A Note on Non-Perfect Secret Sharing *

Oriol Farràs[1], Sebastià Martín[2], and Carles Padró[2]

[1]Universitat Rovira i Virgili, Tarragona, Spain
[2]Universitat Politècnica de Catalunya, Barcelona, Spain

April 1, 2016

Abstract

By using a recently introduced framework for non-perfect secret sharing, several known results on perfect secret sharing are generalized. Specifically, we discuss about ideal secret sharing schemes, constructions of efficient linear secret sharing schemes, and the search for lower bounds on the length of the shares. Similarly to perfect secret sharing, matroids and polymatroids are very useful to analyze these questions.

Key words. Secret sharing, Non-perfect secret sharing, Ideal secret sharing schemes, Matroid ports

1 Introduction

By formalizing several ideas in previous works on non-perfect secret sharing [17, 20, 21, 23, 27, 28], a new framework was introduced in [9, 10] (the latter is the full version of the former). It is based on the concept of *access function* (Definitions 2.2 and 2.4), which measures the amount of information on the secret value that is obtained from the shares of any set of players. Several known results on perfect secret sharing were generalized in [9, 10]. Namely, the existence of a secret sharing scheme for every access function, lower bounds on the information ratio derived from polymatroids, duality in linear secret sharing schemes, and a new proof for the values of the optimal information ratio of uniform access functions, which had been determined in [27, 28]. Moreover, that new framework made it possible to overcome some concerns, which were discussed in [13], on the existing definitions for *ideal non-perfect secret sharing scheme* and to choose the most satisfactory definition for that concept [10, Section 8]. Several results on ideal perfect secret sharing schemes and their connections to matroids were extended to non-perfect secret sharing in [17, 23] and recently in [10, 13].

As in recent preceding papers [9, 10, 13, 27, 28], we consider here several topics that have attracted a lot of attention for perfect secret sharing and we present new extensions of known results to the non-perfect case. Namely, we deal with ideal secret sharing schemes, constructions of efficient linear secret sharing schemes, and the search for lower bounds on the optimal information ratio. Our results are obtained by using access functions with *constant increment* (Definition 2.9), a class that contains the access functions of ideal secret sharing schemes. More

*Oriol Farràs is supported by the Spanish Government through a Juan de la Cierva grant and TIN2014-57364-C2-1-R, by the European Union through H2020-ICT-2014-1-644024, and by the Government of Catalonia through Grant 2014 SGR 537. email: oriol.farras@urv.cat. Sebastià Martín and Carles Padró are supported by the Spanish government under the project MTM2013-41426-R. email: sebastia.martin@upc.edu, cpadro@ma4.upc.edu.

specifically, they are based on the two basic transformations of access functions that are presented in Section 3.

2 Preliminaries

We present in this section the main definitions and basic facts about secret sharing, polymatroids, and the connections between these topics.

We begin by introducing some notation. 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 $X \smallsetminus \{x\}$. For a set E, we notate $\mathcal{P}(E)$ for the power set of E, that is, the set of all subsets of E. Only discrete random variables are considered in this paper. Given a discrete random vector $S = (S_x)_{x \in E}$ and a set $X \subseteq E$, we notate $S_X = (S_x)_{x \in X}$. The Shannon entropy of the random variable S_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* $I(S_X{:}S_Y|S_Z) = H(S_X|S_Z) - H(S_X|S_{YZ})$. Throughout the paper, P and Q stand for finite sets with $Q = Pp_o$ for some $p_o \notin P$. In addition, for every positive integer k, we use P_o^k to denote a set with $|P_o^k| = k$ such that $p_o \in P_o^k$ and $P \cap P_o^k = \emptyset$. Finally, we put $Q_k = PP_o^k$ and $P_k = Q_k \smallsetminus p_o$.

2.1 Secret Sharing Schemes

Definition 2.1 (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 *qualified* sets of the access structure Γ. In a *perfect* access structure, every subset of P is either forbidden or qualified.

