Noname manuscript No.
(will be inserted by the editor)

On the Optimization of Bipartite Secret Sharing Schemes

Oriol Farràs · Jessica Ruth Metcalf-Burton · Carles Padró · Leonor Vázquez

the date of receipt and acceptance should be inserted later

Abstract Optimizing the ratio between the maximum length of the shares and the length of the secret value in secret sharing schemes for general access structures is an extremely difficult and long-standing open problem. In this paper, we study it for bipartite access structures, in which the set of participants is divided in two parts, and all participants in each part play an equivalent role. We focus on the search of lower bounds by using a special class of polymatroids that is introduced here, the tripartite ones. We present a method based on linear programming to compute, for every given bipartite access structure, the best lower bound that can be obtained by this combinatorial method. In addition, we obtain some general lower bounds that improve the previously known ones, and we construct optimal secret sharing schemes for a family of bipartite access structures.

Key words. Cryptography, secret sharing, multipartite secret sharing, polymatroids, linear programming.

1 Introduction

Secret sharing, which was introduced in 1979 by Shamir [37] and Blakley [6], has important applications in cryptography as a building block of many different kinds of cryptographic protocols. A *secret sharing scheme* is a method to protect a secret value by distributing it into *shares* among a set of *participants* in such a way that only certain *qualified* subsets of participants can recover the secret by pooling their shares. Only *unconditionally secure, perfect* secret sharing schemes are considered in this work. In such schemes the shares of the participants in an unqualified subset do not provide any information at all about the secret value. The family of the qualified subsets is called the *access structure* of the scheme. It is *monotone*, which means that any superset of a qualified subset is qualified, and so every access structure is determined by the family of its minimal qualified subsets.

A previous version of this paper appeared in the *Proceedings of the Fourth International Conference on Information Theoretic Security, ICITS 2009*. The authors' work was partially supported by the Spanish Ministry of Education and Science under projects TSI2006-02731 and MTM2009-07694. The first author's work was partially supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", and by the Government of Catalonia through grant 2009 SGR 1135. He is with the UNESCO Chair in Data Privacy, but the views expressed in this paper are his own and do not commit UNESCO. The third author's work was partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

Oriol Farràs
Dep. d'Eng. Informàtica i Matemàtiques, Universitat Rovira i Virgili, Tarragona, Catalonia, E-mail: oriol.farras@urv.cat.

Jessica Ruth Metcalf-Burton
University of Michigan, Ann Arbor, U.S.A., E-mail: jmetcalf@umich.edu.

Carles Padró
Division of Mathematical Sciences, Nanyang Technological University, Singapore, E-mail: carlespl@ntu.edu.sg.

Leonor Vázquez
Instituto Politécnico Nacional, México D. F., México, E-mail: leobaki@hotmail.com.

The relation between the maximum length of the shares and the length of the secret is commonly used as a measure for the efficiency of secret sharing schemes. The *complexity of a secret sharing scheme* is defined as the ratio between the maximum length of the shares and the length of the secret. If all shares have the same length as the secret, which is the best possible situation, then both the scheme and its access structure are said to be *ideal*. Ito, Saito, Nishizeki [26] proved that there is a secret sharing scheme for every access structure, and so it is natural to consider the *optimal complexity* $\sigma(\Gamma)$ *of an access structure* Γ, which is the infimum of the complexities of all secret sharing schemes for Γ. Determining the optimal complexity for general access structures has appeared to be an extremely difficult open problem. The asymptotic behavior of this parameter is unknown and there is a huge gap between the best known general lower and upper bounds.

In a *linear secret sharing scheme*, the secret value and the shares are vectors over some finite field, and they are the values of some given linear maps on a random vector. Because of their homomorphic properties, linear secret sharing schemes are very useful in some applications of secret sharing as, for instance, multiparty computation. Moreover, both the computation of the shares and the recovery of the secret value can be efficiently performed. Specifically, in polynomial time on the number of participants, the number of bits of the secret, and the complexity of the scheme. For an access structure Γ, we notate $\lambda(\Gamma)$ for the infimum of the complexities of all linear secret sharing schemes for Γ. Of course, $\sigma(\Gamma) \leq \lambda(\Gamma)$.

Constructions of secret sharing schemes for a given access structure Γ provide upper bounds on $\sigma(\Gamma)$. Several methods to construct secret sharing schemes with low complexity have been presented in [9,12, 20,28,40] and other works. In most cases, these constructions provide linear schemes, and hence, upper bounds on $\lambda(\Gamma)$. On the other hand, lower bounds on the optimal complexity have been obtained in [7, 8,13,28] and other works by deriving inequalities on the Shannon entropies of the random variables involved in a secret sharing scheme. Csirmaz [15] presented a combinatorial method to find lower bounds that simplifies and unifies the techniques in those previous works. It is based on the fact that the basic Shannon information inequalities, the only ones that are used in the computation of those lower bounds, are equivalent to the axioms defining a polymatroid [23]. Because of that, every secret sharing scheme for a given access structure determines a polymatroid with certain properties. A new parameter, $\kappa(\Gamma)$, was introduced in [29] to denote the best lower bound on $\sigma(\Gamma)$ that can be obtained by this combinatorial method, that is, the best lower bound that can be obtained by using only the Shannon information inequalities. Obviously, $\kappa(\Gamma) \leq \sigma(\Gamma)$. Determining the value of $\kappa(\Gamma)$ for a given access structure is a linear programming problem [16,17,36]. Linear programming has been applied in a different way to secret sharing in [9,40] and other works.

Therefore, most of the known lower and upper bounds on $\sigma(\Gamma)$ are, respectively, lower bounds on $\kappa(\Gamma)$ and upper bounds on $\lambda(\Gamma)$. Even though our knowledge about the behavior of the parameters κ and λ can still be improved, several results indicate that new techniques are needed in the research on the open problem that is considered here. For instance, Csirmaz [15] proved that $\kappa(\Gamma) \leq n$ for every access structure Γ on n participants and, from the current knowledge, it does not seem reasonable that σ grows linearly on the number of participants. In addition, by using non-Shannon information inequalities [43], a separation result between the parameters κ and σ was presented in [2]. A slightly larger gap was proved in [34]. By using the Ingleton inequality [25] and linear programming, several examples of access structures with $\kappa(\Gamma) < \lambda(\Gamma)$ have been found [16,36]. Separation results between the complexities of linear and general (nonlinear) secret sharing schemes have been presented in [1,4,24].

Because of its difficulty, determining the optimal complexity of every given access structure has been considered for several particular families of access structures. The value of that parameter has been determined for almost all access structures on five participants [28]. The same applies for the ones defined by graphs with six vertices [19]. Recently, the problem has been solved for the family of the access structures defined by trees [18]. Nevertheless, only partial results have been obtained for most of the families that have been considered, as the ones defined by graphs [8,16], the weighted threshold ones [5], or the ones with at most four minimal qualified subsets [30].

The qualified sets in a *threshold access structure* are those having at least a certain number of elements, and hence all participants have the same role. Two different methods to construct ideal secret sharing schemes for threshold access structures were proposed in the seminal works on the topic [6, 37]. *Multipartite access structures*, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role in the structure, are a natural generalization of

the threshold case. A number of constructions of ideal secret sharing schemes for different families of multipartite access structures can be found in the literature, for instance [10,38,41,42]. In addition, the characterization of ideal multipartite access structures have been studied in [3,21,22,35]. In particular, the ideal bipartite [35] and tripartite [21] access structures have been completely characterized.

The open problem of determining the optimal complexity is studied in this paper for the family of the bipartite access structures. This line of work was initiated in [35], where several lower and upper bounds were presented. In particular, the results in [35] have interesting consequences about the asymptotic behavior of the optimal complexity of bipartite access structures. On one hand, by using simple decomposition methods as for instance the ones discussed in [39], one can construct linear secret sharing schemes proving that $\lambda(\Gamma) \leq n/2$ for every bipartite access structure on n players. On the other hand, the lower bound on the parameter κ that can be deduced from [35, Proposition 5.4] implies that there exist bipartite access structures with $\kappa(\Gamma) = \Omega(\sqrt{n})$. These are weighted threshold access structures in which the weight of half of the participants equals $m = \lfloor \sqrt{n/2} \rfloor$, the weight of the other half is one, and the threshold is m^2.

Most of our results deal with the value of the parameter κ for bipartite access structures, and hence with lower bounds on the optimal complexity of these structures. We improve previous results by using in a broader and deeper way the geometric representation introduced in [35], in which the sets of participants are represented by integer points on the plane. In particular, we point out in Section 3 that, in order to determine $\kappa(\Gamma)$ for bipartite access structures, the search can be restricted to a special class of polymatroids, the tripartite ones. That is, the symmetry properties among participants in the access structure can be translated into symmetry properties in the corresponding polymatroids.

