Secret sharing schemes with three or four minimal qualified subsets*

Jaume Martí-Farré, Carles Padró
Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034 Barcelona, Spain
e-mail: jaumem@mat.upc.es, matcpl@mat.upc.es

Abstract

In this paper we study secret sharing schemes whose access structure has three or four minimal qualified subsets. The ideal case is completely characterized and for the non-ideal case we provide bounds on the optimal information rate.

Keywords. Cryptography; secret sharing schemes; information rate; ideal schemes.

1 Introduction

A *secret sharing scheme* is a method to distribute a secret value k among a set of participants $\mathcal{P}$ in such a way that only the *qualified subsets* of $\mathcal{P}$ are able to reconstruct the value of k. Secret sharing was introduced by Blakley [1] and Shamir [13]. A comprehensive introduction to this topic can be found in [15, 17, 14]. A secret sharing scheme is said to be *perfect* if the *non-qualified subsets* can not obtain any information about the value of the secret. We are going to consider only unconditionally secure perfect secret sharing schemes.

The *access structure* of a secret sharing scheme is the family of qualified subsets, $\Gamma \subset 2^{\mathcal{P}}$. In general, access structures are considered to be *monotone*, that is, any superset of a qualified subset must be qualified. Then, the access structure Γ is determined by the family of *minimal qualified subsets*, Γ_0, which is called the *basis* of Γ. We assume that every participant belongs to at least one minimal qualified subset. For example, a (t,n)-*threshold access structure* consists of all subsets with cardinality at least t from a set of n participants and its basis is formed by all subsets with exactly t participants.

*This work was partially supported by the Spanish *Ministerio de Ciencia y Tecnología* under project TIC 2000-1044.

Therefore, in a secret sharing scheme Σ with access structure Γ, given a secret value $k \in \mathcal{K}$ and some random election, a special participant $D \notin \mathcal{P}$, called the *dealer*, gives to every participant $p \in \mathcal{P}$ 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 k.

The first works about secret sharing [1, 13] considered only schemes with threshold access structure. Further works considered the problem of finding secret sharing schemes for more general access structures, and Ito, Saito and Nishizeki [9] proved that there exists a secret sharing scheme for any access structure.

An important problem appears when designing secret sharing schemes for general access structures: the size of the shares given to the participants. While in the threshold schemes proposed by Blakley [1] and Shamir [13] the shares have the same size as the secret, in the schemes constructed in [9] for general access structures the shares are, in general, much larger than the secret.

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. Therefore, one of the basic parameters in secret sharing is the *information rate* $\rho(\Sigma, \Gamma, \mathcal{K})$ of the scheme, which is defined as the ratio between the length (in bits) of the secret and the maximum length of the shares given to the participants. That is, $\rho(\Sigma, \Gamma, \mathcal{K}) = \log |\mathcal{K}| / \max_{p \in \mathcal{P}} \log |\mathcal{S}_p|$.

In a secret sharing scheme the length of any share is greater than or equal to the length of the secret, so the information rate can not be greater than one. Secret sharing schemes with information rate equal to one are called *ideal*. We say that an access structure $\Gamma \subset 2^{\mathcal{P}}$ is an *ideal access structure* if there exists an ideal secret sharing scheme for Γ.

It is not possible in general to find an ideal secret sharing scheme for a given access structure Γ. So, we may try to find a secret sharing scheme for Γ with information rate as large as possible. The *optimal information rate* of an access structure Γ is defined by $\rho^*(\Gamma) = \sup(\rho(\Sigma, \Gamma, \mathcal{K}))$, 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 and set of secrets $\mathcal{K}$. Of course, the optimal information rate of an ideal access structure is equal to one.

The above considerations lead to two problems that have received considerable attention: to characterize the 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 [6] in terms of matroids. A sufficient condition is obtained from the vector space construction [5], which is a method to construct ideal secret sharing schemes for a wide family of access structures. Several techniques have been introduced in [4, 7, 16] in order to construct secret sharing schemes for some families of access structures, which provide lower bounds on the optimal information rate. Upper bounds have been found for several particular access structures by using some tools from Information Theory [2, 3, 8].

A general method to find upper bounds was given in [2] and was generalized in [12].

Nevertheless, both problems are far to be solved. There are some important open questions about the characterization of ideal access structures, and there exists a wide gap between the best known upper and lower bounds on the optimal information rate for most access structures.

Due to the difficulty of finding a general solution, those problems have been studied in several particular classes of access structures: access structures on a set of four participants [15]; access structures on a set of five participants [11]; access structures defined by graphs [2, 3, 4, 6, 7, 8, 16]; and bipartite access structures [12]. The ideal access structures in all these families have been completely characterized. The optimal information rate of almost all access structures on a set of at most five participants has been determined. Bounds on the optimal information rate, which are tight in some cases, have been given for the other families.

There exist remarkable coincidences in the results obtained for all these classes of access structures: the ideal access structures coincide with the vector space ones, and there is no access structure Γ whose optimal information rate is such that $2/3 < \rho^*(\Gamma) < 1$. A natural question that arises at this point is to determine to which extent these results can be generalized.

In the present paper, we study these problems in another family of access structures: the access structures with exactly three or four minimal qualified subsets. We obtain similar results as in the previously considered families. Namely, ideal access structures with three or four minimal qualified subsets are completely characterized. Besides, we prove that also in these families the ideal access structures coincide with the vector space ones, and that there is no access structure with optimal information rate between 2/3 and 1. Moreover, we prove that the optimal information rate of any non-ideal access structure with three minimal qualified subsets is equal to 2/3. Finally, we show that the optimal information rate $\rho^*(\Gamma)$ of any non-ideal access structure Γ with four minimal qualified subsets is bounded by $1/2 \leq \rho^*(\Gamma) \leq 2/3$.

The organization of the paper is as follows. Some definitions and the notation together with several general results that will be used in the following are given in Section 2. Section 3 is devoted to access structures with three minimal qualified subsets, while those with four minimal qualified subsets are studied in Section 4.

2 Preliminaries

There are several techniques to find bounds on the optimal information rate $\rho^*(\Gamma)$ of an access structure Γ on a set of participants $\mathcal{P}$. The next two propositions summarize those that will be used later. The first one gives us a method to find upper bounds on the optimal information rate, whereas the second one deals with lower bounds.

The *independent sequence method*, which was introduced by Blundo, De Santis, De Simone and Vaccaro in [2] and was generalized by Padró and Sáez in [12], is the first known general method to find upper bounds on the optimal information rate. Let Γ be an access structure on a set of participants $\mathcal{P}$. We say that a sequence of subsets $\emptyset \neq B_1 \subset \cdots \subset B_m \notin \Gamma$ *is made independent* by a subset $A \subset \mathcal{P}$ if there exist $X_1, \ldots, X_m \subset A$ such that $B_i \cup X_i \in \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$ for any $i = 1, \ldots, m$, where B_0 is the empty set.

Proposition 2.1 *([2, Theorem 3.8] and [12, Theorem 2.1]). Let Γ be an access structure on a set of participants $\mathcal{P}$. Let $\emptyset \neq B_1 \subset \cdots \subset B_m \notin \Gamma$ be a sequence of subsets of $\mathcal{P}$ that is made independent by $A \subset \mathcal{P}$. The following statements hold:*

1. *If $A \in \Gamma$, then $\rho^*(\Gamma) \leq |A|/(m+1)$.*
2. *If $A \notin \Gamma$, then $\rho^*(\Gamma) \leq |A|/m$.*

A *decomposition* of an access structure Γ is a family $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subset \Gamma_0$ such that $\Gamma_{0,1} \cup \cdots \cup \Gamma_{0,r} = \Gamma_0$. Several *decomposition methods* have been presented providing lower bounds on the optimal information rate. The λ-*decomposition method* given by Stinson in [16] is one of the most powerful of them. We apply this method only for decompositions consisting of ideal substructures. Namely, we are going to use the following result, which is a direct consequence from [16, Theorem 2.1].

Proposition 2.2 *Let Γ be an access structure on a set of participants $\mathcal{P}$ having basis Γ_0. Let $\Gamma_{0,1}, \ldots, \Gamma_{0,r} \subset \Gamma_0$ be a decomposition of Γ. Let Γ_i be the access structure with basis $\Gamma_{0,i}$ on the set $\mathcal{P}_i = \bigcup_{A \in \Gamma_{0,i}} A$. Let us suppose that, for any $i = 1, \ldots, r$, there exists an ideal secret sharing scheme Σ_i with access structure Γ_i and set of secrets a finite field K. Then, the optimal information rate of Γ verifies*

$$\rho^*(\Gamma) \geq \frac{\min\{\lambda_A \,:\, A \in \Gamma_0\}}{\max\{r_p \,:\, p \in \mathcal{P}\}},$$

where $\lambda_A = |\{i \in \{1, \ldots, r\} \,:\, A \in \Gamma_{0,i}\}|$ and $r_p = |\{i \in \{1, \ldots, r\} \,:\, p \in \mathcal{P}_i\}|$.

