3, a shortest path joining these to vertices produces an induced subgraph of G that is isomorphic to the first graph in Figure 4.2. Suppose that the diameter of G is equal to 2. Since one of the connected components of the complementary

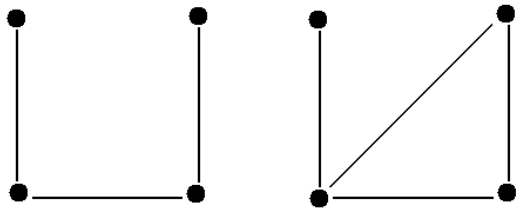

Figure 4.2: Forbidden subgraphs of complete multipartite graphs

graph G' is not a complete graph, there exist three vertices x, y, z of G such that $\{x, y\}$ and $\{y, z\}$ are edges of G' and $\{x, z\}$ is not (and hence it is an edge of G). Since $\{x, y\}$ is not an edge of G, the distance in G between these two vertices is equal to 2, so there exists a vertex t that is adjacent in G to x and to y. Clearly, the subgraph of G induced by the vertices x, y, z, t is isomorphic to one of the graphs in Figure 4.2. □

Theorem 4.3.4. *Let G be a connected graph. Then the following statements are equivalent.*

1. *G is a complete multipartite graph.*
2. *$\Gamma[G]$ is a vector space access structure.*
3. *$\Gamma[G]$ is an ideal access structure.*
4. *$\Gamma[G]$ is a matroid port.*
5. *$\sigma(\Gamma[G]) < 3/2$.*

Proof. The equivalence between the first four statements has been proved already. Therefore, $\sigma(\Gamma[G]) = 1 < 3/2$ if G is a complete multipartite graph. Otherwise, by Lemma 4.3.3, there exist an induced subgraph of G that is isomorphic to one of the graphs in Figure 4.2. This implies that one of the access structures Γ_1 or Γ_2 defined in Section 3.4 is a minor of $\Gamma[G]$. Therefore, $\sigma(\Gamma[G]) \geq 3/2$ by Theorem 3.1.2. □

4.4 A Generalization of Brickell-Davenport Theorem

As a consequence of Theorem 4.3.4, there does not exist any graph G such that the access structure $\Gamma[G]$ satisfies $1 < \sigma(\Gamma[G]) < 3/2$. The ideal access structures have been characterized for other families, and in many of them the same gap in the values of the optimal information ratio appears. This is the case for the access structures on at most five participants [34], the bipartite access structures [45], the structures with at most four minimal qualified subsets [38], and the ones with intersection number equal to one [39].

A common explanation to this repeated phenomenon was provided in [40]. By using Theorem 4.4.1, a characterization of matroid ports by excluded minors presented in 1976 by Seymour [47]. Another characterization of matroid ports was previously given by Lehman [37].

Theorem 4.4.1. *A perfect access structure is a matroid port if and only if it does not have any minor isomorphic to one of the access structures Γ_1, Γ_2, Γ_2^*, or Γ_k with $k \geq 3$ that were defined in Section 3.4.*

Since the value of κ is at least $3/2$ for all those forbidden minors, we obtain the following corollary of Theorems 4.1.2 and 4.4.1.

Corollary 4.4.2. *If Γ is not a matroid port, then $\kappa(\Gamma) \geq 3/2$. As a consequence, the access structure of every secret sharing scheme Σ with $\sigma(\Sigma) < 3/2$ is a matroid port.*

In all the aforementioned families of access structures, the matroid ports coincide with the ideal access structures, and hence the gap in the values of the optimal information ratio is explained by Corollary 4.4.2. This gap does not hold in general, because $1 < \sigma(\Gamma) < 3/2$ if Γ is a port of the Vámos matroid [2]. This result is explained in more detail in Chapter 5.