By using this new technique we prove in Section 4 that the value of the parameter κ depends only on the relative position of the points representing the minimal qualified subsets, and it is independent from the number of participants in every part. It is an open problem to find out whether the parameters σ and λ have a similar behavior.

In addition, we present in Theorem 4 a general lower bound on $\kappa(\Gamma)$ for bipartite access structures. In most of the cases, it improves the only previously known general lower bound on the optimal complexity of bipartite access structures, namely the one that can be deduced from [35, Proposition 4.1]. For the particular case of bipartite weighted threshold structures, our bound coincides with the one that can be obtained from [35, Proposition 5.4]. Unfortunately, our new bound does not improve significatively the previous asymptotic results.

We study bipartite access structures in which there are two minimal points. By the aforementioned basic decomposition techniques, $\lambda(\Gamma) \leq 2$ for these structures [35]. By applying Theorem 4 to this particular case, we obtain in Corollary 1 that $\kappa(\Gamma) \geq 2 - 1/s$, where s is a positive integer that depends on the relative position of the two minimal points. We prove that this bound is tight when one of the minimal points lies on the axes, that is, when the corresponding minimal sets contain only participants in one of the parts.

Finally, we explain in Section 6 how to find the exact value of $\kappa(\Gamma)$ for bipartite access structures by solving a linear programming problem. Actually, linear programming can be used to find the value of this parameter for arbitrary access structures, but we show that, differently to the general case, the size of the linear program is polynomial on the number of participants when dealing with bipartite access structures. This is a consequence of the use of tripartite polymatroids that is introduced in this paper. We use this linear programming approach to determine the value of $\kappa(\Gamma)$ for some particular bipartite access structures. From these examples, we conjecture that, for the case of two minimal points, the value of $\kappa(\Gamma)$ coincides with the lower bound in Corollary 1. Moreover, we found the first known examples of access structures with $3/2 \leq \kappa(\Gamma) < 2$ such that $\kappa(\Gamma)$ is not of the form $2 - 1/s$ for any positive integer s. The question about the existence of such structures arises from the results in [16–18,30].

2 Preliminaries

Several definitions and basic facts as well as the main known results about the optimization of secret sharing schemes for general access structures are surveyed in this section. A more detailed exposition can be found in [29].

Secret sharing schemes are defined as collections of finite random variables whose joint Shannon entropies must satisfy certain conditions. The reader is referred to [14] for a textbook containing basic

information about Shannon entropies. Specifically, consider a finite set Q of *participants*, a finite set E with a probability distribution on it, and, for every $i \in Q$, a finite set E_i and a surjective map $\pi_i \colon E \to E_i$. Every map π_i induces a random variable on the set E_i. Let $H(E_i)$ denote the Shannon entropy of this random variable. For a subset $A = \{i_1, \ldots, i_r\} \subseteq Q$, we write $H(E_A)$ for the joint entropy $H(E_{i_1} \ldots E_{i_r})$, and a similar convention is used for conditional entropies as, for instance, in $H(E_j|E_A) = H(E_j|E_{i_1} \ldots E_{i_r})$. Consider a distinguished participant $p_0 \in Q$, which is usually called *dealer*, and an access structure Γ on the set $P = Q \smallsetminus \{p_0\}$. The maps π_i define an *unconditionally secure perfect secret sharing scheme* Σ with access structure Γ if the following properties are satisfied.

1. $H(E_{p_0}) > 0$.
2. $H(E_{p_0}|E_A) = 0$ if $A \in \Gamma$.
3. $H(E_{p_0}|E_A) = H(E_{p_0})$ if $A \notin \Gamma$.

In this situation, every random choice of an element $\mathbf{x} \in E$ according to the given probability distribution results in a *distribution of shares* $(s_i)_{i \in Q}$, where $s_i = \pi_i(\mathbf{x}) \in E_i$ is the *share* of the participant $i \in P$ and $s = s_{p_0} = \pi_{p_0}(\mathbf{x}) \in E_{p_0}$ is the *shared secret value*. Observe that the second requirement in the definition implies that the qualified subsets can recover the secret value from their shares and, by the third one, the shares of the participants in an unqualified subset do not provide any information at all about the secret value.

We define the *complexity* $\sigma(\Sigma)$ *of a secret sharing scheme* Σ as the ratio between the maximum length of the shares and the length of the secret, that is, $\sigma(\Sigma) = \max_{i \in P} H(E_i)/H(E_{p_0})$. For each participant $i \in P$, $H(E_i) \geq H(E_{p_0})$, and hence $\sigma(\Sigma) \geq 1$. A secret sharing scheme Σ with $\sigma(\Sigma) = 1$ is said to be *ideal*, and its access structure is called *ideal* as well. The *optimal complexity* $\sigma(\Gamma)$ *of an access structure* Γ is defined as the infimum of the complexities $\sigma(\Sigma)$ of the secret sharing schemes for Γ.

A secret sharing scheme is said to be *linear* if E and E_i are vector spaces over a finite field $\mathbb{K}$, the mappings π_i are linear, and the uniform probability distribution is taken on E. Observe that the complexity of a linear secret sharing scheme is equal to $\max_{i \in P} \dim E_i / \dim E_{p_0}$. Therefore a linear scheme is ideal if $\dim E_i = \dim E_{p_0}$ for every $i \in P$. An ideal linear scheme with $E_i = \mathbb{K}$ for every $i \in Q$ is called a $\mathbb{K}$-*vector space secret sharing scheme*, and its access structure is said to be a $\mathbb{K}$-*vector space access structure*. Every access structure admits a linear secret sharing scheme [26], and we notate $\lambda(\Gamma)$ for the infimum of the complexities of the linear secret sharing schemes with access structure Γ. Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$ for every access structure Γ.

We notate $\mathcal{P}(Q)$ for the power set of Q. The map $h \colon \mathcal{P}(Q) \to \mathbb{R}$ defined by $h(X) = H(E_X)/H(E_{p_0})$ satisfies the following properties.

1. $h(\emptyset) = 0$.
2. h is *monotone increasing*: if $X \subseteq Y \subseteq Q$, then $h(X) \leq h(Y)$.
3. h is *submodular*: if $X, Y \subseteq Q$, then $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$.
4. $h(A \cup \{p_0\}) \in \{h(A), h(A) + 1\}$ for every $A \subseteq P$.

Every pair $\mathcal{S} = (Q, h)$ formed by a finite set Q and a map $h \colon \mathcal{P}(Q) \to \mathbb{R}$ satisfying the first three properties above is a *polymatroid*. The set Q and the map h are called, respectively, the *ground set* and the *rank function* of $\mathcal{S}$. This connection between the joint entropies of a family of random variables and polymatroids was first pointed out by Fujishige [23]. If a polymatroid $\mathcal{S} = (Q, h)$ satisfies the fourth property above, we say that p_0 is an *atomic point* of $\mathcal{S}$.

Every polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ defines an access structure $\Gamma_{p_0}(\mathcal{S})$ on the set $P = Q \smallsetminus \{p_0\}$ by

$$\Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P \,:\, h(A \cup \{p_0\}) = h(A)\}.$$

In this situation, we say that $\mathcal{S}$ is a Γ-*polymatroid*.

Therefore, every secret sharing scheme Σ defines a polymatroid $\mathcal{S} = \mathcal{S}(\Sigma) = (Q, h)$ such that the dealer p_0 is an atomic point of $\mathcal{S}$. Moreover, the access structure Γ of Σ is univocally determined by the polymatroid $\mathcal{S}$ because $\Gamma = \Gamma_{p_0}(\mathcal{S})$. For a polymatroid $\mathcal{S} = (Q, h)$, we define $\sigma(\mathcal{S}) = \max\{h(\{i\}) \,:\, i \in Q\}$. Observe that $\sigma(\Sigma) = \sigma(\mathcal{S}(\Sigma))$ for every secret sharing scheme Σ.

The following two propositions will be very useful for our purposes. Proposition 1 contains a characterization of polymatroids given by Matúš [31], while Proposition 2 presents a characterization of Γ-polymatroids.

Proposition 1 ([31]) *A function $h\colon \mathcal{P}(Q) \to \mathbb{R}$ is the rank function of a polymatroid with ground set Q if and only if the following conditions are satisfied.*

1. $h(\emptyset) = 0$.
2. $h(Q \smallsetminus \{p\}) \leq h(Q)$ *for all* $p \in Q$.
3. $h(X) + h(X \cup \{p, q\}) \leq h(X \cup \{p\}) + h(X \cup \{q\})$ *for all* $X \subseteq Q$ *and* $p, q \in Q \smallsetminus X$.

