On the Information Ratio of Non-Perfect Secret Sharing Schemes *

Oriol Farràs [1], Torben Hansen [2], Tarik Kaced [3], and Carles Padró [4]

[1]Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
[2]Aarhus University, Aarhus, Denmark
[3]Université de Paris-Est, LACL, UPEC, France
[4]Universitat Politècnica de Catalunya, Barcelona, Spain

June 2, 2015

Abstract

A secret sharing scheme is non-perfect if some subsets of players that cannot recover the secret value have partial information about it. The information ratio of a secret sharing scheme is the ratio between the maximum length of the shares and the length of the secret. This work is dedicated to the search of bounds on the information ratio of non-perfect secret sharing schemes and the construction of efficient linear non-perfect secret sharing schemes. To this end, we extend the known connections between matroids, polymatroids and perfect secret sharing schemes to the non-perfect case.

In order to study non-perfect secret sharing schemes in all generality, we describe their structure through their access function, a real function that measures the amount of information on the secret value that is obtained by each subset of players. We prove that there exists a secret sharing scheme for every access function.

Uniform access functions, that is, access functions whose values depend only on the number of players, generalize the threshold access structures. The optimal information ratio of the uniform access functions with rational values has been determined by Yoshida, Fujiwara and Fossorier. By using the tools that are described in our work, we provide a much simpler proof of that result and we extend it to access functions with real values.

Key words. Secret sharing, Non-perfect secret sharing, Access function, Information ratio, Polymatroid.

1 Introduction

1.1 Non-Perfect Secret Sharing

A *secret sharing scheme* is a method to protect a *secret value* by distributing it into *shares* among a set of *players* in order to prevent both the disclosure and the loss of the secret. Only *information-theoretically secure* secret sharing schemes are considered in this paper. A set of

*Part of this work was presented in the conference *CRYPTO 2014*, and appeared in its proceedings [23]. Oriol Farràs is supported by the Spanish Government through a *Juan de la Cierva* grant, TIN2011C27076-C03-01, TIN2014-57364-C2-1-R, by the European Union through H2020-ICT-2014-1644024, and by the Government of Catalonia through Grant 2014 SGR 537. Carles Padró is supported by the Spanish Government under the project MTM2013-41426-R. Part of this research work was done while Carles Padró was with Nanyang Technological University, Singapore. emails: oriol.farras@urv.cat, torben.brandt.hansen@post.au.dk, tarik.kaced@ens-lyon.org, cpadro@ma4.upc.edu players is *qualified* if their shares determine the secret value, while the shares of the players in a *forbidden* set do not contain any information on the secret value. The *access structure* $(\mathcal{A}, \mathcal{B})$ of a secret sharing scheme consists of the families $\mathcal{A}$ and $\mathcal{B}$ of the forbidden and, respectively, qualified sets of players. A secret sharing scheme is *perfect* if every subset of players is either qualified or forbidden.

Secret sharing was independently introduced by Shamir [47] and Blakley [8]. They presented constructions of perfect *threshold* secret sharing schemes, in which the qualified sets are those having at least a certain number of players. In these schemes, the shares have the same length as the secret, which is optimal for perfect secret sharing schemes [33].

Blakley and Meadows [9] introduced the *ramp* secret sharing schemes, the first proposed non-perfect secret sharing schemes. Their main purpose was to improve the efficiency of perfect threshold schemes by relaxing the security requirements. Namely, the shares can be shortened if some unqualified sets are allowed to obtain *partial* information on the secret value. The access structure of a ramp scheme is described by means of two thresholds t and r. Every set with at most t players is forbidden, while every set with at least r players is qualified. In the ramp schemes proposed in [9], the length of every share is $1/(r-t)$ times the length of the secret, which is also optimal [40].

The threshold and ramp schemes proposed in those seminal works [8, 9, 47] are *linear*, that is, they can be described in terms of linear maps over a finite field [10, 34] or in terms of linear codes [38, 39]. Because of their efficiency and homomorphic properties, linear perfect secret sharing schemes play a fundamental role in several areas of cryptography such as secure multiparty computation [7, 14, 19] and distributed cryptography [22]. In addition to linear perfect schemes, also linear ramp secret sharing schemes have remarkable applications to secure multiparty computation [15, 18, 26].

Most of the literature on secret sharing deals with perfect schemes. One of the main lines of work is the search for bounds on the length of the shares in perfect secret sharing schemes for general access structures. The main fundamental problems remain unsolved and, in particular, there is a huge gap between the known upper and lower bounds. The reader is referred to [1] for a recent survey on this topic. Most of the known lower bounds are derived from bounds on the *information ratio*, that is, the ratio between the maximum length of the shares and the length of the secret. Such bounds can be found by using the entropy function, a method initiated by Karnin et al. [33] and Capocelli et al. [12]. On the basis of the connections between information theory, matroid theory, and secret sharing found by Fujishige [27, 28], Brickell and Davenport [11], and Csirmaz [20], matroids and polymatroids have appeared to be a powerful tool, as it can be seen from several recent works [2, 4, 5, 36, 37].

Similar questions have been considered for non-perfect secret sharing schemes too, but the research is much less developed in this direction. In addition to the families of forbidden and qualified sets, the amount of information on the secret value that is obtained by every set of players has been taken into account when analyzing those questions. To that end, two equivalent measures have been introduced, the *access hierarchy* [35, 41, 45] and the *mutual information function* [50]. In this paper, we introduce the *access function*, which unifies and generalizes those concepts. Some bounds on the information ratio of non-perfect secret sharing schemes have been presented [40, 41]. The extension to the non-perfect case of the connection between ideal perfect secret sharing schemes and matroids discovered by Brickell and Davenport [11] has attracted some attention [35, 45]. A thorough analysis of this extension is provided in a recent work [25]. A secret sharing scheme is called *uniform* if the values of its access function depend only on the number of players. Uniform non-perfect secret sharing schemes have been analyzed in [49, 50] and other works. Remarkably, the optimal information ratio of the uniform access functions with rational values has been determined recently by Yoshida, Fujiwara and Fossorier [50].

1.2 Our Results

Our main purpose is to further extend results and techniques on perfect secret sharing schemes to the non-perfect case, with a special stress on the search for bounds on the information ratio by using polymatroids and the construction of efficient linear secret sharing schemes.

Our first step is to choose a suitable way to describe the properties of non-perfect secret sharing schemes. We introduce the *access function* of a secret sharing scheme (Definitions 2.2 and 2.3), which unifies and generalizes previously proposed concepts, such as *access hierarchies* [35, 41, 45] and *mutual information functions* [50]. The access function is defined in terms of the entropy function and it is a monotone increasing function on the power set of the set of players. The forbidden and qualified sets are those in which the value of the access function is 0 and, respectively, 1. For all other sets, the access function measures the relative amount of information on the secret value given by the shares. A similar concept, *fractional access structure*, was introduced in [29], but the partial information on the secret is measured in a different way. The relation between the two approaches is discussed in Section 1.3.

In contrast to perfect secret sharing schemes, the access function depends on the probability distribution of the secret value. Because of that, schemes with uniformly distributed secrets are of special interest. Linear secret sharing schemes have this property. Nevertheless, we need to consider other probability distributions in the general construction in Section 4.

Our first result deals with a fundamental question. Namely, given a real-valued access function, does there exist a secret sharing scheme realizing it? By answering this question in the affirmative in Theorem 4.2, we generalize the result by Ito, Saito and Nishizeki [30], who proved that there exists a secret sharing scheme for every perfect access structure. Our result is not entirely obvious since the usual approach of using linear schemes cannot work. Indeed, there are only countably many linear secret sharing schemes over finite fields, while there are uncountably many access functions. Therefore, some access functions are inherently non-linear or might only be realized in the limit by a sequence of linear schemes. Nevertheless, we prove that every rational-valued access function admits a linear secret sharing scheme. If the access function takes non-rational values, then our construction requires a non-uniform probability distribution on the set of possible values of the secret. Similarly to the known general constructions of perfect secret sharing schemes [6, 30], our general construction is inefficient because the length of the shares grows exponentially with the number of players.

The main problem we consider in this work is the search for bounds on the information ratio of secret sharing schemes for general access functions. For the first time, we apply to non-perfect schemes the polymatroid-based techniques that have been so useful for the perfect case. The well known connection between perfect secret sharing and polymatroids is extended to non-perfect schemes in Section 5. Our approach based on access functions appears to be most suitable for our purposes. This can be seen, for instance, in Proposition 5.5, in which the characterization by Csirmaz [20, Proposition 2.3] of the compatibility between polymatroids and access structures is easily extended to non-perfect secret sharing, and also in Theorems 5.7 and 5.9, which generalize the properties of the parameter κ [36]. In addition, the concepts of *minor* and *dual* of an access structure have a natural extension to access functions, as described in Section 6. In particular, we generalize in Theorem 6.10 the known results on duality of linear secret sharing schemes as, for example, the ones in [13, 31]. Moreover, we present in Section 8 a new definition for *ideal non-perfect secret sharing scheme.* Even though our new definition is equivalent to the one proposed in previous works [35, 45], the use of access functions and the results in [25] make it clear that this is the right way to extend the corresponding concept for perfect schemes. In particular, the new framework provides a better insight on the connection between ideal non-perfect schemes and matroids.

Uniform access functions, that is, the ones that take the same value on sets that have the same cardinality, generalize the access structures of perfect threshold secret sharing schemes. We present in Section 7.2 an efficient construction of secret sharing schemes for all rational uniform access functions and, in Section 7.3, we determine the optimal information ratio of all uniform access functions. After the publication of the previous version of this work [23], we became aware that most of those results had been previously presented in previous works [49, 50]. Nevertheless, the connections between secret sharing and polymatroids that are analyzed in the previous sections provide simpler and clearer statements and proofs for those results. Moreover, differently to [50], we determine the optimal information ratio of uniform access functions with non-rational values.

1.3 Related Work

The *almost-perfect secret sharing schemes* introduced in [32] are schemes whose access functions are close to perfect. The possibility of improving the information ratio by realizing a perfect access structure with non-perfect secret sharing schemes with close access functions is explored in that work.

Cascudo, Cramer and Xing [13] consider a related optimization problem in non-perfect secret sharing. Namely, they present bounds on the size of the shares (instead of the information ratio) in terms of the *gap* $r - t$, where r is the minimum value such that every set with r players is qualified and t is the maximum value such that every set with t players is forbidden.

