Optimal Non-Perfect Uniform 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]The Chinese University of Hong Kong, Hong Kong
[4]Nanyang Technological University, Singapore

April 22, 2014

Abstract

A secret sharing scheme is non-perfect if some subsets of participants 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. To this end, we extend the known connections between 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 that every subset of participants obtains about the secret value. We prove that there exists a secret sharing scheme for every access function.

Uniform access functions, that is, the ones whose values depend only on the number of participants, generalize the threshold access strcutures. Our main result is to determine the optimal information ratio of the uniform access functions. Moreover, we present a construction of linear secret sharing schemes with optimal information ratio for the rational uniform access functions.

Key words. Secret sharing, Non-perfect secret sharing, Information Ratio, Polymatroid

1 Introduction

A *secret sharing scheme* is a method to protect a *secret value* by distributing it into *shares* among a set of *participants* 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 participants is *authorized* if their shares determine the secret value, while the shares of the participants in a *forbidden* set do not contain any information on the secret value. The *access structure* $\Gamma = (\mathcal{A}, \mathcal{B})$ of a secret sharing scheme consists of the families $\mathcal{A}$ and $\mathcal{B}$ of the

*The material in this paper has been submitted for publication. Oriol Farràs is supported by the Spanish Government through projects TIN2011C27076-C03-01 "CO-PRIVACY" and CONSOLIDER INGENIO 695 2010 CSD2007-00004 "ARES", and by the Government of Catalonia under Grant 2009 SGR 1135. email: oriol.farras@urv.cat. Tarik Kaced is supported by a grant from University Grants Committee of the Hong Kong S.A.R. (Project No. AoE/E-02/08). email: tarik@inc.cuhk.edu.hk. Carles Padró is supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03. email: carlespl@ntu.edu.sg.

forbidden and, respectively, authorized sets of participants. A secret sharing scheme is *perfect* if every subset of participants is either authorized or forbidden.

Secret sharing was independently introduced by Shamir [45] and Blakley [8]. They presented constructions of perfect *threshold* secret sharing schemes, in which the authorized subsets are those having at least a certain number of participants. In these schemes, the shares have the same length as the secret, which is optimal for perfect secret sharing schemes [32].

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 unauthorized 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 participants is forbidden, while every set with at least r participants is authorized. 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 [39].

The threshold and ramp schemes proposed in those seminal works [8, 9, 45] are *linear*, that is, they can be described in terms of linear maps over a finite field [10, 33] or in terms of linear codes [37, 38]. 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, 25].

Most of the works in the literature on secret sharing deal with perfect schemes. One of the main lines of research 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 refereed 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 Karnin et al. [32] and Capocelli et al. [12]. On the basis of the connections between information theory, matroid theory, and secret sharing found by Fujishige [26, 27], 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, 35, 36]. Similar questions have been considered for non-perfect secret sharing schemes too [24, 28, 34, 39, 40, 43], but the research is much less developed in this direction. In particular, only basic bounds on the information ratio of non-perfect secret sharing schemes are known [39, 40].

This work deals with the search for bounds on the information ratio of non-perfect secret sharing schemes. 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 use of polymatroids and the construction of efficient linear secret sharing schemes.

Our first step is to choose a suitable way to describe the security requirements of non-perfect secret sharing schemes. This description should be more precise than the access structure. That is, in addition to the forbidden and qualified sets, also the amount of information on the secret value that is obtained by the other sets should be taken into account. We introduce the *access function* of a secret sharing scheme (Definitions 3.1 and 3.5), which is a refinement of the *access hierarchies* that are used in [34, 40, 43]. 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 participants. The forbidden and authorized 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 [28], but the partial information on the secret is measured in a different way. The relation between these two approaches is discussed in Section 2.

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 [29], who proved that there exists a perfect secret sharing scheme for every 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 to take 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, 29], our general construction is inefficient because the length of the shares grows exponentially with the number of participants.

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 definition of access function appears to be most suitable for our purposes. This can be seen, for instance, in Proposition 5.6, 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. In addition, the concepts of *minor* and *dual* of an access structure have a natural extension to access functions, as described in Section 7.

Two different lower bounds on the optimal information ratio of access functions are discussed in Section 6. The first one is the extension of the parameter κ [35] to the non-perfect case. The second one, which is denoted by ϵ, is introduced in this paper. It is a lower bound on κ, and hence a lower bound on the optimal information ratio. The value of ϵ is 1 on every perfect access function, and hence this new parameter is relevant only for the non-perfect case. As a consequence of Proposition 6.2, the parameter ϵ improves the previously known lower bound in Proposition 3.12 [39, 40]. We prove in Propositions 6.3 and 6.4 that $\epsilon \leq \kappa \leq n\epsilon$, where n is the number of participants. This generalizes the known bounds $1 \leq \kappa \leq n$ [20, 35] for perfect secret sharing. As in the perfect case, the upper bound on κ indicates the limitations of using only Shannon information inequalities in the search of lower bounds on the information ratio. The behavior of the parameters κ and ϵ with respect to duality is analyzed in Section 7.

Our main result deals with *uniform* access functions, that is, the ones that take the same value on sets that have the same cardinality. They generalize the perfect threshold access structures. Our main result is presented in Section 9. Namely, we determine in Theorem 9.12 the exact value of the optimal information ratio of all uniform access functions. Moreover, our proof provides a method to construct a linear secret sharing scheme with optimal information ratio for every given rational uniform access function. This is done in several steps. First, we prove in Proposition 9.6 that every uniform access function is a suitable convex combination of ramp access functions. As a consequence, the values of κ and ϵ coincide for the uniform access functions. Moreover, combining Proposition 9.6 with the basic concatenation method described in Section 8, one can construct a linear secret sharing scheme with optimal information ratio (that is, equal to the lower bound ϵ) for every rational uniform access function.