The *vector space construction* is a useful method to construct ideal schemes that was introduced by Brickell [5]. Let $\mathcal{P}$ be a set of n participants, Γ an access structure on $\mathcal{P}$, $D \notin \mathcal{P}$ the dealer, and let K be a finite field. We say that Γ is a *K-vector space access structure* if there exists a vector space E over K and a map $\psi : \mathcal{P} \cup \{D\} \longrightarrow E$ such that $\psi(x) \neq 0$ for $x \in \mathcal{P} \cup \{D\}$, and 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 $\psi(A) = \{\psi(p) \,:\, p \in A\}$. In this situation, the map $\psi : \mathcal{P} \cup \{D\} \longrightarrow E$ is said to be a *realization* of the K-vector space access structure Γ. An ideal secret sharing scheme with set of secrets $\mathcal{K} = K$ can be constructed for any K-vector space access structure Γ: given a secret value $k \in K$, the dealer takes at random an element

$v \in E$ such that $v \cdot \psi(D) = k$, and gives the share $s_p = v \cdot \psi(p)$ to the participant $p \in \mathcal{P}$, (see [5] or [15] for proofs).

We say that Γ is a *vector space access structure* if it is a K-vector space access structure for some finite field K. An ideal scheme for Γ constructed in the above way is called a *vector space secret sharing scheme*. Of course, any vector space access structure is ideal. For instance, (see [13] and [15]), the Shamir's scheme can be seen as a vector space secret sharing scheme over $K = GF(q)$ for any prime power $q > |\mathcal{P}|$. Therefore (t, n)-threshold access structures are vector space access structures.

The following lemmas provide some properties of vector space access structures that will be used in this paper. The first one is about decomposition of access structures. The second one deals with an extension operation on access structures that consists of substituting a participant by a set of new ones. Finally, Lemma 2.5 presents another extension operation consisting of adding a set of new participants to every minimal qualified subset.

Lemma 2.3 *Let Γ be an access structure on a set of participants $\mathcal{P}$. Assume that there exists a decomposition $\Gamma_{0,1}, \ldots, \Gamma_{0,r}$ of Γ such that $\mathcal{P}_1, \ldots, \mathcal{P}_r$ form a partition of $\mathcal{P}$, where $\mathcal{P}_i = \bigcup_{A \in \Gamma_{0,i}} A$. Let us denote by Γ_i the access structure on the set of participants $\mathcal{P}_i$ having basis $\Gamma_{0,i}$. Then, if $\Gamma_1, \ldots, \Gamma_r$ are vector space access structures over a finite field K, so it is the access structure Γ.*

Proof. We assume that $\Gamma_1, \ldots, \Gamma_r$ are K-vector space access structures. So, for $1 \leq i \leq r$ there exists a realization $\psi_i : \mathcal{P}_i \cup \{D_i\} \to E_i$ of Γ_i. We can suppose that $E_i = K \times E'_i$ and that $\psi_i(D_i) = (1, 0) \in K \times E'_i$. Let us consider the K-vector space $E = K \times E'_1 \times \cdots \times E'_r$ and the map $\psi : \mathcal{P} \cup \{D\} \to E$ defined by $\psi(D) = (1, 0, \ldots, 0)$ and, if $p \in \mathcal{P}_i$, $\psi(p) = (\xi_p, 0, \ldots, v_p, \ldots, 0) \in K \times E'_1 \times \cdots \times E'_i \times \cdots \times E'_r$, where $\psi_i(p) = (\xi_p, v_p) \in K \times E'_i$. It is not difficult to check that ψ is a realization of Γ as a K-vector space access structure. $\diamond$

Lemma 2.4 *Let Γ be an access structure on a set $\mathcal{P} = \{p_1, \ldots, p_m\}$ of m participants with basis Γ_0. On the set $\mathcal{P}^e = B_{p_1} \cup \cdots \cup B_{p_m}$ of $n = n_1 + \cdots + n_m$ participants, where $B_{p_i} = \{p_{i,1}, \ldots, p_{i,n_i}\}$, we consider the access structure Γ^e with basis $\Gamma_0^e = \{A^e : A \in \Gamma_0\}$, where $A^e = \cup_{p \in A} B_p$. Then, if Γ is a vector space access structure over a finite field K, so it is the access structure Γ^e.*

Proof. We may assume that there is an integer $s \in \{1, \ldots, m\}$ such that $n_i > 1$ if $i \geq s$ and $n_i = 1$ otherwise. Let $\psi : \mathcal{P} \cup \{D\} \to E$ be a realization of the K-vector space access structure Γ. Let $\{e_{s,2}, \ldots, e_{s,n_s}, \ldots, e_{m,2}, \ldots, e_{m,n_m}\}$ be a basis of the vector space $K^{n-m} = K^{n_s - 1} \times \cdots \times K^{n_m - 1}$. We define the map $\psi^e : \mathcal{P}^e \cup \{D\} \to E \times K^{n-m}$ by $\psi^e(D) = (\psi(D), 0)$, by $\psi^e(p_{i,1}) = (\psi(p_i), 0)$ whenever $i < s$, by $\psi^e(p_{i,1}) = (\psi(p_i), \sum_{j=2,\ldots,n_i} e_{i,j})$ in the case $i \geq s$, and by $\psi^e(p_{i,j}) = (0, e_{i,j})$ if

$2 \leq j \leq n_i$. It is not hard to check that ψ^e is a realization of Γ^e as a K-vector space access structure. $\diamond$

Lemma 2.5 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0. Let $\mathcal{P}'$ be a set with $\mathcal{P} \cap \mathcal{P}' = \emptyset$, and consider the access structure Γ' on $\mathcal{P} \cup \mathcal{P}'$ with basis $\Gamma'_0 = \{A \cup \mathcal{P}'$ where $A \in \Gamma_0\}$. Then, if Γ is a vector space access structure over a finite field K, so it is the access structure Γ'.*

Proof. Let $\psi : \mathcal{P} \cup \{D\} \to E$ be a realization of the K-vector space access structure Γ. Let us suppose that $\mathcal{P}' = \{p'_1, \ldots, p'_m\}$ and let us consider the vector space $E' = E \times K^m$. Let $\{e_1, \ldots, e_m\}$ be a basis of K^m. We take the map $\psi' : \mathcal{P} \cup \mathcal{P}' \cup \{D\} \to E' = E \times K^m$ defined by $\psi'(p) = (\psi(p), 0)$ for every $p \in \mathcal{P}$, $\psi'(p'_i) = (0, e_i)$ for every $p'_i \in \mathcal{P}'$ and $\psi'(D) = (\psi(D), e_1 + \cdots + e_m)$. Then, it is clear that ψ' is a realization of Γ' as a K-vector space access structure. $\diamond$

We finish this section with the following proposition that will be used later.

Proposition 2.6 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with one or two minimal qualified subsets. Then Γ is a K-vector space access structure for any finite field K. As a consequence, Γ is an ideal access structure.*

Proof. The result is clear if $|\,\Gamma_0\,| = 1$ since, in such a case, Γ is the (n, n)-threshold access structure, which is a K-vector space access structure for any finite field K. So we may assume that $|\,\Gamma_0\,| = 2$. Let us denote $\Gamma_0 = \{A_1, A_2\}$. From Lemma 2.5, we can suppose that $A_1 \cap A_2 = \emptyset$. Now, the result follows applying Lemma 2.3 with $\Gamma_{0,1} = \{A_1\}$ and $\Gamma_{0,2} = \{A_2\}$. $\diamond$

3 Access structures with three minimal qualified subsets

The purpose of this section is to prove Propositions 3.2 and 3.3. The first one gives us a complete characterization of the access structures with three minimal qualified subsets that can be realized by an ideal secret sharing scheme. The second one deals with the optimal information rate in the non-ideal case. At the end of this section we point out some examples in order to illustrate our results.

The next lemma is a key point in the proof of these results. This lemma determines some forbidden situations in an ideal access structure with three minimal qualified subsets. We need the following notation. Let Γ be an access structure on a set of participants $\mathcal{P}$ having basis $\Gamma_0 = \{A_1, \ldots, A_r\}$. For every $x \in \mathcal{P}$, we define the *incidence vector* of x as $\chi(x) = (x_1, \ldots, x_r)$, where $x_i = 1$ if $x \in A_i$ and $x_i = 0$ otherwise.

Lemma 3.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having three elements, A_1, A_2, A_3. Then the optimal information rate of Γ verifies $\rho^*(\Gamma) \leq 2/3$ if there exist four elements $a, b, c, d \in \mathcal{P}$ whose incidence vectors are $\chi(a) = (1,0,1)$, $\chi(b) = (0,1,1)$, $\chi(c) = (1, c_2, 0)$ and $\chi(d) = (0,1,0)$.*

Proof. Let us consider the subsets $B_1 = \mathcal{P} \setminus \{a,b,c,d\}$, $B_2 = \mathcal{P} \setminus \{a,b,d\}$ and $B_3 = \mathcal{P} \setminus \{a,b\}$. Observe that $A_3 \subset B_1 \cup \{a,b\}$, $A_1 \subset B_2 \cup \{a\}$ and $A_2 \subset B_3 \cup \{b\}$. Therefore, the subsets $B_1 \cup \{a,b\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{b\}$ are qualified. On the other hand, we have that $A_i \not\subset B_3$, $A_i \not\subset B_2 \cup \{b\}$ and $A_i \not\subset B_1 \cup \{a\}$ for any $i = 1,2,3$. So, these three subsets are not qualified. Hence, if $\{a,b\} \in \Gamma$, then the sequence $\emptyset \neq B_2 \subset B_3$ is made independent by the set $\{a,b\}$. While, if $\{a,b\} \notin \Gamma$, then $B_1 \neq \emptyset$ and $\{a,b\}$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3$. In both cases, we can apply Proposition 2.1 and we get $\rho^*(\Gamma) \leq 2/3$. $\diamond$

Proposition 3.2 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having three elements. Let us denote $\Gamma_0 = \{A_1, A_2, A_3\}$. Then, the following conditions are equivalent:*

1. *Γ is a vector space access structure.*
2. *Γ is an ideal access structure.*
3. *$\rho^*(\Gamma) > 2/3$.*
4. *$A_i \cup A_j = \mathcal{P}$ if $i \neq j$, or $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(1)} \cap A_{\sigma(3)}$ for some permutation σ.*

Proof. A vector space access structure is ideal and, hence, its optimal information rate is equal to one. Then, we only have to show that (3) implies (4) and that (4) implies (1).

