Secret sharing schemes on access structures with intersection number equal to one[*]

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

The characterization of ideal access structures and the search for bounds on the optimal information rate are two important problems in secret sharing. These problems are studied in this paper for access structures with intersection number equal to one, that is, access structures such that there is at most one participant in the intersection of any two different minimal qualified subsets. The main result in this work is the complete characterization of the ideal access structures with intersection number equal to one. Besides, bounds on the optimal information rate are provided for the non-ideal case.

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

1 Introduction

A *secret sharing scheme* Σ is a method to distribute shares of a secret value $k \in \mathcal{K}$ 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 from their shares. Secret sharing was introduced by Blakley [1] and Shamir [15]. A comprehensive introduction to this topic can be found in [17]. A secret sharing scheme is said to be *perfect* if no information about the value of the secret can be obtained from the shares of all the participants in a *non-qualified subset*. We are going to consider only perfect secret sharing schemes. The security of these schemes is *unconditional* because it does not depend on the amount of computation that can be carried out by a subset of participants.

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

[*] This work was partially supported by the Spanish *Ministerio de Ciencia y Tecnología* under project TIC 2000-1044. A previous version of this work appeared in the Proceedings of *Third Conference on Security in Communication Networks '02*, Amalfi, Italy, 2002.

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. The *rank* and the *corank* of Γ are, respectively, the maximum and the minimum number of participants in a minimal qualified subset. The *intersection number* of Γ is the maximum number of participants in the intersection of two different minimal qualified subsets.

The first works about secret sharing [1, 15] considered only schemes with a (t, n)-*threshold access structure*, whose basis is formed by all subsets with exactly t participants from a set of n participants. Further works considered the problem of finding secret sharing schemes for more general access structures. Ito, Saito and Nishizeki [10] proved that there exists a secret sharing scheme for any access structure, and Brickell [5] introduced the *vector space construction* which provides secret sharing schemes for a wide family of access structures, the *vector space access structures*. While in the threshold schemes proposed by Blakley [1] and Shamir [15] and in the vector space schemes given by Brickell [5] the shares have the same size as the secret, in the schemes constructed in [10] 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 a key point in the design of secret sharing schemes. Therefore, one of the main 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, $\rho(\Sigma, \Gamma, \mathcal{K}) = \log |\,\mathcal{K}\,| / \max_{p \in \mathcal{P}} \log |\,\mathcal{S}_p\,|$, where $\mathcal{S}_p$ is the set of all possible values of the share s_p corresponding to the participant 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. For example, threshold access structures and the vector space ones are ideal.

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]. Several techniques have been introduced in [4, 7, 18] 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 [14].

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 sets of four [17] and five [12] participants, access structures defined by graphs [2, 3, 4, 6, 7, 8, 18], bipartite access structures [14], and access structures with three or four minimal qualified subsets [13]. 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. Namely, 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 those problems in another family of access structures: the access structures with intersection number equal to one, that is, access structures such that there is at most one participant in the intersection of any two different minimal qualified subsets. We obtain similar results as in the previously considered families. Namely, we prove that the ideal access structures with intersection number equal to one coincide with the vector space ones, and that there is no access structure with intersection number equal to one and optimal information rate between 2/3 and 1. Besides, we completely characterize the ideal access structures with intersection number equal to one, and we provide some bounds on the optimal information rate for the non-ideal case.

These results include those previously obtained for access structures defined by graphs. The access structure $\Gamma = \Gamma\langle G\rangle$ defined by a graph G with vertex set $V(G)$ and edge set $E(G)$ is the access structure on the set of participants $\mathcal{P} = V(G)$ having basis $\Gamma_0 = E(G)$. Observe that Γ has rank and corank equal to two and intersection number equal to one. Therefore, the family of access structures we consider in this paper can be seen as a generalization of those defined by graphs.

The access structures associated to a finite projective plane are other examples of access structures with intersection number equal to one. In this case, the set of participants is the set of points of the plane, while the lines are the minimal qualified subsets. For instance, an access structure with rank and corank equal to three, seven participants and seven minimal qualified subsets is obtained from the *Fano plane*, the projective plane of order two.

Our main result, Theorem 3.1, states that there are relatively few ideal access structures with intersection number equal to one. Namely, we prove that they are one of the following: the access structures defined by complete multipartite graphs, those defined by stars, and the one associated to the Fano plane together with three other access structures related to it.