2 Related Work

Brickell and Davenport [11] proved that every perfect secret sharing scheme in which all shares have the same length as the secret (such perfect schemes are called *ideal*) defines a matroid that is determined by the access structure of the scheme. This connection between secret sharing schemes and matroids was first extended to non-perfect schemes by Kurosawa et al. [34], who characterized the non-perfect secret sharing schemes that define a matroid. Additional results on this connection were given by Paillier [43]. Recently, a characterization with weaker conditions has been presented [24]. Similarly to the results in this paper, its proof is based on the connection between secret sharing and polymatroids.

The polymatroid-based method described in [20, 35] is applied here for the first time to find lower bounds on the optimal information ratio of non-perfect secret sharing schemes. This method is a formalization of the one previously used in [12] and many other works, which is based on the use of the Shannon inequalities of the entropy function. Some lower bounds on the information ratio of non-perfect secret sharing schemes were found by that entropy-based method. Namely, the one given in Proposition 3.12 [39, 40] and a lower bound for a particular access function [40] that proves that the bound in Proposition 3.12 is not always attained.

The *almost-perfect secret sharing schemes* introduced in [31] are schemes whose access functions are close to a perfect access function. 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.

Ishai, Kushilevitz and Strulovich [28] 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 $F : \mathcal{P}(P) \to \{1, \ldots, m\}$, where $\mathcal{P}(P)$ is the power set of the set P of participants. Given the shares of the participants 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 participants in X to find the secret value. The main results in [28] 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 [28] 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 participants. 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 [28, 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 (see Definition 3.13) only if all its values are powers of q.

Our optimality result for uniform access functions (Theorem 9.12) 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 result implies Corollary 9.11 (2). Nevertheless, the other results in Section 9, 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].

3 Secret Sharing Schemes

In this work we consider the definition of secret sharing scheme that is based on information theory, specifically, on the entropy function. For a complete introduction to secret sharing, see [1, 41], and for a textbook on information theory see [17]. We begin by introducing some notation. For a finite set Q, we use $\mathcal{P}(Q)$ to denote its *power set*, 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 $X - Y$ for the set difference and $X - x$ for $X - \{x\}$. Let $X = \{1, \ldots, t\}$ be a set and let $(S_i)_{i \in X}$ be a tuple of discrete random variables. We write S_X for the random variable $S_1 \times \cdots \times S_t$, and $H(S_X)$ for its Shannon entropy. Recall that, for two such random variables S_X, S_Y, one can consider the *conditional entropy* $H(S_X|S_Y) = H(S_{XY}) - H(S_Y)$ and the *mutual information* $I(S_X{:}S_Y) = H(S_X) - H(S_X|S_Y)$. All through the paper, P and Q stand for finite sets with $Q = Pp_o$ for some $p_o \notin P$.

Definition 3.1 (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 3.2 (Access structure)**.** If $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}(P)$ are nonempty families of subsets of P such that $\mathcal{A}$ is monotone decreasing, $\mathcal{B}$ is monotone increasing, and $\mathcal{A} \cap \mathcal{B} = \emptyset$, then the pair $\Gamma = (\mathcal{A}, \mathcal{B})$ is called an *access structure* on P. The sets in $\mathcal{A}$ and the sets in $\mathcal{B}$ are, respectively, the *forbidden* and the *authorized* sets of the access structure Γ. In a *perfect* access structure, every subset of P is either forbidden or authorized.

Definition 3.3. For an access function Φ on P, a set $X \subseteq P$ is *forbidden* for Φ if $\Phi(X) = 0$, and it is *authorized* for Φ if $\Phi(X) = 1$. Then every access function Φ on P determines an access structure $\Gamma(\Phi) = (\mathcal{A}(\Phi), \mathcal{B}(\Phi))$ on P, where $\mathcal{A}(\Phi) \subseteq \mathcal{P}(P)$ and $\mathcal{B}(\Phi) \subseteq \mathcal{P}(P)$ are the families of the forbidden and, respectively, the authorized subsets for Φ.

Definition 3.4 (Secret sharing scheme)**.** Let Q be a finite set of *participants*, let $p_o \in Q$ be a distinguished participant, which is called *dealer*, and take $P = Q - p_o$. A *secret sharing scheme* Σ on the set P is a collection $(S_i)_{i \in Q}$ of discrete random variables such that $H(S_{p_o}) > 0$ and $H(S_{p_o}|S_P) = 0$. The random variable S_{p_o} corresponds to the *secret*, while the random variables $(S_i)_{i \in P}$ correspond to the *shares* of the secret that are distributed among the participants in P.

Definition 3.5 (Access function and access structure of a secret sharing scheme)**.** The access function Φ of a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ is defined by

$$\Phi(X) = \frac{I(S_{p_o}{:}S_X)}{H(S_{p_o})}.$$

In addition, $\Gamma(\Phi)$ is the access structure of the secret sharing scheme Σ. A secret sharing scheme is *perfect* if its access function is perfect.

If $X \subseteq P$ is an authorized set for Σ, then $H(S_{p_o}|S_X) = 0$, which implies that the secret values can be recovered from the shares of the participants in X. On the other hand, the random

variables S_{p_o} and S_X are independent if X is a forbidden set for Σ. In this situation the shares of the participants in X do not provide any information on the secret value. In any other case, the value $\Phi(X)$ determines the amount of information on the secret that is provided by the shares of the participants in X.

