A Note on Non-Perfect Secret Sharing

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

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

February 4, 2017

Abstract

By using a recently introduced framework for non-perfect secret sharing, several known results on perfect secret sharing are generalized to non-perfect secret sharing schemes with constant increment, in which the amount of information provided by adding a single share to a set is either zero or some constant value. Specifically, we discuss 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 [15, 18, 19, 21, 27, 28], a new framework was introduced in [7, 8] (the latter is the full version of the former). It is based on the concept of *access function* (Definitions 2.1 and 2.3), 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 [7, 8]. 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 [11], on the existing definitions for *ideal non-perfect secret sharing scheme* and to choose the most satisfactory definition for that concept [8, Section 8]. Several results on ideal perfect secret sharing schemes and their connections to matroids were extended to non-perfect secret sharing in [15, 21] and recently in [8, 11].

As in recent preceding papers [7, 8, 11, 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. In this paper, we focus on access functions with *constant increment* (Definition 2.5), a class that contains the access functions of ideal secret sharing

Oriol Farràs is supported by the European Union through H2020-ICT-2014-1-644024 and H2020-DS-2015-1-700540, by the Spanish Government through TIN2014-57364-C2-1-R, 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.

schemes. We show that several questions about secret sharing for access functions with constant increment can be reduced to the more studied case of perfect secret sharing schemes. The first example, discussed at the beginning of Section 3, deals with the construction of efficient linear secret sharing schemes. The other reductions are based on the basic transformations of access functions that are introduced in Definitions 3.1 and 4.3.

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. See [1] for a survey on these topics. By using the transformation introduced in Definition 3.1, we prove in Proposition 3.2 that the search of lower bounds for access functions with constant increment can be reduced to the perfect case. Recent results on perfect secret sharing provide explicit examples of families of access functions requiring linear schemes with super-polynomial information ratio [2], and of families requiring linear schemes with shares of exponential length [22]. By using Proposition 3.2, those results are easily extended to access functions with fixed constant increment.

Our main results deal with ideal secret sharing schemes and their connections with matroids. We prove in Proposition 4.7 that an access function with constant increment admits an ideal linear secret sharing scheme if and only if its transform, which is a perfect access function, does so. The access function of every ideal scheme is a generalized matroid port [8, 11]. We present in Proposition 4.9 a generalization to access functions with constant increment of [16, Theorem 4.4], which is a separation result in perfect secret sharing between matroid ports and the other perfect access functions. In particular, Proposition 4.9 provides a lower bound on the optimal information information ratio of access functions with constant increment that are not generalized matroid ports.

A 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 [5, 9, 10, 12, 25, 26]. The results on ideal non-perfect secret sharing in this paper and in [8, 11] should make it possible to extend some of the results from those works to the non-perfect case.

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 $p_o \notin P$. Most of the times, P denotes the set of *players* in a secret sharing scheme while, for convenience, p_o can be thought of as a special player, usually called *dealer*, who holds the secret value. Finally, we need some additional notation to define two useful transformations of access functions. 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 $P \cap P_o^k = \emptyset$, and we put $Q_k = PP_o^k$ and $P_k = Q_k \smallsetminus p_o$.

2.1 Secret Sharing Schemes

Definition 2.1 (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 $\Phi(P) = 1$. The *forbidden* and *qualified* sets of the access function 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 2.2 (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 2.3. 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.

Definition 2.4 (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 $\Phi(Y \smallsetminus z) < 1$.

From now on, only connected access functions are considered. In particular, we avoid in this way the existence of redundant players. Moreover, the results in this paper deal almost exclusively with access functions with constant increment.

Definition 2.5 (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 $1/k$.

There exists a secret sharing scheme for every access function [7, 8]. 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. The length of the shares and the information ratio are among the main parameters to measure the efficiency of a secret sharing scheme.

Definition 2.6 (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.

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. By an abuse of notation, when dealing with linear secret sharing schemes, the symbol S_X denotes both a linear map and a random variable that is determined by it.

Definition 2.7 (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 determined by surjective $\mathbb{K}$-linear maps $S_x : V \to V_x$ by taking the uniform probability distribution on V. In addition, 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 determined by the linear map $S_X \colon V \to \prod_{x \in X} V_x$, is uniform on its support. Because of that, $H(S_X) = \operatorname{rank} S_X \cdot \log |\mathbb{K}|$, and hence

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

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

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

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, if the access function of a $(\mathbb{K}, \ell)$-linear secret sharing scheme has constant increment $1/k$, then ℓ is a multiple of k. Every rational access function admits a linear secret sharing scheme [7, 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 $\dim V_x \le \max\{\ell, \sigma\ell\}$ for every $x \in Q$ and $\dim V \le \sum_{x \in Q} \dim V_x$. Therefore, the computational 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.

