Secret Sharing Schemes with Bipartite Access Structure [*]

Carles Padró and Germán Sáez

Dep. Matemàtica Aplicada i Telemàtica, Universitat Politècnica de Catalunya
Campus Nord, c/Jordi Girona, 1-3, 08034 Barcelona
e-mail: matcpl@mat.upc.es, german@mat.upc.es

Abstract. We study the information rate of secret sharing schemes whose access structure is bipartite. In a bipartite access structure there are two classes of participants and all participants in the same class play an equivalent role in the structure. We characterize completely the bipartite access structures that can be realized by an ideal secret sharing scheme. Both upper and lower bounds on the optimal information rate of bipartite access structures are given.

1 Introduction

A *secret sharing scheme* is a method to distribute a secret value k among a set of participants P in such a way that only qualified subsets of P are able to reconstruct the value of k, while non-qualified subsets can not obtain any information about the value of the secret. Secret sharing schemes were introduced by Blakley [2] and Shamir [12]. A comprehensive introduction to secret sharing schemes can be found in [14, 16, 13].

The family of qualified subsets $\Gamma \subset 2^P$ is called the *access structure*. In general, access structures are considered to be *monotone*, that is, any superset of a qualified subset must be qualified.

In a secret sharing scheme Σ for the access structure Γ, given a secret value $k \in \mathcal{K}$, a special participant $D \notin P$, called the *dealer*, gives to every participant $p \in P$ a *share* $s_p \in \mathcal{S}_p$ in such a way that only the participants that form a subset in Γ can reconstruct the value of k from their shares. Any other subset of participants can not obtain any information about the value of k.

Since the security of a system depends on the amount of information that must be kept secret, the size of the shares given to the participants is an important point in the design of secret sharing schemes. Besides, if the shares are too large, the memory requirements for the participants will be too strong and the algorithms used to compute the shares will become inefficient. Therefore, one of the basic parameters in secret sharing is the *information rate* $\rho(\Sigma, \Gamma, \mathcal{K})$ of the scheme, which is defined to be the ratio between the length (in bits) of the secret and the maximum length of the shares given to the participants. That is,

$$\rho(\Sigma, \Gamma, \mathcal{K}) = \frac{\log |\mathcal{K}|}{\max_{p \in P} \log |\mathcal{S}_p|}.$$

[*] This work was partially supported by CICYT under project TIC97-0963

A secret sharing scheme is said to be *ideal* if its information rate is equal to one, which is the maximum possible value. We say that an access structure Γ is *ideal* if there exists an ideal scheme for Γ. The *optimal information rate* of an access structure Γ is

$$\rho^*(\Gamma) = \sup(\rho(\Sigma, \Gamma, \mathcal{K})),$$

where the supremum is taken over all possible sets of secrets $\mathcal{K}$ with $|\mathcal{K}| \geq 2$ and all secret sharing schemes Σ with access structure Γ. Of course, the optimal information rate of an ideal access structure is equal to one.

This paper deals with two problems that have received considerable attention: to characterize ideal access structures and to find bounds on the optimal information rate.

A necessary condition for an access structure to be ideal was given in [7] in terms of matroids. A sufficient condition is obtained from the vector space construction [6], which is a method to construct ideal secret sharing schemes. Several techniques have been introduced in [8, 5, 15] in order to construct secret sharing schemes for some families of access structures. These schemes provide lower bounds on the optimal information rate. Upper bounds have been found by using some tools from Information Theory [9, 4, 3]. A general method to find upper bounds on the optimal information rate is given in [3], while the techniques that were used in previous works only were applicable to particular access structures.

The above-mentioned problems have been widely studied for a special class of access structures, the structures defined by graphs [8, 5, 9]. Ideal access structures in this class are completely characterized: a connected graph defines an ideal access structure if and only if it is a complete multipartite graph [7]. Besides, the vector space construction can be applied on any ideal access structure defined by a graph. If a graph G is not a complete multipartite graph, the optimal information rate of the structure defined by G is at most $2/3$ [4]. A general lower bound on the optimal information rate of access structures defined by graphs was given in [15]. This lower bound is proved to be tight in [3].

In this paper, we are concerned in another class of access structures: the *bipartite access structures*. In a bipartite access structure Γ, there is a partition of the sets of participants, $P = X \cup Y$, such that, if σ is a permutation on P with $\sigma(X) = X$ and $\sigma(Y) = Y$, then $\sigma(\Gamma) = \Gamma$. That is, in a bipartite structure there are two classes of participants and all participants in the same class play an equivalent role in the structure. It is not difficult to imagine some applications of secret sharing in which such access structures appear. Some examples of these applications can be found among the so called *multilevel* and *multipart* schemes studied by Simmons in [13]. Weighted threshold access structures with two weights are other interesting examples of bipartite access structures. In a weighted threshold structure, each participant $p \in P$ has its own weight $\omega(p) \geq 0$ and a subset $A \subset P$ is qualified if and only if $\omega(A) = \sum_{p \in A} \omega(p) \geq t$, where $t \geq 0$ is the *threshold* of the structure. A bipartite access structure is obtained if there are only two possible values $a, b \geq 0$ for the weights of the participants. Weighted structures were first considered by Shamir [12] in his introductory paper about secret sharing. Even though their interesting applications, weighted threshold access structures have not received the attention they deserve. A particular class of bipartite access structure was considered in [1].