Definition 3.6 (Gap and maximum increment)**.** The *gap* $g(\Gamma)$ of an access structure $\Gamma = (\mathcal{A}, \mathcal{B})$ is defined as $g(\Gamma) = \min\{|B - A| : A \in \mathcal{A}, B \in \mathcal{B}\}$. The gap $g(\Phi)$ of an access function Φ is defined as the gap of the associated access structure. 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 is denoted by $\mu(\Phi)$.

Definition 3.7 (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.

Definition 3.8 (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.

Definition 3.9 (Threshold access structure)**.** Let t, r, n be integers with $0 \leq t < r \leq n$. In the (t, r, n)*-threshold access structure* on a set P with $|P| = n$, the forbidden sets are those with at most t participants, and the authorized sets are those with at least r participants. The values t and r are called, respectively, the *privacy threshold* and the *reconstruction threshold*.

A threshold access structure is perfect if and only if $r = t + 1$. Observe that every uniform access function defines a threshold access structure. The privacy and reconstruction thresholds of a uniform access function are those of the associated threshold access structure. Ramp access functions form an important class of uniform access functions.

Definition 3.10 (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 $|X| \geq r$.

Example 3.11. A variant of Shamir's threshold scheme [45] 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 the (t, r, n)-ramp access function on the set $P = \{1, \ldots, n\}$. Let $\mathbb{K}$ be a finite field of size $|\mathbb{K}| \geq n + g$, where $g = r - t$ is the gap of the access function, and take $n + g$ different elements $y_1, \ldots, y_g, x_1, \ldots, x_n \in \mathbb{K}$. By choosing uniformly at random a polynomial $f \in \mathbb{K}[X]$ with degree at most $r - 1$, one obtains random variables $S_{p_o} = (f(y_1), \ldots, f(y_g)) \in \mathbb{K}^g$ and $S_i = f(x_i) \in \mathbb{K}$ for every $i \in P$. 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.

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,

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

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. A secret sharing scheme attaining $\sigma(\Phi)$ is called *optimal*. The following is a well known lower bound on the optimal information ratio. An alternative proof for this result is presented here in Propositions 6.2 and 6.3.

Proposition 3.12 ([32, 39, 40])**.** *Let Φ be an access function with maximum increment $\mu(\Phi)$ and gap $g(\Phi)$. Then its optimal information ratio $\sigma(\Phi)$ satisfies $\sigma(\Phi) \geq \mu(\Phi) \geq 1/g(\Phi)$. In particular, the optimal information ratio of every perfect access function is at least* 1*.*

Definition 3.13 (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 $S_i : E \to E_i$, where the uniform probability distribution is taken on E and $\dim E_{p_o} = \ell$.

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

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

This implies that the access function of every linear secret sharing scheme is rational and its information ratio is rational too. 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 3.14. The secret sharing scheme presented in Example 3.11 is linear. As a consequence, the (t, r, n)-ramp access function admits a $(\mathbb{K}, g)$-linear secret sharing scheme for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n + g$, where $g = r - t$. By Proposition 3.12, this linear scheme has optimal information ratio, equal to the lower bound $1/g$.

Remark 3.15. A $(\mathbb{K}, \ell)$-linear secret sharing scheme with information ratio σ is determined by linear maps $S_i : E \to E_i$ with $\dim E_i \leq \max\{\ell, \sigma\ell\}$ for every $i \in Q$ and $\dim E \leq \sum_{i\in Q} \dim E_i$. Therefore, the computation time for both the distribution phase (computing the secret value and the shares) 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 participants.

Remark 3.16. Let Φ be a rational access function on P and let $M = M(\Phi)$ be its least common denominator. Clearly, $\ell \geq M$ for every $(\mathbb{K}, \ell)$-linear secret sharing scheme for Φ. Therefore, by Remark 3.15, the efficiency of the linear secret sharing schemes for Φ depends on $M(\Phi)$.

4 A Secret Sharing Scheme for Every Access Function

It is well known that every perfect access function admits a perfect secret sharing scheme [6, 29]. We present in Theorem 4.2 an extension of this result to the general case.

Remark 4.1. Similarly to the construction in [29] for the perfect case, our general construction is based on a very simple perfect secret sharing scheme for which the only authorized set is the full set of participants. Let G be a finite abelian group (with additive notation). Let T_{p_o} be an arbitrary random variable with support G. Fix a participant $q \in P$ and take independent uniform random variables $(T_i)_{i\in P-q}$ with support G. Finally, take $T_q = T_{p_o} - \sum_{i\in P-q} T_i$. It is not difficult to see that $\mathbf{T} = (T_i)_{i\in Q}$ is a perfect secret sharing scheme whose only authorized 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 schemes for every finite field $\mathbb{K}$.*

Proof. Let Φ be an access function on the set of participants 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