Ishai, Kushilevitz and Strulovich [29] introduced the notion of *fractional secret sharing*, which is a restriction of non-perfect secret sharing. The security requirements of a fractional secret sharing scheme are described in terms of its *fractional access structure*, which is a monotone decreasing function $F : \mathcal{P}(P) \to \{1, \dots, m\}$, where $\mathcal{P}(P)$ is the power set of the set P of players. Given the shares of the players in a set $X \subseteq P$, the secret is uniformly distributed over a set of $f(X)$ possible values. In particular, the secret value is uniformly distributed over a set of $m = F(\emptyset)$ elements. Observe that $F(X)$ measures the number of guessing attempts, and hence the amount of work, needed by the players in X to find the secret value. The main results in [29] are the following: every fractional access structure is realizable, and every uniform (or *symmetric* in their terminology) fractional access structure is efficiently realizable.

The main difference between the approaches in [29] and in this paper is that a fractional access structure fixes the size of the set of possible values of the secret. The following observation illustrates this difference. Every fractional access structure determines a unique access function, but the converse is not true because an access function does not fix the size of the secret, but only the ratio with the amount of information obtained by the sets of players. Being a more restrictive concept, the problems related to fractional secret sharing are more difficult. In particular, our results do not appear to have a direct application to fractional secret sharing. For example, no optimality result for uniform fractional access structures (an open problem posed in [29, Section 5]) can be directly obtained from our optimality results on uniform access functions. Another difference between the two approaches is the limited power of linear secret sharing schemes when dealing with fractional secret sharing. Indeed, a fractional access structure can be realized by a linear secret sharing scheme over a field of order q only if all its values are powers of q.

Our optimality result for uniform access functions (Theorem 7.14) is closely related to a recent result by Chen and Yeung [16]. They proved that every $(1, n-1)$-uniform polymatroid is almost entropic. By taking into account that $\kappa = \epsilon$ for the uniform access functions, that implies the result in Remark 7.12. Nevertheless, the other results in Section 7, namely the value of the optimal information ratio of all uniform access functions and the optimal construction for rational uniform access functions cannot be derived from the results in [16].

2 Secret Sharing Schemes and Their Access Functions

We present in this section the main definitions and basic facts about secret sharing and, at the same time, we introduce a new framework to describe the properties of general (i.e., not necessarily perfect) secret sharing schemes. In this work we consider the definition of secret sharing based on Shannon entropy. For a complete introduction to secret sharing, see [1, 43], and for a textbook on information theory see [17].

We begin by introducing some notation. For a set Q, we notate $\mathcal{P}(Q)$ for the power set of Q, that is, the set of all subsets of Q. We use a compact notation for set unions, that is, we write XY for $X \cup Y$ and Xy for $X \cup \{y\}$. In addition, we write $X \smallsetminus Y$ for the set difference and $X \smallsetminus x$ for $X \smallsetminus \{x\}$. Throughout the paper, P and Q stand for finite sets with $Q = Pp_o$ for some $p_o \notin P$. For a vector $s = (s_i)_{i \in Q}$, we put $s_X = (s_i)_{i \in X}$. Given a family $(E_i)_{i \in Q}$ of finite sets, the product $E = \prod_{i \in Q} E_i$, and a set $X \subseteq Q$, we notate $E_X = \prod_{i \in X} E_i$. In addition, for a subset $C \subseteq E$, we write $C_X = \{s_X : s \in C\} \subseteq E_X$. Most of the times, we are going to write s_o, E_o, and C_o instead of s_{p_o}, E_{p_o}, and C_{p_o}, respectively.

Only discrete random variables are considered in this paper. Given a discrete random vector $S = (S_i)_{i \in Q}$ and a set $X \subseteq Q$, the Shannon entropy of the random variable $S_X = (S_i)_{i \in X}$ is denoted by $H(S_X)$. In addition, for such random variables, one can consider the *conditional entropy* $H(S_X|S_Y) = H(S_{XY}) - H(S_Y)$, the *mutual information* $I(S_X{:}S_Y) = H(S_X) - H(S_X|S_Y)$, and the *conditional mutual information* $I(S_X{:}S_Y|S_Z) = H(S_X|S_Z) - H(S_X|S_{YZ})$.

Definition 2.1 (Secret sharing scheme)**.** Let Q be a finite set of *players*, let $p_o \in Q$ be a distinguished player, which is called *dealer*, and take $P = Q \smallsetminus p_o$. A *secret sharing scheme* Σ on the set P is a discrete random vector $(S_i)_{i \in Q}$ such that $H(S_o) > 0$ and $H(S_o|S_P) = 0$. The random variable S_o corresponds to the *secret value*, while the random variables $(S_i)_{i \in P}$ correspond to the *shares* of the secret that are distributed among the players in P.

Definition 2.2 (Access function of a secret sharing scheme)**.** The *access function* Φ_Σ of a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ is the map $\Phi_\Sigma : \mathcal{P}(P) \to [0, 1]$ defined by

$$\Phi_\Sigma(X) = \frac{I(S_{p_o}{:}S_X)}{H(S_{p_o})}$$

for every $X \subseteq P$.

The access function is monotone increasing. In addition, $\Phi_\Sigma(\emptyset) = 0$ and $\Phi_\Sigma(P) = 1$. The value $\Phi_\Sigma(X)$ measures the amount of information on the secret value that is derived from the shares of the players in X. If $\Phi_\Sigma(X) = 1$, then $I(S_{p_o}{:}S_X) = H(S_{p_o})$, which implies that the secret value is determined by the shares of the players in X. The random variables S_{p_o} and S_X are independent if $\Phi_\Sigma(X) = 0$, that is, the shares of the players in X do not provide any information on the secret in that situation.

Definition 2.3 (Access function)**.** An *access function* on a set P is a monotone increasing function $\Phi : \mathcal{P}(P) \to [0, 1]$ with $\Phi(\emptyset) = 0$ and $\Phi(P) = 1$. An access function is said to be *perfect* if its only values are 0 and 1. An access function is called *rational* if it only takes rational values.

Definition 2.4 (Access structure of a secret sharing scheme)**.** Let Σ be a secret sharing scheme with access function $\Phi = \Phi_\Sigma$. A set $X \subseteq P$ is *forbidden* for Σ if $\Phi(X) = 0$, while it is *qualified* for Σ if $\Phi(X) = 1$. The *access structure* of Σ is the pair $(\mathcal{A}, \mathcal{B})$, where $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(P)$ are the families of the forbidden and the qualified sets for Σ, respectively.

Definition 2.5 (Perfect secret sharing scheme)**.** A secret sharing scheme is *perfect* if every set of players is either forbidden or qualified or, equivalently, if its access function is perfect.

Definition 2.6 (Gap and maximum increment)**.** The *gap* $g(\Phi)$ of an access function Φ is defined as the minimum gap between a forbidden and a qualified set, that is,

$$g(\Phi) = \min\{|B \smallsetminus A| \,:\, \Phi(A) = 0,\, \Phi(B) = 1\}.$$

The maximum value $\Phi(Xy) - \Phi(X)$ for $X \subseteq P$ and $y \in P$ is called the *maximum increment* of the access function Φ and is denoted by $\mu(\Phi)$. Obviously, $\mu(\Phi) \geq 1/g(\Phi)$.

Definition 2.7 (Ramp access function)**.** Given integers t, r, n with $0 \leq t < r \leq n$, the (t, r, n)-*ramp access function* on a set P with $|P| = n$ is defined by: $\Phi(X) = 0$ if $|X| \leq t$, and $\Phi(X) = (|X| - t)/(r - t)$ if $t < |X| < r$, and $\Phi(X) = 1$ if $|X| \geq r$.

Definition 2.8 (Uniform access function)**.** An access function Φ on P is *uniform* if $\Phi(A) = \Phi(B)$ for every $A, B \subseteq P$ with $|A| = |B|$. *Uniform* secret sharing schemes are those with uniform access function.

Example 2.9. A variant of Shamir's threshold scheme [47] provides a secret sharing scheme for every ramp access function. This construction was first presented in the seminal work on non-perfect secret sharing by Blakley and Meadows [9]. Consider integers t, r, n with $0 \leq t < r \leq n$. Take a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n + r - t$, and take $n + r - t$ different elements $y_1, \ldots, y_{r-t}, x_1, \ldots, x_n \in \mathbb{K}$. By choosing uniformly at random a polynomial $f \in \mathbb{K}[X]$ with degree at most $r - 1$, one obtains random variables $S_o = (f(y_1), \ldots, f(y_g)) \in \mathbb{K}^g$ and $S_i = f(x_i) \in \mathbb{K}$ for every $i = 1, \ldots, n$. It is not difficult to check that these random variables define a secret sharing scheme for the (t, r, n)-ramp access function on $P = \{1, \ldots, n\}$.

The length of the shares is a measure for the efficiency of a secret sharing scheme. We use the Shannon entropy as an approximation of the shortest binary codification. The *information ratio* $\sigma(\Sigma)$ of a secret sharing $\Sigma = (S_i)_{i \in Q}$ is the ratio between the maximum length of the shares and the length of the secret value, that is,

$$\sigma(\Sigma) = \frac{\max_{i \in P} H(S_i)}{H(S_o)}.$$

The *optimal information ratio* $\sigma(\Phi)$ *of an access function* Φ is defined as the infimum of the information ratios of the secret sharing schemes for Φ.

The following lower bound on the optimal information ratio is a direct consequence of well-known results about non-perfect secret sharing [40, 41, 45]. An alternative proof for this result is presented here in Proposition 5.6.

Proposition 2.10. *Let Φ be an access function with maximum increment $\mu(\Phi)$ and gap $g(\Phi)$. Then its optimal information ratio $\sigma(\Phi)$ satisfies $\sigma(\Phi) \geq \mu(\Phi) \geq 1/g(\Phi)$.*

Remark 2.11. The information ratio of the scheme in Example 2.9 attains the lower bound in Proposition 2.10. Therefore, the optimal information ratio of the (t, r, n)-ramp access function is equal to $1/(r - t)$.

3 Linear Secret Sharing Schemes

Definition 3.1 (Linear secret sharing scheme)**.** Let $\mathbb{K}$ be a finite field and let ℓ be a positive integer. In a $(\mathbb{K},\ell)$-*linear* secret sharing scheme, the random variables $(S_i)_{i\in Q}$ are given by surjective $\mathbb{K}$-linear maps $S_i : V \to E_i$, where the dimension of E_o over the field $\mathbb{K}$ is equal to ℓ and the uniform probability distribution is taken on V.

Most of the secret sharing schemes that have been proposed in the literature are linear. This is due to their efficiency and also to the fact that many cryptographic applications of secret sharing require homomorphic properties that are satisfied by linear schemes.