We are going to prove first that, assuming $\rho^*(\Gamma) > 2/3$, then either $A_i \cup A_j = \mathcal{P}$ if $i \neq j$, or there exists a permutation σ on $\{1,2,3\}$ such that $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(1)} \cap A_{\sigma(3)}$.

Let us suppose that $\rho^*(\Gamma) > 2/3$. We show now that, if $A_1 \cup A_2 = \mathcal{P}$, then $A_1 \cup A_3 = \mathcal{P}$ and $A_2 \cup A_3 = \mathcal{P}$. Otherwise, we may assume that $A_1 \cup A_3 \neq \mathcal{P}$. In such a case, there exist four different elements $a, b, c, d \in \mathcal{P}$ such that: $a \in A_3 \setminus A_2$, so $a \in A_1$; $b \in A_3 \setminus A_1$, so $b \in A_2$; $c \in A_1 \setminus A_3$; and $d \in \mathcal{P} \setminus (A_1 \cup A_3)$, so $d \in A_2$. Therefore, the incidence vectors of these elements are $\chi(a) = (1,0,1)$, $\chi(b) = (0,1,1)$, $\chi(c) = (1, c_2, 0)$ and $\chi(d) = (0,1,0)$. Hence, from Lemma 3.1 we get $\rho^*(\Gamma) \leq 2/3$, which is a contradiction.

Let us consider now the case whenever $A_i \cup A_j \neq \mathcal{P}$ if $i \neq j$. In such a case, we must prove that, if $\rho^*(\Gamma) > 2/3$, then there exists a permutation σ such that $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(1)} \cap A_{\sigma(3)}$. If not, there is at most one pair $\{i,j\} \subset \{1,2,3\}$ such that $A_i \cap A_j = A_1 \cap A_2 \cap A_3$. Then, we may assume that both $A_1 \cap A_3$ and $A_2 \cap A_3$ are different from $A_1 \cap A_2 \cap A_3$ and, hence, $A_1 \cap A_3 \not\subset A_2$ and $A_2 \cap A_3 \not\subset A_1$.

Let us consider the following participants: $a \in (A_1 \cap A_3) \setminus A_2$, $b \in (A_2 \cap A_3) \setminus A_1$, $c \in \mathcal{P} \setminus (A_2 \cup A_3)$, and $d \in \mathcal{P} \setminus (A_1 \cup A_3)$. Since $\chi(a) = (1,0,1)$, $\chi(b) = (0,1,1)$, $\chi(c) = (1,0,0)$ and $\chi(d) = (0,1,0)$, from Lemma 3.1 we have that $\rho^*(\Gamma) \leq 2/3$, a contradiction. This completes the proof of (3) implies (4).

To finish we must demonstrate that (4) implies (1). That is, assuming that $A_i \cup A_j = \mathcal{P}$ if $i \neq j$ or $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(1)} \cap A_{\sigma(3)}$ for some permutation σ, we want to prove that the access structures Γ can be realized by a vector space secret sharing scheme. We have to distinguish two cases.

Case 1: $A_i \cup A_j = \mathcal{P}$ if $i \neq j$. From Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 = \emptyset$. In such a case the incidence vector of any participant is one of the following: $\chi_1 = (1,1,0)$, $\chi_2 = (1,0,1)$ or $\chi_3 = (0,1,1)$. Let $B_i \subset \mathcal{P}$ be the set of participants with incidence vector χ_i. Since $A_i \not\subset A_j$ if $i \neq j$, we have that $B_i \neq \emptyset$ for any $i = 1,2,3$. So, $\{B_1, B_2, B_3\}$ is a partition of $\mathcal{P}$ such that $A_1 = B_1 \cup B_2$, $A_2 = B_1 \cup B_3$, and $A_3 = B_2 \cup B_3$. Therefore $\Gamma = (\widetilde{\Gamma})^e$ where $\widetilde{\Gamma}$ is the access structure on the set of participants $\widetilde{\mathcal{P}} = \{p_1, p_2, p_3\}$ with basis $\widetilde{\Gamma}_0 = \{\{p_1,p_2\},\{p_1,p_3\},\{p_2,p_3\}\}$. Since $\widetilde{\Gamma}$ is the $(2,3)$-threshold access structure, it is a vector space access structure. Hence, from Lemma 2.4, it follows that Γ is so.

Case 2: $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(1)} \cap A_{\sigma(3)}$ for some permutation σ. Without loss of generality we may assume that $A_1 \cap A_2 = A_1 \cap A_3$. On the other hand, from Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 = \emptyset$. So we have that $A_1 \cap A_2 = A_1 \cap A_3 = \emptyset$. Let $\Gamma_{0,1} = \{A_1\}$ and $\Gamma_{0,2} = \{A_2, A_3\}$. Applying Lemma 2.3 and Proposition 2.6 it follows that Γ is a vector space access structure. $\diamond$

Proposition 3.3 *Let Γ be an access structure on a set of participants $\mathcal{P}$ such that its basis Γ_0 has three elements. Assume that Γ is not realizable by an ideal secret sharing scheme. Then $\rho^*(\Gamma) = 2/3$.*

Proof. We assume that Γ is not realizable by an ideal secret sharing scheme. Hence applying Proposition 3.2 it follows that $\rho^*(\Gamma) \leq 2/3$. Therefore we must demonstrate that $\rho^*(\Gamma) \geq 2/3$. Let us denote $\Gamma_0 = \{A_1, A_2, A_3\}$. Let $\Gamma_{0,1} = \{A_2, A_3\}$, $\Gamma_{0,2} = \{A_1, A_3\}$ and $\Gamma_{0,3} = \{A_1, A_2\}$. Observe that $\Gamma_{0,1}, \Gamma_{0,2}, \Gamma_{0,3} \subset \Gamma_0$ is a decomposition of Γ. Let Γ_i be the access structure with basis $\Gamma_{0,i}$ on the set $\mathcal{P}_i = A_j \cup A_k$, where $\{i,j,k\} = \{1,2,3\}$. From Proposition 2.6, for any finite field K, there exists an ideal secret sharing scheme with access structure Γ_i and set of secrets K. On one hand, for every participant $p \in \mathcal{P}$ we have that $r_p = |\,\{i \in \{1,2,3\} \text{ such that } p \in \mathcal{P}_i\}\,| \leq 3$. Therefore $\max\{r_p : p \in \mathcal{P}\} \leq 3$. On the other hand we have that if $A \in \Gamma_0$ then $\lambda_A = |\,\{i \in \{1,2,3\} \text{ such that } A \in \Gamma_{0,i}\}\,| = 2$. Hence, from Proposition 2.2 it follows that $\rho^*(\Gamma) \geq 2/3$ as we wanted to prove. $\diamond$

We conclude this section by providing some examples. The first one is a direct application of our results. In the second one, instead of applying our results directly to a given access structure, we apply them to its dual. See [10] for the definitions and results about dual access structures.

Example 3.4 Let Γ be the access structure on $\mathcal{P} = \{x, y, z\}$ having basis $\Gamma_0 = \{A_1, A_2, A_3\}$ where $A_1 = \{x, y\}, A_2 = \{y, z\}, A_3 = \{x, z\}$. On the set of six participants $\mathcal{P}' = \{x, y, z, a, b, c\}$ we consider the access structures Γ'_1 and Γ'_2 defined by $(\Gamma'_1)_0 = \{A_1 \cup \{a\}, A_2 \cup \{b\}, A_3 \cup \{c\}\}$, and $(\Gamma'_2)_0 = \{A_1 \cup \{a, b\}, A_2 \cup \{b, c\}, A_3 \cup \{a, c\}\}$. Then, applying the above propositions it follows that $\rho^*(\Gamma) = \rho^*(\Gamma'_2) = 1$ while $\rho^*(\Gamma'_1) = 2/3$. Furthermore, we get that Γ and Γ_2 are vector space access structures.

Example 3.5 On the set $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ of seven participants we consider the access structure Γ with basis $\Gamma_0 = \{\{p_2, p_4, p_7\}, \{p_2, p_5, p_7\}, \{p_1, p_3\}, \{p_1, p_4\}, \{p_1, p_5\}, \{p_1, p_6\}, \{p_3, p_6\}, \{p_3, p_7\}, \{p_2, p_6\}\}$. The dual access structure Γ^* of Γ has three elements in its basis. Namely, $(\Gamma^*)_0 = \{A_1, A_2, A_3\}$ where $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_3, p_4, p_5, p_6\}$ and $A_3 = \{p_1, p_6, p_7\}$. Since $A_i \cup A_j \neq \mathcal{P}$ if $i \neq j$, $A_1 \cap A_2 = \{p_3\}$, $A_1 \cap A_3 = \{p_1\}$ and $A_2 \cap A_3 = \{p_6\}$, hence it follows that Γ^* has optimal information rate equal to 2/3. Therefore $\rho^*(\Gamma) = 2/3$ and, in particular, Γ is not an ideal access structure.