- $\Omega = \{\lceil M\Phi(X)\rceil \,:\, X \subseteq P\} - \{0\} \subseteq \{1,\ldots,M\}$, 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_{p_o} corresponding to the secret value. Specifically, we take $S_{p_o} = \prod_{k=1}^{M} S^k$, where $(S^k)_{1\leq k\leq M}$ are 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 $\epsilon_k = k - M\Phi(X)$, which satisfies $0 < \epsilon_k < 1$, and take $S^k = S_0^k \times S_1^k$, where S_0^k and S_1^k are independent random variables with support $\mathbb{F}_2$ such that $\Pr[S_0^k = 0] = h^{-1}(\epsilon_k)$ and $\Pr[S_1^k = 0] = h^{-1}(1-\epsilon_k)$. If $k \in \{1,\ldots,M\} - \Omega_1$, 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 participants. 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

$$T_{p_o}^k = S^1 \times \cdots \times S^{k-1} \times \widehat{S}^k,$$

where $\widehat{S}^k = S_1^k$ if $k \in \Omega_1$ and $\widehat{S}^k = S^k$ otherwise. Observe that $H(T_{p_o}^k) = M\Phi(X)$ for every $X \in \mathcal{C}_k$. The support of $T_{p_o}^k$ is $\mathbb{F}_2^m$ for some integer $m \geq k$. For every $X \in \mathcal{C}_k$, take the secret sharing scheme $\mathbf{T}^{(X)} = (T_i^{(X)})_{i\in Xp_o}$ described in Remark 4.1 with $T_{p_o}^{(X)} = T_{p_o}^k$ and $G = \mathbb{F}_2^m$. The random variable $T_{p_o}^k$ 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 $T_i^{(X)}$ are instantiated independently for different sets X. For every participant $i \in P$ 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 participant $i \in P$ is defined by

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

That is, the share of every participant 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, $H(T_{p_o}^k | S_Y) = 0$ 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 participants in Y do not provide any information about the other components of the secret value, and hence $I(S_{p_o}{:}S_Y) = H(T_{p_o}^k) = M\Phi(Y)$. Since $H(S_{p_o}) = M$, 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 $S_{p_o} = \prod_{k=1}^{M} S^k$, where $(S^k)_{1\leq k\leq M}$ 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 participants. The construction can be refined in order to slightly decrease the information ratio, but no constructions are known in which the information ratio is not exponential.

5 Polymatroids and Secret Sharing

The connection between perfect secret sharing schemes and polymatroids has been used in order to obtain bounds on the information ratio [20, 35]. It is derived from the connection between polymatroids and Shannon entropy that was discovered by Fujishige [26, 27] and is described here in Theorem 5.3. In this section, we discuss the extension of this connection to non-perfect secret sharing schemes. For a function $F : \mathcal{P}(Q) \to \mathbb{R}$, a subset $X \subseteq Q$ and $y, z \in Q$, we notate

$$\Delta_F(X; y, z) = F(Xy) + F(Xz) - F(Xyz) - F(X).$$

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 $f(X) \leq f(Y)$.
- f is *submodular*: $f(X \cup Y) + f(X \cap Y) \leq f(X) + f(Y)$ for every $X, Y \subseteq Q$.

If $\mathcal{S} = (Q, f)$ is a polymatroid, then $\lambda\mathcal{S} = (Q, \lambda f)$ is also a polymatroid for every positive real number λ. We say that $\lambda\mathcal{S}$ is a *multiple* of $\mathcal{S}$. The following characterization of rank functions of polymatroids is a straightforward consequence of [44, 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 $\Delta_f(X; y, z) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q - X$.*

Theorem 5.3 (Fujishige [26, 27])**.** *If $(S_i)_{i\in Q}$ is a tuple of discrete random variables, then the map $f\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $f(X) = H(S_X)$ is the rank function of a polymatroid with ground set Q.*

Because of the connection between polymatroids and the Shannon entropy described in the previous theorem, and by analogy to the conditional entropy, we write $f(X|Y) = f(XY) - f(Y)$ for every $X, Y \subseteq Q$.

As a consequence of Theorem 5.3, every secret sharing scheme determines a polymatroid. For perfect secret sharing schemes, this connection was first used in [20]. This is a useful tool for the study of secret sharing schemes.

Definition 5.4. Let $\Sigma = (S_i)_{i\in Q}$ be a secret sharing scheme on P. Every multiple of the polymatroid (Q, f), where $f(X) = H(S_X)$ for every $X \subseteq Q$, is called a Σ-*polymatroid*.

Definition 5.5. Let Φ be an access function on P and let $\mathcal{S} = (Q, f)$ be a polymatroid. Then $\mathcal{S}$ is an Φ-*polymatroid* if

$$\Phi(X) = \frac{f(p_o) - f(p_o|X)}{f(p_o)}$$

for every $X \subseteq P$.

We say that a polymatroid $\mathcal{S} = (Q, f)$ 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 5.6. *A polymatroid $\mathcal{S} = (P, f)$ is compatible with an access function Φ on P if and only if $\Delta_f(X; y, z) \geq \Delta_\Phi(X; y, z)$ for every $X \subseteq P$ and $y, z \in P - X$.*

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 $\Delta_f(X; y, z) \geq 0$ for every $X \subseteq Q$ and $y, z \in Q - X$. Since (P, f) is a polymatroid, (Q, f) is a polymatroid if and only if the following conditions are satisfied.

1. $\Delta_f(Xp_o; y, z) \geq 0$ for every $X \subseteq P$ and $y, z \in P - X$.
2. $\Delta_f(X; p_o, z) \geq 0$ for every $X \subseteq P$ and $z \in Q - X$.

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

6 Lower Bounds on the Information Ratio

On the basis of the connection between secret sharing and polymatroids, we introduce in this section two parameters, $\kappa(\Phi)$ and $\epsilon(\Phi)$, that provide lower bounds on the optimal information ratio $\sigma(\Phi)$. The first one is a straightforward generalization of the corresponding parameter for perfect secret sharing that was introduced in [35]. The second one is only relevant for non-perfect secret sharing. It makes it possible to generalize a previous results by Csirmaz on the limitation of Shannon inequalities to find lower bounds on the information ratio and, more importantly, to find a tight lower bound on the optimal information ratio of uniform access functions.

