Extending Brickell-Davenport Theorem to Non-Perfect Secret Sharing Schemes

Oriol Farràs[1] and Carles Padró[2]

[1]Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
[2]Nanyang Technological University, Singapore

December 18, 2012

Abstract

One important result in secret sharing is the Brickell-Davenport Theorem: every ideal perfect secret sharing scheme defines a matroid that is uniquely determined by the access structure. Even though a few attempts have been made, there is no satisfactory definition of ideal secret sharing scheme for the general case, in which non-perfect schemes are considered as well. Without providing another unsatisfactory definition of ideal non-perfect secret sharing scheme, we present a generalization of the Brickell-Davenport Theorem to the general case. After analyzing that result under a new point of view and identifying its combinatorial nature, we present a characterization of the (not necessarily perfect) secret sharing schemes that are associated to matroids. Some optimality properties of such schemes are discussed.

Key words. Secret sharing, Non-perfect secret sharing scheme, Matroid, Polymatroid.

1 Introduction

This work deals with the connection between secret sharing and matroid theory. Most of the concepts appearing in this Introduction will be defined later in the paper. The reader is referred to [1] for a survey on secret sharing, to [25, 27, 33] for textbooks containing material about matroids and polymatroids, to [8] for a textbook on information theory, and to [19] for a more detailed description of the connections of secret sharing with matroid theory.

In a perfect secret sharing scheme, the shares of the participants in an unqualified set do not provide any information about the secret value. Because of that, the length of every share is at least the length of the secret [15]. This leads naturally to distinguish the perfect secret sharing schemes in which every share has the same length as the secret, which are called ideal. The best known example of such schemes is Shamir's [30] threshold secret sharing scheme.

Brickell [6] showed how to construct ideal perfect secret sharing schemes for some non-threshold access structures. This construction was described by Massey [21] in terms of linear codes. Namely, given a linear code, every random choice of a codeword provides a distribution of shares. One of the entries corresponds to the secret value while the other ones provide the shares of the participants. In particular, Shamir's [30] threshold scheme can be described in this way. The columns of a generator matrix of a code define a linear (or representable) matroid. As a consequence, the access structures of the ideal perfect secret sharing schemes constructed according to Brickell's method [6] coincide with the ports of linear matroids.

The Brickell-Davenport Theorem [7] generalizes this result. Namely, it states that every ideal perfect secret sharing scheme defines a matroid, which is uniquely determined by the

access structure. That is, different ideal perfect secret sharing schemes with the same access structure define the same matroid. Moreover, the access structure is a port of this matroid. Therefore, being a matroid port is a necessary condition for an access structure to admit an ideal perfect secret sharing scheme. As we saw before, being the port of a linear matroid is a sufficient condition. Nevertheless, the necessary condition is not sufficient [29] and the sufficient one is not necessary [31].

Because of the Brickell-Davenport Theorem, matroid theory plays an important role in secret sharing, as it is demonstrated with some examples in the following. Some results about representability of matroids were used in [4] to obtain an important separation result between the efficiency of linear and non-linear secret sharing schemes. The algebraic properties of ideal perfect secret sharing schemes that can be derived from the induced matroid were explored by Matúš [22]. Matroid ports were introduced by Lehman [17, 18] and a forbidden minor characterization for them was presented by Seymour [28] before the invention of secret sharing. These results were applied in [19] to provide a common explanation for a property that had been observed in several particular families of access structures. Powerful tools for the study of ideal perfect secret sharing schemes with multipartite access structures are given in [11] by applying several well known results about integer polymatroids. These techniques provided a characterization of the hierarchical access structures that admit an ideal perfect secret sharing scheme [12]. Other relevant results on secret sharing have been obtained by using matroid theory as, for instance, the ones in [2, 9, 13, 23].

Our main objective is to extend the connection to matroid theory given by the Brickell-Davenport Theorem to secret sharing schemes that are not necessarily perfect, that is, schemes in which some unqualified sets may obtain partial information about the secret value. Therefore, we consider here secret sharing schemes whose access structures consist of two families of sets of participants. Namely, the qualified sets, which can recover the secret value from the shares of their participants, and the forbidden sets, which do not obtain any information about the secret. The sets that are neither qualified nor forbidden can obtain partial information about the secret value. A secret sharing scheme is perfect if the forbidden sets coincide with the unqualified ones. Non-perfect secret sharing schemes were first considered by Blakley and Meadows [5], who introduced the threshold non-perfect secret sharing schemes, also called ramp schemes.

Differently to the perfect case, in a non-perfect secret sharing scheme, the length of some shares may be smaller than the length of the secret value. The gap of an access structure, which is the minimum gap between forbidden and qualified sets, provides an upper bound on the ratio between the length of the secret and the maximum length of the shares [24]. Non-perfect secret sharing schemes attaining this bound can be obtained from linear codes by generalizing Brickell's [6] construction of ideal perfect secret sharing schemes. Specifically, a codeword is selected uniformly at random from a given linear code with length $n + k$, where n is the number of participants and the first k columns of the generator matrix are supposed to be linearly independent. The first k positions correspond to the secret value, and each of the other n positions corresponds to the share of a participant. The access structure of this scheme is determined by the matroid associated to the code.

On the basis of the main properties of these non-perfect secret sharing schemes constructed from linear codes, Kurosawa et al. [16] proposed a definition for *ideal* secret sharing scheme that applies to non-perfect schemes too, and they proved that every scheme that is ideal according to their definition defines a matroid. Nevertheless, their definition is not as natural as the one for perfect schemes. As in the perfect case, it is required that all shares have the same length, and that the ratio of this length with the length of the secret is minimum according to some lower bound. But, in addition, the definition proposed in [16] requires that the mutual information between the secret value and the shares of every set of participants is an integer multiple of the

length of the shares. Paillier [26] presented additional results about ideal (according to [16]) non-perfect secret sharing schemes and their connections to matroid theory. He proposed as well an alternative definition for ideal scheme, but it has the same requirement as the one in [16].

After considering other possible ways to extend the concept of *ideal* secret sharing scheme to non-perfect schemes, we were not able to find a definition that was as natural and useful as the one for the perfect case. Some examples illustrating this situation are given in Section 8. Because of that, we think that the best option is to restrict the concept of ideal scheme to the perfect case, and try to establish which non-perfect secret sharing schemes are connected to matroids in a similar way as the ideal perfect ones.

Our first step in that direction is to present a new interpretation of the Brickell-Davenport Theorem by identifying its two main ingredients. The first one is the result by Fujishige [14] (Theorem 2.2), which states that the joint Shannon entropies of a collection of random variables define a polymatroid. As a consequence of Theorem 2.2, every secret sharing scheme (perfect or non-perfect) defines a polymatroid that determines the access structure. This leads to a natural connection between polymatroids and access structures that has been used previously for the perfect case in [3, 10, 19] and other works. The second ingredient is a purely combinatorial result (Proposition 4.2) involving polymatroids and their associated access structures.