In a $\mathbb{K}$-linear secret sharing scheme $(S_i)_{i\in Q}$, the random variable S_X is uniform on its support for every $X \subseteq Q$. Because of that, $H(S_X) = \operatorname{rank} S_X \cdot \log|\mathbb{K}|$, and hence

$$I(S_o{:}S_X) = (\operatorname{rank} S_o + \operatorname{rank} S_X - \operatorname{rank} S_{Xp_o}) \log|\mathbb{K}|. \tag{1}$$

This implies that the access function of every linear secret sharing scheme is rational. For a rational access function Φ, we define $\lambda(\Phi)$ as the infimum of the information ratios of the linear secret sharing schemes for Φ. Clearly, $\lambda(\Phi)$ is an upper bound of $\sigma(\Phi)$.

Remark 3.2. A $(\mathbb{K},\ell)$-linear secret sharing scheme with information ratio σ is determined by linear maps $S_i : E \to E_i$ with $\dim E_i \le \max\{\ell, \sigma\ell\}$ for every $i \in Q$ and $\dim E \le \sum_{i\in Q} \dim E_i$. Therefore, the computation time for both the distribution phase (computing the shares from the secret value and some randomness) and the reconstruction phase (partially or totally recovering the secret value from some shares) is polynomial in $\log|\mathbb{K}|$, ℓ, σ, and the number of players.

Definition 3.3 (Least common denominator of a rational access function)**.** The *least common denominator* $M(\Phi)$ of a rational access function Φ is the least common denominator of the values of Φ.

Remark 3.4. Let Φ be a rational access function on P and let $M = M(\Phi)$ be its least common denominator. Clearly, $\ell \ge M$ for every $(\mathbb{K},\ell)$-linear secret sharing scheme for Φ. Therefore, by Remark 3.2, the efficiency of the linear secret sharing schemes for Φ depends on $M(\Phi)$.

The families of access functions that admit efficient linear secret sharing schemes, that is, whose computational complexity is polynomial in the number of players, are of special interest. An example of such a family is given by the ramp access functions

Example 3.5. The secret sharing scheme presented in Example 2.9 is linear. As a consequence, the (t,r,n)-ramp access function admits a $(\mathbb{K}, r-t)$-linear secret sharing scheme with information ratio $1/(r-t)$ for every finite field $\mathbb{K}$ with $|\mathbb{K}| \ge n + r - t$.

Because of Remark 3.4, the least common denominator should not grow too fast in the families of access functions admitting efficient linear secret sharing schemes. To keep things simpler, the search for such families can be restricted to access functions with constant increment.

Definition 3.6. An access function Φ has *constant increment* if $\Phi(Xy) - \Phi(X) \in \{0, \mu(\Phi)\}$ for every $X \subset P$ and $y \in P$. In this situation, Φ is rational and $\mu(\Phi) = 1/k$ for some positive integer k.

Linear secret sharing schemes are closely related to linear codes. In order to describe that connection, we need a more general definition of linear code. Namely, we need to consider codewords in which every entry is a vector instead of a field element. That is, a $\mathbb{K}$-*linear code* will be here a vector subspace C of the $\mathbb{K}$-vector space $E = \prod_{i\in Q} E_i$, where every E_i is a

$\mathbb{K}$-vector space. The codewords of C are of the form $(s_i)_{i\in Q}$, where $s_i \in E_i$ for every $i \in Q$. Let $\Sigma = (S_i)_{i\in Q}$ be a $(\mathbb{K}, \ell)$-linear secret sharing scheme. The linear maps $S_i : V \to E_i$ determine a linear map $S : V \to E = \prod_{i\in Q} E_i$. The image $C \subseteq E$ of S is the linear code associated to Σ. Every codeword $(s_i)_{i\in Q}$ in C corresponds to a distribution of shares.

4 A Secret Sharing Scheme for Every Access Function

It is well known that every perfect access function admits a secret sharing scheme [6, 30]. We present in Theorem 4.2 an extension of this result to the general case.

Remark 4.1. Similarly to the construction in [30] for the perfect case, our general construction is based on a very simple perfect secret sharing scheme for which the only qualified set is the full set of players. Let G be a finite abelian group (with additive notation). Let T_o be an arbitrary random variable with support G. Fix a player $q \in P$ and take independent uniform random variables $(T_i)_{i\in P\smallsetminus q}$ with support G. Finally, take $T_q = T_o - \sum_{i\in P\smallsetminus q} T_i$. It is not difficult to see that $\mathbf{T} = (T_i)_{i\in Q}$ is a perfect secret sharing scheme whose only qualified set is P.

Theorem 4.2. *Every access function admits a secret sharing scheme. Moreover, every rational access function Φ admits a $(\mathbb{K}, M(\Phi))$-linear secret sharing scheme for every finite field $\mathbb{K}$.*

Proof. Let Φ be an access function on the set of players P. Let M be the smallest positive integer such that $\lceil M\Phi(X)\rceil \neq \lceil M\Phi(Y)\rceil$ if $\Phi(X) \neq \Phi(Y)$. Consider the sets

- $\Omega = \{\lceil M\Phi(X)\rceil : X \subseteq P\} \smallsetminus \{0\} \subseteq \{1, \dots, M\}$, and
- $\Omega_1 = \{\lceil M\Phi(X)\rceil : X \subseteq P,\ M\Phi(X) \notin \mathbb{Z}\} \subseteq \Omega$.

We construct in the following a secret sharing scheme $\Sigma = (S_i)_{i\in Q}$ for Φ.

We begin by describing the random variable S_o corresponding to the secret value. Specifically, we take $S_o = \prod_{k=1}^{M} S^k$, where $(S^k)_{1\le k\le M}$ are the independent random variables with entropy $H(S^k) = 1$ that are described next. Let $\mathbb{F}_2$ be the field with order 2 and let h be the binary entropy function. If $k = \lceil M\Phi(X)\rceil \in \Omega_1$, take $\epsilon_k = M\Phi(X) - (k-1)$, which satisfies $0 < \epsilon_k < 1$, and take $S^k = S^k_0 \times S^k_1$, where S^k_0 and S^k_1 are independent random variables with support $\mathbb{F}_2$ such that $\Pr[S^k_0 = 0] = \min h^{-1}(\epsilon_k)$ and $\Pr[S^k_1 = 0] = \min h^{-1}(1-\epsilon_k)$. If $k \in \{1, \dots, M\} \smallsetminus \Omega_1$, then S^k is a uniform random variable with support $\mathbb{F}_2$.

Now, we proceed to describe the random variables corresponding to the shares of the players. Take $k \in \Omega$. Let $\mathcal{C}_k \subseteq \mathcal{P}(P)$ be the family of the subsets $X \subseteq P$ with $\lceil M\Phi(X)\rceil = k$ that are minimal with this property. Consider the random variable

$$T^k_o = S^1 \times \cdots \times S^{k-1} \times \widehat{S}^k,$$

where $\widehat{S}^k = S^k_0$ if $k \in \Omega_1$ and $\widehat{S}^k = S^k$ otherwise. Observe that $H(T^k_o) = M\Phi(X)$ for every $X \in \mathcal{C}_k$. The support of T^k_o is $\mathbb{F}_2^m$ for some integer $m \ge k$. For every $X \in \mathcal{C}_k$, take the secret sharing scheme $\mathbf{T}^{(X)} = (T^{(X)}_i)_{i\in Xp_o}$ described in Remark 4.1 with $T^{(X)}_o = T^k_o$ and $G = \mathbb{F}_2^m$. The random variable T^k_o is the same for all schemes $\mathbf{T}^{(X)}$ with $X \in \mathcal{C}_k$, that is, all these schemes distribute shares for the same secret value. The other random variables $T^{(X)}_i$ are instantiated independently for different sets X. For every player $i \in P$ take the family of subsets

$$\mathcal{D}_i = \bigcup_{k\in\Omega} \{X \in \mathcal{C}_k : i \in X\} \subseteq \mathcal{P}(P).$$

Finally, the random variable S_i corresponding to the share of a player $i \in P$ is defined by

$$S_i = \prod_{X \in \mathcal{D}_i} T_i^{(X)}.$$

That is, the share of every player is composed of sub-shares from the schemes $\mathbf{T}^{(X)}$ corresponding to the sets $X \subseteq P$ such that $i \in X$ and $X \in \mathcal{C}_k$ for some $k \in \Omega$.

Clearly, $H(T_o^k|S_Y) = 0$ for every subset $Y \subseteq P$ with $k = \lceil M\Phi(Y) \rceil$. On the other hand, it is not difficult to prove that the shares of the players in Y do not provide any information about the other components of the secret value, and hence $I(S_o{:}S_Y) = H(T_o^k) = M\Phi(Y)$. Since $H(S_o) = M$, this implies that the scheme $\Sigma = (S_i)_{i \in Q}$ has access function Φ.

Some modifications in the previous construction are needed to prove the second part of the theorem. If Φ is rational, take $M = M(\Phi)$, the least common denominator of Φ. The set Ω is defined analogously but in this case $\Omega_1 = \emptyset$. Given a finite field $\mathbb{K}$, take $S_o = \prod_{k=1}^{M} S^k$, where $(S^k)_{1 \le k \le M}$ are independent random variables and each S^k is a uniform random variable with support $\mathbb{K}$. At this point, a $(\mathbb{K}, M)$-linear secret sharing scheme with access function Φ can be constructed by using the same steps as in the previous construction. □

The above construction is not efficient because the information ratio is exponential in the number of players. The construction can be refined in order to slightly decrease the information ratio but, even for the perfect case, no constructions are known in which the information ratio is not exponential.

5 Polymatroids and Secret Sharing

On the basis of the connection between Shannon entropy and polymatroids that was discovered by Fujishige [27, 28] and is described here in Theorem 5.3, lower bounds on the information ratio of perfect secret sharing schemes can be obtained by using linear programming [20, 36, 44]. Nevertheless, several limitations on this approach have been found [5, 20, 37]. In this section, we discuss the extension of this method to non-perfect secret sharing.

We begin by introducing a notation that will be useful to simplify the presentation of our results. For a function $F : \mathcal{P}(Q) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq Q$, we notate

$$\Delta_F(Y{:}Z|X) = F(XY) + F(XZ) - F(XYZ) - F(X) \tag{2}$$

and $\Delta_F(Y{:}Z) = \Delta_F(Y{:}Z|\emptyset)$.

Definition 5.1. A *polymatroid* is a pair $\mathcal{S} = (Q, f)$ formed by a finite set Q, the *ground set*, and a *rank function* $f \colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties.

- $f(\emptyset) = 0$.
- f is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $f(X) \le f(Y)$.
- f is *submodular*: $f(X \cup Y) + f(X \cap Y) \le f(X) + f(Y)$ for every $X, Y \subseteq Q$.

The following characterization of rank functions of polymatroids is a straightforward consequence of [46, Theorem 44.1].