Proposition 2 *Let Γ be an access structure on P and let $\mathcal{S} = (Q, h)$ be a polymatroid. Then $\mathcal{S}$ is a Γ-polymatroid if and only if the following conditions are satisfied.*

1. $h(\{p_0\}) = 1$.
2. $h(A \cup \{p_0\}) = h(A)$ *for every* $A \in \min \Gamma$.
3. $h(B \cup \{p_0\}) = h(B) + 1$ *for every maximal unqualified subset* $B \subseteq P$.

Proof If $X \in \Gamma$, there exists $A \in \min \Gamma$ with $A \subseteq X$. Since h is submodular, $h(A) + h(X \cup \{p_0\}) \leq h(A \cup \{p_0\}) + h(X)$, and hence $h(X \cup \{p_0\}) = h(X)$. If $Y \notin \Gamma$, then $Y \subseteq B$ for some maximal unqualified set $B \subseteq P$. As before, $h(Y) + h(B \cup \{p_0\}) \leq h(Y \cup \{p_0\}) + h(B)$. In addition, $h(Y \cup \{p_0\}) \leq h(Y) + h(\{p_0\}) = h(Y) + 1$. Therefore, $h(Y \cup \{p_0\}) = h(Y) + 1$. Observe that, in particular, we have proved that p_0 is an atomic point of $\mathcal{S}$. □

A polymatroid is said to be *integer* if its rank function is integer-valued. A *matroid* is an integer polymatroid $\mathcal{M} = (Q, r)$ such that $r(A) \leq |A|$ for all $A \subseteq Q$. For a finite field $\mathbb{K}$, an integer polymatroid $\mathcal{S} = (Q, h)$ is $\mathbb{K}$-*representable* if there exist a $\mathbb{K}$-vector space V and, for every $i \in Q$, a subspace $V_i \subseteq V$ such that $h(X) = \dim(\sum_{i \in X} V_i)$ for every $X \subseteq Q$. In particular, a matroid $\mathcal{M} = (Q, r)$ is $\mathbb{K}$-representable if there exists a set of vectors $\{v_i : i \in Q\}$ in some $\mathbb{K}$-vector space V such that $r(X)$ is equal to the dimension of the subspace spanned by the vectors in $\{v_i : i \in X\}$ for every $X \subseteq Q$.

Let $\mathcal{S}_1 = (Q, h_1)$ and $\mathcal{S}_2 = (Q, h_2)$ be two polymatroids on the same ground set. Clearly, $h = h_1 + h_2$ is the rank function of a polymatroid on Q, which is called the *sum* of $\mathcal{S}_1$ and $\mathcal{S}_2$ and is denoted by $\mathcal{S}_1 + \mathcal{S}_2 = (Q, h)$. For every polymatroid (Q, h), the pair (Q, ah) is also a polymatroid for any $a \in \mathbb{R}$ with $a > 0$.

Proposition 3 *The sum of $\mathbb{K}$-representable integer polymatroids is $\mathbb{K}$-representable.*

Proof Let $\mathcal{S}_1 = (Q, h_1)$ and $\mathcal{S}_2 = (Q, h_2)$ be two integer polymatroids on the same ground set. Consider two $\mathbb{K}$-vector spaces V and W and two families of subspaces, $(V_i)_{i \in Q}$ with $V_i \subseteq V$ and $(W_i)_{i \in Q}$ with $W_i \subseteq W$, that are $\mathbb{K}$-representations of the polymatroids $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively. Then the subspaces $V_i \times W_i \subseteq V \times W$ form a $\mathbb{K}$-representation of the integer polymatroid $\mathcal{S}_1 + \mathcal{S}_2$. □

A polymatroid $\mathcal{S} = (Q, h)$ is said to be *entropic* if there exist a family of random variables $(E_i)_{i \in Q}$ and a real number $a > 0$ such that $h(A) = aH(E_A)$ for every $A \subseteq Q$. If these random variables are $\mathbb{K}$-*linear*, that is, if they are defined from surjective linear maps $\pi_i\colon E \to E_i$, where E and E_i for $i \in Q$ are $\mathbb{K}$-vector spaces and the uniform probability distribution is taken on E, then the polymatroid $\mathcal{S}$ is said to be $\mathbb{K}$-*linearly entropic*. By considering, for $i \in Q$, the subspaces $(\ker \pi_i)^\perp$ of the dual space E^*, it is easy to prove that a polymatroid $\mathcal{S} = (Q, h)$ is $\mathbb{K}$-linearly entropic if and only if there exists a real number $b > 0$ such that (Q, bh) is a $\mathbb{K}$-representable integer polymatroid.

Let Γ be an access structure on the set $P = Q \smallsetminus \{p_0\}$ and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid. Then $\mathcal{S}$ is entropic if and only if there exists a secret sharing scheme Σ with access structure Γ such that $\mathcal{S} = \mathcal{S}(\Sigma)$. Moreover, $\mathcal{S}$ is linearly entropic if and only if there exists a linear secret sharing scheme with these properties. Because of that,

$$\sigma(\Gamma) = \inf\{\sigma(\mathcal{S}) : \mathcal{S} \text{ is an entropic } \Gamma\text{-polymatroid}\}$$

and

$$\lambda(\Gamma) = \inf\{\sigma(\mathcal{S}) : \mathcal{S} \text{ is a linearly entropic } \Gamma\text{-polymatroid}\}.$$

In addition, we define

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) : \mathcal{S} \text{ is a } \Gamma\text{-polymatroid}\}.$$

Clearly, $\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma)$ for every access structure Γ.

All elements in the ground set of a matroid are atomic points. An access structure Γ is a *matroid port* if $\Gamma = \Gamma_{p_0}(\mathcal{S})$ for some matroid $\mathcal{S} = (Q, h)$. In this case $\kappa(\Gamma) = 1$. Brickell and Davenport [11] proved that $\mathcal{S}(\Sigma)$ is a matroid if Σ is an ideal secret sharing scheme. Therefore, every ideal access structure is a matroid port. This result was generalized in [29].

Theorem 1 ([29]) *If an access structure Γ is not a matroid port, then $\kappa(\Gamma) \geq 3/2$. In particular, every access structure with $\sigma(\Gamma) < 3/2$ is a matroid port.*

The *independent sequence method* was introduced in [7] and subsequently improved in [35]. We use the description of this method presented in [29], which is in terms of polymatroids, to obtain bounds on the information rate of bipartite access structures. We present these bounds in Section 5.

Consider $A \subseteq P$ and an increasing sequence of subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$. We say that $(B_1, \ldots, B_m \mid A)$ is an *independent sequence* in Γ with *length* m and *size* s if $|A| = s$ and, for every $i = 1, \ldots, m$ there exists $X_i \subseteq A$ such that $B_i \cup X_i \in \Gamma$, while $B_m \notin \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ if $i \geq 2$. The independent sequence method is based on the following result.

Theorem 2 *Let Γ be an access structure on the set P and let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid on $Q = P \cup \{p_0\}$. If there exists in Γ an independent sequence $(B_1, \ldots, B_m \mid A)$ with length m and size s, then $h(A) \geq m$. As a consequence, $\kappa(\Gamma) \geq m/s$.*

3 Bipartite Access Structures and Tripartite Polymatroids

An *m-partition* $\Pi = (X_1, \ldots, X_m)$ of a set X is a disjoint family of m subsets of X with $X = X_1 \cup \cdots \cup X_m$. A permutation τ on X is said to be a *Π-permutation* if $\tau(X_i) = X_i$ for every $i = 1, \ldots, m$. A combinatorial object defined on X is said to be *Π-partite* if every Π-permutation on X is an automorphism of it. In particular, a family of subsets $\Lambda \subseteq \mathcal{P}(X)$ is Π-partite if and only if $\tau(\Lambda) = \{\tau(A) : A \in \Lambda\} = \Lambda$ for every Π-permutation τ on X, and a polymatroid $\mathcal{S} = (X, h)$ with ground set X is *Π-partite* if and only if $h(A) = h(\tau(A))$ for every $A \subseteq X$ and for every Π-permutation τ on X.

For every m-partition $\Pi = (X_1, \ldots, X_m)$ of P, we consider the $(m+1)$-partition $\Pi_0 = (X_1, \ldots, X_m, \{p_0\})$ of $Q = P \cup \{p_0\}$. We prove in the following that, for every Π-partite access structure $\Gamma \subseteq \mathcal{P}(P)$, the values of $\kappa(\Gamma)$ and $\lambda(\Gamma)$ can be determined by considering only the Γ-polymatroids that are Π_0-partite.

Proposition 4 *Let $\Pi = (X_1, \ldots, X_m)$ be an m-partition of a set P and let Π_0 be the corresponding $(m+1)$-partition of $Q = P \cup \{p_0\}$. Let Γ be a Π-partite access structure on P. Then*

- $\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) : \mathcal{S}$ *is a Π_0-partite Γ-polymatroid*$\}$.
- $\lambda(\Gamma) = \inf\{\sigma(\mathcal{S}) : \mathcal{S}$ *is a linearly entropic Π_0-partite Γ-polymatroid*$\}$.