In particular, the Brickell-Davenport Theorem is a characterization of the perfect secret sharing schemes whose associated polymatroid is a multiple of a matroid. We use this new interpretation of that result to generalize it to non-perfect secret sharing schemes. First, on the basis of the properties of the aforementioned non-perfect secret sharing schemes defined from linear codes, we introduce in Section 5 the concepts of *quasi-matroid* and *generalized matroid port*. Our main result, which is presented in Section 7, is a characterization of the secret sharing schemes whose associated polymatroid is a multiple of a quasi-matroid. In addition, we prove that, in this case, the quasi-matroid is determined by the access structure, which is a generalized matroid port. Since those schemes coincide with the ones that are *ideal* according to the definition proposed in [16], another characterization for the same class of secret sharing schemes can be derived from the results in that work. Nevertheless, our approach to the problem has several advantages. First, our characterization is much simpler, that is, we find a much weaker condition that characterizes that class. Second, our combinatorial restatement of the Brickell-Davenport Theorem (Section 4) provides a more natural way to generalize it to non-perfect schemes. And third, our proofs are simpler and more elegant. They are purely combinatorial and they use varied known results and techniques from matroid theory.

2 Matroids and Polymatroids

Some basic concepts and facts about matroids and polymatroids that are used in the paper are presented here. A more detailed presentation can be found in textbooks on the topic [25, 27, 33]. For a finite set Q, we notate $\mathcal{P}(Q)$ for the power set of Q, that is, the set of all subsets of Q.

Definition 2.1. 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 $A \subseteq B \subseteq Q$, then $f(A) \leq f(B)$.
- f is *submodular*: $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$ for every $A, B \subseteq Q$.

A polymatroid is called *integer* if its rank function is integer-valued. A *matroid* $\mathcal{M} = (Q, r)$ is an integer polymatroid such that $r(\{x\}) \in \{0, 1\}$ for every $x \in Q$.

Because of the connection between polymatroids and the Shannon entropy that is described in the following and by analogy to the conditional entropy, we write $f(X|Y) = f(X \cup Y) - f(Y)$. Clearly, the polymatroid axioms imply that $f(X|Y) \geq 0$ and $f(X|Y) \geq f(X|Y \cup Z)$. In addition,

$$f(X_1 \cup \cdots \cup X_r) = \sum_{i=1}^{r} f(X_i | X_1 \cup \cdots \cup X_{i-1}) \tag{1}$$

for all $X_1, \ldots, X_r \subseteq Q$.

For a polymatroid $\mathcal{S} = (Q, f)$ and a set $Z \subseteq Q$, the polymatroids $\mathcal{S} \setminus Z = (Q - Z, f_{\setminus Z})$ and $\mathcal{S}/Z = (Q - Z, f_{/Z})$ are defined, respectively, by $f_{\setminus Z}(A) = f(A)$ and $f_{/Z}(A) = f(A|Z)$. Every polymatroid that can be obtained from $\mathcal{S}$ by repeatedly applying these operations is called a *minor* of $\mathcal{S}$. Every minor of $\mathcal{S}$ is of the form $(\mathcal{S} \setminus Z_1)/Z_2$ for some disjoint sets $Z_1, Z_2 \subseteq Q$. The minors of a matroid are matroids as well. The *dual* of a matroid $\mathcal{M} = (Q, r)$ is the matroid $\mathcal{M}^* = (Q, r^*)$ with $r^*(A) = |A| - r(Q) + r(Q - A)$ for every $A \subseteq Q$. Clearly, $\mathcal{M}^{**} = \mathcal{M}$. In addition, $(\mathcal{M} \setminus B)^* = \mathcal{M}^*/B$ and $(\mathcal{M}/B)^* = \mathcal{M}^* \setminus B$ for every $B \subseteq Q$. If $\mathcal{S} = (Q, f)$ is a polymatroid and c is a positive real number, then $c\mathcal{S} = (Q, cf)$ is a polymatroid as well, which is called a *multiple* of $\mathcal{S}$.

For a field $\mathbb{K}$, an integer polymatroid $\mathcal{S} = (Q, f)$ is said to be $\mathbb{K}$-*linear* (or $\mathbb{K}$-*linearly representable*, or $\mathbb{K}$-*representable*) if there exists a $\mathbb{K}$-vector space E and a collection $(V_i)_{i \in Q}$ of vector subspaces of E such that $f(X) = \dim \sum_{i \in X} V_i$ for every $X \subseteq Q$. Every minor of a $\mathbb{K}$-linear polymatroid is $\mathbb{K}$-linear as well. The same applies to the dual of a $\mathbb{K}$-linear matroid.

The following result describes the connection between Shannon entropy and polymatroids that was discovered by Fujishige [14]. For a tuple $(S_i)_{i \in Q}$ of discrete random variables and a set $A = \{i_1, \ldots, i_r\} \subseteq Q$, we write S_A for the random variable $S_{i_1} \times \cdots \times S_{i_r}$, and $H(S_A)$ for its Shannon entropy.

Theorem 2.2. *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 $f(A) = H(S_A)$ is the rank function of a polymatroid with ground set Q.*

Entropic polymatroids are the ones that can be defined in this way from a tuple of discrete random variables. If $\mathbb{K}$ is a finite field, then every $\mathbb{K}$-linear polymatroid is a multiple of an entropic polymatroid.

3 Secret Sharing Schemes and Polymatroids

We present first a definition of access structure that is more general than the one usually considered when dealing only with perfect secret sharing schemes.

Definition 3.1. 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.

An access structure is *connected* if every participant $x \in P$ is in a minimal qualified set and in a minimal non-forbidden set. For a family $\mathcal{C} \subseteq \mathcal{P}(P)$ of subsets of P, we notate

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

Access structures of the form $\Gamma = (\overline{\mathcal{B}}, \mathcal{B})$ are called *perfect*. The *dual of an access structure* $\Gamma = (\mathcal{A}, \mathcal{B})$ on P is the access structure $\Gamma^* = (\mathcal{B}^c, \mathcal{A}^c)$ on the same set. It is clear that the dual of a connected access structure is connected as well.

The following definition of an access structure from a polymatroid is well motivated by the connection between secret sharing schemes and polymatroids that is derived from Theorem 2.2. From now on, P will denote a finite set of participants, $p_0 \notin P$ a special participant called *dealer*, and $Q = P \cup \{p_0\}$.

Definition 3.2. Let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(\{p_0\}) > 0$ and $f(\{p_0\}|P) = 0$. The access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$ on P is defined by

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

It is not difficult to check that this is indeed an access structure. If $\mathcal{M}$ is a matroid, then the access structure $\Gamma_{p_0}(\mathcal{M})$ is perfect and it is called the *port of the matroid* $\mathcal{M}$ *at the point* p_0.

Definition 3.3. A *secret sharing scheme* Σ on P is a collection $(S_i)_{i \in Q}$ of discrete random variables such that $H(S_{p_0}) > 0$ and $H(S_{p_0}|S_P) = 0$. The random variable S_{p_0} corresponds to the *secret value* that is distributed into *shares* among the participants in P according to the random variables $(S_i)_{i \in P}$.

Definition 3.4. Let $\Sigma = (S_i)_{i \in Q}$ be a secret sharing scheme on P. Every multiple of the polymatroid (Q, h), where $h(A) = H(S_A)$ for every $A \subseteq Q$, is called a Σ-*polymatroid*.

Definition 3.5. Let Σ be a secret sharing scheme on P and $\mathcal{S}$ a Σ-polymatroid. Then the *access structure of the secret sharing scheme* Σ is $\Gamma(\Sigma) = \Gamma_{p_0}(\mathcal{S})$.