Proposition 5.2. *A map $f \colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if $f(\emptyset) = 0$ and $\Delta_f(y{:}z|X) \ge 0$ for every $X \subseteq Q$ and $y, z \in Q \smallsetminus X$.*

Theorem 5.3 (Fujishige [27, 28]). *If $(S_i)_{i\in Q}$ is a random vector, then the map $h\colon \mathcal{P}(Q)\to\mathbb{R}$ defined by $h(X)=H(S_X)$ is the rank function of a polymatroid with ground set Q.*

The notation introduced in (2) is motivated by the connection between polymatroids and the Shannon entropy described in the previous theorem. Indeed, for every $X,Y,Z\subseteq Q$, the conditional mutual information $I(S_Y{:}S_Z|S_X)$ is equal to $\Delta_h(Y{:}Z|X)$.

Since secret sharing schemes are given by random vectors, a connection between secret sharing and polymatroids arises from Theorem 5.3. Specifically, associated to every secret sharing scheme $\Sigma=(S_i)_{i\in Q}$ there is the polymatroid (Q,h) given by $h(X)=H(S_X)$ for every $X\subseteq Q$. The access function Φ_Σ of Σ is determined by this polymatroid. Indeed, $\Phi_\Sigma(X)=\Delta_h(p_o{:}X)/h(p_o)$ for every $X\subseteq P$. This motivates the following definition.

Definition 5.4. Let Φ be an access function on P and let $\mathcal{S}=(Q,f)$ be a polymatroid. Then $\mathcal{S}$ is a Φ-*polymatroid* if

$$\Phi(X)=\frac{\Delta_f(p_o{:}X)}{f(p_o)}$$

for every $X\subseteq P$.

We say that a polymatroid (Q,f) is *normalized* if $f(p_o)=1$. A polymatroid $\mathcal{S}=(P,f)$ is *compatible* with the access function Φ if $\mathcal{S}$ can be extended to a normalized Φ-polymatroid $\mathcal{S}'=(Q,f)$. The following is a generalization of a result by Csirmaz [20, Proposition 2.3] on perfect secret sharing.

Proposition 5.5. *A polymatroid $\mathcal{S}=(P,f)$ is compatible with an access function Φ on P if and only if $\Delta_f(y{:}z|X)\geq\Delta_\Phi(y{:}z|X)$ for every $X\subseteq P$ and $y,z\in P\smallsetminus X$.*

Proof. Extend the rank function f of $\mathcal{S}$ to $\mathcal{P}(Q)$ by taking $f(Xp_o)=f(X)+1-\Phi(X)$ for every $X\subseteq P$. This is the only possible extension of f that can produce a normalized Φ-polymatroid. Therefore, $\mathcal{S}$ is compatible with Φ if and only if (Q,f) is a polymatroid. By Proposition 5.2, (Q,f) is a polymatroid if and only if $\Delta_f(y{:}z|X)\geq 0$ for every $X\subseteq Q$ and $y,z\in Q\smallsetminus X$. Since (P,f) is a polymatroid, (Q,f) is a polymatroid if and only if the following conditions are satisfied.

1. $\Delta_f(y{:}z|Xp_o)\geq 0$ for every $X\subseteq P$ and $y,z\in P\smallsetminus X$.
2. $\Delta_f(p_o{:}z|X)\geq 0$ for every $X\subseteq P$ and $z\in Q\smallsetminus X$.

The second condition is always satisfied because Φ is monotone increasing and the first one is equivalent to the condition in the statement. □

On the basis of the connection between secret sharing and polymatroids, we introduce in this section the parameter $\kappa(\Phi)$, which provides a lower bound on the optimal information ratio $\sigma(\Phi)$. It is a straightforward generalization of the corresponding parameter for perfect secret sharing that was introduced in [36].

For a polymatroid $\mathcal{S}=(Q,f)$ we define

$$\sigma_o(\mathcal{S})=\frac{\max_{x\in P}f(x)}{f(p_o)}.$$

Observe that $\sigma(\Sigma)=\sigma_o(\mathcal{S})$ if $\mathcal{S}$ is the polymatroid associated to a secret sharing scheme Σ. In addition, we define

$$\kappa(\Phi)=\inf\{\sigma_o(\mathcal{S})\,:\,\mathcal{S}\text{ is a }\Phi\text{-polymatroid}\}.$$

Obviously,

$$\kappa(\Phi)=\inf\{\sigma_o(\mathcal{S})\,:\,\mathcal{S}\text{ is a normalized }\Phi\text{-polymatroid}\}. \tag{3}$$

Since every secret sharing scheme with access function Φ determines a Φ-polymatroid, we have that $\kappa(\Phi) \leq \sigma(\Phi)$. The following lower bound on $\kappa(\Phi)$ is a refinement of the result in Proposition 2.10.

Proposition 5.6. *$\kappa(\Phi) \geq \mu(\Phi) \geq 1/g(\Phi)$ for every access function Φ.*

Proof. Let (Q, f) be a normalized Φ-polymatroid. By Proposition 5.5,

$$f(y) \geq f(Xy) - f(X) = \Delta_f(y{:}y|X) \geq \Delta_\Phi(y{:}y|X) = \Phi(Xy) - \Phi(X)$$

for every $X \subseteq P$ and $y \in P \smallsetminus X$. □

It is clear from Propositions 5.2 and 5.5 and (3) that the value of $\kappa(\Phi)$ can be computed by solving a linear programming problem in which the unknowns are the values $f(X)$ for $X \subseteq P$ and the constraints are $\Delta_f(y{:}z|X) \geq \max\{0, \Delta_\Phi(y{:}z|X)\}$ for every $X \subseteq P$ and $y, z \in P \smallsetminus X$. As a consequence, the infimum in (3) is a minimum and, moreover, $\kappa(\Phi)$ has a rational value if Φ is a rational access function. This linear programming approach has been used in [20, 24, 44] and many other works to find lower bounds on the optimal information ratio of perfect secret sharing schemes, but important limitations to this method have been found [5, 20, 37]. The first of those limitation results [20, Theorem 3.5] can be generalized to the non-perfect case by using the same idea in the proof.

Theorem 5.7. *Let Φ be an access function on a set of n players. Then $\kappa(\Phi) \leq n\mu(\Phi)$.*

Proof. Take a real number μ with $1/n \leq \mu \leq 1$ and a set P with $|P| = n$. The result is proved by presenting a polymatroid (P, f) that is compatible with all access functions Φ on P with maximum increment μ and satisfies $f(x) = n\mu$ for every $x \in P$. Consider the map $f : \mathcal{P}(P) \to \mathbb{R}$ defined by

$$f(X) = \mu\,(n + (n-1) + \cdots + (n - m + 1))$$

for every $X \subseteq P$ with $|X| = m$. Let Φ be an access function on P with $\mu(\Phi) = \mu$. Then

$$\Delta_f(y{:}z|X) = \mu \geq \max\{0, \Delta_\Phi(y{:}z|X)\}$$

for every $X \subseteq P$ and $y, z \in P \smallsetminus X$. By Propositions 5.2 and 5.5, this proves that (P, f) is a polymatroid that is compatible with the access function Φ. □

The upper bound in Theorem 5.7 seems to imply that $\kappa(\Phi)$ is in general much smaller than $\sigma(\Phi)$. Nevertheless, similarly to the perfect case, this is still an open problem. Actually, the best known general lower bound on the information ratio of perfect secret sharing schemes, which was presented by Csirmaz [20, Theorem 3.2], is obtained from the parameter κ. Theorem 5.9 generalizes this result to the non-perfect case.

Lemma 5.8. *Consider sets P, P' with $P \subseteq P'$, and the integers n, k such that $|P| = n$ and $|P'| = n + k - 1$. Let Φ be a perfect access function on P. Then there exists an access function Φ' on P' such that $\mu(\Phi') = 1/k$ and $\kappa(\Phi') = \kappa(\Phi)/k$.*

Proof. Take $P'' = P' \smallsetminus P$ and consider the access function Φ' on P' defined by

$$\Phi'(X) = \frac{1}{k}(\Phi(X \cap P) + |X \cap P''|)$$

for every $X \subseteq P'$. Obviously, $\mu(\Phi') = 1/k$. Let (P, f) be a polymatroid compatible with Φ. Then the polymatroid (P', f') defined by

$$f'(X) = \frac{1}{k}(f(X \cap P) + |X \cap P''|)$$

for every $X \subseteq P'$ is compatible with Φ'. Clearly, this implies that $\kappa(\Phi') \leq \kappa(\Phi)/k$. On the other hand, if (P', f') is a polymatroid compatible with Φ', then the polymatroid (P, f) with $f(X) = kf'(X)$ for every $X \subseteq P$ is compatible with Φ. Therefore, $\kappa(\Phi) \leq k\kappa(\Phi')$. □

Theorem 5.9. *For every positive integer k and for infinitely many positive integers n, there exists an access function Φ_n on a set of size $n+k-1$ satisfying $\mu(\Phi_n) = 1/k$ and $\kappa(\Phi_n) \geq n/(2k \log n)$.*

Proof. As a consequence of [20, Theorem 3.2], for every positive integer n there exists a perfect access function Φ_n on n players with $\kappa(\Phi_n) \geq n/(2 \log n)$. Then apply Lemma 5.8. □

6 Duality and Minors

The operations of deletion and contraction, which are related to puncturing and shortening in codes, produce minors of matroids and polymatroids. Duality is also a fundamental concept in both matroid theory and coding theory. These concepts play an important role in perfect secret sharing too [31, 36]. In this section, we describe their extension to the non-perfect case.

Minors of access functions are related to the situation in which some players leave a secret sharing scheme, maybe revealing their shares. Let $\Sigma = (S_i)_{i \in Q}$ be a secret sharing scheme on P with access function Φ. If the players in a set $Z \subseteq P$ with $\Phi(P \smallsetminus Z) = 1$ leave without revealing their shares, our scheme is reduced to $\Sigma \setminus Z = (S_i)_{i \in Q \smallsetminus Z}$, which is a secret sharing scheme on $P \smallsetminus Z$ whose access function $\Phi \setminus Z$ is given by $(\Phi \setminus Z)(X) = \Phi(X)$ for every $X \subseteq P \smallsetminus Z$. The situation in which the shares of the players leaving the scheme are revealed is slightly more complex. Consider $Z \subseteq P$ such that $\Phi(Z) = 0$. Suppose that the random variable S_Z is uniformly distributed on its support (this is always the case if Σ is a linear secret sharing scheme). Take $s_Z = (s_j)_{j \in Z}$ with $\Pr(S_Z = s_Z) > 0$ and, for every $i \in P \smallsetminus Z$, consider the random variable $S_i/Z = (S_i | S_Z = s_Z)$ (in the particular case that Σ is a linear scheme, it is convenient to take $s_Z = 0$). Then $\Sigma/Z = (S_i/Z)_{i \in P \smallsetminus Z}$ is a secret sharing scheme on $P \smallsetminus Z$ and its access function Φ/Z is determined by $(\Phi/Z)(X) = \Phi(X \cup Z)$ for every $X \subseteq P \smallsetminus Z$.