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

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

If $\mathcal{S}$ is a Σ-polymatroid, then $\sigma(\Sigma) = \sigma_{p_o}(\mathcal{S})$. In addition, we define

$$\kappa(\Phi) = \inf\{\sigma_{p_o}(\mathcal{S}) \,:\, \mathcal{S} \text{ is a } \Phi\text{-polymatroid}\}. \tag{1}$$

Observe that, if Σ is a secret sharing with access function Φ, then every Σ-polymatroid is a Φ-polymatroid. Because of that, $\kappa(\Phi) \leq \sigma(\Phi)$. It is not difficult to prove that $\kappa(\Phi) \geq \mu(\Phi) \geq 1/g(\Phi)$ for every access function Φ [24, 39, 40]. In particular, this implies the well known fact that the information ratio of every perfect secret sharing scheme is at least 1.

The search of $\kappa(\Phi)$ for an access function Φ can be restricted to the family of the normalized Φ-polymatroids. The value of $\kappa(\Phi)$, which is a lower bound on $\sigma(\Phi)$, can be computed by means of the linear programming program determined by the Shannon information inequalities and the access function. This approach has been used in several works on perfect secret sharing, as for instance [42]. The infimum in (1) is a minimum and, moreover, $\kappa(\Phi)$ is rational if Φ is rational.

For an ordering $\tau = (\tau_1, \ldots, \tau_n)$ of the participants in P, we take $A_0^\tau = \emptyset$ and $A_i^\tau = \{\tau_1, \ldots, \tau_i\}$ for every $i = 1, \ldots, n$. For a function $F : \mathcal{P}(P) \to \mathbb{R}$ and for $i = 1, \ldots, n$, consider $\delta_i^\tau(F) = \Delta_F(A_{i-1}^\tau; \tau_i, \tau_n)$. Observe that $\sum_{i=1}^n \delta_i^\tau(F) = F(\tau_n) - F(\emptyset)$.

Definition 6.1. Let Φ be an access function on P, with $|P| = n$. We define $\epsilon(\Phi)$ as the maximum of $\sum_{i=1}^n \max\{0, \delta_i^\tau(\Phi)\}$ among all orderings τ of P.

Observe that $\max\{0, \delta_i^\tau(\Phi)\} \leq \Phi(A_i^\tau) - \Phi(A_{i-1}^\tau)$, and hence $\epsilon(\Phi) \leq 1$. As a consequence of the next proposition, $\epsilon(\Phi) = 1$ if Φ is a perfect access function. In addition, this result provides an alternative proof for the previously known basic lower bounds [39, 43] (see Proposition 3.12).

Proposition 6.2. *Let Φ be an access function on P. Then $\epsilon(\Phi) \geq \Phi(Xy) - \Phi(X)$ for every $X \subseteq P$ and $y \in P - X$. In particular, $\epsilon(\Phi) \geq \mu(\Phi) \geq 1/g(\Phi)$.*

Proof. Take $\ell = |X|$ and $n = |P|$ and consider an ordering τ of P such that $A^\tau_\ell = X$ and $\tau_n = y$. Then $\epsilon(\Phi) \geq \sum_{i=1}^n \max\{0, \delta^\tau_i(\Phi)\} \geq \sum_{i=\ell+1}^n \delta^\tau_i(\Phi) = \Phi(Xy) - \Phi(X)$. □

It is known that $1 \leq \kappa(\Phi) \leq |P|$ for every perfect access function [20, 32]. These bounds on κ are extended to the non-perfect case by proving that $\epsilon(\Phi) \leq \kappa(\Phi) \leq \epsilon(\Phi) \cdot |P|$ in Propositions 6.3 and 6.4. Combined with Proposition 6.2, this implies that $\epsilon(\Phi)$ is in general a better lower bound on $\kappa(\Phi)$ than $1/g(\Phi)$.

Proposition 6.3. *$\kappa(\Phi) \geq \epsilon(\Phi)$ for every access function Φ.*

Proof. Let Φ be an access function on a set P with n participants and let (Q, f) be a normalized Φ-polymatroid. Let τ be an ordering of P such that $\epsilon(\Phi) = \sum_{i=1}^n \max\{0, \delta^\tau_i(\Phi)\}$ and take $x = \tau_n$. By Propositions 5.2 and 5.6, $f(x) = \sum_{i=1}^n \delta^\tau_i(f) \geq \sum_{i=1}^n \max\{0, \delta^\tau_i(\Phi)\} = \epsilon(\Phi)$. □

Proposition 6.4. *Let Φ be an access function on a set of n participants. Then $\kappa(\Phi) \leq n\epsilon(\Phi)$.*

Proof. We prove it constructively by showing that there exists an Φ-polymatroid $\mathcal{S}$ with $\sigma_{p_o}(\mathcal{S}) = n\epsilon(\Phi)$. Consider the polymatroid (P, f) with $f(X) = \epsilon(\Phi) \sum_{i=1}^{|X|}(n-i+1)$ for every nonempty set X. Then $\Delta_f(X; y, z) = \epsilon(\Phi) \geq \Delta_\Phi(X; y, z)$ for every $X \subseteq P$ and $y, z \in P$ with $y, z \notin X$. Therefore, by Proposition 5.6, the polymatroid (P, f) is compatible with the access function Φ. □

7 Duality and Minors

Duality and minors are operations that play a fundamental role in the study of secret sharing, matroids and polymatroids. In this section we analyze these operations for general access functions.