The participants in a qualified set $B \in \mathcal{B}$ can recover the secret value from their shares because $h(\{p_0\}|B) = 0$. Since $h(\{p_0\}|A) = h(\{p_0\})$ if $A \in \mathcal{A}$, the shares of the participants in a forbidden set do not provide any information at all about the secret value. Observe that a set of participants that is neither qualified nor forbidden can obtain partial information about the secret value. A secret sharing scheme is said to be *perfect* if its access structure is perfect, that is, if every subset of P is either forbidden or qualified.

Observe that, for a secret sharing scheme Σ, every Σ-polymatroid is a multiple of an entropic polymatroid. Therefore, it is possible that $\Gamma = \Gamma_{p_0}(\mathcal{S})$ for some polymatroid $\mathcal{S}$ but it does not exist any secret sharing scheme Σ with access structure Γ such that $\mathcal{S}$ is a Σ-polymatroid (see Example 8.1).

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

$$\rho_{p_0}(\mathcal{S}) = \frac{f(\{p_0\})}{\max_{x \in P} f(\{x\})}.$$

The *information rate* $\rho(\Sigma)$ of a secret sharing Σ is the ratio between the length of the secret value and the maximum length of the shares. That is, $\rho(\Sigma) = \rho_{p_0}(\mathcal{S})$ if $\mathcal{S}$ is a Σ-polymatroid. If Σ is a perfect secret sharing scheme with connected access structure and $\mathcal{S} = (Q, f)$ is a Σ-polymatroid, then $f(\{x\}) \geq f(\{p_0\})$ for every participant $x \in P$ [15], and hence $\rho(\Sigma) \leq 1$. A perfect secret sharing scheme is called *ideal* if every share has the same length as the secret, that is, if $\rho(\Sigma) = 1$.

We present in the following the code-based description due to Massey [21] of Brickell's [6] construction of ideal perfect secret sharing schemes. Consider a finite field $\mathbb{K}$ and a $\mathbb{K}$-linear

code $C \subseteq \mathbb{K}^Q$ with length $|Q|$. By considering the uniform probability distribution on C, a collection $(C_i)_{i\in Q}$ of random variables is obtained. Therefore, the code C determines a secret sharing scheme Σ on P. Every codeword $(c_i)_{i\in Q} \in C$ corresponds to a distribution of shares. This scheme is perfect and, since both the secret value c_{p_0} and the shares c_i, where $i \in P$, are elements in the field $\mathbb{K}$, it is ideal. The columns of a generator matrix of C define a $\mathbb{K}$-linear matroid $\mathcal{M}$ with ground set Q. This matroid is the same for all generator matrices of C. The matroid $\mathcal{M}$ is a Σ-polymatroid, and hence the access structure of Σ is the matroid port $\Gamma_{p_0}(\mathcal{M})$. By the Brickell-Davenport Theorem [7], which is restated here in Theorem 4.1, this property of the schemes constructed from linear codes applies as well to every ideal perfect secret sharing scheme.

For $\Gamma = (\mathcal{A}, \mathcal{B})$ and $\Gamma' = (\mathcal{A}', \mathcal{B}')$, access structures on P, we write $\Gamma \preceq \Gamma'$ if $\mathcal{A} \subseteq \mathcal{A}'$ and $\mathcal{B} \subseteq \mathcal{B}'$. This defines a partial order on the access structures on a set P, and the maximal elements coincide with the perfect access structures. An access structure Γ is *realized* by a secret sharing scheme Σ if $\Gamma \preceq \Gamma(\Sigma)$. An optimization problem appears naturally at this point. Namely, to find the optimal information rate among all secret sharing schemes that realize a given access structure Γ. This value is denoted by $\rho(\Gamma)$.

The *gap* $g(\Gamma)$ of an access structure $\Gamma = (\mathcal{A}, \mathcal{B})$ is defined by

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

As a consequence of [24, Theorem 13], the information rate of a secret sharing scheme is upper bounded by the gap of its access structure. For completeness, we present here the combinatorial statement of this result and its proof.

Proposition 3.6. *If $\Gamma = \Gamma_{p_0}(\mathcal{S})$, then $\rho_{p_0}(\mathcal{S}) \leq g(\Gamma)$.*

Proof. Consider a forbidden set A and a qualified set B with $A \subseteq B$. Then

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

and hence

$$f(\{p_0\}) \leq f(B - A) \leq \sum_{y\in B-A} f(\{y\}) \leq |B - A| \max_{x\in P} f(\{x\}) \tag{2}$$

which clearly concludes the proof. □

If $\rho_{p_0}(\mathcal{S}) = g(\Gamma)$, the inequalities in (2) become equalities for every $A \in \mathcal{A}$ and $B \in \mathcal{B}$ with $|B - A| = g(\Gamma)$. In particular, $f(\{y\}) = \max_{x\in P} f(\{x\})$ for every $y \in B - A$. Therefore, all shares have the same length if the access structure Γ is such that for every $x \in P$ there exist $A \in \mathcal{A}$ and $B \in \mathcal{B}$ such that $|B - A| = g(\Gamma)$ and $x \in B - A$. Observe that $g(\Gamma') \leq g(\Gamma)$ if $\Gamma \preceq \Gamma'$. Hence, as a consequence of Proposition 3.6, $\rho(\Gamma) \leq g(\Gamma)$. An access structure with gap g that is maximal with this property is called *g-gap-maximal*.

4 Brickell-Davenport Theorem Revisited

We present in Theorem 4.1 a restatement in our terminology of the Brickell-Davenport Theorem [7, Theorem 1]. This makes it clear that the Brickell-Davenport Theorem can be derived from Theorem 2.2 and Proposition 4.2, being the latter a purely combinatorial result.

Theorem 4.1 (Brickell-Davenport Theorem)**.** *Let Σ be an ideal perfect secret sharing scheme. Then there exists a matroid $\mathcal{M}$ that is a Σ-polymatroid. Consequently, the access structure Γ of Σ is a port of the matroid $\mathcal{M}$. Moreover, the matroid $\mathcal{M}$ is determined by Γ if this access structure is connected*

The last statement of the theorem is due to Lehman [17]. A proof for it can be found in [32] as well. Since we can assume that Γ is connected to prove the first statement, the following combinatorial result is enough to conclude the proof of Theorem 4.1.

Proposition 4.2. *Let $\mathcal{S} = (Q, f)$ be a polymatroid such that the access structure $\Gamma_{p_0}(\mathcal{S})$ is perfect and connected. If $f(\{x\}) = 1$ for every $x \in Q$, then $\mathcal{S}$ is a matroid.*

Proof. Consider $\Gamma_{p_0}(\mathcal{S}) = (\overline{\mathcal{B}}, \mathcal{B})$. If $C \notin \mathcal{B}$ and $C \cup \{x\} \in \mathcal{B}$, then $f(\{x\}|C) = 1$ and $f(\{x\}|C \cup \{p_0\}) = 0$. Indeed, this can be proved by using $f(C) + f(\{p_0\}|C) + f(\{x\}|C \cup \{p_0\}) = f(B) + f(\{p_0\}|B)$, where $B = C \cup \{x\}$.