Another consequence of Corollary 4.4.2 is the existence of a gap in the values of the parameter κ. Indeed, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$. The existence of other gaps in the values of this parameter is a natural question. For instance, from the results in [17, 18, 19, 41], one could conjecture that, if $\kappa(\Gamma) < 2$, then $\kappa(\Gamma) = 2 - 1/s$ for some positive integer s. This is the case as well for the access structures Γ_k that are analyzed in Section 3.4. Nevertheless, two access structures that refute this conjecture were presented in [26], namely one with $\kappa(\Gamma) = 22/13$ and another one with $\kappa(\Gamma) = 99/53$.

Chapter 5

Information Inequalities and Secret Sharing

5.1 Information Inequalities

In 1998, Zhang and Yeung [58] presented for the first time a linear inequality that has to be satisfied by the joint Shannon entropies of every collection of four random variables and cannot be derived from the polymatroid axioms. These axioms are also called Shannon information inequalities, because they are equivalent to the basic inequalities on Shannon entropies that are discussed in Section 1.5. Because of that, Zhang-Yeung inequality is said to be a *non-Shannon information inequality*. Other such linear inequalities have been found in [23, 25, 42] and other works. Matúš [42] found an infinite number of independent linear non-Shannon information inequalities that apply to every family of four random variables. No such inequality exists for families of at most three random variables. Clearly, the rank function of every entropic polymatroid must satisfy all those non-Shannon information inequalities and, since they are linear, this also applies to poly-entropic polymatroids. Therefore, those inequalities can be used to prove that a given polymatroid is not poly-entropic.

Before the discovery of non-Shannon inequalities, Ingleton [31] presented a linear inequality that must be satisfied by the rank function of every linear polymatroid on a ground set with four points. Since it is a linear inequality, it must be satisfied as well by the joint Shannon entropies of every linear collection of four random variables. Ingleton inequality can be derived from a property of linear collections of random variables that does not extend to the general case. Namely, the existence, for every pair of random variables in the collection, of an additional random variable conveying their common information. More specifically, let $(S_i)_{i\in Q}$ be a $\mathbb{K}$-linear family of random variables and $(V_i)_{i\in Q}$ a $\mathbb{K}$-linear representation of the polymatroid (Q, f), where $f(A) = H(S_A)/\log|\mathbb{K}|$ for every $A \subseteq Q$ (see Section 1.6). Then, for every $\{i, j\} \subseteq Q$, the random variable T that can be obtained from the intersection of the vector subspaces V_i and V_j conveys the common information of the random variables S_i and S_j. This means that T can be derived from both S_i and S_j, that is $H(T|S_i) = H(T|S_j) = 0$, and has maximum entropy among all random variables with that property because $H(T) = H(S_i) - H(S_i|S_j)$. This property has been used in [24] to find other linear inequalities that apply to the rank function of linearly representable polymatroids. We present Ingleton inequality in Theorem 5.1.3. Two technical lemmas are needed to prove it.

Lemma 5.1.1. *If f is the rank function of a polymatroid, then*

$$f(\{b\}|\{c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a\}) \geq 0$$

for every four elements a, b, c, d in the ground set.

Proof. Since f is submodular, $f(X|Y) \geq f(X|Y \cup Z)$ for every $X, Y, Z \subseteq Q$, and hence

$$\begin{aligned} & f(\{b\}|\{c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a\}) \\ & \quad \geq \quad f(\{b\}|\{a,c,d\}) - f(\{b\}|\{a,c\}) + f(\{d\}|\{a,c\}) \\ & \quad = \quad f(\{b,d\}|\{a,c\}) - f(\{b\}|\{a,c\}) \\ & \quad \geq \quad 0, \end{aligned}$$

and the proof is finished. □

Lemma 5.1.2. *If f is the rank function of a polymatroid, then*

$$\begin{aligned} f(\{x_5\}) \quad \leq \quad & f(\{x_1\}|\{x_3\}) - f(\{x_1\}|\{x_2,x_3\}) + f(\{x_1\}|\{x_4\}) - f(\{x_1\}|\{x_2,x_4\}) + \\ & + f(\{x_3\}) - f(\{x_3\}|\{x_4\}) + 2f(\{x_5\}|\{x_1\}) + 2f(\{x_5\}|\{x_2\}) \end{aligned}$$

for every five elements $x_1, \ldots, x_5$ in the ground set.