We characterize the ideal bipartite access structures and present methods to find both lower and upper bounds on the optimal information rate of bipartite structures. The main definitions and the notation that will be used in this paper are given in Section 2. We present also in this section a generalization of the method to find upper bounds for general access structures given in [3]. Ideal bipartite access structures are completely characterized in Section 3. Besides, we prove that there exists a vector space secret sharing scheme for any ideal bipartite structure. We also prove that the optimal information rate of a non-ideal bipartite structure is at most 2/3. Two techniques to find lower bounds on the optimal information rate of any bipartite structure are presented in Section 4. We prove that these bounds are tight in the sense that we can find bipartite access structures whose optimal information rate is arbitrarily close to its best lower bound. In order to do that, we compute upper bounds using our generalization of the method given in [3].

2 Preliminaries

Let Γ be an access structure on a set of participants P that is partitioned in two parts, $P = X \cup Y$. We say that Γ is a *(X, Y)-bipartite access structure* if $\sigma(\Gamma) = \Gamma$ for any permutation σ on P with $\sigma(X) = X$ and $\sigma(Y) = Y$. A *(N_1, N_2)-bipartite access structure* is a (X, Y)-bipartite access structure with $|X| = N_1$ and $|Y| = N_2$.

Given a partition $P = X \cup Y$ of the set P, for any subset $A \subset P$, we consider the point $\pi(A) = (x(A), y(A)) \in \mathbb{Z} \times \mathbb{Z}$, where $x(A) = |A \cap X|$ and $y(A) = |A \cap Y|$. Given a (X, Y)-bipartite access structure Γ, let us consider the region

$$\pi(\Gamma) = \{\pi(A) \mid A \in \Gamma\} \subset \mathbb{Z} \times \mathbb{Z}.$$

It is easy to see that $A \in \Gamma$ if and only if $\pi(A) \in \pi(\Gamma)$. Therefore, Γ is determined by the region $\pi(\Gamma) \subset \mathbb{Z} \times \mathbb{Z}$. Moreover, if Γ_0 is the family of the minimal qualified subsets of Γ, we consider

$$\Pi_0 = \pi(\Gamma_0) = \{(x_1, y_1), (x_2, y_2), \dots, (x_r, y_r)\}.$$

Of course, Γ is determined by the points in Π_0, because $A \in \Gamma$ if and only if, for some $i = 1, \dots, r$, $x(A) \geq x_i$ and $y(A) \geq y_i$. The elements of Π_0 will be called the *minimal points* of Γ. We can suppose that $0 \leq x_1 < x_2 < \cdots < x_r$ and, in this situation, it is not difficult to see that $y_1 > y_2 > \cdots > y_r \geq 0$. From now on, we are going to order the set of minimal points of any bipartite access structure in this way.

The *vector space construction* is a useful method to construct ideal schemes that were introduced by Brickell [6]. Let P be a set of n participants. Let Γ be an access structure on P and $D \notin P$ the dealer. Γ is said to be a *vector space* *access structure* if, for some vector space $E = K^r$ over a finite field $K = GF(q)$, there exists a function

$$\psi : P \cup \{D\} \longrightarrow E$$

such that $A \in \Gamma$ if and only if the vector $\psi(D)$ can be expressed as a linear combination of the vectors in the set $\psi(A) = \{\psi(p) \mid p \in A\}$. If Γ is such a vector space access structure, we can construct an ideal secret sharing scheme for Γ with set of secrets $\mathcal{K} = K$ (see [6] or [14] for proofs). Given a secret value $k \in K$, the dealer takes at random an element $\mathbf{v} \in E$, such that $\mathbf{v} \cdot \psi(D) = k$. The share of a participant $p \in P$ is $s_p = \mathbf{v} \cdot \psi(p)$. A scheme constructed in this way is called a *vector space secret sharing scheme*. The Shamir's scheme [12] can be seen as a vector space secret sharing scheme [14].

Blundo et al [3] presented a method to find upper bounds on the optimal information rate. We present here a slight generalization of this method that will be used later.

Let Γ be an access structure on a set of participants P. We say that a sequence $B_1, B_2, \ldots, B_m$, where

$$\emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_m \subset P,$$

is *independent* if

1. $B_m \notin \Gamma$.
2. For all $i = 1, 2, \ldots, m$, there exists a set $X_i \subset P$ such that $B_i \cup X_i \in \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$, where $B_0 = \emptyset$.

We say that a set $A \supset \bigcup_{i=1}^{m} X_i$ makes the sequence $B_1, B_2, \ldots, B_m$ independent.

The proof of the following theorem is almost the same than the proof of Theorem 3.8 in [3].

Theorem 1. *Let Γ be an access structure on a set of participants P. Let $\emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_m \subset P$ be an independent sequence and $A \subset P$ a set that makes this sequence independent. Then,*

- *If $A \in \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|A|}{m+1}$.*
- *If $A \notin \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|A|}{m}$.*

3 Ideal Bipartite Access Structures

In this section, we characterize the bipartite access structures that admit an ideal scheme. We prove that a bipartite access structure is ideal if and only if it is a vector space access structure. Besides we prove that $\rho^*(\Gamma) \leq 2/3$ for any non-ideal bipartite access structure Γ.