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

Suppose that $A \in \mathcal{B}$. Then $A - \{x\} \in \mathcal{B}$ for every $x \in A$ because $f(\{x\}|A - \{x\}) < 1$. Let B be a minimal qualified set with $B \subseteq A$, and take $x \in B$ and $C = B - \{x\}$. Then $f(\{x\}|C \cup \{p_0\}) = 0$ and, since $A - \{x\}$ is qualified, $f(\{x\}|A - \{x\}) = f(\{x\}|(A - \{x\}) \cup \{p_0\}) = 0$, a contradiction.

Suppose now that $A \notin \mathcal{B}$ and consider $B \subseteq P$, minimal with $B \notin \mathcal{B}$ and $A \cup B \in \mathcal{B}$. There exists such a set because Γ is connected. Then $f(\{y\}|(A \cup B) - \{y\}) = 1$ for every $y \in B$, and hence $f(A \cup B) = f(A) + |B|$. Since $f(\{x\}|(A \cup B) - \{x\}) \leq f(\{x\}|A - \{x\}) < 1$ for every $x \in A$, we have that $(A \cup B) - \{x\} \in \mathcal{B}$ for every $x \in A$. This implies that $f((A \cup B) - \{x\}) = f(A - \{x\}) + |B|$. Consider now a minimal qualified subset C such that $B \subseteq C \subseteq A \cup B$ and take $x \in A \cap C$ and the subsets $C' = C - \{x\}$ and $A' = (A \cup B) - \{x\}$. Then $f(\{x\}|C' \cup \{p_0\}) = 0$, and hence $f(\{x\}|A') = f(\{x\}|A' \cup \{p_0\}) = 0$. Therefore, $f(A \cup B) = f(A') + f(\{x\}|A') = f(A')$, which implies that $f(A) = f(A - \{x\})$, a contradiction. □

5 Generalized Matroid Ports

We describe in the following how to generalize Brickell's [6] construction of ideal perfect secret sharing schemes, which has been presented in Section 3, to a code-based construction of non-perfect secret sharing schemes.

Consider a set P of n participants and a set P_0 with $|P_0| = k$ and $P \cap P_0 = \emptyset$. Let $\mathbb{K}$ be a finite field and $C \subseteq \mathbb{K}^{P \cup P_0}$ a $\mathbb{K}$-linear code with length $n + k$. Assume that, for every generator matrix of C, the k columns corresponding to P_0 are linearly independent, that is,

$$C_{P_0} = \{(c_j)_{j \in P_0} : c \in C\} = \mathbb{K}^{P_0}.$$

Every codeword $c \in C$ is of the form $(c_i)_{i \in Q}$, where $c_{p_0} = (c_j)_{j \in P_0} \in \mathbb{K}^{P_0}$ and $c_i \in \mathbb{K}$ for every $i \in P$. The collection $(C_i)_{i \in Q}$ of random variables given by the uniform probability distribution on C defines a secret sharing scheme Σ on P. The properties of such schemes and their access structures are discussed next. In particular, we prove in Section 6 that the bound in Proposition 3.6 is attained.

The columns of a generator matrix of C define a $\mathbb{K}$-linear matroid $\mathcal{M}(C)$ with ground set $P \cup P_0$. The connection between this matroid and the access structure of Σ motivates the following definition.

Definition 5.1. Let P and P_0 be disjoint finite sets and $\mathcal{M} = (P \cup P_0, r)$ a matroid such that $r(P_0) = |P_0|$ and $r(P_0|P) = 0$. Then the *generalized port of the matroid $\mathcal{M}$ at the set P_0* is the access structure $\Gamma_{P_0}(\mathcal{M}) = (\mathcal{A}, \mathcal{B})$ defined by

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

Clearly, the access structure of Σ is the generalized matroid port $\Gamma_{P_0}(\mathcal{M}(C))$. We analyze next the connections between the matroid $\mathcal{M}(C)$ and the Σ-polymatroids. Some notation and terminology are needed. Given a matroid $\mathcal{M} = (P \cup P_0, r)$ such that $r(P_0) = |P_0|$, consider the polymatroid $\mathcal{M}|P_0$ with ground set $Q = P \cup \{p_0\}$ and rank function f defined by $f(A) = r(A)$ and $f(A \cup \{p_0\}) = r(A \cup P_0)$ for every $A \subseteq P$. Observe that $(\mathcal{M}|P_0) \setminus \{p_0\} = \mathcal{M} \setminus P_0$ and $(\mathcal{M}|P_0)/\{p_0\} = \mathcal{M}/P_0$. Polymatroids of the form $\mathcal{M}|P_0$ are called *quasi-matroids*. It is obvious that the quasi-matroid $\mathcal{M}(C)|P_0$ is a Σ-polymatroid. A matroid $\mathcal{M} = (P \cup P_0, r)$ is said to be P_0-*uniform* if $r(P_0) = |P_0|$ and $r(A) = \min\{r(A \cup P_0), r(A - P_0) + |A \cap P_0|\}$ for every $A \subseteq P \cup P_0$. Observe that every permutation of the elements in P_0 is an automorphism of $\mathcal{M}$. The next proposition is a consequence of more general results about the connections between integer polymatroids and matroids that can be found in [27, Section 44.6b] and [11].

Proposition 5.2. *Let $\mathcal{S} = (Q, f)$ be an integer polymatroid with $f(\{x\}) = 1$ for every $x \in P = Q - \{p_0\}$. Then there exists a unique P_0-uniform matroid $\mathcal{M} = \mathcal{M}(\mathcal{S}) = (P \cup P_0, r)$ such that $\mathcal{M}(\mathcal{S})|P_0 = \mathcal{S}$. In particular, $\mathcal{S}$ is a quasi-matroid. In addition, if $\mathcal{S}$ is $\mathbb{K}$-linear for some field $\mathbb{K}$, then $\mathcal{M}(\mathcal{S})$ is $\mathbb{L}$-linear for every large enough finite extension $\mathbb{L}$ of $\mathbb{K}$.*

Proof. For every $A \subseteq P \cup P_0$, consider $A'' = A \cap P_0$ and $A' = A - A'' \subseteq P$. The only possibility for the rank function r of $\mathcal{M}(\mathcal{S})$ is the map defined by

$$r(A) = \min\{f(A' \cup \{p_0\}), f(A') + |A''|\}.$$

The statement about linearity is a consequence of [11, Theorem 6.1]. □

Proposition 5.3. *The dual of a generalized matroid port is a generalized matroid port.*

Proof. Let $\Gamma_{P_0}(\mathcal{M})$ be a generalized port of a matroid $\mathcal{M} = (P \cup P_0, r)$. Consider the dual matroid $\mathcal{M}^*$. It is not difficult to check that $r^*(P_0) = |P_0|$ and $r^*(P_0|P) = 0$. The proof is easily completed by checking that $r^*(A \cup P_0) = r^*(A) + r^*(P_0)$ if and only if $r((P - A) \cup P_0) = r(P - A)$ and that, dually, $r^*(A \cup P_0) = r^*(A)$ if and only if $r((P - A) \cup P_0) = r(P - A) + r(P_0)$. This implies that $(\Gamma_{P_0}(\mathcal{M}))^* = \Gamma_{P_0}(\mathcal{M}^*)$. □