Proof. By using Lemma 5.1.1 twice, the second term in the inequality is greater than or equal to α_1, where

$$\begin{aligned} \alpha_1 \quad = \quad & f(\{x_1\}|\{x_3\}) - f(\{x_1\}|\{x_3,x_5\}) + f(\{x_1\}|\{x_4\}) - f(\{x_1\}|\{x_4,x_5\}) + \\ & + f(\{x_3\}) - f(\{x_3\}|\{x_4\}) + 2f(\{x_5\}|\{x_1\}). \end{aligned}$$

Observe that the sets in Equation (1.1) can be taken in any order. Therefore,

$$\begin{aligned} \alpha_1 \quad = \quad & f(\{x_5\}|\{x_3\}) - f(\{x_5\}|\{x_1,x_3\}) + f(\{x_5\}|\{x_4\}) - f(\{x_5\}|\{x_1,x_4\}) + \\ & + f(\{x_3\}) - f(\{x_3\}|\{x_4\}) + 2f(\{x_5\}|\{x_1\}). \end{aligned}$$

Now we apply again Lemma 5.1.1 twice and we obtain

$$\alpha_1 \geq f(\{x_5\}|\{x_3\}) + f(\{x_5\}|\{x_4\}) + f(\{x_3\}) - f(\{x_3\}|\{x_4\}) = \alpha_2.$$

Applying Lemma 5.1.2 another time,

$$\alpha_2 \geq f(\{x_5\}|\{x_3\}) + f(x_3) - f(x_3|x_5) = f(x_5),$$

which concludes the proof. □

Theorem 5.1.3. ***Ingleton inequality.*** *Let $\mathcal{S} = (Q, f)$ be a poly-linear polymatroid with ground set $Q = \{x_1, x_2, x_3, x_4\}$. Then*

$$f(\{x_1\}) + f(\{x_2\}) + f(\{x_3,x_4\}) + f(\{x_1,x_2,x_3\}) + f(\{x_1,x_2,x_4\}) \leq$$

$$\leq f(\{x_1,x_2\}) + f(\{x_1,x_3\}) + f(\{x_1,x_4\}) + f(\{x_2,x_3\}) + f(\{x_2,x_4\}).$$

Proof. Obviously, we can assume that $\mathcal{S}$ is $\mathbb{K}$-linear for some field $\mathbb{K}$. Let $(V_i)_{1\leq i\leq 4}$ be a $\mathbb{K}$-linear representation of $\mathcal{S}$. Take $V_5 = V_1 \cap V_2$ and consider the polymatroid $\widehat{\mathcal{S}} = (\widehat{Q}, f)$ with ground set $\widehat{Q} = Q \cup \{x_5\}$ that is $\mathbb{K}$-linearly representated by the collection $(V_i)_{1\leq i\leq 5}$. Then $f(\{x_5\}|\{x_1\}) = f(\{x_5\}|\{x_2\}) = 0$ and $f(\{x_5\}) = f(\{x_1\}) - f(\{x_1\}|\{x_2\})$. Therefore, by Lemma 5.1.2,

$$\begin{aligned} f(\{x_1\}) - f(\{x_1\}|\{x_2\}) \quad \leq \quad & f(\{x_1\}|\{x_3\}) - f(\{x_1\}|\{x_2, x_3\}) + \\ & + f(\{x_1\}|\{x_4\}) - f(\{x_1\}|\{x_2, x_4\}) + \\ & + f(\{x_3\}) - f(\{x_3\}|\{x_4\}). \end{aligned}$$

Ingleton inequality is obtained after expanding terms in this expression. □

Ingleton inequality can be generalized by applying it to subsets, instead of elements, of the ground set.