Let $P = X \cup Y$ be a partition of the set of participants with $|X| = N_1$ and $|Y| = N_2$. Let n, n_1, n_2 be integers such that $0 \leq n_i \leq N_i$ and $n_i \leq n \leq n_1 + n_2$, where $i = 1, 2$. An access structure Γ on P is said to be a *quasi-threshold* (X, Y)-*bipartite access structure* if $\Gamma = \Omega_j(n, n_1, n_2) \subset 2^P$ for some $j = 1, 2, 3, 4$, where

- $A \in \Omega_1(n, n_1, n_2)$ if and only if $|A| \geq n$, or $x(A) \geq n_1$, or $y(A) \geq n_2$.
- $A \in \Omega_2(n, n_1, n_2)$ if and only if $|A| \geq n$ and $y(A) \geq n - n_1$, or $y(A) \geq n_2$.
- $A \in \Omega_3(n, n_1, n_2)$ if and only if $|A| \geq n$ and $x(A) \geq n - n_2$, or $x(A) \geq n_1$.
- $A \in \Omega_4(n, n_1, n_2)$ if and only if $|A| \geq n$, and $x(A) \geq n - n_2$, and $y(A) \geq n - n_1$.

The main goal of this section is to prove that a bipartite access structure Γ is ideal if and only if it is a quasi-threshold bipartite access structure.

We are going to prove first that any quasi-threshold bipartite access structure is a vector space access structure.

Theorem 2. *Let $P = X \cup Y$ be a bipartite set of participants with $|X| = N_1$ and $|Y| = N_2$. Let n, n_1, n_2, N_1, N_2 be integers such that $0 \leq n_i \leq N_i$ and $n_i \leq n \leq n_1 + n_2$, where $i = 1, 2$. Then, for any $j = 1, \ldots, 4$, there exists a positive integer $M = M(j, n, n_1, n_2, N_1, N_2)$ such that, if q is a prime power $q > M$ and E is an n-dimensional vector space over the finite field $GF(q)$, there exists a mapping $\psi : P \cup \{D\} \to E$ that defines in P the (X, Y)-bipartite access structure $\Omega_j(n, n_1, n_2)$.*

Sketch of the proof. Let us consider two subspaces $E_1, E_2 \subset E$ with $\dim(E_1) = n_1$, $\dim(E_2) = n_2$ and $E_1 + E_2 = E$. If q is large enough, it is possible to define the access structure $\Omega_4(n, n_1, n_2)$ by a mapping $\psi : P \cup \{D\} \to E$ with $\psi(X) \subset E_1$, $\psi(Y) \subset E_2$ and $\psi(D) \in E - (E_1 \cup E_2)$. In order to do that we have to find N_1 vectors in E_1 and N_2 vectors in E_2 in "general position". That is, in such a way that any set of n of those vectors with at least $n - n_2$ vectors in E_1 and $n - n_1$ vectors in E_2 is a basis of E. Besides, the vector $\psi(D)$ must not appear in any subspace generated by $n - 1$ of those vectors. The access structures $\Omega_j(n, n_1, n_2)$ for $j = 1, 2, 3$ can be defined by a similar mapping. The only difference is the position of the vector $\psi(D)$:

- if $j = 1$, then $\psi(D) \in E_1 \cap E_2$,
- if $j = 2$, then $\psi(D) \in E_2 - E_1$,
- if $j = 3$, then $\psi(D) \in E_1 - E_2$,

The complete proof can be found in the Appendix. □

The following lemma, which is not difficult to check, is used to prove the reciprocal of Theorem 2.

Lemma 3. *Let Γ be a bipartite access structure with set of minimal points*

$$\Pi_0 = \{(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)\}.$$

Then, if Γ is not a quasi-threshold bipartite access structure, one of the following situations occurs:

1. $x_1 = 0$ *and* $y_2 \neq y_1 - 1, 0$.
2. $y_r = 0$ *and* $x_{r-1} \neq x_r - 1, 0$.

3. *For some $i = 1, 2, \ldots, r-1$, $x_i \neq 0$, $y_{i+1} \neq 0$ and $(x_{i+1}, y_{i+1}) \neq (x_i + 1, y_i - 1)$.*

Theorem 4. *Let Γ be a bipartite access structure that is not a quasi-threshold bipartite access structure. Then, $\rho^*(\Gamma) \leq 2/3$.*