Proof Let Ψ be the set of the Π_0-permutations on Q. Let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid, and consider the mapping $\widetilde{h} \colon \mathcal{P}(Q) \to \mathbb{R}$ defined by

$$\widetilde{h}(X) = \frac{1}{|\Psi|} \sum_{\tau \in \Psi} h(\tau(X)).$$

It is not difficult to check that $\widetilde{\mathcal{S}} = (Q, \widetilde{h})$ is a Π_0-partite Γ-polymatroid with $\sigma(\widetilde{\mathcal{S}}) \leq \sigma(\mathcal{S})$. Suppose now that $\mathcal{S}$ is $\mathbb{K}$-linearly entropic for some finite field $\mathbb{K}$. Then there exists a real number $b > 0$ such that $\mathcal{S}' = (Q, bh)$ is a $\mathbb{K}$-representable integer polymatroid. For a permutation τ on Q, consider the integer polymatroid $\tau\mathcal{S}' = (Q, b(h\tau))$, where $(h\tau)(X) = h(\tau(X))$ for every $X \subseteq Q$. Clearly, $\tau\mathcal{S}'$ is $\mathbb{K}$-representable. Then the integer polymatroid $\widetilde{\mathcal{S}}' = \sum_{\tau \in \Psi} \tau\mathcal{S}'$ is $\mathbb{K}$-representable by Proposition 3, and hence $\widetilde{\mathcal{S}} = 1/(b|\Psi|)\widetilde{\mathcal{S}}'$ is linearly entropic. □

We describe in the following the geometric representation of bipartite access structures that was introduced in [21,35]. We notate $\mathbb{Z}_+$ for the set of the non-negative integers, and we consider in $\mathbb{Z}_+^2$ the order relation defined by $(x_1, y_1) \leq (x_2, y_2)$ if $x_1 \leq x_2$ and $y_1 \leq y_2$. For a bipartition $\Pi = (X, Y)$ of a set P, consider the mapping $\Pi \colon \mathcal{P}(P) \to \mathbb{Z}_+^2$ defined by $\Pi(A) = (|A \cap X|, |A \cap Y|)$. We notate $\mathbf{P} = \Pi(\mathcal{P}(P)) = \{(x, y) \in \mathbb{Z}_+^2 : (x, y) \leq \Pi(X)\}$. For a Π-partite access structure Γ on P, we consider the set of integer points $\Pi(\Gamma) = \{\Pi(A) : A \in \Gamma\} \subseteq \mathbb{Z}_+^2$. Obviously, $\Pi(\Gamma) \subseteq \mathbf{P}$. Observe that $A \subseteq P$ is in Γ if and only if $\Pi(A) \in \Pi(\Gamma)$. Then Γ is completely determined by the set of points $\Pi(\Gamma)$. The set of points $\Pi(\Gamma)$ is monotone increasing, that is, if $(x_1, y_1), (x_2, y_2) \in \mathbf{P}$ are such that $(x_1, y_1) \in \Pi(\Gamma)$ and $(x_1, y_1) \leq (x_2, y_2)$, then $(x_2, y_2) \in \Pi(\Gamma)$. Therefore, Γ is determined by the family $\min \Pi(\Gamma)$ of the minimal points of $\Pi(\Gamma)$. Observe that the points in $\min \Pi(\Gamma) = \{(x_1, y_1), \ldots, (x_r, y_r)\}$ can be ordered

in such a way that $0 \leq x_1 < x_2 < \cdots < x_r$ and, in this situation, $y_1 > y_2 > \cdots > y_r \geq 0$. We are going to assume always that the points in $\min \Pi(\Gamma)$ are ordered in this way.

Consider the tripartition $\Pi_0 = (X, Y, \{p_0\})$ of the set $Q = P \cup \{p_0\}$. As before, for every $A \subseteq Q$, we consider $\Pi_0(A) = (|A \cap X|, |A \cap Y|, |A \cap \{p_0\}|) \in \mathbf{P} \times \{0,1\} \subseteq \mathbb{Z}_+^3$. If $\mathcal{S} = (Q, h)$ is a Π_0-partite polymatroid, then $h(A) = h(B)$ if $\Pi_0(A) = \Pi_0(B)$. Therefore, the polymatroid $\mathcal{S}$ is univocally determined by its *reduced rank function*, which is the map $\widehat{h} \colon \mathbf{P} \times \{0,1\} \to \mathbb{R}$ defined by $\widehat{h}(x, y, z) = h(A)$, where $A \subseteq Q$ is such that $\Pi(A) = (x, y, z)$. The following proposition, which is a straightforward consequence of Propositions 1 asn 2, provides a characterization of the reduced rank functions of tripartite polymatroids associated to bipartite access structures.

Proposition 5 *Let Γ be a bipartite access structure. Then a map $\widehat{h} \colon \mathbf{P} \times \{0,1\} \to \mathbb{R}$ is the reduced rank function of a Π_0-partite Γ-polymatroid if and only if the following conditions are satisfied.*

1. $\widehat{h}(0,0,0) = 0$.
2. $\widehat{h}((|X|, |Y|, 1) - \mathbf{e}_i) \leq \widehat{h}(|X|, |Y|, 1)$ *for* $i = 1, 2, 3$, *where* $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$, *and* $\mathbf{e}_3 = (0,0,1)$.
3. $\widehat{h}(\mathbf{x}) + \widehat{h}(\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j) \leq \widehat{h}(\mathbf{x} + \mathbf{e}_i) + \widehat{h}(\mathbf{x} + \mathbf{e}_j)$ *for every pair* $(i, j) \in \{1,2,3\} \times \{1,2,3\}$ *with* $i \leq j$ *and for every* $\mathbf{x} \in \mathbf{P} \times \{0,1\}$ *such that* $\mathbf{x} + \mathbf{e}_i + \mathbf{e}_j \in \mathbf{P} \times \{0,1\}$.
4. $\widehat{h}(0,0,1) = 1$.
5. $\widehat{h}(x, y, 1) = \widehat{h}(x, y, 0)$ *for every* $(x, y) \in \min \Pi(\Gamma)$.
6. $\widehat{h}(x, y, 1) = \widehat{h}(x, y, 0) + 1$ *for every* $(x, y) \in \max(\mathbf{P} \smallsetminus \Pi(\Gamma))$.

4 Duality and Minors

Duality and minors are operations on access structures, and also on matroids and polymatroids, that are important in secret sharing. This is mainly due to the fact of the parameters that are considered here have a good behavior with respect to those operations. In addition, minors of access structures correspond to a natural scenario in secret sharing. Namely, if several participants leave the scheme and maybe some of them reveal their shares, then the new access structure will be a minor of the original one.

Let Γ be an access structure on a set P. For any $B \subseteq P$, we consider on the set $P \smallsetminus B$ the access structures $\Gamma \setminus B$ and Γ / B defined by

$$\Gamma \setminus B = \{A \subseteq P \smallsetminus B \,:\, A \in \Gamma\} \quad \text{and} \quad \Gamma / B = \{A \subseteq P \smallsetminus B \,:\, A \cup B \in \Gamma\}.$$

These operations are called *deletion* and *contraction*, respectively. Any access structure obtained by a sequence of deletions and contractions of subsets of P is a *minor* of Γ. The *dual* Γ^* of an access structure Γ on P is the access structure on the same set defined by

$$\Gamma^* = \{A \subseteq P \,:\, P \smallsetminus A \notin \Gamma\}.$$

Obviously, $\Gamma^{**} = \Gamma$. The next proposition, whose proof is straightforward, describes a useful connection between these operations on access structures.

Proposition 6 *Let Γ be and access structure on a set P. Then $(\Gamma / B)^* = \Gamma^* \setminus B$ for every subset $B \subseteq P$.*

For a polymatroid $\mathcal{S} = (Q, h)$ and a subset $B \subseteq Q$, we consider the polymatroids $\mathcal{S} \setminus B = (Q \smallsetminus B, h_{\setminus B})$ and $\mathcal{S} / B = (Q \smallsetminus B, h_{/B})$ with $h_{\setminus B}(X) = h(X)$ and $h_{/B}(X) = h(X \cup B) - h(B)$ for every $X \subseteq Q \smallsetminus B$. Every polymatroid that is obtained from $\mathcal{S}$ by a sequence of such operations is a *minor* of $\mathcal{S}$. If $\mathcal{S}$ is a Γ-polymatroid and $B \subseteq P$, then $\mathcal{S} \setminus B$ is a $(\Gamma \setminus B)$-polymatroid and $\mathcal{S} / B$ is a (Γ / B)-polymatroid. Because of that, $\kappa(\Gamma') \leq \kappa(\Gamma)$ if Γ' is a minor of Γ. In addition, the aforementioned connection between minors and secret sharing implies that $\sigma(\Gamma') \leq \sigma(\Gamma)$ and $\lambda(\Gamma') \leq \lambda(\Gamma)$. The parameters λ and κ are invariant by duality, as it was proved, respectively, in [27] and [29]. The relation between $\sigma(\Gamma)$ and $\sigma(\Gamma^*)$ is an open problem.