Corollary 5.1.4. ***Ingleton inequality, general version.*** *Let $\mathcal{S} = (Q, f)$ be a poly-linear polymatroid. Then*

$$f(X_1) + f(X_2) + f(X_3 \cup X_4) + f(X_1 \cup X_2 \cup X_3) + f(X_1 \cup X_2 \cup X_4) \leq$$

$$\leq f(X_1 \cup X_2) + f(X_1 \cup X_3) + f(X_1 \cup X_4) + f(X_2 \cup X_3) + f(X_2 \cup X_4)$$

for every four subsets $X_1, X_2, X_3, X_4 \subseteq Q$.

Proof. As before, we can assume that $\mathcal{S}$ is linear. Consider the polymatroid $\mathcal{S}' = (Q', f')$ with ground set $Q' = \{1, 2, 3, 4\}$ and rank function defined by $f'(J) = f(\bigcup_{i\in J} X_i)$ for every $J \subseteq Q'$. Clearly, $\mathcal{S}'$ is linear too. The proof is concluded by applying Theorem 5.1.3 to $\mathcal{S}'$. □

We can prove that the integer polymatroid in Problem 1.4 is not linear by using Theorem 5.1.3. Indeed, if we substitute $x_1 = 2$, $x_2 = 3$, $x_3 = 1$, and $x_4 = 4$ in Ingleton inequality, the first term is equal to 16 while the second one is equal to 15. Therefore, this polymatroid does not satisfy Ingleton inequality, and hence it is not poly-linear. One can use Corollary 5.1.4 to prove that the Vámos matroid, as defined in Section 4.2, is not poly-linear by taking $X_1 = \{3, 4\}$, $X_2 = \{5, 6\}$, $X_3 = \{1, 2\}$, and $X_4 = \{7, 8\}$.

By applying a similar but more elaborate idea, Zhang and Yeung [58] found a linear inequality that is satisfied by every poly-entropic polymatroid.

Theorem 5.1.5. ***Zhang-Yeung inequality.*** *Let $\mathcal{S} = (Q, f)$ be a poly-entropic polymatroid. Then*

$$2f(X_1) + 2f(X_2) + f(X_3) + f(X_3 \cup X_4) + 4f(X_1 \cup X_2 \cup X_3) + f(X_1 \cup X_2 \cup X_4) \leq$$

$$\leq 3f(X_1 \cup X_2) + 3f(X_2 \cup X_3) + 3f(X_1 \cup X_3) + f(X_1 \cup X_4) + f(X_2 \cup X_4)$$

for every four subsets $X_1, X_2, X_3, X_4 \subseteq Q$.

If we apply Theorem 5.1.5 to the Vámos matroid in the same way as we applied Corollary 5.1.4, the first term in the inequality is equal to 34 while the second one is equal to 33. Therefore, the Vámos matroid is not poly-entropic. The same applies to the polymatroid in Problem 1.4.

5.2 Better Lower Bounds on the Optimal Information Ratio

We saw in Section 3.3 that, for a given perfect access structure Γ, the values of $\kappa(\Gamma)$ and $\widetilde{\kappa}(\Gamma)$, and hence lower bounds on $\sigma(\Gamma)$ and $\widetilde{\sigma}(\Gamma)$, can be obtained by solving a linear programming problem. Nevertheless, these lower bounds are not tight in general. In fact, better lower bounds on $\sigma(\Gamma)$ can be obtained for some access structures by using non-Shannon inequalities, which are linear inequalities, to add new constraints to the linear program used to compute $\kappa(\Gamma)$. The same applies to $\widetilde{\sigma}(\Gamma)$. Ingleton inequality can be used similarly to obtain better lower bounds on $\lambda(\Gamma)$ and $\widetilde{\lambda}(\Gamma)$.