6 Optimality Properties of Generalized Matroid Ports

For a polymatroid $\mathcal{S} = (Q, f)$ and the access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$, we define

$$\beta_{p_0}(\mathcal{S}) = \frac{\min\{f(\{p_0\}|C) : C \in \overline{\mathcal{B}}\}}{f(\{p_0\})} \qquad \text{and} \qquad \alpha_{p_0}(\mathcal{S}) = \frac{\min\{f(\{p_0\}) - f(\{p_0\}|C) : C \in \overline{\mathcal{A}}\}}{f(\{p_0\})}.$$

We define the *secrecy* $\beta(\Sigma)$ and the *co-secrecy* $\alpha(\Sigma)$ of a secret sharing scheme Σ by $\beta(\Sigma) = \beta_{p_0}(\mathcal{S})$ and $\alpha(\Sigma) = \alpha_{p_0}(\mathcal{S})$ for some Σ-polymatroid $\mathcal{S}$. That is, the secrecy and the co-secrecy are, respectively, the minimum uncertainty about the secret among all unqualified subsets and the minimum amount of information about the secret that is obtained by a non-forbidden subset, both in relation to the length of the secret. Observe that $0 < \alpha(\Sigma) \leq 1$ and $0 < \beta(\Sigma) \leq 1$. In addition, a secret sharing scheme is perfect if and only if one of the values $\alpha(\Sigma)$ or $\beta(\Sigma)$ is equal to 1, in which case both values are equal to 1. We prove in the next proposition that both the secrecy and the co-secrecy provide lower bounds on the length of the shares.

Proposition 6.1. *Let $\mathcal{S} = (Q, f)$ be a polymatroid such that the access structure $\Gamma_{p_0}(\mathcal{S})$ is connected. Then $f(\{x\})/f(\{p_0\}) \geq \max\{\alpha_{p_0}(\mathcal{S}), \beta_{p_0}(\mathcal{S})\}$ for every participant $x \in P$. In particular, $1/\rho_{p_0}(\mathcal{S}) \geq \max\{\alpha_{p_0}(\mathcal{S}), \beta_{p_0}(\mathcal{S})\}$.*

Proof. For a participant $x \in P$, consider a minimal qualified set B with $x \in B$ and take $C = B - \{x\}$. By Equation (1),

$$f(B \cup \{p_0\}) = f(\{x\}) + f(C|\{x\}) + f(\{p_0\}|B) = f(C) + f(\{p_0\}|C) + f(\{x\}|C \cup \{p_0\}). \quad (3)$$

Since $f(\{p_0\}|B) = 0$ and $f(\{p_0\}|C) \geq \beta_{p_0}(\mathcal{S})f(\{p_0\})$, we have that $f(\{x\})/f(\{p_0\}) \geq \beta_{p_0}(\mathcal{S})$. Equation (3) can be used as well to prove that $f(\{x\})/f(\{p_0\}) \geq \alpha_{p_0}(\mathcal{S})$ by considering now a minimal non-forbidden set B with $x \in B$ and $C = B - \{x\}$. □

We prove in the following that the bounds in Propositions 3.6 and 6.1 are attained if $\Gamma_{p_0}(\mathcal{S})$ is a generalized matroid port. As a consequence, the code-based secret sharing schemes described in Section 5 have optimal information rate.

Proposition 6.2. *If Γ is a connected generalized matroid port and $\mathcal{S} = (Q, f)$ is a quasi-matroid with $\Gamma = \Gamma_{p_0}(\mathcal{S})$, then*

$$\rho_{p_0}(\mathcal{S}) = g(\Gamma) = \frac{1}{\alpha_{p_0}(\mathcal{S})} = \frac{1}{\beta_{p_0}(\mathcal{S})}.$$

Proof. Since $\mathcal{S}$ is a quasi-matroid, $f(\{x\}) = 1$ for every $x \in P$, and hence $\rho_{p_0}(\mathcal{S}) = f(\{p_0\})$. In addition, $\alpha_{p_0}(\mathcal{S}), \beta_{p_0}(\mathcal{S}) \geq 1/f(\{p_0\})$ because $\mathcal{S}$ is an integer polymatroid. For a participant $x \in P$, consider a minimal qualified set $B \subseteq P$ with $x \in B$ and take $C = B - \{x\}$. By Equation (3), $f(\{p_0\}|C) \leq 1$, and hence $\beta_{p_0}(\mathcal{S}) = 1/f(\{p_0\})$. One can prove in a similar way that $\alpha_{p_0}(\mathcal{S}) = 1/f(\{p_0\})$.

We prove next that $f(B) = |B|$ if B is a minimal qualified subset. Obviously, $f(B) \leq |B|$. Take $x \in B$ and $C = B - \{x\}$. Since $f(B) = f(B \cup \{p_0\}) = f(C) + f(\{p_0\}|C) + f(\{x\}|C \cup \{p_0\})$, we have that $f(B) \geq f(C) + f(\{p_0\}|C) \geq f(C) + 1$. Therefore, $f(\{x\}|B - \{x\}) = 1$ for every $x \in B$. Finally, $f(B) \geq \sum_{x \in B} f(\{x\}|B - \{x\}) = |B|$ by Equation (1). In particular, this implies that $f(A) = |A|$ for every $A \subseteq B$.

Let B be a minimal qualified set and let $A \subseteq B$ be a maximal forbidden subset of B. Then $f(A \cup \{p_0\}) = f(A) + f(\{p_0\})$ and

$$f(A \cup \{y\} \cup \{p_0\}) < f(A \cup \{y\}) + f(\{p_0\}) = f(A) + 1 + f(\{p_0\}) = f(A \cup \{p_0\}) + 1$$

for every $y \in B - A$. Therefore, $f(A \cup \{y\} \cup \{p_0\}) = f(A \cup \{p_0\})$ for every $y \in B - A$, which implies that $f(A \cup \{p_0\}) = f(B \cup \{p_0\}) = f(B)$, and hence $|B - A| = f(\{p_0\}) = \rho_{p_0}(\mathcal{S})$. □

Corollary 6.3. *If Γ is a connected generalized matroid port with $g(\Gamma) = 1$, then Γ is a matroid port, and hence it is perfect.*

Proof. Straightforward from the proof of Proposition 6.2. □

7 Generalizing Brickell-Davenport Theorem

This section is devoted to prove Theorem 7.1, which generalizes the Brickell-Davenport Theorem (Theorem 4.1) to secret sharing schemes that are not necessarily perfect.

Theorem 7.1. *Let Σ be a secret sharing scheme with connected access structure Γ and such that the secrecy and the co-secrecy of Σ are both equal to the inverse of the information rate. Then there exists a Σ-polymatroid that is a quasi-matroid. In particular, Γ is a generalized matroid port. Moreover, there exists a unique P_0-uniform matroid $\mathcal{M} = (P \cup P_0, r)$ such that $\Gamma = \Gamma_{P_0}(\mathcal{M})$.*

Clearly, the first statement is a straightforward consequence of Proposition 7.2, while the uniqueness result is proved by Propositions 5.2 and 7.9. Combined with Proposition 6.2, Theorem 7.1 characterizes the secret sharing schemes that have a quasi-matroid among their associated polymatroids.