Definition 2.2 (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 $\Phi(P) = 1$. The forbidden and qualified sets of the *access structure associated to* Φ are those with $\Phi(X) = 0$ and, respectively, $\Phi(X) = 1$. 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 2.3 (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 of players* P is a discrete random vector $(S_x)_{x \in Q}$ 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 value*, while the random variables $(S_x)_{x \in P}$ correspond to the *shares* of the secret that are distributed among the players in P. Most of the times, we are going to write S_o instead of S_{p_o}.

Definition 2.4. The *access function* Φ of a secret sharing scheme $\Sigma = (S_i)_{i \in Q}$ on P is defined by

$$\Phi(X) = \frac{I(S_o{:}S_X)}{H(S_o)}$$

for every $X \subseteq P$, while its *access structure* is the one associated to its access function. A secret sharing scheme is *perfect* if its access function is so.

The access function of a secret sharing scheme measures the amount of information on the secret value that is derived from any set of shares. In particular, if $X \subseteq P$ is qualified, then

$I(S_o{:}S_X) = H(S_o)$, which implies that the secret value is determined by the shares of the players in X. The random variables S_o and S_X are independent if X is a forbidden set, that is, the shares of the players in X do not provide any information on the secret. From now on, we consider only access functions without any *redundant* player. That is, we assume that, for every $y \in P$, there exists $X \subseteq P$ such that $\Phi(Xy) > \Phi(X)$.

Definition 2.5 (Information ratio)**.** The *information ratio* of a secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ is defined as $\max_{x\in P} H(S_x)/H(S_o)$. It approximates the ratio between the maximum length of the shares and the length of the secret.

There exists a secret sharing scheme for every access function [9, 10]. Nevertheless, all known general constructions are inefficient because the length of the shares is exponential in the number of players. This is also the situation for perfect secret sharing schemes. Therefore, the search for families of access functions that admit efficient secret sharing schemes is worth considering. Most of the known efficient constructions involve *linear* secret sharing schemes. In addition, the homomorphic properties of linear schemes make them suitable for the main applications of secret sharing.

Definition 2.6 (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 $(S_x)_{x\in Q}$ are given by surjective $\mathbb{K}$-linear maps $S_x : V \to V_x$, where the uniform probability distribution is taken on V and the dimension of $V_{p_o} = V_o$ over the field $\mathbb{K}$ is equal to ℓ.

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

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

Therefore, the access function of a $(\mathbb{K}, \ell)$-linear secret sharing scheme is

$$\Phi(X) = \frac{\operatorname{rank} S_o + \operatorname{rank} S_X - \operatorname{rank} S_{Xp_o}}{\operatorname{rank} S_o} = 1 - \frac{\operatorname{rank} S_{Xp_o} - \operatorname{rank} S_X}{\ell}$$

and its information ratio is

$$\frac{\max_{x\in P} \operatorname{rank} S_x}{\operatorname{rank} S_o} = \frac{\max_{x\in P} \dim V_x}{\ell}.$$

Observe that all values of the access function are integer multiples of $1/\ell$. In particular, it is a rational access function. Every rational access function admits a linear secret sharing scheme [9, 10].

Definition 2.7 (Optimal information ratio)**.** The *optimal information ratio* $\sigma(\Phi)$ of an access function Φ is the infimum of the information ratios of the secret sharing schemes for Φ. We notate $\lambda(\Phi)$ for the infimum of the information ratios of the *linear* secret sharing schemes for Φ. Obviously, $\sigma(\Phi) \le \lambda(\Phi)$.

The optimal information ratio of the uniform access functions, which are the natural generalization of threshold perfect access structures, was determined in [27, 28] and a new proof for that result was given in [9, 10].

Remark 2.8. A $(\mathbb{K}, \ell)$-linear secret sharing scheme with information ratio σ is determined by linear maps $S_x : V \to V_x$ with $\dim V_x \leq \max\{\ell, \sigma\ell\}$ for every $x \in Q$ and $\dim V \leq \sum_{x\in Q} \dim V_x$. Therefore, the overall complexity of the scheme, which comprises the required amount of randomness and the computation time and space 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.