4 Access structures with four minimal qualified subsets

A complete characterization of ideal access structures with four minimal qualified subsets is provided in this section by Propositions 4.2, 4.3, 4.4, 4.5 and 4.7. Besides, these propositions state that ideal access structures coincide with the vector space ones and with those having optimal information rate greater than 2/3. Bounds on the optimal information rate are given for the non-ideal case in Proposition 4.8. Finally, some examples are presented.

As in the case of three minimal qualified subsets, we need a lemma determining some forbidden situations in an ideal access structure.

Lemma 4.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$ such that its basis Γ_0 has four elements, A_1, A_2, A_3, A_4. Then, the optimal information rate of Γ verifies $\rho^*(\Gamma) \leq 2/3$ if there exist elements $a, b, c, d \in \mathcal{P}$ whose incidence vectors are in one of the following situations:*

1. $\chi(a) = (1, 0, 1, 1)$, $\chi(b) = (0, 1, 1, 1)$, $\chi(c) = (1, c_2, 0, c_4)$, $\chi(d) = (0, 1, 0, d_4)$.
2. $\chi(a) = (1, 0, 1, 1)$, $\chi(b) = (0, 1, 1, b_4)$, $\chi(c) = (1, c_2, 0, c_4)$, $\chi(d) = (0, 1, 0, 1)$.
3. $\chi(a) = (1, 0, 1, a_4)$, $\chi(b) = (0, 1, 1, 1)$, $\chi(c) = (1, c_2, 0, c_4)$, $\chi(d) = (0, 1, 0, 1)$.
4. $\chi(a) = (1, 0, 1, a_4)$, $\chi(b) = (0, 1, 1, b_4)$, $\chi(c) = (1, c_2, 0, c_4)$, $\chi(d) = (0, 1, 0, d_4)$ *and, besides, there exists a participant $x \in \mathcal{P}$ with $\chi(x) = (0, 0, 0, 1)$.*

Proof. Let us suppose that one of the first three conditions holds. We consider the subsets $B_1 = \mathcal{P} \setminus \{a, b, c, d\}$, $B_2 = \mathcal{P} \setminus \{a, b, d\}$ and $B_3 = \mathcal{P} \setminus \{a, b\}$. Since

$A_3 \subset B_1 \cup \{a,b\}$, $A_1 \subset B_2 \cup \{a\}$ and $A_2 \subset B_3 \cup \{b\}$, we have that these three subsets are qualified. On the other hand, one can check that, for any $i = 1,2,3,4$, $A_i \not\subset B_3$, $A_i \not\subset B_2 \cup \{b\}$ and $A_i \not\subset B_1 \cup \{a\}$, and hence these three subsets are not qualified. Therefore, if $\{a,b\} \in \Gamma$, then the sequence $\emptyset \neq B_2 \subset B_3$ is made independent by the set $\{a,b\}$. While, if $\{a,b\} \notin \Gamma$, then $B_1 \neq \emptyset$ and the set $\{a,b\}$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3$. We apply Proposition 2.1 in both cases in order to conclude that $\rho^*(\Gamma) \leq 2/3$.

The proof is finished by checking that $\rho^*(\Gamma) \leq 2/3$ if the fourth condition holds. In this case, we consider the subsets $B_1 = \mathcal{P} \setminus \{a,b,c,d,x\}$, $B_2 = \mathcal{P} \setminus \{a,b,d,x\}$ and $B_3 = \mathcal{P} \setminus \{a,b,x\}$. As before, the subsets $B_1 \cup \{a,b\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{b\}$ are qualified, while B_3, $B_2 \cup \{b\}$ and $B_1 \cup \{a\}$ are not qualified. At this point, we finish the proof by applying Proposition 2.1 in the same way as in the previous case. $\diamond$

We begin the characterization of ideal access structures with four minimal qualified subsets by studying, in Propositions 4.2 and 4.3, the case in which the set of participants can be covered by two minimal qualified subsets.

Proposition 4.2 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having four elements, $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $\alpha = |\{\{i,j\}$ such that $A_i \cup A_j = \mathcal{P}\}| \geq 2$. Then, the following conditions are equivalent:*

1. *Γ is a vector space access structure.*

2. *Γ is an ideal access structure.*

3. *$\rho^*(\Gamma) > 2/3$.*

4. *$\alpha = 6$ or $\alpha = 2$, and if $\alpha = 2$ then there exists a permutation σ on $\{1,2,3,4\}$ such that $A_{\sigma(1)} \cup A_{\sigma(2)} = A_{\sigma(3)} \cup A_{\sigma(4)} = \mathcal{P}$ and $A_{\sigma(1)} \cap A_{\sigma(2)} = A_{\sigma(3)} \cap A_{\sigma(4)}$.*

Proof. We only must show that (3) implies (4) and that (4) implies (1). In order to demonstrate the first implication we shall proceed by proving three claims. Assume that $\rho^*(\Gamma) > 2/3$.

Claim 1. If $A_1 \cup A_2 = A_2 \cup A_3 = \mathcal{P}$, then $A_1 \cup A_3 = \mathcal{P}$.
Proof: First let us show that $A_2 \cap A_3 \cap A_4 \not\subset A_1$. Otherwise we consider the following participants: $a \in A_4 \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in A_3 \setminus A_1$, so $\chi(b) = (0,1,1,0)$; $c \in A_1 \setminus A_3$, so $\chi(c) = (1,1,0,c_4)$; and $d \in A_4 \setminus A_1$, so $\chi(d) = (0,1,0,1)$. Applying Lemma 4.1 (2) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction. Therefore we have that, if $A_1 \cup A_2 = A_2 \cup A_3 = \mathcal{P}$, then $A_2 \cap A_3 \cap A_4 \not\subset A_1$. We want to prove that $A_1 \cup A_3 = \mathcal{P}$. In order to do it let us consider $a \in A_4 \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in (A_2 \cap A_3 \cap A_4) \setminus A_1$, so $\chi(b) = (0,1,1,1)$; and $c \in A_1 \setminus A_3$, so $\chi(c) = (1,1,0,c_4)$. If $A_1 \cup A_3 \neq \mathcal{P}$ then there exists $d \in \mathcal{P} \setminus (A_1 \cup A_3)$, hence $\chi(d) = (0,1,0,d_4)$, and applying Lemma 4.1 (1) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Claim 2. If $A_1 \cup A_2 = A_1 \cup A_3 = A_2 \cup A_3 = \mathcal{P}$, then $A_i \cup A_4 = \mathcal{P}$ for any $i = 1, 2, 3$.
Proof: It is enough to show that $\rho^*(\Gamma) \leq 2/3$ if $A_1 \cup A_4 \neq \mathcal{P}$. Let us suppose that $A_1 \cup A_4 \neq \mathcal{P}$. Let $a \in A_4 \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in A_4 \setminus A_1$, so $\chi(b) = (0,1,1,1)$; $c \in A_1 \setminus A_4$, so $\chi(c) = (1, c_2, c_3, 0)$; and $d \in \mathcal{P} \setminus (A_1 \cup A_4)$, so $\chi(d) = (0,1,1,0)$. By changing the roles of A_3 and A_4 in Lemma 4.1 (2) it follows that $\rho^*(\Gamma) \leq 2/3$.

Claim 3. If $A_1 \cup A_2 = A_3 \cup A_4 = \mathcal{P}$ and $A_i \cup A_j \neq \mathcal{P}$ otherwise, then $A_1 \cap A_2 = A_3 \cap A_4$.
Proof: If $A_1 \cap A_2 \neq A_3 \cap A_4$, then we can suppose that $A_3 \cap A_4 \not\subset A_1 \cap A_2$. Since $A_1 \cup A_2 = \mathcal{P}$ hence, without loss of generality, we may assume that there exists a participant $a \in (A_1 \cap A_3 \cap A_4) \setminus A_2$, so $\chi(a) = (1,0,1,1)$. Besides, we consider the following participants: $b \in \mathcal{P} \setminus (A_1 \cup A_4)$, so $\chi(b) = (0,1,1,0)$; $c \in \mathcal{P} \setminus (A_2 \cup A_3)$, so $\chi(c) = (1,0,0,1)$; and $d \in \mathcal{P} \setminus (A_1 \cup A_3)$, so $\chi(d) = (0,1,0,1)$. Applying Lemma 4.1 (2) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

These claims complete the proof of (3) implies (4). To finish, assuming that (4) holds, we must demonstrate that the access structures Γ can be realized by a vector space secret sharing scheme. We distinguish two cases.

Case $\alpha = 6$: We have that $A_i \cup A_j = \mathcal{P}$ if $i \neq j$ and, from Lemma 2.5, we may assume that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$. In such a case the incidence vector of any participant is one of the following: $\chi_1 = (1,1,1,0)$, $\chi_2 = (1,1,0,1)$, $\chi_3 = (1,0,1,1)$ or $\chi_4 = (0,1,1,1)$. Observe that the subsets $B_i = \{p \in \mathcal{P}$ such that $\chi(p) = \chi_i\}$ are not empty because $A_i \not\subset A_j$ if $i \neq j$. Hence we have that $\{B_1, B_2, B_3, B_4\}$ is a partition of $\mathcal{P}$. Furthermore, $A_1 = B_1 \cup B_2 \cup B_3$, $A_2 = B_1 \cup B_2 \cup B_4$, $A_3 = B_1 \cup B_3 \cup B_4$ and $A_4 = B_2 \cup B_3 \cup B_4$. Therefore $\Gamma = \widetilde{\Gamma}^e$ where $\widetilde{\Gamma}$ is the access structure on the set of participants $\widetilde{\mathcal{P}} = \{p_1, p_2, p_3, p_4\}$ with basis $\widetilde{\Gamma}_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$. Since $\widetilde{\Gamma}$ is a $(3,4)$-threshold access structure, hence it is a vector space access structure. Therefore applying Lemma 2.4 it follows that Γ is so.