Definition 2.8 (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 [7, 8].

Let Φ be an access function with constant increment $1/k$. By a well known result in non-perfect secret sharing [18, 19, 21], $H(S_x) \ge H(S_o)/k$ for every $x \in P$ if $(S_x)_{x \in Q}$ is a secret sharing scheme for Φ. Therefore, $\sigma(\Phi) \ge 1/k$. A secret sharing scheme is *ideal* if its access function has constant increment and this lower bound is attained.

Definition 2.9 (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 2.10 (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 [4], which is described in [8, 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 [13, 14]. Because of that, these combinatorial objects play a fundamental role in secret sharing.

We introduce some notation before presenting the definition of polymatroid. For a function $F : \mathcal{P}(E) \to \mathbb{R}$ and subsets $X, Y, Z \subseteq E$, we notate

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

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

Definition 2.11. A *polymatroid* is a pair $\mathcal{S} = (E, f)$ formed by a finite set E, the *ground set*, and a *rank function* $f\colon \mathcal{P}(E) \to \mathbb{R}$ such that

1. $f(\emptyset) = 0$,
2. f is *monotone increasing*: if $X \subseteq Y \subseteq E$, then $f(X) \leq f(Y)$, and
3. f is *submodular*: $f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y)$ for every $X, Y \subseteq E$.

A *matroid* is a polymatroid such that its rank function f is integer-valued and satisfies $f(X) \leq |X|$ for every $X \subseteq E$.

Observe that $f\colon \mathcal{P}(E) \to \mathbb{R}$ is the rank function of a polymatroid if and only if $f(\emptyset) = 0$ and $\Delta_f(Y{:}Z|X) \geq 0$ for every $X, Y, Z \subseteq E$.

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 [13, 14]. 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 $I(S_Y{:}S_Z|S_X)$ is equal to $\Delta_h(Y{:}Z|X)$.

Since secret sharing schemes are given by random vectors, a connection between secret sharing and polymatroids arises 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 2.12. 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 [8] 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 [17, 20], 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 $\kappa(\Phi) \geq 1/k$ [8].

We discuss next some well known facts about linear representations of polymatroids and their associated linear random vectors. The reader is referred to [17] 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 $\max_{x \in P} f(x)/f(p_o)$.

3 On the Information Ratio

For an access function Φ with constant increment $1/k$ and for every $i = 1, \ldots, k$, consider the perfect access function Φ_i whose qualified sets are those with $\Phi(B) \geq i/k$. 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 [8, 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 have lower information ratio than the concatenation of perfect schemes. For instance, the access functions of ideal linear secret sharing schemes.

We introduce next a transformation from perfect access functions to access functions with any given constant increment. It makes it possible to reduce the search of lower bounds for non-perfect secret sharing with constant increment to the more studied case of perfect secret sharing.

Definition 3.1. 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 3.2. *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 [8, 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 On Ideal 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 this section that no new difficulties appear when extending this problem to non-perfect secret sharing.

We begin recalling the known results about the connections between ideal secret sharing schemes and matroids. Then we present in Definition 4.3 an operation that transforms any given access function Φ with constant increment k into an associated perfect access function $\widehat{\Phi}$. We prove in Proposition 4.7 that Φ admits an ideal secret sharing scheme if and only if so does $\widehat{\Phi}$. Finally, in Proposition 4.9, we generalize to non-perfect secret sharing the separation result from [16] between matroid ports and the other perfect access functions.

Definition 4.1. 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 [6], the access function of every ideal perfect secret sharing scheme is a matroid port. A generalization of matroid ports was introduced in [11] to extend that result to non-perfect secret sharing.

Definition 4.2 (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.*

Observe that matroid k-ports are access functions with constant increment $1/k$. As a consequence of [11, 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 [11, Proposition 7], a connected access function Φ with constant increment $1/k$ is a matroid k-port if and only if $\kappa(\Phi) = 1/k$.

Definition 4.3. For an access function Φ on P with constant increment $1/k$, we define the perfect access function $\widehat{\Phi}$ on P_k as the one in which a set $X \subseteq P_k$ is qualified if and only if $k\,\Phi(X \cap P) + |X \smallsetminus P| \geq k$.

Definition 4.4. 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 $Z \subseteq P_o^k$.