As a consequence of the previous discussion, the denominators of the values of rational access functions are relevant in the search for families of efficient linear secret sharing schemes. Restricting the search to access functions with constant increment is a way to avoid this problem. In addition, it is enough to consider access functions of this kind to prove our extension results.

Definition 2.9 (Constant increment)**.** An access function Φ has *constant increment* μ if $\Phi(Xy) - \Phi(X) \in \{0, \mu\}$ for every $X \subseteq P$ and $y \in P$. In this situation, $\mu = 1/k$ for some positive integer k and the values of Φ are integer multiples of $1/k$.

Let Φ be an access function with constant increment $1/k$. By a well known result in non-perfect secret sharing [20, 21, 23], $H(S_x) \geq H(S_o)/k$ for very $x \in P$ if $(S_x)_{x\in Q}$ is a secret sharing scheme for Φ. Therefore, $\sigma(\Phi) \geq 1/k$. A secret sharing scheme is *ideal* if its access function has constant increment and this lower bound is attained.

Definition 2.10 (Ideal secret sharing scheme)**.** A secret sharing scheme $\Sigma = (S_x)_{x\in Q}$ is *ideal* if its access function has constant increment $1/k$ and $H(S_x) = H(S_o)/k$ for every $x \in P$.

Example 2.11 (Ramp access functions)**.** 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 $|X| \geq r$. Clearly, this access function has constant increment $1/(r - t)$. By the construction presented by Blakley and Meadows [5], which is described in [10, Example 2.9], there is an ideal $(\mathbb{K}, r - t)$-linear secret sharing scheme for the (t, r, n)-ramp access function for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n + r - t$.

2.2 Polymatroids, Matroids, and Matroid Ports

The joint Shannon entropies of a collection of random variables define a polymatroid [15, 16]. Because of that, these combinatorial objects play a fundamental role in secret sharing.

Definition 2.12. A *polymatroid* is a pair $\mathcal{S} = (E, f)$ formed by a finite set E, the *ground set*, and a monotone increasing and submodular *rank function* $f\colon \mathcal{P}(E) \to \mathbb{R}$ with $f(\emptyset) = 0$. If f is integer-valued and $f(X) \leq |X|$ for every $X \subseteq E$, then $\mathcal{S}$ is called a *matroid*.

For a function $F : \mathcal{P}(E) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq E$, we notate

$$\Delta_F(Y\colon Z|X) = F(XY) + F(XZ) - F(XYZ) - F(X) \tag{1}$$

and $\Delta_F(Y\colon Z) = \Delta_F(Y\colon Z|\emptyset)$.

If $(S_x)_{x\in E}$ is a random vector, then the map $h\colon \mathcal{P}(E) \to \mathbb{R}$ defined by $h(X) = H(S_X)$ is the rank function of a polymatroid with ground set E [15, 16]. This connection between polymatroids and the Shannon entropy is a consequence of the conditional mutual information being nonnegative. The notation introduced in (1) is motivated by this connection. Indeed, for every $X, Y, Z \subseteq E$, the conditional mutual information $I(S_Y\colon S_Z|S_X)$ is equal to $\Delta_h(Y\colon Z|X)$.

Since secret sharing schemes are given by random vectors, a connection between secret sharing and polymatroids arises naturally. Specifically, associated to every secret sharing scheme

$\Sigma = (S_x)_{x\in Q}$ there is the polymatroid (Q, h) given by $h(X) = H(S_X)$ for every $X \subseteq Q$. The access function Φ and the information ratio σ of Σ are determined by this polymatroid. Indeed, $\Phi(X) = \Delta_h(p_o{:}X)/h(p_o)$ for every $X \subseteq P$ and $\sigma = \max_{x\in P} h(x)/h(p_o)$. This motivates the following definition.