Definition 6.1 (Minor of an access function)**.** Let Φ be an access function on a set P and let Z_1, Z_2 be disjoint subsets of P with $\Phi(P \smallsetminus Z_1) = 1$ and $\Phi(Z_2) = 0$. Then the access function $(\Phi \setminus Z_1)/Z_2$ on $P \smallsetminus (Z_1 \cup Z_2)$ is said to be a *minor* of Φ.

The loss of some shares may prevent the reconstruction of the secret. The loss of information on the secret value if some shares are missing is measured by the dual access function.

Definition 6.2 (Dual access function)**.** The *dual* Φ^* of an access function Φ on P is defined by $\Phi^*(X) = 1 - \Phi(P \smallsetminus X)$ for every $X \subseteq P$. Clearly, Φ^* is an access function on P and $\Phi^{**} = \Phi$.

The two operations that are used to determine the minors of an access function are dual of each other.

Proposition 6.3. $(\Phi/Z)^* = \Phi^* \setminus Z$ *and* $(\Phi \setminus Z)^* = \Phi^*/Z$.

Example 6.4. Let Φ be the (t, r, n)-ramp access function on a set P. Then Φ^* is the $(n-r, n-t, n)$-ramp access function on P. Suppose that $1 < t < r < n$ and take $p \in P$. Then $\Phi \setminus \{p\}$ and $\Phi/\{p\}$, are ramp access functions on $P \smallsetminus p$ with parameters $(t, r, n-1)$ and $(t-1, r-1, n-1)$, respectively.

The following result is a consequence of the previous discussion. In the perfect case, it applies to the optimal information ratio $\sigma(\Phi)$ too [36].

Proposition 6.5. *If Φ is a rational access function and Φ' is a minor of Φ, then $\lambda(\Phi') \le \lambda(\Phi)$.*

For a polymatroid $\mathcal{S} = (Q, f)$ and a set $Z \subseteq Q$, we consider the polymatroids $\mathcal{S} \setminus Z = (Q \smallsetminus Z, f \setminus Z)$ and $\mathcal{S}/Z = (Q \smallsetminus Z, f/Z)$ with $(f \setminus Z)(X) = f(X)$ and $(f/Z)(X) = f(X \cup Z) - f(Z)$ for every $X \subseteq Q \smallsetminus Z$. Every polymatroid of the form $(\mathcal{S} \setminus Z_1)/Z_2$ is a *minor* of $\mathcal{S}$.

Proposition 6.6. *If Φ' is a minor of Φ, then $\kappa(\Phi') \le \kappa(\Phi)$.*

Proof. Let $\mathcal{S}$ be a normalized Φ-polymatroid and take disjoint sets $Z_1, Z_2 \subseteq P$ with $\Phi(P \smallsetminus Z_1) = 1$ and $\Phi(Z_2) = 0$. It is easy to check that $\mathcal{S}' = (\mathcal{S} \setminus Z_1)/Z_2$ is a normalized $((\Phi \setminus Z_1)/Z_2)$-polymatroid with $\sigma_{p_o}(\mathcal{S}') \le \sigma_{p_o}(\mathcal{S})$. □

The parameters λ and κ for perfect secret sharing are invariant by duality, as it was proved in [31] and [36], respectively. We extend these results to the non-perfect case. The relation between $\sigma(\Phi)$ and $\sigma(\Phi^*)$ is an open problem, even for perfect access functions. Similarly to the corresponding result for perfect secret sharing, the proof of Proposition 6.7 is based on duality in polymatroids. The reader is addressed to [46, Chapter 44.6f] or [36] for more information on this topic.

Proposition 6.7. *$\kappa(\Phi) = \kappa(\Phi^*)$ for every access function Φ.*

Proof. Let Φ be an access function on P. Since $\Phi^{**} = \Phi$, it is enough to prove that $\kappa(\Phi^*) \le \kappa(\Phi)$. We affirm that, for every normalized Φ-polymatroid $\mathcal{S} = (Q, f)$, there exists a normalized Φ^*-polymatroid $\mathcal{S}^*$ with $\sigma_{p_o}(\mathcal{S}^*) \le \sigma_{p_o}(\mathcal{S})$. Indeed, consider the dual polymatroid $\mathcal{S}^* = (Q, f^*)$ defined by

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

for every $X \subseteq Q$. Since $f(Q) = f(P)$, we have that $f^*(\{p_o\}) = f(\{p_o\}) = 1$. For every $X \subseteq P$,

$$\Delta_{f^*}(p_o{:}X) = 1 + f^*(X) - f^*(Xp_o) = f(Q \smallsetminus X) - f(P \smallsetminus X) = 1 - \Delta_f(p_o{:}P \smallsetminus X),$$

and hence $\mathcal{S}^*$ is a normalized Φ^*-polymatroid. In addition, $f^*(x) = f(Q \smallsetminus x) - f(Q) + f(x) \le f(x)$ for every $x \in P$. □

We prove next that, from any given $(\mathbb{K}, \ell)$-linear secret sharing scheme Σ with access function Φ, one can construct a $(\mathbb{K}, \ell)$-linear secret sharing scheme Σ^*, which is called the *dual* of Σ, that has access function Φ^* and the same information ratio as Σ. This result is based on the connection between linear secret sharing schemes and linear codes that is described in Section 3.

Let $\Sigma = (S_i)_{i \in Q}$ be a $(\mathbb{K}, \ell)$-linear secret sharing scheme determined by $\mathbb{K}$ linear maps $S_i : V \to E_i$ and let $C \subseteq E = \prod_{i \in Q} E_i$ be the linear code associated to Σ. The notation introduced at the beginning of Section 2 is broadly used in the following.

Lemma 6.8. *For a set $X \subseteq P$, consider the subspace $C' \subseteq C$ formed by the codewords $s \in C$ with $s_X = 0$. Then $\Phi_\Sigma(X) = 1 - \dim C'_o / \dim E_o$.*

Proof. By (1), $\Phi_\Sigma(X) = (\operatorname{rank} S_o + \operatorname{rank} S_X - \operatorname{rank} S_{Xp_o}) / \operatorname{rank} S_o$. On one hand, $\operatorname{rank} S_o = \dim E_o$. On the other hand, $C'_o = S_o(\ker S_X)$, and hence $\dim C'_o = \dim \ker S_X - \dim \ker S_{Xp_o} = \operatorname{rank} S_{Xp_o} - \operatorname{rank} S_X$. □

Fixing a scalar product in every space E_i, we can consider the orthogonal complement of C, that is, the vector subspace $C^\perp \subseteq E$ formed by all vectors $w \in E$ such that $w \cdot s = \sum_{i \in Q} w_i \cdot s_i = 0$ for every $s \in C$. Then $C^\perp$ is called the *dual code* of C.

Lemma 6.9. *The dual code $C^\perp$ defines a $(\mathbb{K}, \ell)$-linear secret sharing scheme Σ^* whose information ratio satisfies $\sigma(\Sigma^*) \leq \sigma(\Sigma)$.*

Proof. To simplify the notation, put $D = C^\perp$. Clearly, it is enough to prove that $D_o = E_o$ and $\dim D_P = \dim D$. Suppose that $D_o \subsetneq E_o$. Then there exists a nonzero vector $s_o \in E_o$ such that $s_o \cdot v = 0$ for every $v \in D_o$, and hence the vector $(s_o, 0) \in E_o \times E_P$ is in $C = D^\perp$. Since P is a qualified set of Σ, this is a contradiction by Lemma 6.8. Suppose now that $\dim D_P < \dim D$. This implies that there exists a vector $\widehat{s} \in D$ with $\widehat{s}_o \neq 0$ and $\widehat{s}_P = 0$. Therefore, $\widehat{s}_o \in (C_o)^\perp$, and hence $C_o \neq E_o$, a contradiction again. □

The $(\mathbb{K}, \ell)$-linear secret sharing scheme Σ^* defined by the dual code $C^\perp$ is called the *dual* of Σ. The following result generalizes the known results on duality in linear secret sharing. Its proof is based on the one for [13, Theorem 3.24].

Theorem 6.10. *If Σ is a linear secret sharing scheme with access function Φ, then the access function of the dual scheme Σ^* is Φ^*.*

Proof. Let Φ' be the access function of Σ^*. Consider $X \subseteq P$ and $Y = P \smallsetminus X$. Let $C'' \subseteq C^\perp$ be the subspace formed by the codewords $w \in C^\perp$ with $w_X = 0$. Consider also $C' \subseteq C$ formed by the codewords $s \in C$ with $s_Y = 0$. It is enough to prove $(C''_o)^\perp = C'_o$, because, by Lemma 6.8, this implies that

$$\Phi'(X) = \frac{\dim E_o - \dim C''_o}{\dim E_o} = \frac{\dim C'_o}{\dim E_o} = 1 - \Phi(Y) = \Phi^*(X).$$

If $w \in C''$ and $s \in C'$, then $0 = s \cdot w = s_o \cdot w_o + s_X \cdot w_X + s_Y \cdot w_Y = s_o \cdot w_o$. Therefore, $C'_o \subseteq (C''_o)^\perp$. Consider $s_o \in E_o \smallsetminus C'_o$. Then $(s_o, 0) \in E_{Yp_o}$ is not in C_{Yp_o}, and hence there exists $(w_o, w_Y) \in (C_{Yp_o})^\perp$ such that $(s_o, 0) \cdot (w_o, w_Y) = s_o \cdot w_o \neq 0$. Extend (w_o, w_Y) to a vector $w = (w_o, w_X, w_Y) \in E$ by taking $w_X = 0$. Clearly, $w \in C^\perp$, and hence $w \in C''$ and $w_o \in C''_o$. Therefore, $s_o \notin (C''_o)^\perp$. □

Corollary 6.11. $\lambda(\Phi) = \lambda(\Phi^*)$ *for every rational access function Φ.*

7 Uniform Secret Sharing Schemes

Uniform access functions generalize the perfect threshold access structures. It is well known that these access structures admit a linear secret sharing scheme with optimal information ratio, namely Shamir's secret sharing scheme [47]. This fundamental result was generalized by Yoshida, Fujiwara and Fossorier [50] by determining the optimal information ratio of all rational uniform access functions. By using the results in the previous sections, we present a much simpler proof of the result in [50], which is restated here in Theorem 7.9. Moreover, we extend it to non-rational access functions in Theorem 7.14. In particular, we present a construction of linear secret sharing schemes with optimal information ratio for all rational uniform access functions. Nevertheless, these optimal schemes may not be efficient. A construction of efficient linear secret sharing schemes for every rational uniform access functions is presented in Section 7.2. A similar construction was presented in [49].