Case $\alpha = 2$: Without loss of generality we may assume that $A_1 \cup A_2 = A_3 \cup A_4 = \mathcal{P}$. On the other hand, from Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$. So we have that $A_1 \cap A_2 = A_3 \cap A_4 = \emptyset$. Hence, the incidence vector of any participant is one of the following: $\chi_1 = (1,0,1,0)$, $\chi_2 = (1,0,0,1)$, $\chi_3 = (0,1,1,0)$ or $\chi_4 = (0,1,0,1)$. Let $B_i = \{p \in \mathcal{P}$ such that $\chi(p) = \chi_i\}$. As before, $\{B_1, B_2, B_3, B_4\}$ is a partition of $\mathcal{P}$, and now we have that $A_1 = B_1 \cup B_2$, $A_2 = B_3 \cup B_4$, $A_3 = B_1 \cup B_3$ and $A_4 = B_2 \cup B_4$. Therefore $\Gamma = (\widetilde{\Gamma})^e$ where $\widetilde{\Gamma}$ is the access structure on the set of participants $\widetilde{\mathcal{P}} = \{p_1, p_2, p_3, p_4\}$ with basis $\widetilde{\Gamma}_0 = \{\{p_1, p_2\}, \{p_3, p_4\}, \{p_1, p_3\}, \{p_2, p_4\}\}$. Since $\widetilde{\Gamma}$ corresponds to a complete bipartite graph, hence it is a vector space access structure. Therefore, from Lemma 2.4, it follows that Γ is so, as we wanted to prove. $\diamond$

Proposition 4.3 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having four elements, $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $A_1 \cup A_2 = \mathcal{P}$ and that*

$A_i \cup A_j \neq \mathcal{P}$ in any other case. Then, the following conditions are equivalent:

1. *Γ is a vector space access structure.*
2. *Γ is an ideal access structure.*
3. *$\rho^*(\Gamma) > 2/3$.*
4. *$A_1 \cup A_3 \cup A_4 = A_2 \cup A_3 \cup A_4 = \mathcal{P}$ and $A_i \cap A_j \cap A_k \subset A_\ell$ if $\{i,j,k,\ell\} = \{1,2,3,4\}$.*

Proof. As in the previous proposition, we only must show that (3) implies (4) and that (4) implies (1). First we are going to prove that if $\rho^*(\Gamma) > 2/3$ then $A_1 \cup A_3 \cup A_4 = A_2 \cup A_3 \cup A_4 = \mathcal{P}$ and $A_i \cap A_j \cap A_k \subset A_\ell$ if $\{i,j,k,\ell\} = \{1,2,3,4\}$. We proceed by five steps.

Step 1. $A_k \not\subset A_i \cup A_\ell$ if $i \in \{1,2\}$ and $\{k,\ell\} = \{3,4\}$.
Proof: It is enough to show that $A_3 \not\subset A_2 \cup A_4$. Assume that $A_3 \subset A_2 \cup A_4$. We are going to prove first that, in such a case, $\chi(p) \neq (0,1,1,1)$ for any participant $p \in \mathcal{P}$. Otherwise we consider $a \in A_3 \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in \mathcal{P}$ with $\chi(b) = (0,1,1,1)$; $c \in \mathcal{P} \setminus (A_2 \cup A_4)$, so $\chi(c) = (1,0,0,0)$; and $d \in \mathcal{P} \setminus (A_1 \cup A_3)$, so $\chi(d) = (0,1,0,d_4)$. Applying Lemma 4.1 (1) it follows a contradiction. To finish the proof of Step 1 now we take the following participants: $a \in A_3 \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in A_3 \setminus A_1$, so $\chi(b) = (0,1,1,b_4)$ and hence $\chi(b) = (0,1,1,0)$; $c \in \mathcal{P} \setminus (A_2 \cup A_4)$, so $\chi(c) = (1,0,0,0)$; and $d \in A_4 \setminus A_1$, so $\chi(d) = (0,1,d_3,1)$ and hence $\chi(d) = (0,1,0,1)$. Applying Lemma 4.1 (2) it follows a contradiction.

Step 2. $A_1 \cup A_3 \cup A_4 = A_2 \cup A_3 \cup A_4 = \mathcal{P}$.
Proof: We only must check that $A_2 \subset A_1 \cup A_3 \cup A_4$ and that $A_1 \subset A_2 \cup A_3 \cup A_4$. We demonstrate the first statement being the second one proved in the same way. Let us suppose that there exists $x \in A_2 \setminus (A_1 \cup A_3 \cup A_4)$, so $\chi(x) = (0,1,0,0)$. From Step 1 there exist participants $a \in A_3 \setminus (A_2 \cup A_4)$, so $\chi(a) = (1,0,1,0)$; $b \in A_4 \setminus (A_2 \cup A_3)$, so $\chi(b) = (1,0,0,1)$; $c \in A_3 \setminus (A_1 \cup A_4)$, so $\chi(c) = (0,1,1,0)$; and $d \in A_4 \setminus (A_1 \cup A_3)$, so $\chi(d) = (0,1,0,1)$. By changing the roles of A_1 and A_3 and the roles of A_2 and A_4 in Lemma 4.1 (4) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Step 3. $A_1 \cap A_2 \cap A_3 \subset A_4$ and $A_1 \cap A_2 \cap A_4 \subset A_3$.
Proof: We demonstrate the first statement being the second one proved in the same way. If $A_1 \cap A_2 \cap A_3 \not\subset A_4$ then there exists a participant b such that $\chi(b) = (1,1,1,0)$. On the other hand from Step 1 we have that $A_k \not\subset A_i \cup A_\ell$ if $i \in \{1,2\}$ and $\{k,\ell\} = \{3,4\}$. Therefore we can consider $a \in A_4 \setminus (A_1 \cup A_3)$, so $\chi(a) = (0,1,0,1)$; $c \in A_4 \setminus (A_2 \cup A_3)$, so $\chi(c) = (1,0,0,1)$; and $d \in A_3 \setminus (A_2 \cup A_4)$, so $\chi(d) = (1,0,1,0)$. By considering the order $\Gamma_0 = \{A_4, A_3, A_2, A_1\}$ in Lemma 4.1 (3), it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Step 4. $A_1 \cap A_3 \cap A_4 \subset A_2$ or $A_2 \cap A_3 \cap A_4 \subset A_1$.
Proof: Otherwise there exist participants $a, b \in \mathcal{P}$ such that $\chi(a) = (1,0,1,1)$ and $\chi(b) = (0,1,1,1)$. Let us consider $c \in A_1 \setminus A_3$, so $\chi(c) = (1,c_2,0,c_4)$, and let

$d \in \mathcal{P} \setminus (A_1 \cup A_3)$, so $\chi(d) = (0,1,0,d_4)$. Applying Lemma 4.1 (1) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Step 5. $A_1 \cap A_3 \cap A_4 \subset A_2$ and $A_2 \cap A_3 \cap A_4 \subset A_1$.
Proof: Otherwise we may assume that $A_1 \cap A_3 \cap A_4 \not\subset A_2$ and $A_2 \cap A_3 \cap A_4 \subset A_1$. We consider the following participants: $a \in (A_1 \cap A_3 \cap A_4) \setminus A_2$, so $\chi(a) = (1,0,1,1)$; $b \in A_3 \setminus A_1$, so $\chi(b) = (0,1,1,0)$; $c \in A_1 \setminus A_3$, so $\chi(c) = (1,c_2,0,c_4)$; and $d \in A_4 \setminus A_1$, so $\chi(d) = (0,1,0,1)$. Applying Lemma 4.1 (2) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

This completes the proof of (3) implies (4).

To finish we must demonstrate that (4) implies (1). So let Γ be an access structure on a set of participants $\mathcal{P}$ with basis $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $A_1 \cup A_2 = \mathcal{P}$ and $A_i \cup A_j \neq \mathcal{P}$ in any other case, and that $A_1 \cup A_3 \cup A_4 = A_2 \cup A_3 \cup A_4 = \mathcal{P}$ and $A_i \cap A_j \cap A_k \subset A_\ell$ if $\{i,j,k,\ell\} = \{1,2,3,4\}$. We want to prove that Γ can be realized by a vector space secret sharing scheme.

From Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$. So we have that $A_i \cap A_j \cap A_k = \emptyset$ for any different $i,j,k \in \{1,2,3,4\}$. Therefore, the incidence vector of any participant is one of the following: $\chi_1 = (1,1,0,0)$, $\chi_2 = (1,0,1,0)$, $\chi_3 = (0,1,1,0)$, $\chi_4 = (1,0,0,1)$ or $\chi_5 = (0,1,0,1)$. Let us consider $B_i = \{p \in \mathcal{P}$ such that $\chi(p) = \chi_i\}$. Since $A_i \cup A_j \neq \mathcal{P}$ for any different $i,j \in \{1,2,3,4\}$ with $\{i,j\} \neq \{1,2\}$, hence it follows that $B_i \neq \emptyset$ for any i. Therefore $\{B_1, B_2, B_3, B_4, B_5\}$ is a partition of $\mathcal{P}$, and $A_1 = B_1 \cup B_2 \cup B_4$, $A_2 = B_1 \cup B_3 \cup B_5$, $A_3 = B_2 \cup B_3$, $A_4 = B_4 \cup B_5$. In such a case we have that $\Gamma = \widetilde{\Gamma}^e$ where $\widetilde{\Gamma}$ is the access structure on the set of participants $\widetilde{\mathcal{P}} = \{p_1, p_2, p_3, p_4, p_5\}$ with basis $\widetilde{\Gamma}_0 = \{\{p_1,p_2,p_4\}, \{p_1,p_3,p_5\}, \{p_2,p_3\}, \{p_4,p_5\}\}$. If $\widetilde{\Gamma}$ is a vector space access structure hence, from Lemma 2.4, it follows that Γ is so. Therefore, in order to finish the proof we must demonstrate that $\widetilde{\Gamma}$ can be realized by a vector space access structure.