Definition 2.13. For an access function Φ on P, every polymatroid (Q, f) such that $\Phi(X) = \Delta_f(p_o{:}X)/f(p_o)$ for every $X \subseteq P$ is called a Φ-*polymatroid*.

For an access function Φ, the value $\kappa(\Phi)$ is defined as the infimum, over all Φ-polymatroids (Q, f), of $\max_{x\in P} f(x)/f(p_o)$. Clearly, $\kappa(\Phi) \leq \sigma(\Phi)$. The reader is referred to [10] for additional results on this lower bound on the optimal information ratio. Similarly to the perfect case, $\kappa(\Phi)$ is the optimal value of a linear programming problem [19, 22], and hence the infimum is a minimum and $\kappa(\Phi)$ is a rational number if Φ is a rational access function. If Φ is an access function with constant increment $1/k$, then $\kappa(\Phi) \geq 1/k$ [10].

Remark 2.14. We discuss here some well known facts about linear representations of polymatroids and their associated linear random vectors. The reader is referred to [19] for a more detailed explanation. An integer-valued polymatroid (E, f) is said to be $\mathbb{K}$-*linearly representable* or simply $\mathbb{K}$-*linear* if there exists a vector space W over the field $\mathbb{K}$ and a collection $(W_x)_{x\in E}$ of vector subspaces of E such that $f(X) = \dim\left(\sum_{x\in X} W_x\right)$ for every $X \subseteq E$. In this situation, the collection $(W_x)_{x\in E}$ is called a $\mathbb{K}$-*linear representation* of the polymatroid (E, f). Every $(\mathbb{K}, \ell)$-linear secret sharing scheme $(S_x)_{x\in Q}$ with access function Φ determines a $\mathbb{K}$-linear representation of the Φ-polymatroid (Q, f) defined by $f(X) = \operatorname{rank}(S_X)$. Conversely, every $\mathbb{K}$-linear representation of an integer-valued Φ-polymatroid (Q, f) determines a $(\mathbb{K}, f(p_o))$-linear secret sharing scheme with access function Φ and information ratio $\max_{x\in P} f(x)/f(p_o)$.

Definition 2.15. Let $\mathcal{M} = (Q, f)$ be a matroid. The perfect access function Φ on P defined by $\Phi(X) = \Delta_f(p_o{:}X)$ for every $X \subseteq P$ is called the *port of the matroid* $\mathcal{M}$ *at* p_o.

Observe that $\mathcal{M} = (Q, f)$ is a Φ-polymatroid if Φ is the port of the matroid $\mathcal{M}$ at p_o. By Brickell-Davenport theorem [7], the access function of every ideal perfect secret sharing scheme is a matroid port. A generalization of matroid ports was introduced in [13] to extend that result to non-perfect secret sharing. We use here the notation introduced at the beginning of Section 2.

Definition 2.16. A polymatroid (Q_k, f) is called P_o^k-*normalized* if $f(P_o^k) = k$ and

$$f(XZ) = \min\{f(XP_o^k), f(X) + |Z|\}$$

for every $X \subseteq P$ and $Z \subseteq P_o^k$.

Definition 2.17 (Generalized matroid port)**.** Let $\mathcal{N} = (Q_k, f)$ be a P_o^k-normalized matroid. Then the access function Φ on P defined by

$$\Phi(X) = \frac{\Delta_f(P_o^k{:}X)}{k}$$

for every $X \subseteq P$ is the k-*port of* $\mathcal{N}$ *at* P_o^k. In this situation, we say that Φ is a *matroid* k-*port* or a *generalized matroid port*.

Definition 2.18 (Connected access function)**.** An access function Φ on P is *connected* if, for every player $z \in P$, there exist a forbidden set $X \subseteq P$ and a qualified set $Y \subseteq P$ with $z \in Y$ such that $\Phi(Xz) > 0$ and $\Phi(Y \smallsetminus z) < 1$.