Proof. From Lemma 3, we can distinguish three cases.
Case 1: $x_1 = 0$ and $y_2 \neq y_1 - 1, 0$. If $(x_2, y_2) = (1,1)$, consider $B_1, B_2 \subset P$ such that $B_1 \subset B_2$, $\pi(B_1) = (0,1)$ and $\pi(B_2) = (0, y_1 - 1)$. Let us consider $p \in X$ and $q \in Y$ such that $q \notin B_2$. Then, if we take $X_1 = \{p\}$ and $X_2 = \{q\}$, the sequence $B_1 \subset B_2$ is independent. Since $A = \{p,q\} \in \Gamma$, we have that $\rho^*(\Gamma) \leq |A|/(m+1) = 2/3$. If $(x_2, y_2) \neq (1,1)$, we consider a sequence $B_1 \subset B_2 \subset B_3$ such that $\pi(B_1) = (x_2 - 1, y_2 - 1)$, $\pi(B_2) = (x_2 - 1, y_2)$ and $\pi(B_3) = (x_2 - 1, y_1 - 1)$. Let us consider $p \in X$ and $q \in Y$ such that $p, q \notin B_3$ and the subsets $X_1 = \{p,q\}$, $X_2 = \{p\}$ and $X_3 = \{q\}$. Then, the sequence $B_1 \subset B_2 \subset B_3$ is independent. Therefore, since $A = \{p,q\} \notin \Gamma$, we obtain $\rho^*(\Gamma) \leq |A|/m = 2/3$.
Case 2: $y_r = 0$, $x_{r-1} \neq x_r - 1, 0$. This case is symmetric to Case 1.
Case 3: for some $i = 1, 2, \ldots, r-1$, $x_i \neq 0$, $y_{i+1} \neq 0$ and $(x_{i+1}, y_{i+1}) \neq (x_i + 1, y_i - 1)$. If $y_{i+1} \neq y_1 - 1$, let us a sequence $B_1 \subset B_2 \subset B_3$ such that $\pi(B_1) = (x_{i+1} - 1, y_{i+1} - 1)$, $\pi(B_2) = (x_{i+1} - 1, y_{i+1})$ and $\pi(B_3) = (x_{i+1} - 1, y_i - 1)$. Let us take $X_1 = \{p,q\}$, $X_2 = \{p\}$, $X_3 = \{q\}$, where $p \in X$, $q \in Y$ and $p, q \notin B_3$. Then, the sequence $B_1 \subset B_2 \subset B_3$ is made independent by $A = \{p,q\} \notin \Gamma$. Therefore $\rho^*(\Gamma) \leq |A|/m = 2/3$. If $x_{i+1} \neq x_i + 1$, we can find analogously an independent sequence that proves that $\rho^*(\Gamma) \leq 2/3$. □

The following theorem summarizes the results of this section.

Theorem 5. *Let Γ be a bipartite access structure. Then, the following statements are equivalent:*

1. *Γ is a quasi-threshold bipartite access structure.*
2. *Γ is a vector space access structure.*
3. *Γ is an ideal access structure.*
4. *$\rho^*(\Gamma) > 2/3$.*

Observe that there does not exist any bipartite access structure whose optimal information rate is in the interval $(2/3, 1)$. We present in Section 4 a bipartite access structure with $\rho^*(\Gamma) = 2/3$.

Finally, observe that Theorem 5 is also true for the class of access structures defined by graphs if we put “multipartite complete graph” instead of “quasi-threshold bipartite access structure”.

4 Bounds on the Optimal Information Rate

We present in this section two techniques to find secret sharing schemes for bipartite access structures. Lower bounds on the optimal information rate of such access structures are obtained from these constructions. We prove that these bounds are tight in the sense that we can find bipartite access structures whose optimal information rate is arbitrarily close to the lower bound. In order to do that, we use upper bounds calculated from Theorem 1.

The first technique is a covering technique: we look for some ideal bipartite access structures such that can be combined in order to obtain the given structure. For example, let us consider the weighted threshold access structure Γ defined by a threshold $t = 40$ and a weight function $w : P \to \mathbb{R}^+$ such that, for any $p \in P$, $w(p) = 4$ or $w(p) = 5$. Then, $P = X \cup Y$, where $X = w^{-1}(4)$ and $Y = w^{-1}(5)$ and Γ is the (X, Y)-bipartite access structure defined by $\pi(\Gamma) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 4x + 5y \geq 40\}$. The set of minimal points of Γ is $\Pi_0(\Gamma) = \{(0,8), (2,7), (3,6), (4,5), (5,4), (7,3), (8,2), (9,1), (10,0)\}$. We observe that $\Gamma = \Gamma_1 \cup \Gamma_2$, where Γ_1 is the bipartite access structure with set of minimal points $\Pi_0(\Gamma_1) = \{(0,8), (2,7), (3,6), (4,5), (5,4)\}$ and Γ_2 is the (t, N)-threshold structure with $t = 10$. Since both Γ_1 and Γ_2 are ideal access structures, we can find a secret sharing scheme realizing Γ with information rate equal to $1/2$. Therefore, $\rho^*(\Gamma) \geq 1/2$.

In general, since any bipartite access structure with only one minimal point can be realized by an ideal scheme, a bipartite access structure Γ with r minimal points has optimal information rate $\rho^*(\Gamma) \geq 1/r$, because it is the union of r ideal access structures.

The second technique that we are going to use to find lower bounds on the optimal information rate is based on the next proposition.