7.1 Concatenating Secret Sharing Schemes

We analyze here a simple way to combine secret sharing schemes. A similar technique was used in [49, 50]. For each $j = 1, \ldots, m$ consider a positive integer q_j and a secret sharing scheme

$\Sigma_j = (S_i^j)_{i \in Q}$ with access function Φ^j. A secret sharing scheme $\Sigma = \prod_{j=1}^m \Sigma_j^{q_j}$ is obtained by concatenating m secret sharing schemes, each consisting of q_j instances of Σ_j. That is, $\Sigma = (S_i)_{i \in Q}$ with $S_i = (S_i^1)^{q_1} \times \cdots \times (S_i^m)^{q_m}$ for every $i \in Q$. Observe that $H(S_X) = \sum_{j=1}^m q_j H(S_X^j)$ for every $X \subseteq Q$. Because of that, the access function Φ of Σ is given by

$$\Phi(X) = \frac{I(S_o{:}S_X)}{H(S_o)} = \frac{\sum_{j=1}^m q_j I(S_o^j{:}S_X^j)}{\sum_{k=1}^m q_k H(S_o^k)}$$

for every $X \subseteq Q$. Therefore,

$$\Phi = \sum_{j=1}^m \rho_j \Phi^j,$$

where, for every $j = 1, \ldots, m$,

$$\rho_j = \frac{q_j H(S_o^j)}{\sum_{k=1}^m q_k H(S_o^k)}.$$

That is, Φ is a convex combination of the access functions $\Phi^1, \ldots, \Phi^m$. Moreover, if σ_j is the information ratio of Σ_j, then the information ratio σ of Σ satisfies $\sigma \leq \sum_{j=1}^m \rho_j \sigma_j$. Indeed,

$$\sigma = \max_{i \in P} \frac{\sum_{j=1}^m q_j H(S_i^j)}{\sum_{k=1}^m q_k H(S_o^k)} \leq \frac{\sum_{j=1}^m q_j \sigma_j H(S_o^j)}{\sum_{k=1}^m q_k H(S_o^k)} = \sum_{j=1}^m \rho_j \sigma_j. \tag{4}$$

If there is a player in P that holds the largest share in all schemes Σ_j, then the inequality in (4) holds with equality. Clearly, if Σ_j is a $(\mathbb{K}, \ell_j)$-linear secret sharing scheme for $j = 1, \ldots, m$, then the concatenation $\Sigma = \prod_{j=1}^m \Sigma_j^{q_j}$ is a $(\mathbb{K}, \ell)$-linear secret sharing scheme with $\ell = \sum_{j=1}^m q_j \ell_j$. This leads to the following result, which will be used in our construction of optimal secret sharing schemes for rational uniform access functions.

Proposition 7.1. *For $j = 1, \ldots, m$, let Φ^j be an access function on P that admits a $(\mathbb{K}, \ell_j)$-linear secret sharing scheme with information ratio σ_j. Let $\rho_1, \ldots, \rho_n$ be rational numbers with $0 < \rho_j < 1$ and $\sum_{j=1}^m \rho_j = 1$. Let N be a positive integer such that $N\rho_j$ is integer for every $j = 1, \ldots, m$. Then the access function $\Phi = \sum_{j=1}^m \rho_j \Phi^j$ admits a $(\mathbb{K}, \ell)$-linear secret sharing scheme with information ratio $\sigma \leq \sum_{j=1}^m \rho_j \sigma_j$ and $\ell = N\ell_1 \cdots \ell_m$.*

Proof. For $j = 1, \ldots, m$, take $q_j = LN\rho_j / \ell_j$, where $L = \ell_1 \cdots \ell_m$. Then

$$\frac{q_j \ell_j}{q_1 \ell_1 + \cdots + q_m \ell_m} = \rho_j.$$

The concatenation scheme $\Sigma = \prod_{j=1}^m \Sigma_j^{q_j}$ satisfies the required properties. □

7.2 Efficient Uniform Secret Sharing Schemes

A uniform access function Φ on a set P with $|P| = n$ is determined by the values

$$0 = \Phi_0 \leq \Phi_1 \leq \cdots \leq \Phi_n = 1,$$

where $\Phi(X) = \Phi_i$ for every $X \subseteq P$ with $|X| = i$. Therefore, a uniform access function is determined by its *increment vector*

$$\Phi' = (\Phi'_1, \ldots, \Phi'_n),$$

where $\Phi'_i = \Phi_i - \Phi_{i-1}$. Observe that $\Phi'_i \geq 0$ and $\sum_{i=1}^n \Phi'_i = 1$. We use the convention $\Phi'_{n+1} = 0$.

Proposition 7.2. *Every (rational) uniform access function is a (rational) convex combination of perfect ramp access functions.*

Proof. Let Φ be a uniform access function on a set P of n players. For $i = 1, \ldots, n$, let Ψ^i be the $(i-1, i, n)$-ramp access function on P. Clearly, $\Phi = \sum_{i=1}^{n} \Phi'_i \Psi^i$. □

Similarly to the perfect case, every rational uniform access function admits a linear secret sharing scheme with information ratio equal to 1.

Corollary 7.3. *Let Φ be a rational uniform access function on a set P of n players and let $M = M(\Phi)$ be the least common denominator of Φ. Then, for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n+1$, the access function Φ admits a $(\mathbb{K}, M)$-linear secret sharing scheme with information ratio equal to* 1.

Proof. Combine Remark 2.11 and Propositions 7.1 and 7.2. □

Remark 7.4. By Remark 3.2, the efficiency of this linear scheme depends on the least common denominator of the access function. Specifically, the computation time for both the distribution phase and the reconstruction phase is polynomial in $\log |\mathbb{K}|$, $M(\Phi)$ and n.

7.3 Uniform Secret Sharing Schemes with Optimal Information Ratio

We present here a construction of optimal linear secret sharing schemes for all rational uniform access functions. Nevertheless, the schemes that are obtained in this way are in general less efficient than the ones in Section 7.2. This is due to the size of the secret value.

We begin by introducing a new parameter that is a lower bound on $\kappa(\Phi)$ for uniform access functions. For a uniform access function Φ and for $i = 1, \ldots, n$, we notate $\delta_i(\Phi) = \Phi'_i - \Phi'_{i+1}$.

Definition 7.5. For a uniform access function Φ on n players, we define

$$\epsilon(\Phi) = \sum_{i=1}^{n} \max\{0, \Phi'_i - \Phi'_{i+1}\} = \sum_{i=1}^{n} \max\{0, \delta_i(\Phi)\}$$

Example 7.6. Let Φ be the (t, r, n)-ramp access function, which is uniform and has maximum increment $\mu = 1/(r-t)$. The increment vector Φ' is given by $\Phi'_i = 0$ if $1 \leq i \leq t$ or $r+1 \leq i \leq n+1$, and $\Phi'_i = \mu$ if $t+1 \leq i \leq r$. Therefore, $\epsilon(\Phi) = \mu$.

Proposition 7.7. *Let Φ be a uniform access function. Then $\mu(\Phi) \leq \epsilon(\Phi) \leq \kappa(\Phi)$.*

Proof. Take $n = |P|$. Since $\epsilon(\Phi) \geq \sum_{i=j}^{n} (\Phi'_i - \Phi'_{i+1}) = \Phi'_j - \Phi'_{n+1} = \Phi'_j$ for every $j = 1, \ldots, n$, the first inequality holds. For the second inequality, we prove that $\epsilon(\Phi) \leq f(x)$ for every $x \in P$ if (P, f) is a polymatroid compatible with Φ. Indeed, take an arbitrary ordering $(x_1, \ldots, x_n)$ of the elements in P. Then

$$f(x_n) = \sum_{i=1}^{n} \Delta_f(x_i{:}x_n | x_1 \ldots x_{i-1}) \geq \sum_{i=1}^{n} \max\{0, \Delta_\Phi(x_i{:}x_n | x_1 \ldots x_{i-1})\} = \epsilon(\Phi).$$

Here, the equalities are derived by straightforward calculations and the inequality is a consequence of Propositions 5.2 and 5.5. □

We proved in Proposition 7.2 that every uniform access function is a convex combination of ramp access functions. The next proposition is a refinement of that result that makes it possible to find an optimal secret sharing scheme for every rational uniform access function.

Proposition 7.8. *Let Φ be a uniform access function on a set P. Then there exist ramp access functions $\Phi^1, \dots, \Phi^m$ on P and positive real numbers $\rho_1, \dots, \rho_m$ with $\sum_{j=1}^{m} \rho_i = 1$ such that*

$$\Phi = \rho_1 \Phi^1 + \cdots + \rho_m \Phi^m$$

and $\epsilon(\Phi) = \rho_1 \epsilon(\Phi^1) + \cdots + \rho_m \epsilon(\Phi^m)$. Moreover, if Φ is rational, then the values $\rho_1, \dots, \rho_m$ are rational.

Proof. We use induction on the gap $g = g(\Phi)$. If $g = 1$, then Φ is a ramp access function and the result obviously holds. Suppose that $g > 1$. Take $n = |P|$. Let t be the maximum index with $\Phi_t = 0$ and r the minimum one with $\Phi_r = 1$. Then $g = r - t$ and $\Phi'_i = 0$ if $1 \leq i \leq t$ or $r + 1 \leq i \leq n + 1$, while $\Phi'_{t+1}, \Phi'_r > 0$. Let ℓ be the smallest integer satisfying $t + 1 \leq \ell \leq r$ and $\Phi'_\ell = \min\{\Phi'_{t+1}, \dots, \Phi'_r\}$. We distinguish two cases.