Proposition 7 ([27, 29]) *For every access structure, $\lambda(\Gamma) = \lambda(\Gamma^*)$ and $\kappa(\Gamma) = \kappa(\Gamma^*)$.*

If Γ is Π-partite for some partition $\Pi = (P_1, \ldots, P_m)$ of the set P, then the dual access structure Γ^* is Π-partite as well. If $B \subseteq P$, the minors $\Gamma\backslash B$ and Γ/B are $(\Pi\backslash B)$-partite access structures, where $\Pi\backslash B = (P_1 \smallsetminus B, \ldots, P_m \smallsetminus B)$.

We present in Propositions 8 and 9 two different minors Γ', Γ'' of a bipartite access structure Γ such that $\kappa(\Gamma) = \kappa(\Gamma') = \kappa(\Gamma'')$. The validity of the analogous results for the parameters σ and λ is an open problem.

Proposition 8 *Let Γ be a bipartite access structure with $\min \Pi(\Gamma) = \{(x_1, y_1), \ldots, (x_r, y_r)\}$ and let $B \subseteq P$ be such that $\Pi(P \smallsetminus B) = (x_r, y_1)$. Then $\kappa(\Gamma \setminus B) = \kappa(\Gamma)$.*

Proof Let $\mathcal{S} = (Q \smallsetminus B, h)$ be a tripartite $(\Gamma \setminus B)$-polymatroid, and consider its reduced rank function $\widehat{h}\colon \Pi(\mathcal{P}(P \smallsetminus B)) \times \{0,1\} \to \mathbb{R}$. Consider the map $\widehat{h}'\colon \mathbf{P} \times \{0,1\} \to \mathbb{R}$ defined by

$$\widehat{h}'(x, y, z) = \widehat{h}(\min\{x, x_r\}, \min\{y, y_1\}, z).$$

The proof is concluded by checking that $\widehat{h}'$ is the reduced rank function of a tripartite Γ-polymatroid $\mathcal{S}'$ with $\sigma(\mathcal{S}') = \sigma(\mathcal{S})$. This can be easily done by using Proposition 5 and by taking into account that the minimal points of $\Gamma \setminus B$ coincide with the ones of Γ because $\Pi(P \smallsetminus B) = (x_r, y_1)$. □

Obviously, $|X| \geq x_r$ and $|Y| \geq y_1$ for every bipartite access structure Γ with minimal points $\{(x_1, y_1), \ldots, (x_r, y_r)\}$, and hence the access structure $\Gamma \setminus B$ has the smallest set of participants among all bipartite access structures with the same family of minimal points. Therefore, as a consequence of Proposition 8, the value of $\kappa(\Gamma)$ for a bipartite access structure depends only on the family of minimal points, and it does not depend on the number of participants in every part. One can prove analogously that this holds as well for all m-partite access structures with $m > 2$. The next result proves that the value of $\kappa(\Gamma)$ for a bipartite access structure depends only on the relative position of its minimal points.

Proposition 9 *Let Γ be a bipartite access structure with $\min \Pi(\Gamma) = \{(x_1, y_1), \ldots, (x_r, y_r)\}$. Consider $\alpha = \min\{i : x_i > 0\}$ and $\beta = \max\{i : y_i > 0\}$. Observe that $\alpha \in \{1, 2\}$ and $\beta \in \{r-1, r\}$. Let $B \subseteq P$ be such that $\Pi(B) = (x_\alpha - 1, y_\beta - 1)$. Then $\kappa(\Gamma/B) = \kappa(\Gamma)$.*

Proof Consider $\max(\mathbf{P} \smallsetminus \Pi(\Gamma)) = \{(u_1, v_1), \ldots, (u_s, v_s)\}$, that is, the family of the points representing the maximal unqualified subsets. We can suppose that they are ordered in such a way that $u_1 > \cdots > u_s$, and hence $v_1 < \cdots < v_s$. Suppose that $\beta = r$, and hence $y_r > 0$. Then $(|X|, y_r - 1)$ is maximal in $\mathbf{P} \smallsetminus \Pi(\Gamma)$, and obviously $(u_1, v_1) = (|X|, y_r - 1)$. Suppose now that $\beta = r - 1$. In this case $(x_r - 1, y_{r-1} - 1)$ represents a maximal unqualified set. In addition, since $y_r = 0$, every point $(x, y) \in \mathbf{P}$ with $x \geq x_r$ is in $\Pi(\Gamma)$. This implies that $(u_1, v_1) = (x_r - 1, y_{r-1} - 1)$. Therefore, $v_1 = y_\beta - 1$, and symmetrically $u_s = x_\alpha - 1$. The minimal points of Γ^* (ordered in the usual way) are $\{(x_1^*, y_1^*), \ldots, (x_s^*, y_s^*)\}$, where $(x_i^*, y_i^*) = (|X| - u_i, |Y| - v_i)$. Then $\Pi(P \smallsetminus B) = (|X| - (x_\alpha - 1), |Y| - (y_\beta - 1)) = (x_s^*, y_1^*)$ and, by Proposition 8, $\kappa(\Gamma^* \setminus B) = \kappa(\Gamma^*)$. Finally, by Propositions 6 and 7, $\kappa(\Gamma/B) = \kappa((\Gamma/B)^*) = \kappa(\Gamma^* \setminus B) = \kappa(\Gamma^*) = \kappa(\Gamma)$. □

5 Optimal Complexity of Bipartite Access Structures

In this section we present new general lower bounds on the optimal complexity of bipartite access structures that improve the ones given in [35]. In addition, we present an optimal construction of linear secret sharing schemes that determines the optimal complexities of all bipartite access structures with $\min \Pi(\Gamma) = \{(x_1, y_1), (x_2, 0)\}$. We begin by recalling the characterization of ideal bipartite access structures.

Theorem 3 ([35]) *Let Γ be a bipartite access structure. Then Γ is a matroid port if and only if $\min \Pi(\Gamma) = \min(\mathcal{B}_1 \cup \mathcal{B}_2)$, where, for some point $(x_0, y_0) \in \mathbb{Z}_+^2$ and for some integer k with $0 \leq k \leq x_0 + y_0$,*

- *$\mathcal{B}_1 \subseteq \{(0, y_0), (x_0, 0)\}$ and*
- *$\mathcal{B}_2 = \{(x, y) \in \mathbb{Z}_+^2 : (x, y) \leq (x_0, y_0)$ and $x + y = k\}$.*

In addition, Γ admits a vector space secret sharing scheme if it is a matroid port. Therefore, $\lambda(\Gamma) = 1$ if and only if $\kappa(\Gamma) = 1$ and, moreover, $\sigma(\Gamma) \geq 3/2$ if Γ is not ideal.

Differently to the general case, the asymptotic behavior of the parameter σ is known for bipartite access structures. Actually, if Γ is bipartite, then $\lambda(\Gamma) \leq \min\{|X|, |Y|\}$. This is due to the fact that the bipartite access structures with one minimal point admit a vector space secret sharing scheme and $\min \Pi(\Gamma)$ consists of at most $\min\{|X|, |Y|\}$ points. It can be proved by using well known basic decomposition techniques (see [39], for instance) that Γ admits a linear secret sharing scheme Σ with $\sigma(\Sigma) = |\min \Pi(\Gamma)|$.

We present next a new lower bound on κ for bipartite access structures. Our result generalize and improve the bound presented in [35, Proposition 4.1]. First, we present two lemmas that are needed in the proof of the result. The first one deals with independent sequences in bipartite access structures. The second one is a consequence of [19, Theorem 2.5]. Nevertheless, since we are using here different notation and terminology, we give its proof. For a polymatroid $\mathcal{S} = (Q, h)$ and subsets $X, Y, Z \subseteq Q$, we notate $h(X \mid Y) = h(X \cup Y) - h(Y) \geq 0$.