Let K be any finite field and let $E = K^3$. Then we define the map $\psi : \widetilde{\mathcal{P}} \cup \{D\} \longrightarrow E$ by $\psi(D) = (1,0,0)$, $\psi(p_1) = (1,1,1)$, $\psi(p_2) = (1,0,1)$, $\psi(p_3) = (0,0,1)$, $\psi(p_4) = (1,1,0)$, and $\psi(p_5) = (0,1,0)$. For any subset $A \subset \widetilde{\mathcal{P}}$ we have that, $A \in \widetilde{\Gamma}$ if and only if the vector $\psi(D)$ can be expressed as a K-linear combination of the vectors in the set $\psi(A) = \{\psi(p) : p \in A\}$, as we wanted to prove. $\diamond$

The characterization of ideal access structures with four minimal qualified subsets is completed by the following three propositions, which consider the case that the set of participants is not covered by any pair of minimal qualified subsets.

Proposition 4.4 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having four elements, $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $A_i \cup A_j \neq \mathcal{P}$ for any $i,j \in \{1,2,3,4\}$ and that $A_i \cup A_j \cup A_k = \mathcal{P}$ for any different $i,j,k \in \{1,2,3,4\}$. Then, the following conditions are equivalent:*

1. *Γ is a vector space access structure.*

2. Γ *is an ideal access structure.*

3. $\rho^*(\Gamma) > 2/3$.

4. $A_i \cap A_j \cap A_k \subset A_\ell$ *if* $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$.

Proof. Let us show that (3) implies (4). That is, assuming $\rho^*(\Gamma) > 2/3$ we want to demonstrate that $A_i \cap A_j \cap A_k \subset A_\ell$ if $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$. By symmetry it is enough to show that $A_2 \cap A_3 \cap A_4 \subset A_1$. First notice that since $A_i \cup A_j \cup A_k = \mathcal{P}$ for any different $i, j, k \in \{1, 2, 3, 4\}$, hence it follows that $A_k \not\subset A_i \cup A_j$ for any different $i, j, k \in \{1, 2, 3, 4\}$. So we can consider the following participants: $a \in A_3 \setminus (A_2 \cup A_4)$, so $\chi(a) = (1, 0, 1, 0)$; $c \in A_1 \setminus (A_3 \cup A_4)$, so $\chi(c) = (1, 1, 0, 0)$; and $d \in A_2 \setminus (A_1 \cup A_3)$, so $\chi(d) = (0, 1, 0, 1)$. If $A_2 \cap A_3 \cap A_4 \not\subset A_1$, then we can take $b \in \mathcal{P}$ with $\chi(b) = (0, 1, 1, 1)$. Applying Lemma 4.1 (3) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

We have to prove now that (4) implies (1). That is, assuming that (4) holds we want to prove that the access structures Γ can be realized by a vector space secret sharing scheme.

Applying Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$. So $A_i \cap A_j \cap A_k = \emptyset$ for any different $i, j, k \in \{1, 2, 3, 4\}$. Hence, the incidence vector of any participant is one of the following: $\chi_1 = (1, 0, 1, 0)$, $\chi_2 = (1, 0, 0, 1)$, $\chi_3 = (1, 1, 0, 0)$, $\chi_4 = (0, 1, 0, 1)$, $\chi_5 = (0, 1, 1, 0)$ or $\chi_6 = (0, 0, 1, 1)$. We define $B_i = \{p \in \mathcal{P}$ such that $\chi(p) = \chi_i\}$. From our assumptions it is not hard to check that $B_i \neq \emptyset$. Therefore, $\{B_1, B_2, B_3, B_4, B_5, B_6\}$ is a partition of $\mathcal{P}$, and $A_1 = B_1 \cup B_2 \cup B_3$, $A_2 = B_3 \cup B_4 \cup B_5$, $A_3 = B_1 \cup B_5 \cup B_6$ and $A_4 = B_2 \cup B_4 \cup B_6$. So we have that $\Gamma = \widetilde{\Gamma}^e$ where $\widetilde{\Gamma}$ is the access structure on the set of participants $\widetilde{\mathcal{P}} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ with basis $\widetilde{\Gamma}_0 = \{\{p_1, p_2, p_3\}, \{p_3, p_4, p_5\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}\}$. We are going to prove that $\widetilde{\Gamma}$ is a K-vector space access structure, where K is a finite field with characteristic 2. Let us consider $E = K^4$ and $\psi : \widetilde{\mathcal{P}} \cup \{D\} \longrightarrow E$ the map defined by $\psi(D) = (1, 0, 0, 0)$, $\psi(p_1) = (1, 0, 1, 0)$, $\psi(p_2) = (0, 1, 1, 0)$, $\psi(p_3) = (0, 1, 0, 0)$, $\psi(p_4) = (1, 1, 1, 1)$, $\psi(p_5) = (0, 0, 1, 1)$ and $\psi(p_6) = (0, 0, 0, 1)$. Let $A \subset \widetilde{\mathcal{P}}$. It is easy to check that $A \in \widetilde{\Gamma}$ if and only if $\psi(D) \in \langle \psi(p) : p \in A \rangle$. Therefore $\widetilde{\Gamma}$ is a K-vector space access structure and hence, from Lemma 2.4, it follows that Γ is so. $\diamond$

Proposition 4.5 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having four elements, $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $A_i \cup A_j \neq \mathcal{P}$ for any $i, j \in \{1, 2, 3, 4\}$, and that $A_i \cup A_j \cup A_k \neq \mathcal{P}$ for any different $i, j, k \in \{1, 2, 3, 4\}$. Then, the following conditions are equivalent:*

1. Γ *is a vector space access structure.*

2. Γ *is an ideal access structure.*

3. $\rho^*(\Gamma) > 2/3$.

4. *For any different* $i, j, k \in \{1,2,3,4\}$ *there exists a permutation* σ *on* $\{i, j, k\}$ *such that* $A_{\sigma(i)} \cap A_{\sigma(j)} = A_{\sigma(i)} \cap A_{\sigma(k)}$.

Proof. We demonstrate that (3) implies (4). Assume that $\rho^*(\Gamma) > 2/3$.

First let us show that, if $A_i \cap A_j \neq A_j \cap A_k$, then $A_i \cap A_k \subset A_j$ for any three different $i, j, k \in \{1,2,3,4\}$. We can suppose that $\{i, j, k\} = \{1,2,3\}$, and that $A_1 \cap A_2 \neq A_2 \cap A_3$. So, without loss of generality, we may assume that $A_2 \cap A_3 \not\subset A_1$. In such a case we want to prove that $A_1 \cap A_3 \subset A_2$. Otherwise, there exists $a \in (A_1 \cap A_3) \setminus A_2$, and hence $\chi(a) = (1,0,1,a_4)$. Besides, we can consider the following participants: $b \in (A_2 \cap A_3) \setminus A_1$, so $\chi(b) = (0,1,1,b_4)$; $c \in \mathcal{P} \setminus (A_2 \cup A_3 \cup A_4)$, so $\chi(c) = (1,0,0,0)$; $d \in \mathcal{P} \setminus (A_1 \cup A_3 \cup A_4)$, so $\chi(d) = (0,1,0,0)$; and $x \in \mathcal{P} \setminus (A_1 \cup A_2 \cup A_3)$, so $\chi(x) = (0,0,0,1)$. Applying Lemma 4.1 (4) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Now let us show that, for any different $i, j, k \in \{1,2,3,4\}$, there exists a permutation σ on $\{i, j, k\}$ such that $A_{\sigma(i)} \cap A_{\sigma(j)} = A_{\sigma(i)} \cap A_{\sigma(k)}$. We can suppose that $\{i, j, k\} = \{1,2,3\}$. Assume that $A_1 \cap A_2 \neq A_2 \cap A_3$ and that $A_1 \cap A_3 \neq A_2 \cap A_3$. Therefore, from above, it follows that $A_1 \cap A_3 \subset A_2$ and $A_1 \cap A_2 \subset A_3$. Hence we get that $A_1 \cap A_3 = A_1 \cap A_2$.

This completes the proof of (3) implies (4).

To finish we must demonstrate that (4) implies (1). That is, assuming that (4) holds we want to prove that the access structures Γ can be realized by a vector space secret sharing scheme. We have to distinguish two cases.

Case 1: $A_{\tau(1)} \cap (A_{\tau(2)} \cup A_{\tau(3)} \cup A_{\tau(4)}) = \emptyset$ for some permutation τ on $\{1,2,3,4\}$. We can suppose that $A_1 \cap (A_2 \cup A_3 \cup A_4) = \emptyset$. By condition (4), there exists a permutation σ on $\{2,3,4\}$ such that $A_{\sigma(2)} \cap A_{\sigma(3)} = A_{\sigma(2)} \cap A_{\sigma(4)}$. In such a case we consider $\Gamma_{0,1} = \{A_2, A_3, A_4\}$ and $\Gamma_{0,2} = \{A_1\}$. From Propositions 2.6 and 3.2 we get that $\Gamma_{0,1}$ and $\Gamma_{0,2}$ define K-vector space access structures for some finite field K. Hence applying Lemma 2.3 it follows that Γ is so.