This is the case for the ports of the Vámos matroid. One can prove that their optimal information ratios are greater than 1 (the value of κ for them) by adding to the linear program the instance of the Zhang-Yeung inequality that is not satisfied by the rank function of the Vámos matroid (see Section 5.1). This was the first known separation result between the values of the parameters κ and σ, and it was proved in a different way in [2]. Moreover, since the existence of linear secret sharing schemes for the those access structures with information ratio equal to 4/3 was proved in [40], the ports of the Vámos matroid were the first know examples of access structures with $1 < \sigma(\Gamma) < 3/2$. The bounds from [2] were improved in [43] by using some of the non-Shannon inequalities presented in [23].

Every port of the Vámos matroid M is isomorphic to $\Gamma_1 = \Gamma_1(M)$ or $\Gamma_3 = \Gamma_3(M)$. Moreover, $\Gamma_1^* = \Gamma_3$, and hence $\lambda(\Gamma_1) = \lambda(\Gamma_3)$. The best known upper and lower bounds on the optimal information ratios of those access structures, which are obtained from the results in [2, 40, 43], are given in the following.

- $\kappa(\Gamma_1) = 1 < 9/8 \leq \sigma(\Gamma_1) \leq \lambda(\Gamma_1) \leq 4/3$.
- $\kappa(\Gamma_3) = 1 < 19/17 \leq \sigma(\Gamma_3) \leq \lambda(\Gamma_3) \leq 4/3$.
- $5/4 \leq \lambda(\Gamma_1) = \lambda(\Gamma_3) \leq 4/3$.

Ingleton inequality has been used to find separation results between the values of the parameters κ and λ for an infinite family of graph access structures [17].

Even though non-Shannon information inequalities provide better bounds on the optimal information ratio, Beimel and Orlov [3] proved that the best asymptotic lower bounds on the optimal information ratio that can be obtained by using all known non-Shannon information inequalities are at most linear on the number of participants.

Bibliography

[1] A. Beimel. Secret-Sharing Schemes: A Survey. *International Workshop on Coding and Cryptology IWCC2011, Lecture Notes in Computer Science* **6639** (2011) 11–46.

[2] A. Beimel, N. Livne, C. Padró. Matroids Can Be Far From Ideal Secret Sharing. *Fifth IACR Theory of Cryptography Conference, TCC 2008, Lecture Notes in Comput. Sci.* **4948** (2008) 194–212.

[3] A. Beimel, I. Orlov. Secret Sharing and Non-Shannon Information Inequalities. *IEEE Trans. Inform. Theory* **57** (2011) 5634–5649.

[4] J. Benaloh, J. Leichter. Generalized Secret Sharing and Monotone Functions. *Advances in Cryptology - CRYPTO'88, Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

[5] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proc. ACM STOC'88* (1988) 1–10.

[6] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*. **48** (1979) 313–317.

[7] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography.* **11** (1997) 107–122.

[8] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.

[9] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.

[10] E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology.* **4** (1991) 123–134.

[11] D. Chaum, C. Crépeau, I. Damgård. Multi-party unconditionally secure protocols. *Proc. ACM STOC'88* (1988) 11–19.

[12] H. Chen, R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields. *Advances in Cryptology - CRYPTO 2006 Lecture Notes in Comput. Sci.* **4117** (2006) 521–536.

[13] T.M. Cover, J.A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991.

[14] R. Cramer, I. Damgård, U. Maurer. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Comput. Sci.* **1807** (2000) 316–334.

[15] R. Cramer, S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups. *Advances in Cryptology - CRYPTO 2002, Lecture Notes in Comput. Sci.* **2442** (2002) 272–287.

[16] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.

[17] L. Csirmaz. An impossibility result on graph secret sharing *Des. Codes Cryptogr.* **53** (2009) 195-209.

[18] L. Csirmaz, P. Ligeti. On an infinite families of graphs with information ratio $2-1/k$. *Computing* **85** (2009) 127-136.