Lemma 1 *Let Γ be a bipartite access structure on a set P. Suppose that there exist a vector $(u, v) \in \mathbb{Z}_+^2$ and a monotone increasing sequence $(a_1, b_1) \leq \cdots \leq (a_m, b_m)$ of vectors in $\mathbf{P}$ such that, for every $i = 1, \ldots, m$, there exists a vector $(u_i, v_i) \leq (u, v)$ with $(a_i + u_i, b_i + v_i) \in \Pi(\Gamma)$ while $(a_m, b_m) \notin \Pi(\Gamma)$ and $(a_{i-1} + u_i, b_{i-1} + v_i) \notin \Pi(\Gamma)$ if $i \geq 2$. Then Γ admits an independent sequence $(B_1, \ldots, B_m|A)$ with length m and size $u + v$ such that $\Pi(A) = (u, v)$.*

Proof Take subsets $B_1 \subseteq \cdots \subseteq B_m \subseteq P$ and $A \subseteq P$ such that $\Pi(A) = (u, v)$, and $\Pi(B_i) = (a_i, b_i)$. In addition, for every $i = 1, \ldots, m$, consider a subset $X_i \subseteq A$ with $\Pi(X_i) = (u_i, v_i)$ and $X_i \cap B_i = \emptyset$. □

Lemma 2 ([19]) *Let $\mathcal{S} = (Q, h)$ be a Γ-polymatroid and X, Y, Z subsets of $P = Q \setminus \{p_0\}$. If $X \cup Z$ and $Y \cup Z$ are in Γ but Z is not in Γ, then $h(X \mid Z) - h(X \mid Y \cup Z) \geq 1$.*

Proof From the above definition of $h(A \mid B)$ and the submodularity of h, it is not difficult to prove that $h(A \mid B \cup C) \leq h(A \mid B)$ for every $A, B, C \subseteq Q$. Checking that

$$h(A \mid B) + h(\{p_0\} \mid A \cup B) = h(\{p_0\} \mid B) + h(A \mid B \cup \{p_0\})$$

for every $A, B \subseteq P$ is a straightforward calculation, and from this equality we obtain that $h(X \mid Y \cup Z) = h(X \mid Y \cup Z \cup \{p_0\})$ and $h(X \mid Z) = 1 + h(X \mid Z \cup \{p_0\})$. The proof is now easily concluded. □

Theorem 4 *Let Γ be a bipartite access structure with minimal points $\{(x_1, y_1), \ldots, (x_r, y_r)\}$, with $x_1 = 1$ and $y_r = 0$. Consider $k = \max_{i=1,\ldots,r-1}(x_{i+1} - x_i)$ and take $s = x_r$ and $t = y_1$. Then*

$$\kappa(\Gamma) \geq \frac{k + s - 2}{k + t - 1}.$$

Proof We prove first, by using Lemma 1, that Γ admits an independent sequence $(B_1, \ldots, B_s|A)$ with length s and size $k + t - 1$ such that $\Pi(A) = (k - 1, t)$. Consider the vectors $(u, v) = (k - 1, t)$ and $(a_i, b_i) = (i - 1, 0)$ for $i = 1, \ldots, s$. For every $i = 1, \ldots, s$, we define $\gamma(i)$ as the smallest integer for which $x_{\gamma(i)} \geq a_i$. Then for each $i = 1, \ldots, s$, consider the vector $(u_i, v_i) = (x_{\gamma(i)} - a_i, y_{\gamma(i)}) \leq (u, v)$. Clearly, those vectors satisfy the conditions in Lemma 1. Therefore, $h(A) \geq s$ by Theorem 2. Consider $A \cap P_1 = \{p_1, \ldots, p_{k-1}\}$ and $A \cap P_2 = \{q_1, \ldots, q_t\}$. In the following computation, we simplify the notation by writing p instead of $\{p\}$ and, for instance, $q_t \ldots q_1$ instead of $\{q_t, \ldots, q_1\}$. Here, (1), (2), and (4) are straightforward from $h(X \cup Y|Z) = h(X \mid Y \cup Z) + h(Y|Z)$ and $h(X \mid Y \cup Z) \geq h(X|Z)$ for every $X, Y, Z \subseteq Q$. In addition, $h(p_i \mid q_t \ldots q_1) - h(p_i \mid p_1 q_t \ldots q_1) \geq 1$ for every $i = 2, \ldots, k - 1$ by Lemma 2,

because $(1,t) \in \min \Pi(\Gamma)$. This proves inequality (3).

$$\begin{aligned} h(A) &= h(q_1) + \sum_{i=2}^{t} h(q_i \mid q_{i-1} \dots q_1) + h(p_1 \mid q_t \dots q_1) + \sum_{i=2}^{k-1} h(p_i \mid p_{i-1} \dots p_1 q_t \dots q_1) && (1) \\ &\leq \sum_{i=1}^{t} h(q_i) + h(p_1) + \sum_{i=2}^{k-1} h(p_i \mid p_1 q_t \dots q_1) && (2) \\ &\leq \sum_{i=1}^{t} h(q_i) + h(p_1) + \sum_{i=2}^{k-1} h(p_i \mid q_t \dots q_1) - (k-2) && (3) \\ &\leq \sum_{i=1}^{t} h(q_i) + \sum_{i=1}^{k-1} h(p_i) - (k-2). && (4) \end{aligned}$$

Therefore, $\sum_{p \in A} h(p) \geq h(A) + k - 2 \geq k + s - 2$, and hence there is some $p \in A$ that satisfies $h(p) \geq (k+s-2)/(k+t-1)$. □

Theorem 4 can be used to find lower bounds on $\kappa(\Gamma)$ for every bipartite access structure Γ, because $\kappa(\Gamma) \geq \kappa(\Gamma')$ for every minor Γ' of Γ whose minimal points are in the conditions of Theorem 4. In addition, other lower bounds can be obtained from that result by changing the order of the parts in the bipartition of the set of participants. The best lower bound for a given bipartite access strucutre that is obtained in this way from Theorem 4 is in most situations better than the one that can be derived from [35, Proposition 4.1]. This occurs, for instance, for the bipartite access structures with two minimal points that are discussed in the following. Nevertheless, for the particular case of bipartite weighted threshold structures, our bound coincides with the one from [35, Proposition 5.4].

We apply next Theorem 4 to find a lower bound for the particular case of bipartite access structures having exactly two minimal points.

Corollary 1 *Let $\{(x_1,y_1),(x_2,y_2)\}$ be the set of minimal points of a bipartite access structure Γ. If $x_1 = y_2 = 0$, then Γ is ideal. If $x_1 > 0$, then*

$$\kappa(\Gamma) \geq 2 - \frac{1}{x_2 - x_1}.$$

Proof Suppose that $x_1 > 0$ and consider $B \subseteq P$ with $\Pi(B) = (x_1 - 1, y_1 - 1)$. The minimal points of the minor Γ/B are $\{(1,1),(x_2 - x_1 + 1, 0)\}$. By Theorem 4,

$$\kappa(\Gamma/B) \geq \frac{2(x_2 - x_1) - 1}{x_2 - x_1}.$$

□

The exact values of the optimal complexities of the bipartite access structures with minimal points $\min \Pi(\Gamma) = \{(1,1),(x_2,0)\}$ such that $|X| = x_2$ and $|Y| = 1$ were given in [33]. Specifically, for those access structures,

$$\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 2 - \frac{1}{x_2 - 1}.$$

Next theorem generalizes this result. Observe that the number of participants in each part can be arbitrarily large.

Theorem 5 *Let Γ be a bipartite access structure with set of minimal points $\{(x_1,y_1),(x_2,0)\}$, where $x_1 > 0$. Then*

$$\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = 2 - \frac{1}{x_2 - x_1}.$$

Proof By Corollary 1, $\kappa(\Gamma) \geq 2 - 1/(x_2 - x_1)$. The proof is concluded by constructing a linear secret sharing scheme Σ for Γ whose complexity is equal to this lower bound on $\kappa(\Gamma)$, because then $\lambda(\Gamma) \leq 2 - 1/(x_2 - x_1) \leq \kappa(\Gamma)$.

Set $N_1 = |X|$ and $N_2 = |Y|$ and consider a finite field $\mathbb{K}$ with $|\mathbb{K}| > \max\{N_1 + x_2 - x_1, N_2\}$. The scheme Σ is constructed by combining two $\mathbb{K}$-linear secret sharing schemes with access structure Γ.

In the first scheme, the secret value $k \in \mathbb{K}$ is distributed into shares among the participants in X by using Shamir's (x_2, N_1)-threshold scheme. In addition, Shamir's (x_1, N_1)-threshold scheme is used to distribute a random value $k_1 \in \mathbb{K}$ into shares among the participants in X, and the value $k_2 = k - k_1$ is distributed into shares among the participants in Y by Shamir's (y_1, N_2)-threshold scheme. We obtain in this way a $\mathbb{K}$-linear secret sharing scheme Σ_1 for Γ such that the secret value and the shares of the participants in Y are elements in $\mathbb{K}$, while the shares of the participants in X are in $\mathbb{K}^2$.