Observe that matroid k-ports are access functions with constant increment $1/k$. As a consequence of [13, Theorem 3], the access function of every ideal secret sharing scheme is a generalized matroid port. In addition, every connected matroid k-port is the k-port of a unique P_o^k-normalized matroid. Moreover, as a consequence of [13, Proposition 7], a connected access function Φ with constant increment $1/k$ is a matroid k-port if and only if $\kappa(\Phi) = 1/k$.

3 Two Basic Transformations

We discuss in the following two transformations of access functions that will be used to generalize several results from perfect to non-perfect secret sharing. The first one produces a perfect access function associated to a given access function with constant increment, and the second one works in the opposite direction.

Definition 3.1. For an access function Φ on P with constant increment $1/k$, a set $X \subseteq P_k$ is qualified for the associated perfect access function $\widehat{\Phi}$ on P_k if and only if $k\,\Phi(X \cap P) + |X \smallsetminus P| \geq k$.

Definition 3.2. For a perfect access function Φ on P and a positive integer k, we define the access function $\widetilde{\Phi}^k$ on P_k by $\widetilde{\Phi}^k(XZ) = (\Phi(X) + |Z|)/k$ for every $X \subseteq P$ and $Z \subseteq P_k \smallsetminus P$. Clearly, the access function $\widetilde{\Phi}^k$ has constant increment $1/k$.

Proposition 3.3. *Let Φ be an access function on P with constant increment $1/k$ and $\widehat{\Phi}$ the associated perfect access function on P_k. Then $\kappa(\widehat{\Phi}) \leq k\kappa(\Phi)$ and $\lambda(\widehat{\Phi}) \leq k\lambda(\Phi)$*

Proof. For a Φ-polymatroid $\mathcal{S} = (Q, f)$ with $f(p_o) = k$, consider the only P_o^k-normalized polymatroid $\widehat{\mathcal{S}} = (Q_k, g)$ with $g(X) = f(X)$ and $g(XP_o^k) = f(Xp_o)$ for every $X \subseteq P$.

We affirm that $\widehat{\mathcal{S}}$ is a $\widehat{\Phi}$-polymatroid. Indeed, take $X \subseteq P$ and $Z \subseteq P_k \smallsetminus P$. Then $\widehat{\Phi}(XZ) = 1$ if and only if $k - |Z| \leq k\Phi(X) = k + f(X) - f(Xp_o)$, which is equivalent to $|Z| \geq f(Xp_o) - f(X) = g(XP_o^k) - g(X)$, and hence equivalent to $\Delta_g(p_o{:}XZ) = 1 + g(XZ) - g(XZp_o) = 1$. This proves our affirmation, which clearly implies that $\kappa(\widehat{\Phi}) \leq k\kappa(\Phi)$.

For a positive integer α, consider the polymatroids $(Q, \alpha f)$ and $(Q_k, \alpha g)$. As a consequence of the results in [11], if $(Q, \alpha f)$ is $\mathbb{K}$-linearly representable, then $(Q_k, \alpha g)$ is $\mathbb{L}$-linearly representable for some finite extension $\mathbb{L}$ of $\mathbb{K}$. Therefore, if there exists a $(\mathbb{K}, \alpha k)$-linear secret sharing scheme for Φ with information ratio σ, then there exists, for some finite extension $\mathbb{L}$ of $\mathbb{K}$, an $(\mathbb{L}, \alpha)$-linear secret sharing scheme for $\widehat{\Phi}$ with information ratio $k\sigma$. This proves that $\lambda(\widehat{\Phi}) \leq k\lambda(\Phi)$. □

Proposition 3.4. *Let Φ be a perfect access function on P and let $\widetilde{\Phi}^k$ be its associated access function on P_k with constant increment $1/k$. Then $\kappa(\widetilde{\Phi}^k) = \kappa(\Phi)/k$ and $\lambda(\widetilde{\Phi}^k) = \lambda(\Phi)/k$*

Proof. The result about the parameter κ was proved in [10, Lemma 5.8].