Case 2: $A_{\tau(1)} \cap (A_{\tau(2)} \cup A_{\tau(3)} \cup A_{\tau(4)}) \neq \emptyset$ for any permutation τ on $\{1,2,3,4\}$. Furthermore, by Lemma 2.5, we can suppose that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$.

We prove first that, in this case, for any different $i, j, k \in \{1,2,3,4\}$ there exists a permutation σ on $\{i, j, k\}$ such that $A_{\sigma(i)} \cap A_{\sigma(j)} = A_{\sigma(i)} \cap A_{\sigma(k)} = \emptyset$. Otherwise, we may assume that $\{i, j, k\} = \{1,2,3\}$ and that $A_1 \cap A_2 = A_1 \cap A_3 \neq \emptyset$. Let us take $\ell \in \{2,3\}$. Then, since condition (4) holds, we have $A_1 \cap A_\ell = A_\ell \cap A_4$ or $A_1 \cap A_\ell = A_1 \cap A_4$ or $A_1 \cap A_4 = A_\ell \cap A_4$. By assumption, $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$ and $A_1 \cap A_2 = A_1 \cap A_3 \neq \emptyset$. Hence it follows that $A_1 \cap A_4 = A_\ell \cap A_4$. Therefore, $A_1 \cap A_4 = A_2 \cap A_4 = A_3 \cap A_4 = \emptyset$ and, hence, $A_4 \cap (A_1 \cup A_2 \cup A_3) = \emptyset$, a contradiction.

We conclude the proof by checking that, in this case, Γ is a vector space access structure. Since $A_1 \cap (A_2 \cup A_3 \cup A_4) \neq \emptyset$, we can suppose that $A_1 \cap A_4 \neq \emptyset$. So, from above with $\{i, j, k\} = \{1,3,4\}$ and $\{i, j, k\} = \{1,2,4\}$, we get that $A_1 \cap A_3 = A_3 \cap A_4 = \emptyset$ and $A_1 \cap A_2 = A_2 \cap A_4 = \emptyset$. Hence, $(A_1 \cup A_4) \cap (A_2 \cup A_3) = \emptyset$. In such a case we consider $\Gamma_{0,1} = \{A_1, A_4\}$ and $\Gamma_{0,2} = \{A_2, A_3\}$. Applying Lemma 2.3 and

Proposition 2.6 it follows that Γ is a vector space access structures over any finite field K, as we wanted to prove. $\diamond$

At this point, only one case is left to conclude the characterization of ideal access structures with four minimal qualified subsets. We are going to use the following lemma to solve it.

Lemma 4.6 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$ and having optimal information rate $\rho^*(\Gamma) > 2/3$. Assume that $A_i \cup A_j \neq \mathcal{P}$ for any $i, j \in \{1,2,3,4\}$. Then, for any different $i, j, k \in \{1,2,3,4\}$ we have that, if $A_i \subset A_j \cup A_k$ then $A_i \cup A_j = A_i \cup A_k = A_j \cup A_k$.*

Proof. We can suppose that $\{i,j,k\} = \{1,2,3\}$ and that $A_3 \subset A_1 \cup A_2$. We must demonstrate that $A_2 \subset A_1 \cup A_3$ and $A_1 \subset A_2 \cup A_3$. By symmetry it is enough to show that $A_2 \subset A_1 \cup A_3$. To do it let us consider the following participants: $x \in \mathcal{P} \setminus (A_1 \cup A_2)$, so $\chi(x) = (0,0,0,1)$; $a \in A_3 \setminus A_2$, so $\chi(a) = (1,0,1,a_4)$; $b \in A_3 \setminus A_1$, so $\chi(b) = (0,1,1,b_4)$; and $c \in A_1 \setminus A_3$, so $\chi(c) = (1, c_2, 0, c_4)$. If $A_2 \not\subset A_1 \cup A_3$ then there exists $d \in \mathcal{P}$ such that $\chi(d) = (0,1,0,d_4)$ and hence, applying Lemma 4.1 (4) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction. $\diamond$

Proposition 4.7 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with basis Γ_0 having four elements, $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$. Assume that $A_i \cup A_j \neq \mathcal{P}$ for any $i, j \in \{1,2,3,4\}$, that $A_1 \cup A_2 \cup A_3 = \mathcal{P}$, and that $A_2 \cup A_3 \cup A_4 \neq \mathcal{P}$. Then, the following conditions are equivalent:*

1. *Γ is a vector space access structure.*
2. *Γ is an ideal access structure.*
3. *$\rho^*(\Gamma) > 2/3$.*
4. *$A_2 \cup A_3 = A_2 \cup A_4 = A_3 \cup A_4$ and $A_1 \cap (A_2 \cup A_3) \subset A_2 \cap A_3 \cap A_4$.*

Proof. In order to demonstrate that (3) implies (4), we are going to prove first that $A_2 \cup A_3 = A_2 \cup A_4 = A_3 \cup A_4$. If $A_4 \subset A_1 \cup A_3$ or $A_4 \subset A_1 \cup A_2$ then from Lemma 4.6 it follows that $A_1 \cup A_3 = A_1 \cup A_4 = A_3 \cup A_4$, or $A_1 \cup A_2 = A_1 \cup A_4 = A_2 \cup A_4$. Therefore $A_1 \subset A_3 \cup A_4$ or $A_1 \subset A_2 \cup A_4$ which leads us to a contradiction since $A_2 \cup A_3 \cup A_4 \neq \mathcal{P}$. So we have that there exist participants $a \in A_4 \setminus (A_1 \cup A_3)$ and $b \in A_4 \setminus (A_1 \cup A_2)$. Hence, their incidence vectors are $\chi(a) = (0,1,0,1)$ and $\chi(b) = (0,0,1,1)$. On the other hand $A_2 \cup A_3 \cup A_4 \neq \mathcal{P}$, so there exists $x \in \mathcal{P}$ with $\chi(x) = (1,0,0,0)$. Assume that $A_2 \not\subset A_3 \cup A_4$ and that $A_3 \not\subset A_2 \cup A_4$. In such a case let us consider $c \in A_2 \setminus (A_3 \cup A_4)$ and $d \in A_3 \setminus (A_2 \cup A_4)$, so $\chi(c) = (c_1, 1, 0, 0)$ and $\chi(d) = (d_1, 0, 1, 0)$. Therefore by considering the order $\Gamma_0 = \{A_2, A_3, A_4, A_1\}$ in Lemma 4.1 (4) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction. So either $A_2 \subset A_3 \cup A_4$

or $A_3 \subset A_2 \cup A_4$. In any case we can apply Lemma 4.6 and, hence, we get that $A_2 \cup A_3 = A_2 \cup A_4 = A_3 \cup A_4$ as we wanted to prove.

Next we prove that $A_1 \cap B \subset A_2 \cap A_3 \cap A_4$, where $B = A_2 \cup A_3 = A_2 \cup A_4 = A_3 \cup A_4$. If $A_1 \cap B \not\subset A_2 \cap A_3 \cap A_4$ then there exists $a \in A_1 \cap B$ such that $a \notin A_2 \cap A_3 \cap A_4$. Since $a \in B$, there are two different $i, j \in \{2, 3, 4\}$ such that $a \in A_i \cap A_j$ and, hence, $a \notin A_\ell$, where $\ell \in \{2, 3, 4\} \setminus \{i, j\}$. Without loss of generality, we can suppose that $a \in A_3 \cap A_4$ and that $a \notin A_2$. Therefore, a has incidence vector $\chi(a) = (1, 0, 1, 1)$. Now observe that $A_2 \not\subset A_1 \cup A_i$ for $i = 3, 4$. In effect, if $A_2 \subset A_1 \cup A_i$ then, from Lemma 4.6, $A_1 \cup A_2 = A_1 \cup A_i = A_2 \cup A_i$, hence $A_1 \subset A_2 \cup A_i$, and so $A_2 \cup A_3 \cup A_4 = \mathcal{P}$, a contradiction. At this point we consider $b \in A_2 \setminus (A_1 \cup A_4)$, so $\chi(b) = (0, 1, 1, 0)$; $c \in \mathcal{P} \setminus (A_2 \cup A_3 \cup A_4)$, so $\chi(c) = (1, 0, 0, 0)$; and $d \in A_2 \setminus (A_1 \cup A_3)$, so $\chi(d) = (0, 1, 0, 1)$. Applying Lemma 4.1 (2) it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

This completes the proof of (3) implies (4). To finish we must demonstrate that (4) implies (1). That is, assuming that (4) holds we want to prove that the access structures Γ can be realized by a vector space secret sharing scheme.

Applying Lemma 2.5 we may assume that $A_1 \cap A_2 \cap A_3 \cap A_4 = \emptyset$. So we have that $A_2 \cup A_3 = A_2 \cup A_4 = A_3 \cup A_4$ and $A_1 \cap (A_2 \cup A_3) = \emptyset$. In such a case we consider $\Gamma_{0,1} = \{A_1\}$ and $\Gamma_{0,2} = \{A_2, A_3, A_4\}$. From Proposition 2.6 and Proposition 3.2 we get that $\Gamma_{0,1}$ and $\Gamma_{0,2}$ define K-vector space access structures for some finite field K. Hence applying Lemma 2.3 it follows that Γ is so. $\diamond$

The characterization of ideal access structures with four minimal qualified subsets has been completed with Proposition 4.7. Next, we present bounds on the optimal information rate for the non-ideal case.