Case 1: $\Phi'_\ell = 0$. Then $t + 1 < \ell < r$ and $0 < \Phi_\ell < 1$. Take $\rho = \Phi_\ell$ and consider the uniform access functions Ψ^1 and Ψ^2 defined by

$$\Psi^1_i = \min\left\{\frac{\Phi_i}{\Phi_\ell}, 1\right\}, \quad \Psi^2_i = \max\left\{\frac{\Phi_i - \Phi_\ell}{1 - \Phi_\ell}, 0\right\}$$

for every $i = 0, 1, \dots, n$. Clearly, $\Phi = \rho\Psi^1 + (1 - \rho)\Psi^2$. Since $\Phi'_\ell = \Phi_\ell - \Phi_{\ell-1} = 0$, we have that $\Psi^1_i = 1$ if $i \geq \ell - 1$. In addition, $\Psi^2_i = 0$ if $i \leq \ell$. Therefore,

$$\begin{aligned} \epsilon(\Phi) &= \rho \sum_{i=1}^{\ell-1} \max\{0, \delta_i(\Psi^1)\} + (1 - \rho) \sum_{i=\ell+1}^{n} \max\{0, \delta_i(\Psi^2)\} \\ &= \rho\epsilon(\Psi^1) + (1 - \rho)\epsilon(\Psi^2). \end{aligned}$$

Since $g(\Psi^1) \leq \ell - t < g(\Phi)$ and $g(\Psi^2) \leq r - \ell < g(\Phi)$ the theorem holds for Φ by the induction hypothesis.
Case 2: $\Phi'_\ell > 0$. Let Ψ^1 be the (t, r, n)-ramp access function on P and take $\rho = g\Phi'_\ell$. If $\rho = 1$, then $\Phi = \Psi^1$ and the proof is concluded. Suppose that $\rho < 1$ and take

$$\Psi^2 = \frac{\Phi - \rho\Psi^1}{1 - \rho}.$$

Observe that $\Psi^2_0 = 0$ and $\Psi^2_n = 1$. We claim that $(\Psi^2)'_i \geq 0$ for every $i = 1, \dots, n$, and hence Ψ^2 is a uniform access function on P. Indeed, $(\Psi^2)'_i = 0$ if $1 \leq i \leq t$ or $r + 1 \leq i \leq n$, and $(\Psi^2)'_i = (\Phi'_i - \rho(\Psi^1)'_i)/(1 - \rho) = (\Phi'_i - \Phi'_\ell)/(1 - \rho) \geq 0$ if $t + 1 \leq i \leq r$. Since Ψ_1 is a ramp access function, $\delta_t(\Psi^1) = -1/g$ and $\delta_r(\Psi^1) = 1/g$, and $\delta_i(\Psi^1) = 0$ if $i \neq r, t$. So the three values $\delta_i(\Phi)$, $\delta_i(\Psi^1)$ and $\delta_i(\Psi^2)$ are non-positive for $i = t$ and are non-negative for $i = r$. Therefore, $\Phi = \rho\Psi^1 + (1 - \rho)\Psi^2$ and $\epsilon(\Phi) = \rho\epsilon(\Psi^1) + (1 - \rho)\epsilon(\Psi^2)$. The proof is concluded by checking that Ψ^2 is a convex combination of ramp access functions in the required conditions. Observe that $(\Psi^2)'_\ell = 0$. If $\ell = t + 1$ or $\ell = r$, then $g(\Psi^2) < g(\Phi)$ and the result holds by the induction hypothesis. Finally, we can reduce to Case 1 if $t + 1 < \ell < r$. □

Theorem 7.9. *Let Φ be a rational uniform access function on a set of players P. For every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq |P| + g(\Phi)$, there exists a $\mathbb{K}$-linear secret sharing scheme with access function Φ and information ratio $\sigma = \epsilon(\Phi)$. As a consequence, every rational uniform access function admits a linear secret sharing scheme with optimal information ratio.*

Proof. Combine Proposition 7.8 with Remark 2.11 and Proposition 7.1. □

Corollary 7.10. *For every rational uniform access function Φ, $\epsilon(\Phi) = \kappa(\Phi) = \sigma(\Phi) = \lambda(\Phi)$.*

The fact that $\kappa(\Phi) = \sigma(\Phi)$ for a rational uniform access function Φ, proved in Corollary 7.10, can also be derived from [16]. The result was obtained independently by means of different techniques. However, the computation of the explicit optimal information ratio, and the construction of the optimal scheme was an open problem.

The results presented in Theorem 7.9 and Corollary 7.10 deal with rational access functions. For some non-rational access functions, we can also apply the techniques used in the proof of Proposition 7.8 and construct optimal schemes, as we can see in the following example.

Example 7.11. Let Φ be a uniform access function on a set P of size 3 with $\Phi_0 = \Phi_1 = 0$, $\Phi_2 = \log 5/(2\log 5 + \log 7)$, and $\Phi_3 = 1$. Observe that $\epsilon(\Phi) = 1 - \Phi_2$. Let Σ_1 be a $(\mathbb{F}_5, 2)$-linear secret sharing scheme for the $(1, 3, 3)$-ramp access function with information ratio $\sigma(\Sigma_1) = 1/2$. Let Σ_2 be a $(\mathbb{F}_7, 1)$-linear secret sharing scheme for the $(2, 3, 3)$-ramp access function with information ratio $\sigma(\Sigma_2) = 1$. The access function of the concatenation of Σ_1 and Σ_2 is Φ, and its information ratio is $(\log 5 + \log 7)/(2\log 5 + \log 7) = 1 - \Phi_2$. Therefore, we have found a secret sharing scheme with optimal information ratio for the access function Φ.

We do not have a general method to construct a scheme with optimal information ratio for every uniform access function but, as it is demonstrated in the following remark, we can find secret sharing schemes whose parameters are arbitrarily close to the required ones.

Remark 7.12. For every non-rational uniform access function Φ on a set P with n players, there is a sequence of rational uniform access functions $(\Phi^k)_{k\in\mathbb{N}}$ such that $\lim_{k\to\infty} \sum_{i=0}^{n} |\Phi_i - \Phi_i^k| = 0$. Since $\lim_{k\to\infty} \epsilon(\Phi^k) = \epsilon(\Phi)$ and $\epsilon(\Phi^k) = \sigma(\Phi^k)$, there is a sequence of linear secret sharing schemes $(\Sigma_k)_{k\in\mathbb{N}}$ satisfying $\lim \Phi(\Sigma_k) = \Phi$ and $\lim \sigma(\Sigma_k) = \epsilon(\Phi)$.

Nevertheless, this is not enough to prove our main result, Theorem 7.14. Instead, the following proposition is needed.

Proposition 7.13. *For every uniform access function Φ, there exists a sequence of secret sharing schemes $(\Sigma^k)_{k\in\mathbb{N}}$ realizing Φ whose information ratios $\sigma(\Sigma^k)$ converge to $\epsilon(\Phi)$ as k tends to infinity.*

Proof. By Theorem 7.9, the result is obvious for rational access functions. Let Φ be a non-rational uniform access function on a set P with n players. By Proposition 7.8, there exist ramp access functions $\Phi^1, \dots, \Phi^m$ on P and positive real numbers $\rho_1, \dots, \rho_m$ with $\sum_{j=1}^{m} \rho_i = 1$ such that $\Phi = \rho_1\Phi^1 + \dots + \rho_m\Phi^m$ and $\epsilon(\Phi) = \rho_1\epsilon(\Phi^1) + \dots + \rho_m\epsilon(\Phi^m)$. For every $j = 1, \dots, m$, there exists a sequence of rational numbers $(\rho_{jk})_{k\in\mathbb{N}}$ with $\lim_{k\to\infty} \rho_{jk} = \rho_j$ and $\rho_{jk} \le \rho_j$ for every $k \in \mathbb{N}$. For every $k \in \mathbb{N}$, consider $\alpha_k = \sum_{j=1}^{m} \rho_{jk}$ and the uniform access functions

$$\Psi^k = \frac{\rho_{1k}}{\alpha_k}\Phi^1 + \dots + \frac{\rho_{mk}}{\alpha_k}\Phi^m \quad \text{and} \quad \Upsilon^k = \frac{\rho_1 - \rho_{1k}}{1 - \alpha_k}\Phi^1 + \dots + \frac{\rho_m - \rho_{mk}}{1 - \alpha_k}\Phi^m.$$

Let s be a positive integer with $2^s \ge n + g(\Phi)$ and let $\mathbb{K}$ be the finite field with order 2^s. Since Ψ^k is rational and $g(\Psi^k) \le g(\Phi)$, by Theorem 7.9 there exists a $(\mathbb{K}, \ell_k)$-linear secret sharing scheme $\Sigma_1^k = (S_i^k)_{i\in Q}$ with access function Ψ^k and information ratio

$$\sigma(\Sigma_1^k) = \sum_{j=1}^{m} \frac{\rho_{jk}}{\alpha_k}\epsilon(\Phi^j) = \epsilon(\Psi^k).$$

Observe that $H(S_{p_o}^k) = s\ell_k$. Moreover, we can take ℓ_k large enough such that $\lceil s\ell_k\Upsilon_i^k\rceil \ne \lceil s\ell_k\Upsilon_{i+1}^k\rceil$ for every $0 \le i \le n-1$ with $\Upsilon_i^k \ne \Upsilon_{i+1}^k$. From the proof of Theorem 4.2, there exists a secret sharing scheme $\Sigma_2^k = (T_i^k)_{i \in Q}$ with access function Υ^k and $H(T_{p_o}^k) = s\ell_k$. The information ratio of Σ_2^k is upper bounded by a quantity ν_n that only depends on the number n of players. Take positive integers q_k and q'_k such that $1 + q_k/q'_k = 1/\alpha_k$. Let Σ^k be the concatenation of q_k copies of Σ_1^k and q'_k copies of Σ_2^k. Then the access function of Σ_k is $\alpha_k \Psi^k + (1-\alpha_k)\Upsilon^k = \Phi$ and its information ratio satisfies $\epsilon(\Phi) \leq \sigma(\Sigma^k) \leq \alpha_k \epsilon(\Psi^k) + (1-\alpha_k)\nu_n$. The proof is concluded by taking into account that $\lim \epsilon(\Psi^k) = \epsilon(\Phi)$ and $\lim \alpha_k = 1$. □

Theorem 7.14. *The optimal information ratio of every uniform access function Φ is equal to $\epsilon(\Phi)$.*

Proof. Straightforward from Proposition 7.13. □

Corollary 7.15. *For every uniform access function Φ, $\epsilon(\Phi) = \kappa(\Phi) = \sigma(\Phi)$.*

8 Ideal Secret Sharing Schemes

In an ideal perfect secret sharing scheme, the length of every share equals a basic lower bound, namely the length of the secret. Brickell and Davenport [11] proved that every ideal perfect secret sharing scheme determines a matroid. As a consequence, its access structure is a port of that matroid. Moreover, the optimal information ratio of every perfect access structure that is not a matroid port is at least 3/2 [36].

This section deals with the extension to the non-perfect case of those results on ideal secret sharing schemes. The existing definition of ideal (non-perfect) secret sharing scheme [35, 45] is motivated by the connection with matroids, but it is not as natural as the one for the perfect case. This is argued in a recent work [25], in which the connection between non-perfect secret sharing and matroids is thoroughly analyzed. The framework introduced in this paper provides a more satisfactory definition of ideal secret sharing scheme.

Definition 8.1. A secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ is *ideal* if its access function Φ has constant increment μ and $H(S_y) = \mu H(S_o)$ for every $y \in P$. An access function is called *ideal* if it admits an ideal secret sharing scheme.