Let Σ be a $(\mathbb{K}, \ell)$-linear secret sharing scheme with information ratio σ and access function Φ. Observe that $\sigma \geq 1$ because Φ is a perfect access function. We define next a $(\mathbb{K}, k\ell)$-linear secret sharing scheme $\widetilde{\Sigma}$ on P_k. For a secret value $(s_0, s_1, \ldots, s_{k-1}) \in (\mathbb{K}^\ell)^k$, the $k-1$ players in $P_k \smallsetminus P$ receive the shares $s_1, \ldots, s_{k-1}$, while the players in P receive shares for the secret value s_0 according to the scheme Σ. Clearly, the access function of $\widetilde{\Sigma}$ is $\widetilde{\Phi}^k$ and its information ratio is equal to σ/k. Therefore, $\lambda(\widetilde{\Phi}^k) \leq \lambda(\Phi)/k$.

Consider now a $(\mathbb{K}, k\ell)$-linear secret sharing scheme $\widetilde{\Sigma}$ with access function $\widetilde{\Phi}^k$. Recall that $\widetilde{\Sigma}$ is determined by a tuple $(S_x)_{x \in Q_k}$ of $\mathbb{K}$-linear maps $S_x \colon V \to V_x$. Take $Z = P_k \smallsetminus P$ and $W = \ker S_Z$, and consider the linear secret sharing scheme $\Sigma = (S'_x)_{x \in Q}$, where $S'_x \colon W \to S_x(W)$ is the restriction of S_x to the subspace $W \subseteq V$. Observe that

$$\operatorname{rank} S'_X = \dim W - \dim \ker S'_X = \dim W - \dim(W \cap \ker S_X) = \operatorname{rank} S_{XZ} - \operatorname{rank} S_Z$$

for every $X \subseteq Q$. In particular, $\operatorname{rank} S'_o = \operatorname{rank} S_{Zp_o} - \operatorname{rank} S_Z = k\ell(1 - \widetilde{\Phi}^k(Z)) = \ell$, and hence Σ is a $(\mathbb{K}, \ell)$-linear secret sharing scheme. We affirm that Σ has access function Φ. Indeed, if Ψ is the access function of Σ, then, for every $X \subseteq P$,

$$\Psi(X) = 1 - \frac{\operatorname{rank} S'_{Xp_o} - \operatorname{rank} S'_X}{\ell} = 1 - \frac{\operatorname{rank} S_{XZp_o} - \operatorname{rank} S_{XZ}}{\ell}.$$

On the other hand,

$$\Phi(X) = k\,\widetilde{\Phi}^k(XZ) - (k-1) = k\left(1 - \frac{\operatorname{rank} S_{XZp_o} - \operatorname{rank} S_{XZ}}{k\ell}\right) - k + 1 = \Psi(X)$$

and our affirmation is proved. Finally, since $\operatorname{rank} S'_x \leq \operatorname{rank} S_x$ for every $x \in P$, the information ratio of Σ is at most k times the information ratio of $\widetilde{\Sigma}$. Therefore, $\lambda(\Phi) \leq k\lambda(\widetilde{\Phi})$. □

4 The Extensions

For an access function Φ with constant increment $1/k$ and for every $i = 1, \ldots, k$, consider the families $\mathcal{A}_i = \{A \subseteq P : \Phi(A) < i/k\}$ and $\mathcal{B}_i = \{B \subseteq P : \Phi(B) \geq i/k\}$. Clearly, for every $i = 1, \ldots, k$, the pair $(\mathcal{A}_i, \mathcal{B}_i)$ is a perfect access structure, which determines a perfect access function Φ_i. For a finite field $\mathbb{K}$ and a positive integer ℓ consider, for every $i = 1, \ldots, k$, a $(\mathbb{K}, \ell)$-linear secret sharing scheme with access function Φ_i and information ratio at most σ. The *concatenation* (as in [10, Section 7.1]) of these schemes produces a $(\mathbb{K}, k\ell)$-linear secret sharing scheme with information ratio at most σ for the access function Φ. Therefore, the search for efficient linear secret sharing schemes for access functions with constant increment can be reduced to the search for efficient *perfect* linear secret sharing schemes. Nevertheless, some access functions can be realized by linear secret sharing schemes that are more efficient than the concatenation of perfect schemes. For instance, the access functions of ideal linear secret sharing schemes.