The second linear secret sharing scheme Σ_2 for Γ is described in the following. Consider a set Z of virtual participants with $|Z| = x_2 - x_1$. The secret value $k \in \mathbb{K}$ is distributed into shares among the participants in $X \cup Z$ by using Shamir's $(x_2, N_1 + x_2 - x_1)$-threshold scheme, and the share $s_i \in \mathbb{K}$ of every virtual participant $i \in Z$ is distributed among the participants in Y by using Shamir's (y_1, N_2)-threshold scheme. Clearly, Σ_2 is a $\mathbb{K}$-linear secret sharing scheme for Γ in which the secret value and the shares of the participants in X are taken from the finite field $\mathbb{K}$ while the participants in Y receive a share in $\mathbb{K}^{x_2 - x_1}$.

Finally, a $\mathbb{K}$-linear secret sharing scheme Σ is constructed by combining the scheme Σ_2 with $x_2 - x_1 - 1$ copies of the scheme Σ_1. Specifically, the secret value in the scheme Σ is a vector $(k_1, k_2, \ldots, k_{x_2 - x_1}) \in \mathbb{K}^{x_2 - x_1}$. Every one of the values $k_1, k_2, \ldots, k_{x_2 - x_1 - 1}$ is distributed by using the scheme Σ_1, while the value $k_{x_2 - x_1}$ is distributed by using the scheme Σ_2. Observe that the share of a participant in X is formed by $2(x_2 - x_1 - 1) + 1 = 2(x_2 - x_1) - 1$ elements in $\mathbb{K}$, while the share of a participant in Y is formed by $(x_2 - x_1 - 1) + (x_2 - x_1) = 2(x_2 - x_1) - 1$ elements in $\mathbb{K}$. Therefore, $\sigma(\Sigma) = (2(x_2 - x_1) - 1)/(x_2 - x_1)$. □

6 A Linear Programming Approach

To find the value of $\kappa(\Gamma)$ for a given access structure Γ can be formulated as a linear programming problem [16,17,36]. Observe that, by ordering in some way the elements in $\mathcal{P}(Q)$, a polymatroid $\mathcal{S} = (Q, h)$ can be represented as a vector $(h(A))_{A \subseteq Q} \in \mathbb{R}^k$, where $k = |\mathcal{P}(Q)| = 2^{n+1}$. By considering an additional variable v, the value of $\kappa(\Gamma)$ can be computed by solving the optimization problem

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & (h(A))_{A \subseteq Q} \text{ is a } \Gamma\text{-polymatroid and} \\ & v \geq h(\{i\}) \text{ for every } i \in Q. \end{array}$$

Clearly, the constraints on the vector $(v, (h(A))_{A \subseteq Q}) \in \mathbb{R}^{k+1}$ are given by linear inequalities, and hence this is actually a linear programming problem. In general, the number of variables and the number of constraints grow exponentially with the number of participants. In addition, as it was pointed out in [16, 17], the system of conditions is overdetermined, even after reducing it by using the characterization of polymatroids given by Matúš [31].

Nevertheless, if Γ is bipartite, the optimization problem to determine $\kappa(\Gamma)$ can be restricted to $(X, Y, \{p_0\})$-partite Γ-polymatroids by Proposition 4. Such a polymatroid $\mathcal{S} = (Q, h)$ is determined by its reduced rank function $\widehat{h}\colon \mathbf{P} \times \{0,1\} \to \mathbb{R}$, where $\widehat{h}(x, y, z) = h(A)$ for every $A \subseteq Q$ with $\Pi(A) = (x, y, z)$. Therefore, the value of $\kappa(\Gamma)$ for a bipartite access structure Γ can be determined by solving the linear programming problem

$$\begin{array}{ll} \text{Minimize} & v \\ \text{subject to} & (\widehat{h}(\mathbf{x}))_{\mathbf{x} \in \mathbf{P} \times \{0,1\}} \text{ determines a } \Pi_0\text{-partite } \Gamma\text{-polymatroid and} \\ & v \geq \widehat{h}(1,0,0) \text{ and } v \geq \widehat{h}(0,1,0). \end{array}$$

In this way, the number of variables has been reduced from $2^{N_1 + N_2} + 1$ to $2(|X| + 1)(|Y| + 1) + 1$. In addition, the number of constraints grows also polynomially on the number of participants, because it is enough to consider the ones given by the conditions in Proposition 5. By using this linear programming approach, we have computed the value of $\kappa(\Gamma)$ for several bipartite access structures.

For instance, some bipartite access structures such that $\min \Pi(\Gamma) = \{(x_1, y_1), (x_2, y_2)\}$ with $x_1, y_2 > 0$ and $y_2 - y_1 \leq x_2 - x_1$ have been checked, and in all of them the lower bound in Corollary 1 is attained.

Because of that, we conjecture that $\kappa(\Gamma) = 2 - 1/(x_2 - x_1)$ for every such access structure. Recall that this fact has been proved in Theorem 5 for the case $y_2 = 0$.

A gap in the values of the parameter κ was proved in [29]. Namely, there does not exist any access structure Γ with $1 < \kappa(\Gamma) < 3/2$. The existence of other gaps in the values of this parameter is thus a natural question. For instance, from the results in [16–18,30], one could conjecture that, if $\kappa(\Gamma) < 2$, then $\kappa(\Gamma) = 2 - 1/s$ for some positive integer s. Moreover, the values of $\kappa(\Gamma)$ for the bipartite access structures with two minimal points seem to confirm this conjecture. Nevertheless, we have found some bipartite access structure that do not satisfy this property. Specifically, by solving the corresponding linear programming problem, we obtained that the bipartite access structure Γ with minimal points $\{(1,4),(3,3),(5,1)\}$ has $\kappa(\Gamma) = 22/13$. Another example is the structure with minimal points $\{(1,4),(4,3),(6,1)\}$, which satisfies $\kappa(\Gamma) = 99/53$.

Finally, the value of the parameter κ has been computed for a number of bipartite access structures whose families of minimal points are of the form

$$\{(x_i, y_i) = (1 + m(i-1), r - i) \,:\, i = 1, \ldots, r\}$$

for some integer $m \geq 2$. For all of them, $\kappa(\Gamma)$ equals the lower bound in Theorem 4.

7 Conclusion and Open Problems

In the previous sections, some ideas and techniques to study the optimization of secret sharing schemes with bipartite access structure have been presented. They improve the first results on this topic that were presented in [35].

Nevertheless, the problem is very far from being solved for this family. For instance, some fundamental questions about the construction of optimal linear secret sharing schemes for bipartite access structures remain open. Namely, it is not known if there exists some separation between the parameters κ and λ among the bipartite access structures. But even more basic questions have not been solved. For instance, it is not known whether the value of $\lambda(\Gamma)$ depends only on the minimal points of Γ or it depends as well on the number of participants in each part.

Let Γ be a bipartite access structure such that there exists a $\mathbb{K}$-linear secret sharing scheme Σ for Γ with complexity $\sigma(\Sigma) = \kappa(\Gamma)$. In this situation, $\kappa(\Gamma) = \lambda(\Gamma)$. Moreover, by using a similar argument as in the proof of Proposition 4, we can assume that $\mathcal{S}(\Sigma)$ is a Π_0-partite polymatroid. In particular $\mathcal{S}(\Sigma) \setminus \{p_0\}$ is a $\mathbb{K}$-linearly entropic bipartite polymatroid. Therefore, characterizing the linearly entropic bipartite polymatroids and, by extension, the representable integer bipartite polymatroids, are interesting open problems for the optimization of bipartite secret sharing schemes.

We prove in the following that the *uniform* integer polymatroids, which are precisely the m-partite integer polymatroids with $m = 1$, are representable. In addition, all m-partite matroids with $m \leq 3$ are representable [21]. Unfortunately, this does not apply to bipartite polymatroids. Actually, we present a bipartite integer polymatroid that is not entropic, and hence it is not representable.

A polymatroid $\mathcal{S} = (Q, h)$ is said to be *uniform* if the value of $h(X)$ depends only on the cardinality of X, that is, $h(X) = h(Y)$ if $|X| = |Y|$. A uniform polymatroid is determined by the values $h_0, h_1, \ldots, h_n$, where $n = |Q|$ and $h(X) = h_i$ if $|X| = i$. For $i = 1, \ldots, n$, consider the values $\delta_i = h_i - h_{i-1}$, which form the *increment vector* $(\delta_1, \ldots, \delta_n)$ of $\mathcal{S}$. A sequence $(h_i)_{0 \leq i \leq n}$ of real numbers determines a uniform polymatroid if and only if $h_0 = 0$ and $\delta_1 \geq \cdots \geq \delta_n \geq 0$. Obviously, a uniform polymatroid is determined by its increment vector, and it is an integer polymatroid if and only if its increment vector has integer components. If $\mathcal{S} = (Q, h)$ is a uniform matroid, then there exists an integer r with $0 \leq r \leq |Q|$ such that the increment vector of $\mathcal{S}$ satisfies $\delta_i = 1$ if $i \leq r$ and $\delta_i = 0$ otherwise. We notate $U_{r,n}$ for such a uniform matroid. It is well known that the uniform matroid $U_{r,n}$ is $\mathbb{K}$-representable for every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n$.