[19] L. Csirmaz, G. Tardos. Secret sharing on trees: problem solved. Preprint (2009). Available at *Cryptology ePrint Archive*.

[20] H. Delfs, H. Knebl. *Introduction to cryptography. Principles and applications*. Second edition. Information Security and Cryptography. Springer, Berlin, 2007.

[21] W. Diffie, M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory* **22** (1976) 644-654.

[22] M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.* **6** (1995) 143–169.

[23] R. Dougherty, C. Freiling, K. Zeger. Six new non-Shannon information inequalities. In *2006 IEEE International Symposium on Information Theory*, 2006, pp. 233-236.

[24] R. Dougherty, C. Freiling, K. Zeger. Linear rank inequalities on five or more variables. Available at arXiv.org, arXiv:0910.0284v3 (2009).

[25] R. Dougherty, C. Freiling, K. Zeger. Non-Shannon Information Inequalities in Four Random Variables. Available at arXiv.org, arXiv:1104.3602v1 (2011).

[26] O. Farràs, J.R. Metcalf-Burton, C. Padró, L. Vázquez. On the Optimization of Bipartite Secret Sharing Schemes. *Des. Codes Cryptogr.* **63** (2012) 255–271.

[27] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.

[28] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.

[29] O. Goldreich, M. Micali, A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. *Proc.19th ACM Symposium on the Theory of Computing STOC'87* (1987) 218–229.

[30] M. Hirt and U. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation. *Proc. 16th Symposium on Principles of Distributed Computing PODC '97* (1997) 25–34.

[31] A.W. Ingleton. Representation of matroids. In *Combinatorial Mathematics and its Applications*, D.J.A Welsh, Ed., pp. 149–167. Academic Press, London, 1971.

[32] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.* (1987) 99–102.

[33] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.

[34] W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.

[35] M. Karchmer and A. Wigderson. On span programs. *Proceedings of the Eighth Annual Structure in Complexity Theory Conference* (San Diego, CA, 1993), 102–111, 1993.

[36] A. Lehman. A solution of the Shannon switching game. *J. Soc. Indust. Appl. Math.* **12** (1964) 687–725.

[37] A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1965) 356–360.

[38] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets, *Des. Codes Cryptogr.* **34** (2005), 17–34.

[39] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one, *Discrete Appl. Math.* **154** (2006) 552–563.

[40] J. Martí-Farré, C. Padró. On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.* **4** (2010) 95-120.

[41] J. Martí-Farré, C. Padró, L. Vázquez. Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets. *Des. Codes Cryptogr.* **61** (2011) 167–186.

[42] F. Matúš. Infinitely many information inequalities. In *Proc. IEEE International Symposium on Information Theory, (ISIT)*, 2007, pp. 2101–2105.

[43] J.R. Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Math.* **311** (2011) 651-662.

[44] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[45] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory* **46** (2000) 2596–2604.

[46] R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* **21** (1978) 120-126.

[47] P. D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.* **27** (1976) 407–413.

[48] P. D. Seymour. On secret-sharing matroids. *J. Combin. Theory Ser. B* **56** (1992) 69–73.

[49] A. Shamir. How to share a secret. *Commun. of the ACM.* **22** (1979) 612–613.

[50] C. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal* **28** (1949) 656-715.

[51] G.J. Simmons. Message authentication without secrecy. In *Secure Communications and Asymmetric Cryptosystems*, G.J. Simmons, ed., Westview Press, 1982, 105–139.

[52] G.J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO '88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448.

[53] J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) 179–197.

[54] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.

[55] D.R. Stinson, Decomposition constructions for secret-sharing schemes, *IEEE Trans. Inform. Theory* **40** (1994), 118–125.

[56] D.R. Stinson. *Cryptography. Theory and practice*. Third edition. Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[57] D.J.A. Welsh. *Matroid Theory*. Academic Press, London, 1976.

[58] Z. Zhang, R.W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory* **44** (1998) 1440–1452.