The problem of determining which perfect access functions can be realized by an ideal secret sharing scheme has attracted a lot of attention. We argue in the following that no new difficulties appear when extending this problem to non-perfect secret sharing.

Proposition 4.1. *Let Φ be an access function with constant increment $1/k$. Then Φ is a matroid k-port if and only if $\widehat{\Phi}$ is a matroid port. Moreover, Φ admits an ideal linear secret sharing scheme if and only if $\widehat{\Phi}$ does so.*

Proof. If Φ is the k-port at P_o^k of a P_o^k-normalized matroid $\mathcal{N} = (Q_k, f)$, then $\widehat{\Phi}$ is the port of $\mathcal{N}$ at p_o. Conversely, if $\widehat{\Phi}$ is the port of a matroid $\mathcal{N} = (Q_k, f)$ at p_o, then $\mathcal{N}$ is P_o^k-normalized and Φ is the k-port of $\mathcal{N}$ at P_o^k. In that situation, these access functions admit ideal linear secret sharing schemes if and only if there is a positive integer α such that the polymatroid $(Q_k, \alpha r)$ is linearly representable over some finite field. □

Definition 4.2 (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 $\Phi(Z_2) = 0$. We define the access function $\Psi = (\Phi \setminus Z_1)/Z_2$ on $P \smallsetminus (Z_1 \cup Z_2)$ by $\Psi(X) = \Phi(XZ_2)$. Every access function that can be defined in this way is called a *minor* of Φ.

By the next proposition, Φ_i is a minor of $\widehat{\Phi}$ for every $i = 1, \ldots, k$. See [10, Section 6] for more information about minors of access functions.

Proposition 4.3. *Let Φ be an access function on P with constant increment $1/k$ and let $\widehat{\Phi}$ be its associated perfect access function on P_k. Consider a set $Z \subseteq P_k \smallsetminus P$ with $|Z| = k - i$ and take $Z' = (P_k \smallsetminus P) \smallsetminus Z$. Then $\Phi_i = (\widehat{\Phi} \setminus Z')/Z$.*

Proof. Straightforward from the definitions. □

Every minor of a matroid port is a matroid port [18, 24]. If Φ is a matroid k-port, then the access functions Φ_i for $i = 1, \ldots, k$ are matroid ports because they are minors of the matroid port $\widehat{\Phi}$. Moreover, as a consequence of the results in [13], every connected matroid k-port Φ is determined by Φ_1 and Φ_k.

As a consequence of the forbidden minor characterization of matroid ports by Seymour [24], $\kappa(\Phi) \geq 3/2$ if Φ is a perfect access function that is not a matroid port [18, Theorem 4.4]. Therefore, every perfect secret sharing scheme whose access function is not a matroid port has information ratio at least 3/2. We discuss in the following the extension of these results to non-perfect secret sharing.

Proposition 4.4. *Let Φ be a perfect access function on P and let $\mathcal{S} = (Q, f)$ be a Φ-polymatroid with $f(p_o) = 1$. If Φ is not a matroid port, then there exist $x, y \in P$ such that $f(xy) \geq 3$.*

Proof. Immediate from [18, Theorems 3.4 and 4.4]. □

Theorem 4.5. *Let Φ be an access function on P with constant increment $1/k$ that is not a matroid k-port. Then $\kappa(\Phi) \geq 3/(2k)$ and, as a consequence, the information ratio of every secret sharing scheme for Φ is at least $3/(2k)$.*