Proposition 7.2. *Let $\mathcal{S} = (Q, f)$ be a polymatroid such that the access structure $\Gamma_{p_0}(\mathcal{S})$ is connected. Assume that $f(x) = 1$ for some $x \in P$ and $\alpha_{p_0}(\mathcal{S}) = \beta_{p_0}(\mathcal{S}) = 1/\rho_{p_0}(\mathcal{S})$. Then $\mathcal{S}$ is a quasi-matroid.*

The proof of Proposition 7.2 is quite involved and is divided into several partial results. In particular, we are going to use the following result by Csirmaz [10, Proposition 2.3].

Proposition 7.3. *Let $\Gamma = (\overline{\mathcal{B}}, \mathcal{B})$ be a perfect access structure on a set P and let $\mathcal{S}' = (P, f)$ be a polymatroid with ground set P. The polymatroid $\mathcal{S}'$ can be extended to a polymatroid $\mathcal{S} = (Q, f)$ with $f(\{p_0\}) = 1$ such that $\mathcal{S} \setminus \{p_0\} = \mathcal{S}'$ and $\Gamma = \Gamma_{p_0}(\mathcal{S})$ if and only if the following conditions are satisfied.*

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

From now on, we assume that $\mathcal{S} = (Q, f)$ is a polymatroid in the conditions of Proposition 7.2 and we take $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$. By Proposition 6.1, $f(x) \geq f(\{p_0\})/\rho_{p_0}(\mathcal{S})$ for every $x \in P$, and hence $f(x) = 1$ for every $x \in P$. Therefore, it is enough to prove that that $\mathcal{S}$ is an integer polymatroid.

Lemma 7.4. *There exists a matroid $\mathcal{M}_1 = (Q, r_1)$ such that $\mathcal{M}_1 \setminus \{p_0\} = \mathcal{S} \setminus \{p_0\}$ and $\Gamma_{p_0}(\mathcal{M}_1) = (\overline{\mathcal{B}}, \mathcal{B})$.*

Proof. We claim that the perfect access structure $\Gamma_1 = (\overline{\mathcal{B}}, \mathcal{B})$ and the polymatroid $\mathcal{S}' = \mathcal{S} \setminus \{p_0\} = (P, f)$ satisfy the conditions in Proposition 7.3. Indeed, if $A \notin \mathcal{B}$ and $B \in \mathcal{B}$, then $f(\{p_0\}|A) \geq 1$, and hence $f(A) \leq f(A \cup \{p_0\}) - 1 \leq f(B \cup \{p_0\}) - 1 = f(B) - 1$. This proves the first property. For the second one, $f(A \cup B) + f(A \cap B) \leq f(A \cup B \cup \{p_0\}) + f((A \cap B) \cup \{p_0\}) - 1 \leq f(A \cup \{p_0\}) + f(B \cup \{p_0\}) - 1 = f(A) + f(B) - 1$ if $A, B \in \mathcal{B}$ and $A \cap B \notin \mathcal{B}$. Therefore, the polymatroid $\mathcal{S}'$ can be extended to a polymatroid $\mathcal{M}_1 = (Q, r_1)$ with $r_1(\{p_0\}) = 1$ and $r_1(\{p_0\}|P) = 0$ such that $\mathcal{M}_1 \setminus \{p_0\} = \mathcal{S}'$ and $\Gamma_{p_0}(\mathcal{M}_1) = (\overline{\mathcal{B}}, \mathcal{B})$. By Proposition 4.2, $\mathcal{M}_1$ is a matroid. □

Lemma 7.5. *$f(Q - \{x\}) = f(Q)$ for every $x \in Q$.*

Proof. Observe that $f(Q) - f(Q - \{p_0\}) = f(\{p_0\}|P) = 0$. If $x \in P$, there exists a minimal qualified set $B \in \mathcal{B}$ with $x \in B$. Take $C = B - \{x\}$. By Equation (3),

$$0 \leq f(\{x\}|C \cup \{p_0\}) = f(\{x\}) - f(\{p_0\}|C) + f(C|\{x\}) - f(C) \leq 0,$$

which implies that $f(\{x\}|Q - \{x\}) = 0$. □

Lemma 7.6. *Consider the map $f^*\colon \mathcal{P}(Q) \to \mathbb{R}$ defined by*

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

for every $A \subseteq Q$. The following properties hold.

1. *$\mathcal{S}^* = (Q, f^*)$ is a polymatroid.*
2. *$f^*(\{x\}) = f(\{x\})$ and $f^*(Q - \{x\}) = f^*(Q)$ for every $x \in Q$.*
3. *$\Gamma_{p_0}(\mathcal{S}^*) = (\Gamma_{p_0}(\mathcal{S}))^* = (\mathcal{B}^c, \mathcal{A}^c)$.*
4. *$\alpha_{p_0}(\mathcal{S}^*) = \beta_{p_0}(\mathcal{S}^*) = 1/f^*(\{p_0\})$.*

Proof. Obviously, $f^*(\emptyset) = 0$. It is easy to prove that $f^*(X) \leq f^*(X \cup \{y\})$ if $X \subseteq Q$ and $y \notin X$. Consider two arbitrary subsets $X, Y \subseteq Q$. Then from the definition of f^* and the submodularity of f,

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

This completes the proof of the first statement. The second statement is a direct consequence of Lemma 7.5. Since $f^*(\{p_0\}) = f(\{p_0\}) > 0$ and $f^*(\{p_0\}|P) = 0$, we can consider the access structure $\Gamma_{p_0}(\mathcal{S}^*)$. The third and fourth statements are proved by taking into account that

$$f^*(\{p_0\}|C) = f(\{p_0\}) - f(\{p_0\}|P - C)$$

for every $C \subseteq P$. □

Lemma 7.7. *There exists a matroid $\mathcal{M}_2$ with ground set Q such that $\mathcal{M}_2/\{p_0\} = \mathcal{S}/\{p_0\}$ and $\Gamma_{p_0}(\mathcal{M}_2) = (\mathcal{A}, \overline{\mathcal{A}})$.*

Proof. As a consequence of Lemma 7.6, we can apply Lemma 7.4 to the polymatroid $\mathcal{S}^*$. Therefore, there exists a matroid $\mathcal{M}_3 = (Q, r_3)$ such that $\mathcal{M}_3 \setminus \{p_0\} = \mathcal{S}^* \setminus \{p_0\}$ and $\Gamma_{p_0}(\mathcal{M}_3) = (\overline{\mathcal{A}^c}, \mathcal{A}^c)$. Take $\mathcal{M}_2 = \mathcal{M}_3^*$. Then $\Gamma_{p_0}(\mathcal{M}_2) = (\Gamma_{p_0}(\mathcal{M}_3))^* = (\mathcal{A}, \overline{\mathcal{A}})$ and

$$\mathcal{M}_2/\{p_0\} = (\mathcal{M}_3 \setminus \{p_0\})^* = \mathcal{S}/\{p_0\},$$

where the second equality can be easily checked from the definitions of the corresponding rank functions. □

Lemma 7.8. *The polymatroid $\mathcal{S} = (Q, f)$ is integer.*

Proof. By Lemma 7.4, $f(A) = r_1(A) \in \mathbb{Z}$ for every $A \subseteq P$. Moreover, $f(A \cup \{p_0\}) - f(\{p_0\}) = r_2(A \cup \{p_0\}) - r_2(\{p_0\}) \in \mathbb{Z}$ for every $A \subseteq P$ by Lemma 7.7, and $f(\{p_0\}) \in \mathbb{Z}$ because $f(P \cup \{p_0\}) = f(P) \in \mathbb{Z}$. □

This concludes of course the proof of Proposition 7.2. The proof of Theorem 7.1 requires the following proposition. It generalizes a well known result that applies to perfect access structures. Namely, a connected matroid port is the port of a unique matroid [17, 20, 32].