Proposition 4.8 *Let Γ be an access structure on a set of participants $\mathcal{P}$ such that its basis Γ_0 has four elements. Assume that Γ is not realizable by an ideal secret sharing scheme. Then $1/2 \leq \rho^*(\Gamma) \leq 2/3$.*

Proof. We assume that Γ is not realizable by an ideal secret sharing scheme. Hence applying the above propositions it follows that $\rho^*(\Gamma) \leq 2/3$. Now we must show that $\rho^*(\Gamma) \geq 1/2$. In order to do it let us consider $\Gamma_{0,1}, \Gamma_{0,2} \subset \Gamma_0 = \{A_1, A_2, A_3, A_4\}$ the decomposition of Γ defined by $\Gamma_{0,1} = \{A_1, A_2\}$ and $\Gamma_{0,2} = \{A_3, A_4\}$. Let Γ_i be the access structure with basis $\Gamma_{0,i}$ on the set $\mathcal{P}_i = A_{2i-1} \cup A_{2i}$, where $i = 1, 2$. From Proposition 2.6, for any finite field K, there exists an ideal secret sharing scheme with access structure Γ_i and set of secrets K. Besides, for every participant $p \in \mathcal{P}$ we have that $r_p = |\{i \in \{1, 2\}$ such that $p \in \mathcal{P}_i\}| \leq 2$ and that $\lambda_A = |\{i \in \{1, 2\}$ such that $A \in \Gamma_{0,i}\}| = 1$ for any $A \in \Gamma_0$. Therefore, from Proposition 2.2 it follows that $\rho^*(\Gamma) \geq 1/2$, as we wanted to prove. $\diamond$

To finish, we provide some examples of access structures with four minimal qualified subsets. Namely, we present access structures in each one of the following situations: $1/2 \leq \rho^*(\Gamma) \leq 3/5$, $3/5 \leq \rho^*(\Gamma) \leq 2/3$, $\rho^*(\Gamma) = 2/3$ and $\rho^*(\Gamma) = 1$.

Example 4.9 Let Γ be the access structure on the set of six participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ with basis $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$ where $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_2, p_3, p_5\}$, $A_3 = \{p_2, p_6\}$, and $A_4 = \{p_1, p_3, p_4\}$. Observe that $A_i \cup A_j \neq \mathcal{P}$ for any different i, j, that $A_2 \cup A_3 \cup A_4 = \mathcal{P}$ and that $A_1 \cup A_2 \cup A_3 \neq \mathcal{P}$. Then, since $A_1 \cup A_2 \neq A_1 \cup A_3$, from Propositions 4.7 and 4.8, we obtain $1/2 \leq \rho^*(\Gamma) \leq 2/3$. In this case, we can find a better upper bound: $\rho^*(\Gamma) \leq 3/5$. In order to do it, let us consider the subsets $B_1 = \{p_4\}$, $B_2 = \{p_4, p_5\}$, $B_3 = \{p_4, p_5, p_6\}$ and $B_4 = \{p_4, p_5, p_6, p_1\}$. Equally, we take the subsets $X_1 = \{p_1, p_3\}$, $X_2 = \{p_2, p_3\}$, $X_3 = \{p_2\}$ and $X_4 = \{p_3\}$. It is not difficult to check that the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \subset B_4$ is made independent by the set $A = \{p_1, p_2, p_3\}$. Since $A \in \Gamma$, we have, from Proposition 2.1, that $\rho^*(\Gamma) \leq 3/5$.

Example 4.10 Let us consider now the access structure Γ on a set of seven participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ having minimal qualified subsets $A_1 = \{p_1, p_5\}$, $A_2 = \{p_2, p_6\}$, $A_3 = \{p_3, p_7\}$ and $A_4 = \{p_4, p_5, p_6, p_7\}$. In this case, $A_i \cup A_j \cup A_k \neq \mathcal{P}$ for any different $i, j, k \in \{1, 2, 3, 4\}$ and $A_1 \cap A_4 = \{p_5\}$, $A_1 \cap A_2 = \emptyset$ and $A_2 \cap A_4 = \{p_6\}$. Therefore, from Proposition 4.5, we have that Γ is not ideal and, hence, $1/2 \leq \rho^*(\Gamma) \leq 2/3$. In this case we can improve the lower bound by checking that $\rho^*(\Gamma) \geq 3/5$. In effect, we consider the decomposition of Γ given by the six substructures $\Gamma_{0,\{i,j\}} = \{A_i, A_j\}$, where $i \neq j$, and we obtain $\rho^*(\Gamma) \geq 3/5$ by applying Propositions 2.2 and 2.6.

Example 4.11 Let Γ be the access structure on the set of seven participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ with basis $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$ where $A_1 = \{p_1, p_2, p_4, p_5\}$, $A_2 = \{p_2, p_3, p_5, p_6\}$, $A_3 = \{p_1, p_3, p_4, p_6\}$, and $A_4 = \{p_2, p_5, p_7\}$. We have that $A_3 \cup A_4 = \mathcal{P}$ and that $A_i \cup A_j \neq \mathcal{P}$ otherwise. Besides, $A_1 \cup A_2 \cup A_3 \neq \mathcal{P}$. Therefore, from Proposition 4.3, Γ is not an ideal access structure and so its optimal information rate is bounded by $1/2 \leq \rho^*(\Gamma) \leq 2/3$. We are going to prove now that $\rho^*(\Gamma) = 2/3$. Let us consider the decomposition of Γ given by $\Gamma_{0,1} = \{A_1, A_2, A_3\}$, $\Gamma_{0,2} = \{A_1, A_2, A_4\}$ and $\Gamma_{0,3} = \{A_3, A_4\}$. From Propositions 2.6 and 3.2, we have that the access structures Γ_1, Γ_2 and Γ_3, having basis $\Gamma_{0,1}$, $\Gamma_{0,2}$ and $\Gamma_{0,3}$, respectively, are K-vector space access structure for some finite field K. Applying Proposition 2.2, we have that $\rho^*(\Gamma) \geq 2/3$.

Example 4.12 Let Γ be the access structure on $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ defined by $\Gamma_0 = \{\{p_1, p_2, p_3\}, \{p_3, p_4, p_5\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_1, p_4\}, \{p_2, p_5\}, \{p_3, p_6\}\}$. The dual access structure Γ^* of Γ has basis $(\Gamma^*)_0 = \{A_1, A_2, A_3, A_4\}$ where $A_1 = \{p_1, p_2, p_3\}, A_2 = \{p_3, p_4, p_5\}, A_3 = \{p_1, p_5, p_6\}, A_4 = \{p_2, p_4, p_6\}$. Here we have that $A_i \cup A_j \neq \mathcal{P}$ for any $i, j \in \{1, 2, 3, 4\}$, while $A_i \cup A_j \cup A_k = \mathcal{P}$ and $A_i \cap A_j \cap A_k = \emptyset$ for any different $i, j, k \in \{1, 2, 3, 4\}$. Hence, applying Proposition 4.4 it follows that Γ^* is a vector space access structure and so it is Γ. In particular, $\rho^*(\Gamma) = 1$.

5 Conclusion and open problems

The characterization of ideal access structures and the search for bounds on the optimal information rate are two of the main open problems in secret sharing. These problems are studied in this paper for the access structures with three or four minimal qualified subsets.

We completely characterize the ideal access structures in this family. One of the results we obtain in this paper is that the ideal access structures, in the family we consider, coincide with the vector space ones and, besides, there is no access structure whose optimal information rate is such that $2/3 < \rho^*(\Gamma) < 1$. This situation is the same as in other families of access structures considered in previous works. An interesting open problem is to find out to which extent these results can be generalized. For instance, as far as we know, no access structure with optimal information rate between 2/3 and 1 has been found.

Besides, we prove that the optimal information rate of any non-ideal access structure with three minimal qualified subsets is equal to 2/3, and we provide bounds on the optimal information rate for the non-ideal access structures with four minimal qualified subsets. Namely, we prove that $1/2 \leq \rho^*(\Gamma) \leq 2/3$ for any non-ideal access structure Γ with four minimal qualified subsets. While the upper bound is tight, we do not know if the lower bound is so. Moreover, another open problem is the determination of the optimal information rate of *all* access structures with four minimal qualified subsets.

References

[1] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.* 48 (1979), 313–317.

[2] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography.* 11 (1997), 107–122.

[3] 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.

[4] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro. Graph decompositions and secret sharing schemes. *J. Cryptology.* 8 (1995), 39–64.

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

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

[7] E.F. Brickell, D.R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology.* 5 (1992), 153–166.

[8] 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.

[9] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.* (1987), 99–102.

[10] W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Designs, Codes and Cryptography.* 4 (1994), 83–95.

[11] W.-A. Jackson, K.M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography.* 9 (1996), 267–286.

[12] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory.* Vol. 46, No. 7 (2000), 2596–2604.

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

[14] 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.

[15] D.R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography.* 2 (1992), 357–390.

[16] D.R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Trans. on Information Theory.* 40 (1994), 118–125.

[17] D.R. Stinson. *Cryptography: Theory and Practice.* CRC Press Inc., Boca Raton (1995).