Proposition 6. *Let a, b be positive integers and let Γ' be an ideal (aN_1, bN_2)-bipartite access structure. Let Γ be a (N_1, N_2)-bipartite access structure such that $(x, y) \in \pi(\Gamma)$ if and only if $(ax, by) \in \pi(\Gamma')$. Then, $\rho^*(\Gamma) \geq \min\{1/a, 1/b\}$.*

Proof. Let $P' = X' \cup Y'$ and $P = X \cup Y$ be, respectively, the sets of participants of the access structures Γ' and Γ. In order to define a secret sharing scheme Σ on Γ, we identify each participant $p_i \in X$, where $1 \leq i \leq N_1$, with a subset $S_i \subset X'$ with cardinality a in such a way that $X' = \cup_{i=1}^{N_1} S_i$. Equally, each participant $q_j \in Y$, where $1 \leq j \leq N_2$, is identified with a subset $T_j \subset Y'$ with cardinality b and, as before, $Y' = \cup_{j=1}^{N_2} T_j$. Let Σ' be an ideal scheme with access structure Γ' and set of secrets $\mathcal{K}$. The scheme Σ is defined as follows: given a secret $k \in \mathcal{K}$, the share of a participant $p_i \in X$ is formed by the a shares that correspond to the participants in the set $S_i' \subset X'$ by the ideal scheme Σ' and the share of a participant $q_j \in Y$ consists in the b shares of the participants in $T_j \subset Y'$. It is not difficult to see that Σ is a secret sharing scheme on Γ with information rate $\rho(\Sigma, \Gamma, \mathcal{K}) = \min\{1/a, 1/b\}$. □

This proposition can be used, for instance, to find lower bounds for the optimal information rate of weighted threshold access structures with two weights. These are bipartite access structures such that $(x, y) \in \pi(\Gamma)$ if and only if $ax + by \geq t$, where a, b, t are positive integers. We can suppose that $a \leq b$.

In this case, we can apply Proposition 6 being Γ' the $(t, aN_1 + bN_2)$-threshold structure. Then, $\rho^*(\Gamma) \geq 1/b$.

In order to prove that the lower bounds obtained by these two techniques are in some cases tight, we consider, for any positive integers r, b, the weighted access structure $\Gamma_{r,b}$ defined by the equation $x + by \geq rb$.

From Proposition 6, $\rho^*(\Gamma_{r,b}) \geq 1/b$. On the other hand, the set of minimal points of $\Gamma_{r,b}$ is $\Pi_0(\Gamma_{r,b}) = \{(kb, r-k) \in \mathbb{Z} \times \mathbb{Z} \,|\, 0 \leq k \leq r\}$. Let Γ_0 be the bipartite access structure whose set of minimal points is $\{(0,r),(rb,0)\}$. For any $k = 1, \ldots, r-1$, we consider Γ_k such that $(kb, r-k)$ is its only minimal point. Observe that, for any $k = 0, 1, \ldots, r-1$, Γ_k is and ideal access structure and, besides, $\Gamma_{r,b} = \cup_{k=0}^{r-1} \Gamma_k$. Therefore, $\rho^*(\Gamma_{r,b}) \geq 1/r$.

In order to find an upper bound on $\rho^*(\Gamma_{r,b})$, let us consider the sequence $B_1 \subset B_2 \subset \cdots \subset B_{rb-1}$, where $\pi(B_j) = (j, 0)$. Let us take X_1 such that $X_1 \cap B_1 = \emptyset$ and $\pi(X_1) = (b-1, r-1)$ and $X_{kb+s} \subset X_1$, where $0 \leq k \leq r-1$ and $0 \leq s \leq b-1$, such that $X_{kb+s} \cap B_{kb+s} = \emptyset$ and $\pi(X_{kb+s}) = (b-s, r-k-1)$. Then $A = X_1 \notin \Gamma$ makes independent the sequence $B_1 \subset B_2 \subset \cdots \subset B_{rb-1}$. Therefore,

$$\max\left\{\frac{1}{r}, \frac{1}{b}\right\} \leq \rho^*(\Gamma_{r,b}) \leq \frac{b+r-2}{rb-1}$$

This lower bound is tight because for any positive integer r and for any $\epsilon > 0$, there exists a positive integer b such that

$$\frac{1}{r} \leq \rho^*(\Gamma_{r,b}) \leq \frac{1}{r} + \epsilon.$$

On the other hand, if we fix b, for any $\epsilon > 0$ we can find a value of r such that

$$\frac{1}{b} \leq \rho^*(\Gamma_{r,b}) \leq \frac{1}{b} + \epsilon.$$

Finally, we present a bipartite access structure Γ such that $\rho^*(\Gamma) = 2/3$. Let Γ be a (N_1, N_2)-bipartite access structure with set of minimal points $\Pi_0 = \{(0,3),(1,1)\}$. Let us consider the ideal $(2N_1, N_2)$-bipartite access structure $\Gamma' = \Omega_4(3,2,3)$ with set of minimal points $\Pi'_0 = \{(0,3),(1,2),(2,1)\}$. It is clear that $(x,y) \in \pi(\Gamma)$ if and only if $(2x, y) \in \pi(\Gamma')$. Let Σ' be an ideal scheme with access structure Γ' and set of secrets $\mathcal{K}$. Let Σ_1 be the secret sharing scheme with access structure Γ and set of secrets $\mathcal{K}$ contructed from Σ' by using the idea in the proof of Proposition 6. Then, in the scheme Σ_1, each participant $p \in X$ receives as its share two elements in $\mathcal{K}$, that are the shares corresponding to two participants in the scheme Σ', and the shares for the participants in Y are taken from $\mathcal{K}$. On the other hand, $\Gamma = \Gamma_1 \cup \Gamma_2$, where the only minimal point of Γ_1 is $(0,3)$ and the only minimal point of Γ_2 is $(1,1)$. We consider the scheme Σ_2 for Γ with set of secrets $\mathcal{K}$ defined from ideal schemes for Γ_1 and Γ_2. Since the participants in X do not appear in Γ_1, their shares are taken from $\mathcal{K}$. The share of a participant in Y is taken from $\mathcal{K}^2$. Finally, let us consider the scheme Σ for Γ defined as follows: given a secret $(k_1, k_2) \in \mathcal{K}^2$, the dealer distributes k_1 using Σ_1 and k_2 using Σ_2. Every participant receives a share in $\mathcal{K}^3$. Therefore, $\rho^*(\Gamma) \geq 2/3$. From Theorem 4, $\rho^*(\Gamma) \leq 2/3$. Then, $\rho^*(\Gamma) = 2/3$.