Proposition 7.9. *If $\Gamma = (\mathcal{A}, \mathcal{B})$ is a connected generalized matroid port, then there exists a unique quasi-matroid $\mathcal{S}$ such that $\Gamma = \Gamma_{p_0}(\mathcal{S})$.*

Proof. Let $\mathcal{S} = (Q, f)$ be a quasi-matroid such that $\Gamma = \Gamma_{p_0}(\mathcal{S})$. By Lemmas 7.4 and 7.7, there exist matroids $\mathcal{M}_1 = (Q, r_1)$ and $\mathcal{M}_2 = (Q, r_2)$ such that $\Gamma_{p_0}(\mathcal{M}_1) = (\overline{\mathcal{B}}, \mathcal{B})$ and $\Gamma_{p_0}(\mathcal{M}_2) = (\mathcal{A}, \overline{\mathcal{A}})$. Since $(\overline{\mathcal{B}}, \mathcal{B})$ and $(\mathcal{A}, \overline{\mathcal{A}})$ are connected perfect access structures, the matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ are uniquely determined by Γ. If $A \subseteq P$, then $f(A) = r_1(A)$ and $f(A \cup \{p_0\}) - f(\{p_0\}) = r_2(A \cup \{p_0\}) - r_2(\{p_0\})$. By Proposition 6.2, $f(\{p_0\})$ is equal to the gap of Γ. Therefore, the rank function f is determined by Γ. □

The following proposition provides a sufficient condition for a secret sharing scheme to admit a quasi-matroid among its associated polymatroids. Namely, this is the case if the bound in Proposition 3.6 is attained and the access structure is gap-maximal.

Proposition 7.10. *Let $\mathcal{S} = (Q, f)$ be a polymatroid with $f(\{p_0\}) = g \in \mathbb{Z}$ and $f(\{x\}) = 1$ for every $x \in P$ such that the access structure $\Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$ is connected and g-gap-maximal. Then $\alpha_{p_0}(\mathcal{S}) = \beta_{p_0}(\mathcal{S}) = 1/f(\{p_0\})$.*

Proof. Suppose that $\beta_{p_0}(\mathcal{S}) < 1/f(\{p_0\})$. Then there exists $C \in \overline{\mathcal{B}}$ such that $f(\{p_0\}|C) < 1$. Take a forbidden set $A \in \mathcal{A}$ with $A \subseteq C$. Then

$$g = f(\{p_0\}) = f(\{p_0\}|A) \leq f(\{p_0\}|C) + f(C - A) < 1 + |C - A|,$$

and hence $|C - A| \geq g$. Consider the access structure $\Gamma' = (\mathcal{A}, \mathcal{B}')$, where $\min \mathcal{B}' = \min \mathcal{B} \cup \{C\}$. Clearly, $g(\Gamma') = g(\Gamma) = g$, a contradiction with the fact that Γ is g-gap-maximal. One can prove in a similar way that $\alpha_{p_0}(\mathcal{S}) = 1/f(\{p_0\})$. □

8 Examples

In this section we provide some examples to illustrate the connection between non-perfect secret sharing schemes, generalized matroid ports, and quasi-matroids. In Example 8.1 we show that the converse of the first statement of Theorem 7.1 is not true. The optimality of non-perfect schemes is discussed in Example 8.2, and the gap-maximality of access structures is analyzed in Examples 8.3 and 8.4.

Example 8.1. We have seen in Sections 6 and 7 that the secret sharing schemes whose access structure is a generalized matroid port satisfy some optimal properties. Nevertheless, being a generalized matroid port does not imply that there exist such an optimal secret sharing scheme for a given access structure. Consider a set $P = P_1 \cup P_2 \cup P_3$ with $|P_i| = 2$ and $P_i \cap P_j = \emptyset$ if $i \neq j$, and the access structure $\Gamma = (\mathcal{A}, \mathcal{B})$ on P determined as follows.

- $\mathcal{A}$ is formed by all subsets of P with at most 2 participants.
- $\mathcal{B}$ consists of all subsets of P with at least 4 participants except $P_1 \cup P_2$, $P_2 \cup P_3$ and $P_3 \cup P_1$.

The *Vamos matroid* $\mathcal{V}$ has ground set $P \cup P_0$ with $|P_0| = 2$ and its rank function r is determined by $r(X) = |X|$ if $|X| \leq 3$ and $r(X) = 4$ if $|X| \geq 4$ except for $r(P_0 \cup P_1) = r(P_0 \cup P_2) = r(P_1 \cup P_2) = r(P_1 \cup P_3) = r(P_2 \cup P_3) = 3$. Clearly, the access structure Γ is the generalized matroid port $\Gamma_{P_0}(\mathcal{V})$. The quasi-matroid $\mathcal{V}|P_0 = (P \cup \{p_0\}, f)$ satisfies that $f(\{p_0\}) = f(P_i) = 2$, and $f(P_i \cup P_j) = f(\{p_0\} \cup P_j) = 3$ except for $r(\{p_0\} \cup P_3) = 4$, and $f(P_1 \cup P_2 \cup P_3) = 4$. By using information inequalities, it can be proved that such a polymatroid is not the multiple of any entropic polymatroid [23]. Therefore, the quasi-matroid $\mathcal{V}|P_0$ is not a Σ-polymatroid for any secret sharing scheme Σ. By Theorem 7.1 and Proposition 7.9, this implies that there does not exist any secret sharing scheme Σ with access structure Γ and secrecy and co-secrecy equal to the inverse of the information rate.

We present next several examples of *linear* non-perfect secret sharing schemes, that is, schemes defined from linear collections of random variables. For a finite field $\mathbb{K}$, consider a family $(V_i)_{i\in Q}$ of vector subspaces of $\mathbb{K}^k$ and the $\mathbb{K}$-linear polymatroid $\mathcal{S} = (Q, f)$ determined by $f(X) = \dim \sum_{i\in X} V_i$. For every $i \in Q$, take $k_i = \dim V_i$ and consider a $k \times k_i$ matrix M_i whose columns are a basis of V_i. By choosing uniformly at random a (row) vector $x \in \mathbb{K}^d$, one obtains a secret value $s_0 = xM_{p_0}$ and shares $s_i = xM_i$ for $i \in P$. Clearly, $\Gamma_{p_0}(\mathcal{S})$ is the access structure of this linear secret sharing scheme.

Example 8.2. We present a secret sharing scheme Σ such that its access structure Γ is not a generalized matroid port. Even though the information rate of Σ is equal to the gap of Γ, the scheme is not optimal because the length of some shares can be improved. This example provides and argument against defining *ideal non-perfect secret sharing scheme* as the ones with information rate equal to the gap of the access structure. Consider a set $P = P_1 \cap P_2$ with $P_1 \cap P_2 = \emptyset$ and the access structure $\Gamma = (\mathcal{A}, \mathcal{B})$ defined by

- $A \in \mathcal{A}$ if and only if $|A \cap P_i| \leq 1$ for $i = 1, 2$,
- $B \in \mathcal{B}$ if and only if $|B \cap P_1| \geq 2$ or $|B \cap P_2| \geq 3$.