Proposition 10 *Every uniform integer polymatroid is a sum of uniform matroids.*

Proof Let $\mathcal{S} = (Q, h)$ be a uniform integer polymatroid, with increment vector $(\delta_1, \ldots, \delta_n)$. Then there exists a sequence of integers $n = r_0 \geq r_1 \geq \cdots \geq r_{\delta_1} \geq r_{\delta_1+1} = 0$ such that $r_{\delta_i} \geq i > r_{\delta_i+1}$ for every $i = 1, \ldots, n$. We claim that $\mathcal{S} = U_{r_1,n} + \cdots + U_{r_{\delta_1},n}$. We have to check that $\delta_i = \delta_i^1 + \cdots + \delta_i^{\delta_1}$ for every $i = 1, \ldots, n$, where δ^k is the increment vector of the uniform matroid $U_{r_k,n}$. Indeed, recall that $\delta_i^k = 1$ if $r_k \geq i$ and $\delta_i^k = 0$ otherwise. $\square$

Theorem 6 *Every uniform integer polymatroid is representable, and hence entropic.*

Proof Straightforward from Propositions 3 and 10 and the fact that the uniform matroid $U_{r,n}$ is representable over every finite field with at least n elements. □

Proposition 11 *There exist bipartite integer polymatroids that are not entropic.*

Proof The Vamos matroid V is the matroid of dimension four on the set $\{1,\ldots,8\}$ with rank function r such that $r(A) = 4$ for every $A \subseteq \{1,\ldots,8\}$ of size 4 except $\{1,2,3,4\}$, $\{1,2,5,6\}$, $\{3,4,5,6\}$ $\{3,4,7,8\}$ and $\{5,6,7,8\}$. Take $a = \{1,2\}$, $b = \{3,4\}$, $c = \{5,6\}$, $d = \{7,8\}$, and the set $Q = \{a,b,c,d\}$. Let $\mathcal{S} = (Q,h)$ be the integer polymatroid whose rank function is derived from the rank function of V. It is not difficult to check that $\mathcal{S}$ is Π-partite with $\Pi = (\{a,b\},\{c,d\})$. Matúš [32] pointed out that the rank function of $\mathcal{S}$ violates the non-Shannon information inequality given by Zhang and Yeung [43]. This implies that $\mathcal{S}$ is not entropic. □

Nevertheless, Proposition 11 does not exclude the possibility that $\kappa(\Gamma) = \lambda(\Gamma)$ for every bipartite access structure. Separation results between these parameters could be obtained by adding Ingleton inequality [25], an information inequality that applies only to linear random variables, to the linear programming approach that was presented in Section 6. In this way, lower bounds on $\lambda(\Gamma)$ would be obtained and, maybe, a bipartite access structure with $\kappa(\Gamma) < \lambda(\Gamma)$ could be found. Similarly, the use of non-Shannon information inequalities, as for instance the one from [43], could provide some separation result between the parameters κ and σ for bipartite access structures.

As a consequence of the results in [21,35], the existence of a vector space secret sharing scheme for a multipartite access structure Γ does not depend on the number of participants in every part, but only on the minimal points. The same applies to the parameter κ, as we proved in Proposition 8 for the bipartite case. The validity of a similar result for the parameters σ and λ is an open problem.

Actually, much easier questions remain open about the optimization of bipartite secret sharing schemes. For instance, even though partial results have been presented in Corollary 1 and Theorem 5, the problem of determining κ, σ and λ has not been solved for bipartite access structures with only two minimal points.

References

1. A. Beimel, Y. Ishai. On the power of nonlinear secret sharing schemes. *SIAM J. Discrete Math.*, **19** (2005), 258–280.
2. A. Beimel, N. Livne, C. Padró. Matroids Can Be Far From Ideal Secret Sharing. *Theory of Cryptography Conference, TCC 2008. Lecture Notes in Comput. Sci.*, **4948** (2008) 194–212.
3. A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *SIAM J. Discrete Math.* **22** (2008) 360–397.
4. A. Beimel and E. Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.*, **34** (2005) 1196–1215.
5. A. Beimel, E. Weinreb. Monotone Circuits for Monotone Weighted Threshold Functions. *Information Processing Letters* **97** (2006) 12–18.
6. G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.*, **48** (1979) 313–317.
7. C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Des. Codes Cryptogr.* **11** (1997) 107–122.
8. C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology - CRYPTO'92. Lecture Notes in Comput. Sci.* **740** (1993) 148–167.
9. C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology* **8** (1995) 39–64.
10. E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.*, **9** (1989) 105–113.
11. E.F. Brickell and D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, **4** (1991) 123–134.
12. E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology* **5** (1992) 153–166.
13. R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* **6** (1993) 157–168.
14. T.M. Cover, J.A. Thomas. *Elements of Information Theory*, 2nd ed. Wiley, New York, 2006.
15. L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.
16. L. Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptogr.* **53** (2009) 195–209.
17. L. Csirmaz, P. Ligeti. On an infinite family of graphs with information ratio $2 - 1/k$. *Computing* **85** (2009) 127-136.
18. L. Csirmaz, G. Tardos. Secret sharing on trees: problem solved. Preprint (2009). Available at *Cryptology ePrint Archive*, `http://eprint.iacr.org/2009/071`.

19. M. van Dijk. On the information rate of perfect secret sharing schemes. *Des. Codes Cryptogr.* **6** (1995) 143–169.
20. M. van Dijk, T. Kevenaar, G. Schrijen, P. Tuyls. Improved constructions of secret sharing schemes by applying (λ, ω)-decompositions. *Inf. Process. Lett.* **99** (2006) 154–157.
21. O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *Advances in Cryptology, EUROCRYPT 2007, Lecture Notes in Comput. Sci.*, **4515** (2007) 448–465. The full version of this paper is available at the *Cryptology ePrint Archive*, Report **2006/292**, `http://eprint.iacr.org/2006/292`.
22. O. Farràs and C. Padró. Ideal Hierarchical Secret Sharing Schemes. *Seventh IACR Theory of Cryptography Conference, TCC 2010, Lecture Notes in Comput. Sci.* **5978** (2010) 219–236. The full version of this paper is available at the *Cryptology ePrint Archive*, Report **2009/141**, `http://eprint.iacr.org/2009/141`.
23. S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control*, **39** (1978) 55–72.
24. A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Proceedings of 30th ACM Symposium on the Theory of Computing, STOC 1998* (1998) 429–437.
25. A. W. Ingleton. Conditions for representability and transversability of matroids. In *Proc. Fr. Br. Conf 1970*, pages 62–67. Springer-Verlag, 1971.
26. M. Ito and A. Saito and T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.*, (1987) 99–102.
27. W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.
28. W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Des. Codes Cryptogr.* **9** (1996) 267–286.
29. J. Martí-Farré and C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120.
30. J. Martí-Farré, C. Padró, L. Vázquez. Optimal Complexity of Secret Sharing Schemes with Four Minimal Qualified Subsets. *Des. Codes Cryptogr.* Online First (2010). DOI: 10.1007/s10623-010-9446-0.
31. F. Matúš. Adhesivity of polymatroids. *Discrete Math.* **307** (2007) 2464–2477.
32. F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. on Information Theory* **53** (2007) 320–330.
33. J.R. Metcalf-Burton. Information Rates of Minimal Non-Matroid-Related Access Structures. `arxiv.org/pdf/0801.3642`
34. J.R. Metcalf-Burton. Improved Upper Bounds for the Information Rates of the Secret Sharing Schemes Induced by the Vamos Matroid. *Discrete Math.* **311** (2011) 651–662.
35. C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. Inform. Theory*, **46** (2000) 2596–2604.
36. C. Padró, L. Vázquez. Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Ninth Latin American Theoretical Informatics Symposium, LATIN 2010, Lecture Notes in Computer Science* **6034** (2010) 344–355.
37. A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.
38. G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO'88, Lecture Notes in Comput. Sci.*, **403** (1990) 390–448.
39. D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.
40. D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, **40** (1994) 118-125.
41. T. Tassa. Hierarchical Threshold Secret Sharing. *J. Cryptology* **20** (2007) 237-264.
42. T. Tassa and N. Dyn. Multipartite Secret Sharing by Bivariate Interpolation. *J. Cryptology* **22** (2009) 227–258.
43. Z. Zhang, R.W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. Inform. Theory* **44** (1998) 1440–1452.