As in the perfect case, all shares in an ideal secret sharing scheme have the same length, equal to a basic lower bound. Indeed, if the access function has constant increment, then the length of each share is at least the maximum increment (here, we naturally assume that all players are significant in the access function). As a consequence of the results in this section, our definition of ideal secret sharing scheme is equivalent to the one proposed in previous works [35, 45].

Example 8.2. Every $(\mathbb{K}, \ell)$-linear secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ with $\operatorname{rank} S_i = 1$ for every $i \in P$ is ideal. In particular, the ramp secret sharing schemes in Example 2.9 are of this form, and hence they are ideal.

A weaker sufficient condition for a secret sharing scheme to be ideal is obtained as a consequence of the results in [25]. An access structure is *connected* if every player is in a minimal qualified set and in a minimal non-forbidden set.

Theorem 8.3. *A secret sharing scheme $\Sigma = (S_x)_{x \in Q}$ with access function Φ and connected access structure $(\mathcal{A}, \mathcal{B})$ is ideal if and only if there exists a real number ν with $0 < \nu \leq 1$ such that*

- $\Phi(Ay) \in \{0, \nu\}$ *for every $A \in \mathcal{A}$ and $y \in P$,*

- $\Phi(B \setminus y) \in \{1-\nu, 1\}$ *for every* $B \in \mathcal{B}$ *and* $y \in B$*, and*
- $H(S_y) = \nu H(S_o)$ *for every* $y \in P$*.*

The rest of the section is dedicated to explore the connection between ideal secret sharing schemes and matroids. Basically, we rewrite the results in [25] in terms of access functions. A *matroid* $\mathcal{M} = (Q, r)$ is an integer polymatroid such that $r(x) \in \{0, 1\}$ for every $x \in Q$. The reader is referred to [42, 46, 48] for textbooks on matroid theory.

Definition 8.4. Let P, P_o be a pair of nonempty, disjoint sets and $\mathcal{M} = (P \cup P_o, r)$ a matroid such that $r(P_o) = |P_o|$ and $\Delta_r(P_o{:}P) = r(P_o)$. The *generalized port of the matroid* $\mathcal{M}$ *at the set* P_o is the access function Φ on P defined by

$$\Phi(X) = \frac{\Delta_r(P_o{:}X)}{r(P_o)} = \frac{\Delta_r(P_o{:}X)}{|P_o|}$$

for every $X \subseteq P$. Generalized matroid ports with $|P_o| = 1$ are perfect and they are called *matroid ports.*

Theorem 8.5 ([25])**.** *The access function of every ideal secret sharing scheme is a generalized matroid port.*

Proposition 8.6 ([25])**.** *If* Φ *is a generalized matroid port, then* Φ *has constant increment and* $\kappa(\Phi) = \mu(\Phi) = 1/g(\Phi)$*.*

Corollary 8.7. *If* Φ *is an ideal access function, then* $\sigma(\Phi) = \mu(\Phi) = 1/g(\Phi)$*.*

Example 8.8. By Proposition 8.6, a uniform access function is a generalized matroid port if and only if it is a ramp access function. Hence, the ideal uniform access functions are precisely the ramp ones.

Remark 8.9. Both classes of ideal linear secret sharing schemes and of generalized matroid ports are closed by duality.

9 Conclusion and Open Problems

In this work we present a new framework, based on the concept of access function, for the analysis of non-perfect secret sharing schemes. We prove that every access function admits a secret sharing scheme. By extending the polymatroid technique to non-perfect secret sharing schemes, we pursue the search for bounds on the information ratio.

Determining the optimal information ratio for general access functions appeared to be extremely difficult even for the particular case of perfect access structures, which has been extensively studied. One of the main open problems is to find superpolynomial lower bounds. By Proposition 5.7, this is not possible by using the polymatroid technique, which is based only on the Shannon information inequalities. Better lower bounds could be found by using non-Shannon information inequalities, but limitations on this approach for perfect secret sharing schemes have been found [5, 37].

Superpolynomial lower bounds on the information ratio have been found for perfect linear secret sharing schemes [2]. The extension of this result to non-perfect secret sharing schemes is worth considering.

Due to the difficulty of finding general bounds, a number of works have considered this problem for particular families of perfect access structures. Recent examples are [3, 21, 24].

We determined the optimal information ratio for a family of non-perfect access functions, the uniform ones. Surely, the techniques that are introduced in this paper will be useful to analyze other families of access functions.

In several scenarios, the access function provide too many details about the structure of the scheme. Optimization questions should be considered also when only lower and upper bounds on the access function are given.

As we saw for uniform access functions, secret sharing schemes with optimal information ratio are not necessarily the most efficient ones. This leads to the search of bounds on the length of the shares instead of the information ratio. This line of work has been initiated already in [13].

References

[1] A. Beimel. Secret-Sharing Schemes: A Survey. *Coding and Cryptology, Third International Workshop, IWCC 2011, Lecture Notes in Comput. Sci.* **6639** (2011) 11–46.

[2] A. Beimel, A. Ben-Efraim, C. Padró, I. Tyomkin. Multi-linear Secret-Sharing Schemes. *Theory of Cryptography, TCC 2014, Lecture Notes in Comput. Sci.* **8349** (2014) 394–418.

[3] A. Beimel, O. Farràs, Y. Mintz. Secret Sharing Schemes for Very Dense Graphs. *Advances in Cryptology, CRYPTO 2012, Lecture Notes in Comput. Sci.* **7417** (2012) 144–161.

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

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

[6] J. Benaloh, J. Leichter. Generalized secret sharing and monotone functions. *Advances in Cryptology, CRYPTO'88, Lecture Notes in Comput. Sci.* **403** (1990) 27–35.

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

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

[9] G. R. Blakley, C. Meadows. Security of Ramp Schemes. *Advances in Cryptology, Crypto'84. Lecture Notes in Comput. Sci.* **196** (1985) 242–268.

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

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

[12] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. *J. Cryptology* **6** (1993) 157–167.

[13] I. Cascudo, R. Cramer, C. Xing. Bounds on the Threshold Gap in Secret Sharing and its Applications. *IEEE Transactions on Information Theory* **59** (2013) 5600–5612.

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

[15] H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo. Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves. *Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Comput. Sci.* **4965** (2008) 451–470.

[16] Q. Chen, R.W Yeung. Two-Partition-Symmetrical Entropy Function Regions. *ITW* (2013) 1–5.

[17] T.M. Cover, J.A. Thomas. *Elements of Information Theory*, 2nd ed. Wiley, New York, 2006.

[18] R. Cramer, I. Damgård, Robbert de Haan. Atomic Secure Multi-party Multiplication with Low Communication. *Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Comput. Sci.* **4515** (2007) 329–346.

[19] 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.

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

[21] L. Csirmaz, G. Tardos. Optimal Information Rate of Secret Sharing Schemes on Trees. *IEEE Trans. Inform. Theory* **59** (2013) 2527–2630.

[22] Y. Desmedt. Threshold cryptography. *European Transactions on Telecommunications* **5** (1994) 449–457.

[23] O. Farràs, T. Hansen, T. Kaced, C. Padró. Optimal Non-Perfect Uniform Secret Sharing Schemes. *Advances in Cryptology, CRYPTO 2014. Lecture Notes in Comput. Sci.* **8617** (2014) 217–234.

[24] 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.

[25] O. Farràs, C. Padró. Extending Brickell–Davenport theorem to non-perfect secret sharing schemes. *Des. Codes Cryptogr.*, **74(2)** (2015) 495–510.

[26] M. Franklin, M. Yung. Communication Complexity of Secure Computation, *STOC 1992* 699–710.

[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] Y. Ishai, E. Kushilevitz, O. Strulovich. Lossy Chains and Fractional Secret Sharing. *STACS 2013, LIPICS*, **20** (2013) 160–171.

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

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

[32] T. Kaced. Almost-perfect secret sharing. *Proceedings of 2011 IEEE International Symposium on Information Theory, ISIT 2011* (2011) 1603–1607. Full version available at *arXiv.org*, http://arxiv.org/abs/1103.2544.

[33] E.D. Karnin, J.W. Greene, and M.E. Hellman, On secret sharing systems, *IEEE Trans. Inform. Theory* **29** (1983), 35–41.

[34] S.C. Kothari. Generalized Linear Threshold Scheme. *Advances in Cryptology, CRYPTO'84. Lecture Notes in Comput. Sci.* **196** (1985) 231–241.

[35] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii. Nonperfect Secret Sharing Schemes and Matroids. *Advances in Cryptology, EUROCRYPT 1993, Lecture Notes in Comput. Sci.* **765** (1994) 126–141.

[36] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120.

[37] S. Martín, C. Padró, A. Yang. Secret Sharing, Rank Inequalities and Information Inequalities. *Advances in Cryptology, CRYPTO 2013. Lecture Notes in Comput. Sci.* **8043** (2012) 277–288.

[38] J.L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, Molle, Sweden, August 1993, pp. 269–279 (1993).

[39] R.J. McEliece, D.V. Sarwate. On Sharing Secrets and Reed-Solomon Codes. *Commun. ACM* **24** (1981) 583–584.

[40] W. Ogata, K. Kurosawa, S. Tsujii. Nonperfect Secret Sharing Schemes. *Advances in Cryptology, Auscrypt 92, Lecture Notes in Comput. Sci.* **718** (1993) 56–66.

[41] K. Okada, K. Kurosawa. Lower Bound on the Size of Shares of Nonperfect Secret Sharing Schemes. *Advances in Cryptology, Asiacrypt 94, Lecture Notes in Comput. Sci.* **917** (1995) 33–41.

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

[43] C. Padró. Lecture Notes in Secret Sharing. *Cryptology ePrint Archive* 2012/674.

[44] C. Padró, L. Vázquez, A. Yang. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Discrete Appl. Math.* **161** (2013) 1072–1084.

[45] P. Paillier. On ideal non-perfect secret sharing schemes. *Security Protocols, 5th International Workshop, Lecture Notes in Comput. Sci.* **1361** (1998) 207–216.

[46] A. Schrijver. *Combinatorial Optimization. Polyhedra and Efficiency.* Springer-Verlag, Berlin, 2003.

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

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

[49] M. Yoshida, T. Fujiwara. Secure Construction for Nonlinear Function Threshold Ramp Secret Sharing. *IEEE International Symposium on Information Theory, ISIT 2007* (2007) 1041–1045.

[50] M. Yoshida, T. Fujiwara, M. Fossorier. Optimum General Threshold Secret Sharing. *Information Theoretic Security, ICITS 2012, Lecture Notes in Comput. Sci.* **7412** (2012) 187–204.