Lemma 4.5. *Let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(p_o) = k$. Then there exists a unique 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 $X \subseteq P$.*

Proof. The only possibility for g is $g(XZ) = \min\{f(Xp_o), f(X) + |Z|\}$ for every $X \subseteq P$ and $Z \subseteq P_o^k$. One can prove that this is the rank function of a polymatroid. □

Proposition 4.6. *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 $\kappa(\widehat{\Phi}) \le k\kappa(\Phi)$ and $\lambda(\widehat{\Phi}) \le k\lambda(\Phi)$*

Proof. Let $\mathcal{S} = (Q, f)$ be a Φ-polymatroid with $f(p_o) = k$. By Lemma 4.5, there exists a unique 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 $k - |Z| \le k\Phi(X) = k + f(X) - f(Xp_o)$, which is equivalent to $|Z| \ge f(Xp_o) - f(X) = g(XP_o^k) - g(X)$, and hence equivalent to $g(XZ) = g(XP_o^k)$. Finally, this is equivalent to $\Delta_g(p_o{:}XZ) = 1 + g(XZ) - g(XZp_o) = 1$. This proves our affirmation, which clearly implies that $\kappa(\widehat{\Phi}) \le k\kappa(\Phi)$.

For a positive integer α, consider the polymatroids $(Q, \alpha f)$ and $(Q_k, \alpha g)$. As a consequence of the results in [9], 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 $\lambda(\widehat{\Phi}) \le k\lambda(\Phi)$. □

Proposition 4.7. *Let Φ be a connected access function with constant increment $1/k$. Then Φ is a matroid k-port if and only if its associated perfect access function $\widehat{\Phi}$ is a matroid port. Moreover, Φ admits an ideal linear secret sharing scheme if and only if $\widehat{\Phi}$ admits an ideal linear secret sharing scheme.*

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. □

As a consequence of the forbidden minor characterization of matroid ports by Seymour [23], $\kappa(\Phi) \ge 3/2$ if Φ is a perfect access function that is not a matroid port [16, 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.

Lemma 4.8. *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 $f(xy) \ge 3$.*

Proof. Immediate from [16, Theorems 3.4 and 4.4]. □

Proposition 4.9. *For a connected access function Φ on P with constant increment $1/k$, the following statements are equivalent.*

1. *Φ is a matroid k-port.*
2. *$\kappa(\Phi) = 1/k$.*
3. *$\kappa(\Phi) < 3/(2k)$.*

In particular, there is no such access function Φ with $1/k < \kappa(\Phi) < 3/(2k)$. This gap in the values of κ does not apply to the optimal information ratio, that is, there exists an access function Φ with constant increment k such that $1 < \sigma(\Phi) \leq \lambda(\Phi) < 2/3$.

Proof. The first two statements are equivalent by [11, Proposition 7]. We prove next that $\kappa(\Phi) \geq 3/(2k)$ if Φ is not a matroid k-port. 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 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 4.6, $\widehat{\mathcal{S}}$ is a $\widehat{\Phi}$-polymatroid. By Proposition 4.7, $\widehat{\Phi}$ is not a matroid port, and hence, by Lemma 4.8, 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, $f(x) = g(x) \geq 3/2$.

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 3.2. □

As a consequence of Proposition 4.9, the optimal information ratio of every connected access function Φ with constant increment $1/k$ that is not a matroid k-port is at least $3/(2k)$. This bound is tight. Indeed, there exist perfect access functions Φ that are not matroid ports and satisfy $\kappa(\Phi) = \sigma(\Phi) = \lambda(\Phi) = 3/2$ [24, Table 1]. By Proposition 3.2, the associated access functions $\widetilde{\Phi}^k$ satisfy $\kappa(\widetilde{\Phi}^k) = \sigma(\widetilde{\Phi}^k) = \lambda(\widetilde{\Phi}^k) = 3/(2k)$. Observe that $\widetilde{\Phi}^k$ are not matroid k-ports because $\kappa(\widetilde{\Phi}^k) \neq 1/k$.

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

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

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

[7] 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.

[8] O. Farràs, T. Hansen, T. Kaced, C. Padró. On the Information Ratio of Non-Perfect Secret Sharing Schemes. *Algorithmica* (2016). doi:10.1007/s00453-016-0217-9

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

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

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

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

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

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

[15] 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.

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

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

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

[19] 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.

[20] 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.

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

[22] T. Pitassi, R. Robere. Strongly Exponential Lower Bounds for Monotone Computation. *Electronic Colloquium on Computational Complexity* **23** Report No. 188 (2016).

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

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

[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.