References

1. A. Beutelspacher and F. Wettl. On 2–Level Secret Sharing. *Designs, Codes and Cryptography* **3** (1993) 127–134.
2. G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings* **48** (1979) 313-317.
3. C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. Tight Bounds on the Information Rate of Secret Sharing Schemes. *Designs, Codes and Cryptography* **11** (1997) 107–122.
4. 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 Computer Science* **740** 148–167. Springer-Verlag.
5. C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph Decompositions and Secret Sharing Schemes. *J. Cryptology* **8** (1995) 39–64.
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. E.F. Brickell and D.R. Stinson. Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes. *J. Cryptology* **5** (1992) 153–166.
9. R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro. On the Size of Shares of Secret Sharing Schemes. In *Advances in Cryptology-CRYPTO 91*, Lecture Notes in Computer Science **576**, Springer-Verlag, 101–113. To appear in *J. Of Cryptology.*
10. M. Ito, A. Saito and T, Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87* (1987) 99–102.
11. E.D. Karnin, J.W. Greene and M.E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory* **29** (1983) 35–41.
12. A. Shamir. How to share a secret. *Commun. of the ACM* **22** (1979) 612–613.
13. G.J. Simmons. An Introduction to Shared Secret and/or Shared Control Schemes and Their Application. *Contemporary Cryptology. The Science of Information Integrity.* IEEE Press (1991) 441-497.
14. D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography* **2** (1992) 357–390.
15. D.R. Stinson. Decomposition Constructions for Secret-Sharing Schemes. *IEEE Trans. on Information Theory* **40** (1994) 118–125.
16. D.R. Stinson. *Cryptography: Theory and Practice.* CRC Press Inc., Boca Raton (1995).

Appendix

We present in this Appendix the complete proof of Theorem 2. In order to do that we have to introduce some notation and to prove some technical lemmas.

Given a finite field $GF(q)$, a positive integer n and $\alpha \in GF(q)$, we notate $V_n(\alpha) = (1, \alpha, \alpha^2, \dots, \alpha^{n-1}) \in GF(q)^n$. It is well known that, if $\alpha_1, \dots, \alpha_n$ are n distinct elements of $GF(q)$, then $\{V_n(\alpha_1), \dots, V_n(\alpha_n)\}$ is a basis of $GF(q)^n$.

Let n, n_1, n_2 be integers with $0 \leq n_1, n_2 \leq n \leq n_1 + n_2$. Let E be an n-dimensional vector space over a finite field $GF(q)$ and let $E_1, E_2 \subset E$ be two subspaces with $\dim(E_1) = n_1$, $\dim(E_2) = n_2$ and $E_1 + E_2 = E$. Observe that

$r = \dim(E_1 \cap E_2) = n_1 + n_2 - n$. Let us consider r different elements $\lambda_1, \ldots, \lambda_r$ in $GF(q)$ and two isomorphisms, $\phi_i : GF(q)^{n_i} \to E_i$, where $i = 1, 2$, such that $\phi_1(V_{n_1}(\lambda_j)) = \phi_2(V_{n_2}(\lambda_j))$ for any $j = 1, \ldots, r$. Therefore, $\{\phi_1(V_{n_1}(\lambda_j))\}_{1 \le j \le r}$ is a basis of $E_1 \cap E_2$. Let us consider the mappings $\mathbf{v} : GF(q) \to E_1$ and $\mathbf{w} : GF(q) \to E_2$ defined by $\mathbf{v}(\alpha) = \phi_1(V_{n_1}(\alpha))$ and $\mathbf{w}(\alpha) = \phi_2(V_{n_2}(\alpha))$. Observe that $\mathbf{v}(\lambda_j) = \mathbf{w}(\lambda_j) \in E_1 \cap E_2$ for any $j = 1, \ldots, r$. We notate $\Lambda = \{\lambda_1, \ldots, \lambda_r\}$.

Lemma 7. *Let $\mathcal{A}, \mathcal{B}$ be two subsets of $GF(q) - \Lambda$ such that $|\mathcal{A}| = n_1$ and $|\mathcal{B}| = n - n_1$, or $|\mathcal{A}| = n - n_2$ and $|\mathcal{B}| = n_2$. Then, $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E.*

Proof. Let us suppose that $|\mathcal{A}| = n_1$ and $|\mathcal{B}| = n - n_1$, being the other case proved analogously. Observe that $\mathbf{w}(\Lambda)$, $\mathbf{w}(\Lambda) \cup \mathbf{w}(\mathcal{B})$ and $\mathbf{v}(\mathcal{A})$ are, respectively, basis of $E_1 \cap E_2$, E_2 and E_1. □

Lemma 8. *Let $\mathcal{A}, \mathcal{B}$ be two subsets of $GF(q) - \Lambda$ such that $|\mathcal{A}| = k - 1$ and $|\mathcal{B}| = n - k$, where $n - n_2 + 1 \le k \le n_1$, and the subspace $F \subset E$ generated by $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ has dimension $n - 1$. Then,* $\dim(F \cap (E_1 \cap E_2)) = r - 1$.