Let Φ be an access function on a set P. For any $B \subseteq P$, we consider on the set $P - B$ the access functions $\Phi \setminus B$ and Φ/B defined by $(\Phi \setminus B)(A) = \Phi(A)$ and $(\Phi/B)(A) = \Phi(A \cup B)$. These operations are called *deletion* and *contraction*, respectively. Any access function obtained by a sequence of deletions and contractions of subsets of P is a *minor* of Φ. Minors of access functions correspond to natural scenarios. Namely, if several participants leave the scheme and maybe some of them reveal their shares, then the new access function will be a minor of the original one.

The *dual* Φ^* of an access function Φ on P is the access function on P defined by $\Phi^*(A) = 1 - \Phi(P - A)$. Obviously, $\Phi^{**} = \Phi$. Moreover, it is not difficult to check that $(\Phi/B)^* = \Phi^* \setminus B$ and $(\Phi \setminus B)^* = \Phi^*/B$.

For a polymatroid $\mathcal{S} = (Q, h)$ and a subset $B \subseteq Q$, we consider the polymatroids $\mathcal{S} \setminus B = (Q - B, h_{\setminus B})$ and $\mathcal{S}/B = (Q - B, h_{/B})$ with $h_{\setminus B}(X) = h(X)$ and $h_{/B}(X) = h(X \cup B) - h(B)$ for every $X \subseteq Q \setminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by a sequence of such operations is a *minor* of $\mathcal{S}$. If $\mathcal{S}$ is a Φ-polymatroid and $B \subseteq P$, then $\mathcal{S} \setminus B$ is a $(\Phi \setminus B)$-polymatroid and $\mathcal{S}/B$ is a (Φ/B)-polymatroid. Thus $\kappa(\Phi') \leq \kappa(\Phi)$ for every minor Φ' of Φ. In addition, the aforementioned connection between minors and secret sharing implies that $\sigma(\Phi') \leq \sigma(\Phi)$ and $\lambda(\Phi') \leq \lambda(\Phi)$.

Example 7.1. 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 $P - p$ with parameters $(t, r, n-1)$ and $(t-1, r-1, n-1)$, respectively.

Proposition 7.2. *For every access function* Φ, $\epsilon(\Phi) = \epsilon(\Phi^*)$.

Proof. Let Φ be an access function on a set P of size n and let τ be an ordering of P with $\epsilon(\Phi) = \sum_{i=1}^{n} \max\{0, \delta_i^\tau(\Phi)\}$. Consider the ordering $\tau^* = (\tau_{n-1}, \ldots, \tau_1, \tau_n)$ of P. Clearly,

$$\delta_i^\tau(\Phi) = -\delta_{n-i}^{\tau^*}(\Phi^*)$$

for all $i = 1, \ldots, n-1$. Let $I \subseteq \{1, \ldots, n-1\}$ be the set of indices i with $\delta_i^\tau(\Phi) > 0$. Then

$$\epsilon(\Phi) = \delta_n^\tau(\Phi) + \sum_{i \in I} \delta_i^\tau(\Phi) = \Phi^*(\tau_n^*) - \sum_{i \in I} \delta_{n-i}^{\tau^*}(\Phi^*).$$

Since $\sum_{i=1}^{n} \delta_i^{\tau^*}(\Phi^*) = \Phi^*(\tau_n^*)$,

$$\epsilon(\Phi) = \sum_{i=1}^{n} \max\{0, \delta_i^{\tau^*}(\Phi^*)\} \leq \epsilon(\Phi^*).$$

Finally, $\epsilon(\Phi) \geq \epsilon(\Phi^*)$ because $\Phi^{**} = \Phi$. □

In the perfect case, the parameters λ and κ are invariant by duality, as it was proved in [30] and [35], respectively. We extend the result on κ and λ to the non-perfect case. The relation between $\sigma(\Phi)$ and $\sigma(\Phi^*)$ is an open problem, even in the perfect case. Similarly to the perfect case, the proof of Proposition 7.3 is based on duality in polymatroids. The reader is addressed to [44, Chapter 44.6f] or [35] for more information on this topic.

Proposition 7.3. *For every access function* Φ, $\kappa(\Phi) = \kappa(\Phi^*)$.

Proof. Let Φ be an access function on P and let $\mathcal{S} = (Q, f)$ be a normalized Φ-polymatroid. We will show that there is a normalized Φ^*-polymatroid $\mathcal{S}^*$ with $\sigma_{p_o}(\mathcal{S}^*) \leq \sigma_{p_o}(\mathcal{S})$. Indeed, consider the dual polymatroid $\mathcal{S}^* = (Q, f^*)$ defined by

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

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

$$1 - f^*(p_o|X) = 1 - f^*(Xp_o) + f^*(X) = f(p_o|P - X) = 1 - \Phi(P - X) = \Phi^*(X),$$

and hence $\mathcal{S}^*$ is an Φ^*-polymatroid. In addition, $f^*(x) = f(Q - x) - f(Q) + f(x) \leq f(x)$ for every $x \in P$. Therefore, $\sigma_{p_o}(\mathcal{S}^*) \leq \sigma_{p_o}(\mathcal{S})$. □

Proposition 7.4. *For every rational access function* Φ, $\lambda(\Phi) = \lambda(\Phi^*)$.