Since $g(\Gamma) = 1$ and Γ is not perfect, this access structure is not a generalized matroid port by Corollary 6.3. Consider a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq 2|P| + 1$ and the following subspaces $(V_i)_{i\in Q}$ of $\mathbb{K}^7$.

- $V_{p_0} = \langle (1, 0, 0, 0, 0, 0, 0), (0, 0, 0, 1, 0, 0, 0)\rangle$,
- $V_i = \langle (1, x_i, 0, 0, 0, 0, 0), (0, 0, 0, 1, y_i, 0, 0)\rangle$ if $i \in P_1$,
- $V_j = \langle (1, 0, z_j, 0, 0, 0, 0), (0, 0, 0, 1, 0, t_j, t_j^2)\rangle$ if $j \in P_2$,

where all values x_i, y_i, z_j, t_j are different and different from 0. Let $\mathcal{S} = (Q, f)$ be the $\mathbb{K}$-linear polymatroid defined by this collection of vector subspaces. It is not difficult to check that $\Gamma = \Gamma_{p_0}(\mathcal{S})$. Moreover, these vector subspaces define a linear secret sharing scheme Σ with $\sigma(\Sigma) = g(\Gamma) = 1$. Nevertheless, since Γ is not a generalized matroid port, no Σ-polymatroid is a quasi-matroid. This can be proved as well by checking the values of the secrecy and co-secrecy of Σ. A set $C = \{i, j\} \subseteq P_2$ with $i \neq j$ is minimally non-forbidden. Observe that

$$f(\{p_0\}) - f(\{p_0\}|C) = \dim(V_{p_0} \cap (V_i + V_j)) = 1,$$

and hence $\alpha(\Sigma) = 1/2 < 1/\rho(\Sigma)$. One can check similarly that $\beta(\Sigma) = 1/2$. Moreover, we present next another linear secret sharing scheme for Γ that improves Σ because some the shares have shorter length. Indeed, consider the following vector subspaces $(W_i)_{i\in Q}$ of $\mathbb{K}^5$.

- $W_{p_0} = \langle (1, 0, 0, 0, 0), (1, 1, 1, 0, 0)\rangle$,
- $W_i = \langle (1, 0, 0, 0, x_i), (1, 1, 1, y_i, 0)\rangle$ if $i \in P_1$,
- $W_j = \langle (1, z_j, z_j^2, 0, 0)\rangle$ if $j \in P_2$,

where all values x_i, y_i, z_j are different and different from 0 and $z_j \neq 1$. These subspaces define a linear secret sharing scheme for Γ in which the length of the shares of the participants in P_2 is half the length of the secret.

Example 8.3. If $\dim V_i = 1$ for every $i \in P$, then the linear polymatroid $\mathcal{S} = (Q, f)$ defined by the collection $(V_i)_{i\in Q}$ is a quasi-matroid. Consider $P = P_1 \cup P_2$ with $P_1 \cap P_2 = \emptyset$ and the subspaces of $\mathbb{K}^4$

- $V_{p_0} = \langle (1,1,1,0), (1,a,a^2,0) \rangle$,
- $V_i = \langle (1, x_i, x_i^2, 0) \rangle$ if $i \in P_1$,
- $V_j = \langle (1,0,0,y_j) \rangle$ if $j \in P_2$,

where a, x_i, y_j are different elements in $\mathbb{K} - \{0,1\}$. Then the access structure $\Gamma = \Gamma_{p_0}(\mathcal{S}) = (\mathcal{A}, \mathcal{B})$ is given by

- $A \in \mathcal{A}$ if and only if $A \subseteq P_2$ or $|A \cap P_i| \leq 1$ for $i = 1, 2$.
- $B \in \mathcal{B}$ if and only if $|A \cap P_1| \geq 3$, or $|A \cap P_i| \geq 2$ for $i = 1, 2$.

The information rate of the secret sharing scheme defined by this collection is equal to 2, and hence it coincides with the gap of the access structure. Since Γ is gap-maximal, by Proposition 7.10 every secret sharing scheme Σ for Γ with $\rho(\Sigma) = g(\Gamma) = 2$ admits a quasi-matroid among its associated polymatroids.

Example 8.4. We present next a quasi-matroid $\mathcal{S} = (Q, f)$ such that there exists a secret sharing scheme Σ on P associated to $\mathcal{S}$ but the generalized matroid port $\Gamma_{p_0}(\mathcal{S})$ is not gap-maximal. As before, take a partition $P = P_1 \cup P_2$ of the set of participants. Consider quasi-matroid $\mathcal{S} = (Q, f)$ defined by the following collection $(V_i)_{i \in Q}$ of vector subspaces of $\mathbb{K}^3$.

- $V_{p_0} = \langle (0,1,0), (0,0,1) \rangle$,
- $V_i = \langle (1, x_i, 0) \rangle$ if $i \in P_1$,
- $V_j = \langle (1,0,y_j) \rangle$ if $j \in P_2$,

where x_i, y_j are different nonzero elements in $\mathbb{K}$. Then the generalized matroid port $\Gamma = \Gamma_{p_0}(\mathcal{Z}) = (\mathcal{A}, \mathcal{B})$ is given by

- $A \in \mathcal{A}$ if and only if $|A| \leq 1$,
- $A \in \mathcal{B}$ if and only if $|A| \geq 3$ and $|A \cap P_i| \geq 1$ for some $i = i, 2$.

Nevertheless, Γ is not gap-maximal. Indeed, let Γ' be the access structures whose forbidden sets and qualified sets are, respectively, those with at most 1 participant and those with at least 3 participants. Clearly, $\Gamma \preceq \Gamma'$ and $g(\Gamma) = g(\Gamma') = 2$.

9 Acknowledgements

The first author's work was partially supported by the Spanish Government through the projects CONSOLIDER INGENIO 2010 CSD2007-00004 and TIN2011/27076-C03-01, and by the Government of Catalonia under grant 2009 SGR 1135. The second author's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

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

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

[4] A. Beimel, E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.* **34** (2005) 1196–1215.

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

[9] R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, G. Leander, J. Martí-Farré, C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *IEEE Trans. Inform. Theory* **54** (2008) 2644–2657.

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

[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 Trans. Inform. Theory* **58** (2012) 3273–3286.

[13] O. Farràs, C. Padró, C. Xing, A. Yang. Natural Generalizations of Threshold Secret Sharing. *Advances in Cryptology, Asiacrypt 2011, Lecture Notes in Comput. Sci.* **7073** (2011) 610–627.

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

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

[16] 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

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

[18] A. Lehman. Matroids and Ports. *Notices Amer. Math. Soc.* **12** (1976) 356–360.

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

[20] K.M. Martin. *Discrete Structures in the Theory of Secret Sharing*. Ph.D. Thesis, University of London, 1991.

[21] 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).

[22] F. Matúš. Matroid representations by partitions. *Discrete Math.* **203** (1999) 169–194.

[23] F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. Inform. Theory* **53** (2007) 320–330.

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

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

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

[27] A. Schrijver. *Combinatorial optimization. Polyhedra and efficiency*. Springer-Verlag, Berlin, 2003.

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

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

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

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

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

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