Proof. Observe that $k - 1 \ge n - n_2$ and $n - k \ge n - n_1$. We take $\mathcal{A}' \subset \mathcal{A}$ and $\mathcal{B}' \subset \mathcal{B}$ such that $|\mathcal{A}'| = n - n_2$ and $|\mathcal{B}'| = n - n_1$. Then, $\mathbf{v}(\Lambda) \cup \mathbf{v}(\mathcal{A}')$ is a basis of E_1 and $\mathbf{v}(\Lambda) \cup \mathbf{w}(\mathcal{B}')$ is a basis of E_2. Therefore, $\mathbf{v}(\Lambda) \cup \mathbf{v}(\mathcal{A}') \cup \mathbf{w}(\mathcal{B}')$ is a basis of E. Then, from Steinitz' Exchange Theorem, there is a vector $\mathbf{v}(\lambda_j) \in \mathbf{v}(\Lambda)$ such that $\{\mathbf{v}(\lambda_j)\} \cup \mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E. Since $\dim(F) = n - 1$ and $(E_1 \cap E_2) + F = E$, we have that $\dim(F \cap (E_1 \cap E_2)) = r - 1$. □

Lemma 9. *For any pair of integers N_1, N_2 with $N_1 \ge n - n_2$ and $N_2 \ge n_2$, there exists a positive integer $L = L(n, n_1, n_2, N_1, N_2)$ such that, for any prime power $q > L$, there exist two subsets $\mathcal{X}, \mathcal{Y} \subset GF(q) - \Lambda$, with $|\mathcal{X}| = N_1$ and $|\mathcal{Y}| = N_2$, such that for any $k = n - n_2, \ldots, \min\{N_1, n_1\}$ and for any $\mathcal{A} \subset \mathcal{X}$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k$ and $|\mathcal{B}| = n - k$, the set $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E.*

Proof. Using induction on N_1, we are going to prove that, if q is large enough, for any $\mathcal{Y} \subset GF(q) - \Lambda$ with $|\mathcal{Y}| = N_2$ there exists $\mathcal{X} \subset GF(q) - \Lambda$ with $|\mathcal{X}| = N_1$ verifying the required condition.

If $N_1 = n - n_2$, we can take any subset $\mathcal{X} \subset GF(q) - \Lambda$ with $|\mathcal{X}| = N_1$, because, from Lemma 7, for any $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{B}| = n_2$, the set $\mathbf{v}(\mathcal{X}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E. In this case, q must be greater than $L(n, n_1, n_2, n - n_2, N_2) = \max\{n - n_2, N_2\}$.

If $N_1 \ge n - n_2 + 1$, by induction hypothesis, there exists an integer $L_1 = L(n, n_1, n_2, N_1 - 1, N_2)$ such that, if $q > L_1$, there exists $\mathcal{X}' \subset GF(q) - \Lambda$ with $|\mathcal{X}'| = N_1 - 1$ such that for any $k = n - n_2, \ldots, \min\{N_1 - 1, n_1\}$ and for any $\mathcal{A} \subset \mathcal{X}'$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k$ and $|\mathcal{B}| = n - k$, the set $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E. From Lemma 8, for any $k = n - n_2 + 1, \ldots, \min\{N_1, n_1\}$ and for any $\mathcal{A} \subset \mathcal{X}'$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k - 1$ and $|\mathcal{B}| = n - k$, if $F_{\mathcal{A},\mathcal{B}} \subset E$ is the subspace generated by $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$, then, $\dim(F_{\mathcal{A},\mathcal{B}} \cap E_1) = n_1 - 1$. Therefore, there exist at most $n_1 - k$ different elements $\alpha \in GF(q) - (\Lambda \cup \mathcal{X}')$ such that

$\mathbf{v}(\alpha) \in F_{\mathcal{A},\mathcal{B}} \cap E_1$. Then, if

$$q > L_2 = \sum_{k=n-n_2+1}^{\min\{N_1,n_1\}} \binom{N_1-1}{k-1}\binom{N_2}{n-k}(n_1-k)+N_1-1$$

there exists $\alpha_{N_1} \in GF(q)-(\Lambda \cup \mathcal{X}')$ such that $\mathbf{v}(\alpha_{N_1}) \notin F_{\mathcal{A},\mathcal{B}}$ for any $\mathcal{A} \subset \mathcal{X}'$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k-1$ and $|\mathcal{B}| = n-k$, where $n-n_2+1 \le k \le \min\{N-1, n_1\}$. Therefore, if $q > L(n,n_1,n_2,N_1,N_2) = \max\{L_1, L_2\}$ there exists $\mathcal{X} = \mathcal{X}' \cup \{\alpha_{N_1}\} \subset GF(q)-\Lambda$, with $|\mathcal{X}| = N_1$, such that for any $k = n-n_2,\ldots,\min\{N_1,n_1\}$ and for any $\mathcal{A} \subset \mathcal{X}$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k$ and $|\mathcal{B}| = n-k$, the set $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ is a basis of E. □