Sketch of the proof. Let $\Sigma = (S_i)_{i \in Q}$ be a $\mathbb{K}$-linear secret sharing scheme with access function Φ. One can construct a $\mathbb{K}$-linear code C from Σ. The generator matrix of this code is obtained by concatenating the matrices of the linear maps S_i, and every codeword is a concatenation of vectors that correspond to the secret value and to the shares. Similarly to the perfect case, one can prove that the dual code $C^\perp$ defines a $\mathbb{K}$-linear secret sharing scheme Σ^* with access function Φ^* and with the same information ratio as Σ. □

8 Concatenating Secret Sharing Schemes

We analyze here a simple way to combine secret sharing schemes. For each $j = 1, \ldots, m$ consider a positive integer q_j and a secret sharing scheme $\Sigma_j = (S_{ji})_{i \in Q}$ 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 $S_i = (S_{1i})^{q_1} \times \cdots \times (S_{mi})^{q_m}$ for every $i \in Q$. Observe that $H(S_X) = \sum_{j=1}^m q_j H(S_{jX})$ for every $X \subseteq Q$. Because of that, the access function Φ of Σ is given by

$$\Phi(X) = \frac{I(S_{p_o}:S_X)}{H(S_{p_o})} = \frac{\sum_{j=1}^m q_j I(S_{jp_o}:S_{jX})}{\sum_{j=1}^m q_j H(S_{jp_o})}$$

for every $X \subseteq Q$. Therefore,

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

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

$$\rho_j = \frac{q_j H(S_{jp_o})}{\sum_{k=1}^m q_k H(S_{kp_o})}.$$

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,

$$\sigma = \max_{i \in P} \frac{\sum_{j=1}^m q_j H(S_{ji})}{\sum_{j=1}^m q_j H(S_{jp_o})} \leq \frac{\sum_{j=1}^m q_j \sigma_j H(S_{jp_o})}{\sum_{j=1}^m q_j H(S_{jp_o})} = \sum_{j=1}^m \rho_j \sigma_j. \tag{2}$$

If there is a participant in P that holds the largest share in all schemes Σ_j, then the inequality in (2) holds with equality. Clearly, if Σ_j is a $(\mathbb{K}, \ell_j)$-linear secret sharing scheme for $j = 1, \ldots, m$, then Σ 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 8.1. *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 M be a positive integer such that $M\rho_j$ 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 $\ell = M\ell_1 \cdots \ell_m$.*

Proof. For $j = 1, \ldots, m$, take $q_j = LM\rho_j/\ell_j$, 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. □

9 Uniform Secret Sharing Schemes

Uniform access functions generalize the perfect threshold access structure. It is well known that these access structures admit a linear secret sharing scheme with optimal information ratio, namely Shamir's secret sharing scheme [45]. We extend here this fundamental result by determining the optimal information ratio of all uniform access functions and presenting

a construction of linear secret sharing schemes with optimal information ratio for all rational uniform access functions.

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 9.1. *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 participants. 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 9.2. *Let Φ be a rational uniform access function on a set P of n participants 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 3.14 and Propositions 8.1 and 9.1. □

Remark 9.3. By Remark 3.15, 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.

In the rest of this section we present a construction of optimal linear secret sharing schemes for all rational uniform access functions. Nevertheless, the schemes that are obtained in this way are not efficient in general because the size of the secret value is too large.

Clearly, $\delta_i^\tau(\Phi) = \Phi'_i - \Phi'_{i+1}$ for $i = 1, \ldots, n$ and for every ordering τ of P. Because of that, we notate $\delta_i(\Phi) = \Phi'_i - \Phi'_{i+1}$. In particular, the value of $\epsilon(\Phi)$ is determined by the increment vector.

Lemma 9.4. *Let Φ be a uniform access function on a set P of size n. Then*

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

Example 9.5. Let Φ be the (t, r, n)-ramp access function, which is uniform and has gap $g = r - t$. 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 $\Phi'_i = 1/g$ if $t+1 \leq i \leq r$. Therefore, $\delta_t(\Phi) = -1/g$ and $\delta_r(\Phi) = 1/g$, and $\delta_i(\Phi) = 0$ if $i \neq r, t$, and hence $\epsilon(\Phi) = 1/g$.

We proved in Proposition 9.1 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 9.6. *Let Φ be a uniform access function on a set P. Then there exist ramp access functions $\Phi^1, \ldots, \Phi^m$ on P and positive real numbers $\rho_1, \ldots, \rho_m$ 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 $\rho_1, \ldots, \rho_m$ 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 $n = |P|$ and let t and r be, respectively, the privacy and the reconstruction thresholds of Φ. 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 $\Phi'_\ell = \min\{\Phi'_{t+1}, \ldots, \Phi'_r\}$. 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 $i = 0, 1, \ldots, n$. 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 $i \geq \ell - 1$, and hence $\delta_i(\Psi^1) = 0$ if $i \geq \ell$. In addition, $\Psi^2_i = 0$ if $i \leq \ell$, and hence $\delta_\ell(\Psi^2) \leq 0$ and $\delta_i(\Psi^2) = 0$ if $i \leq \ell - 1$. Therefore,

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

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 $i = 1, \ldots, n$, 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 $i \neq r, t$. Then the three values $\delta_t(\Phi)$, $\delta_t(\Psi^1)$ and $\delta_t(\Psi^2)$ are non-positive, while $\delta_r(\Phi)$, $\delta_r(\Psi^1)$ and $\delta_r(\Psi^2)$ are non-negative. 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 $t + 1 < \ell < r$. □