Proof. Let $\mathcal{S} = (Q, f)$ be a Φ-polymatroid with $f(p_o) = k$. Consider the associated perfect access function $\widehat{\Phi}$ on P_k and the the only P_o^k-normalized polymatroid $\widehat{\mathcal{S}} = (Q_k, g)$ with $g(XP_o^k) = f(Xp_o)$ for every $X \subseteq P$. By the proof of Proposition 3.3, $\widehat{\mathcal{S}}$ is a $\widehat{\Phi}$-polymatroid. Since $\widehat{\Phi}$ is not a matroid port by Proposition 4.4, there exist $x, y \in P_k$ such that $g(xy) \geq 3$. Then we can assume that $g(x) \geq 3/2$, and hence $x \in P$ because $g(z) = 1$ for every $z \in P_k \smallsetminus P$. Therefore, $f(x) = g(x) \geq 3/2$, which concludes the proof. □

By Theorem 4.5, there is no access function Φ with constant increment $1/k$ such that $1/k < \kappa(\Phi) < 3/(2k)$. Moreover, Φ is a matroid k-port if $\sigma(\Phi) < 3/(2k)$. If Φ is a port of the Vamos matroid, then $1 < \sigma(\Phi) \leq \lambda(\Phi) < 3/2$ [3], and hence $1/k < \sigma(\widetilde{\Phi}^k) \leq \lambda(\widetilde{\Phi}^k) < 3/(2k)$ by Proposition 3.4. Therefore, the gap in the values of κ does not apply to the optimal information ratio.

One of the main open problems in secret sharing is to prove that, for general access functions, the length of the shares must grow exponentially with the number of players [1, Conjecture 1]. This leads to the search for lower bounds on the length of the shares or, more restrictively, on the information ratio. Several super-polynomial lower bounds on the length of the shares in linear secret sharing schemes have been presented. See [1] for a survey on these topics. A recent result is the existence of a family of perfect access functions requiring linear secret sharing schemes with super-polynomial information ratio [2]. By using Proposition 3.4, this result is easily extended to access functions with fixed constant increment.

One of the available techniques to find lower bounds on the length of the shares is using linear programs with constraints derived from information inequalities. Several limitations of this method when applied to perfect secret sharing have been found [4, 8, 19]. The negative result in [8] was generalized to non-perfect secret sharing [10, Theorem 5.7], and we believe that this is also possible for the ones in [4, 19].

Another line of research on perfect secret sharing is the search for families of access functions that admit ideal perfect secret sharing schemes and have some practical interest [6, 11, 12, 14, 25, 26]. The results on ideal non-perfect secret sharing in this paper and in [10, 13] should make it possible to extend some of the results from those works to the non-perfect case.

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, 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.

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

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

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

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

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

[9] 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.

[10] O. Farràs, T. Hansen, T. Kaced, C. Padró. On the Information Ratio of Non-Perfect Uniform Secret Sharing Schemes. Manuscript. Available at *Cryptology ePrint Archive* **2014/124** (2014).

[11] O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *J. Cryptology* **25** (2012) 434–463.

[12] O. Farràs, C. Padró. Ideal Hierarchical Secret Sharing Schemes. *IEEE Transactions on Information Theory* **58** (2012) 3273–3286.

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

[14] O. Farràs, C. Padró, C. Xing, A. Yang. Natural Generalizations of Threshold Secret Sharing. *IEEE Trans. Inform. Theory* **60** (2014) 1652–1664.

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

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

[17] 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.

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

[19] S. Martín, C. Padró, A. Yang. Secret Sharing, Rank Inequalities, and Information Inequalities. *IEEE Trans. Inform. Theory* **62** (2016) 599–609.

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

[21] 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.

[22] 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.

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

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

[25] T. Tassa. Hierarchical Threshold Secret Sharing. *J. Cryptology* **20** (2007) 237–264.

[26] T. Tassa, N. Dyn. Multipartite Secret Sharing by Bivariate Interpolation. *J. Cryptology* **22** (2009) 227–258.

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

[28] 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.