Proof of Theorem 2. Let us take a prime power $q > L = L(n,n_1,n_2,N_1,N_2)$ and consider the subsets $\mathcal{X},\mathcal{Y} \subset GF(q)-\Lambda$, with $|\mathcal{X}| = N_1$ and $|\mathcal{Y}| = N_2$, whose existence is given by Lemma 9. Let us consider two one-to-one mappings $\psi_X : X \to \mathbf{v}(\mathcal{X})$ and $\psi_Y : Y \to \mathbf{w}(\mathcal{Y})$.

Let us take an isomorphism $\phi : GF(q)^r \to E_1 \cap E_2$ and the mapping $\mathbf{u} : GF(q) \to E_1 \cap E_2$ defined by $\mathbf{u}(\lambda) = \phi(V_r(\lambda))$. From Lemma 8, for any $k = n-n_2+1,\ldots,n_1$ and for any $\mathcal{A} \subset \mathcal{X}$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k-1$ and $|\mathcal{B}| = n-k$, if $F_{\mathcal{A},\mathcal{B}} \subset E$ is the subspace generated by $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$, then $\dim(F_{\mathcal{A},\mathcal{B}} \cap (E_1 \cap E_2)) = r-1$. Then, there are at most $r-1$ different elements $\lambda \in GF(q)$ such that $\mathbf{u}(\lambda) \in F_{\mathcal{A},\mathcal{B}}$. Therefore, if

$$q > M_1 = \sum_{k=n-n_2+1}^{n_1} \binom{N_1}{k-1}\binom{N_2}{n-k}(r-1)$$

there exists $\lambda_0 \in GF(q)$ such that for any $k = n-n_2+1,\ldots,n_1$ and for any $\mathcal{A} \subset \mathcal{X}$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k-1$ and $|\mathcal{B}| = n-k$, the subspace $F_{\mathcal{A},\mathcal{B}}$ do not contain the vector $\mathbf{u}(\lambda_0)$. Therefore, for any $q > M(1,n,n_1,n_2,N_1,N_2) = \max\{L, M_1\}$, the access structure $\Omega_1(n,n_1,n_2)$ is the vector space access structure given by the mapping $\psi_1 : P \cup \{D\} \to E$ that is defined by $\psi_1(p) = \psi_X(p) \in E_1$ if $p \in X$, $\psi_1(q) = \psi_Y(q) \in E_2$ if $q \in Y$ and $\psi_1(D) = \mathbf{u}(\lambda_0) \in E_1 \cap E_2$.

Analogously, we can see that if

$$q > M_4 = \sum_{k=n-n_2}^{n_1+1} \binom{N_1}{k-1}\binom{N_2}{n-k}(n-1)$$

there exists a vector $\mathbf{u}_0 \in E$ such that for any $k = n-n_2,\ldots,n_1+1$ and for any $\mathcal{A} \subset \mathcal{X}$ and $\mathcal{B} \subset \mathcal{Y}$ with $|\mathcal{A}| = k-1$ and $|\mathcal{B}| = n-k$, the subspace $F_{\mathcal{A},\mathcal{B}} \subset E$ generated by $\mathbf{v}(\mathcal{A}) \cup \mathbf{w}(\mathcal{B})$ do not contain $\mathbf{u}_0$. Therefore, for any $q > M(4,n,n_1,n_2,N_1,N_2) = \max\{L, M_4\}$, the access structure $\Omega_4(n,n_1,n_2)$ is the vector space access structure given by the mapping $\psi_4 : P \cup \{D\} \to E$ that is defined by $\psi_4(p) = \psi_X(p) \in E_1$ if $p \in X$, $\psi_4(q) = \psi_Y(q) \in E_2$ if $q \in Y$ and $\psi_4(D) = \mathbf{u}_0 \in E-(E_1 \cup E_2)$.

Given a prime power $q > L(n,n_1,n_2,N_1,N_2+1)$, let us consider the subsets $\mathcal{X},\mathcal{Y} \subset GF(q)-\Lambda$, with $|\mathcal{X}| = N_1$ and $|\mathcal{Y}| = N_2+1$, whose existence is given by Lemma 9. Let us consider the mapping $\psi_2 : P \cup \{D\} \to E$ defined from two one-to-one mappings $\psi_X : X \to \mathbf{v}(\mathcal{X})$ and $\psi_Y : Y \cup \{D\} \to \mathbf{w}(\mathcal{Y})$. It is not difficult to see that ψ_2 defines the access structure $\Omega_2(n, n_1, n_2)$. Therefore, $M(2, n, n_1, n_2, N_1, N_2) = L(n, n_1, n_2, N_1, N_2 + 1)$.

Symmetrically, if $q > M(3, n, n_1, n_2, N_1, N_2) = L(n, n_1, n_2, N_1 + 1, N_2)$, we can find a mapping $\psi_3 : P \cup \{D\} \to E$ that determines the access structure $\Omega_3(n, n_1, n_2)$. □