Corollary 9.7. *For every uniform access function Φ, $\kappa(\Phi) = \epsilon(\Phi)$.*

Proof. By Proposition 9.6, $\Phi = \sum_{j=1}^{m} \rho_j \Phi^j$ and $\epsilon(\Phi) = \sum_{j=1}^{m} \rho_j \epsilon(\Phi^j)$ for some positive real numbers $\rho_1, \ldots, \rho_m$ with $\sum_{j=1}^{m} \rho_i = 1$ and some ramp access functions $\Phi^1, \ldots, \Phi^m$. By Remark 3.14, for every $j = 1, \ldots, m$, there exist a normalized Φ^j-polymatroid $\mathcal{S}_j = (Q, f_j)$ with $\sigma_{p_o}(\mathcal{S}_j) = 1/g(\Phi^j) = \epsilon(\Phi^j)$. The proof is concluded by taking into account that $\mathcal{S} = (Q, \sum_{j=1}^{m} \rho_j f_j)$ is a normalized Φ-polymatroid with $\sigma_{p_o}(\mathcal{S}) \leq \sum_{j=1}^{m} \rho_j \sigma_{p_o}(\mathcal{S}_j) = \sum_{j=1}^{m} \rho_j \epsilon(\Phi^j) = \epsilon(\Phi)$. □

Theorem 9.8. *Let Φ be a rational uniform access function on a set of participants 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 9.6 with Remark 3.14 and Proposition 8.1. □

Corollary 9.9. *For every rational uniform access function Φ, $\epsilon(\Phi) = \kappa(\Phi) = \sigma(\Phi) = \lambda(\Phi)$.*

The fact that $\kappa(\Phi) = \sigma(\Phi) = \lambda(\Phi)$ for a rational uniform access function Φ, proved in Corollary 9.9, 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 9.8 and the consequent corollaries deal with rational access functions. For some non-rational access functions, we can also apply the techniques used in the proof of Theorem 9.8 and construct optimal schemes (see Example 9.10). Nevertheless, in general we do not have a method to construct an optimal scheme for every non-rational access function. For every non-rational access function Φ on a set P, there is a sequence of rational access functions $(F_i)_{i \in \mathbb{N}}$ satisfying that $\lim_{i \to \infty} \sum_{A \subseteq P} |\Phi(A) - \Phi_i(A)| \to 0$. Since $\lim_{i \to \infty} \epsilon(F_i) \to \epsilon(F)$ and $\epsilon(F_i) = \sigma(F_i)$, there is a sequence of linear secret sharing schemes $(\Sigma_i)_{i \in \mathbb{N}}$ satisfying $\Phi(\Sigma_i) \to \Phi$ and $\sigma(\Sigma_i) \to \epsilon(F)$.

Example 9.10. Let Φ be a uniform access function on a set P of size 3 with $r_0 = r_1 = 0$, $r_2 = \log 5/(2 \log 5 + \log 7)$, and $r_3 = 1$. Observe that $\epsilon(\Phi) = 1 - r_2$. Let Σ_1 be a $(1, 3)$-ramp secret sharing scheme over $\mathbb{F}_5$, and let Σ_2 be a 3-threshold secret sharing scheme over $\mathbb{F}_7$. The access function of the concatenation of Σ_1 and Σ_2 is Φ, and its information ratio is $(\log 5 + \log 7)/(2 \log 5 + \log 7) = 1 - r_2$. Hence it is an optimal scheme for Φ.

Corollary 9.11. *For every uniform access function Φ there exist*

1. *a sequence of secret sharing schemes (Σ_i) realizing Φ whose information ratio $\sigma(\Sigma_i)$ converges to $\epsilon(\Phi)$ as $i \to \infty$; and*

2. *a sequence of linear secret sharing schemes (Σ'_i) realizing Φ_i whose information ratio $\sigma(\Sigma'_i)$ converges to $\epsilon(\Phi)$ as $i \to \infty$ and such that $\lim_{i \to \infty} \sum_{A \subseteq P} |\Phi(A) - \Phi_i(A)| \to 0$.*

Theorem 9.12. *The optimal information ratio of every uniform access function Φ is equal to $\epsilon(\Phi)$.*

10 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. Our main result is the determination of the optimal information ratio of the uniform access functions.

Determining the optimal information ratio for general access functions is 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 6.4, 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, 36].

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, 23]. The optimal information ratio is determined here 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.

Superpolynomial lower bounds on the information ratio have been found for perfect linear secret sharing schemes [2]. Extending this result to non-perfect secret sharing schemes is an interesting problem.

We proved that every rational uniform access function admits a linear secret sharing schemes with optimal information ratio. Nevertheless, this schemes may not be efficient because the length of the secret value is too large. An interesting open problem is to find bounds on the length of the shares for linear secret sharing schemes by extending the results in [13] on perfect secret sharing schemes.

In several scenarios, the access function provide too many details about the structure of the scheme. For instance, only the access structure may be required to be satisfied or, more generally, the requirements may be given by lower and upper bounds on the access function. We think that the ideas and techniques in this paper can be also useful in those relaxed frameworks too.

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

[24] O. Farràs, C. Padró. Extending Brickell–Davenport theorem to non-perfect secret sharing schemes. *Des. Codes Cryptogr.*, Online First (2013).

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

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

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

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

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

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

[31] 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.

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

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

[34] 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.

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

[36] 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.

[37] 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).

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

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

[40] 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.

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

[42] 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.

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

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

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