The organization of the paper is as follows. The above mentioned access structures are introduced in Section 2 and we prove there that they are vector space access structures. Section 3 is devoted to characterize the ideal access structures having intersection number equal to one by proving that they are precisely the access structures considered in Section 2. Finally, some bounds on the optimal information rate are presented in Section 4.

2 Some vector space access structures

An access structure Γ on a set of participants $\mathcal{P}$ is said to be a *vector space access structure* over a finite field $\mathbb{K}$ if there exist a vector space E over $\mathbb{K}$ and a map $\psi : \mathcal{P} \cup \{D\} \longrightarrow E \setminus \{0\}$, where $D \notin \mathcal{P}$ is called the *dealer*, 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 ψ is said to be a *realization* of the $\mathbb{K}$-vector space access structure Γ. Any vector space access structure can be realized by an ideal scheme (see [5] or [17] for proofs). For instance, the threshold access structures and those defined by a complete multipartite graph $K_{n_1,\ldots,n_\ell}$ are vector space access structures [17] and, hence, they are ideal.

The purpose of this section is to point out some vector space access structures with intersection number equal to one. Namely we present the access structures $\Gamma\langle S(p_0)\rangle$ defined by a star (Proposition 2.1), the access structure Γ_2 associated to the Fano plane (Proposition 2.2), and its related access structures $\Gamma_{2,1}$, $\Gamma_{2,2}$ and $\Gamma_{2,3}$ (Propositions 2.3, 2.4 and 2.5). In fact, as we will prove later, these access structures together with those defined by a complete multipartite graph are the only ideal access structures with intersection number equal to one.

It is said that an access structure Γ on a set of participants $\mathcal{P}$ is a *star access structure* if there exists $p_0 \in \mathcal{P}$ such that $A \cap A' = \{p_0\}$ for any two different minimal qualified subsets $A, A' \in \Gamma_0$. In such a case we denote $\Gamma_0 = S(p_0)$ and $\Gamma = \Gamma\langle S(p_0)\rangle$. Observe that the intersection number of a star access structure is equal to one.

Proposition 2.1 *Let $\Gamma\langle S(p_0)\rangle$ be a star access structure on the set of participants $\mathcal{P}$. Then, $\Gamma\langle S(p_0)\rangle$ is a vector space access structure.*

Proof. Let $\Gamma = \Gamma\langle S(p_0)\rangle$ be a star with basis $\Gamma_0 = S(p_0) = \{A_1, \ldots, A_r\}$. For any $i = 1, \ldots, r$ we select a participant $p_i \in A_i \setminus \{p_0\}$ and we identify all participants in $A_i \setminus \{p_0\}$ to p_i. We obtain in this way the access structure $\widetilde{\Gamma}$ on the set of $r+1$ participants $\widetilde{\mathcal{P}} = \{p_0, p_1, \ldots, p_r\}$ having basis $\widetilde{\Gamma}_0 = \{\{p_0, p_1\}, \ldots, \{p_0, p_r\}\}$. Since $\widetilde{\Gamma}_0 = K_{1,r}$ is a complete multipartite graph, then $\widetilde{\Gamma}$ is a vector space access structure over any finite field $\mathbb{K}$. In this situation, it is not difficult to prove that Γ is also a vector space access structure over any finite field $\mathbb{K}$. □

A *finite projective plane* of order n consists of n^2+n+1 points and n^2+n+1 lines with $n+1$ points on each line, $n+1$ lines through each point, each pair of lines meeting at one point, and dually each pair of points lying on one line. The finite projective plane of order $n = 2$ is called the *Fano plane*. See [9] for a complete introduction to finite projective planes.

For any finite projective plane, we can consider its associated access structure Γ_n, whose set of participants $\mathcal{P}$ is the set of n^2+n+1 points of the plane, and whose basis $(\Gamma_n)_0$ consists of its n^2+n+1 lines. Notice that Γ_n has intersection number equal to one and rank and corank equal to $n+1$.

Proposition 2.2 *Let Γ_2 be the access structure associated to the Fano plane. That is, Γ_2 is the access structure on the set $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ of seven participants with basis $(\Gamma_2)_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_7\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_7\}, \{p_3, p_4, p_5\}, \{p_3, p_6, p_7\}\}$. Then, Γ_2 is a vector space access structure.*

Proof. Let $\mathbb{K}$ be a finite field of characteristic two and let $\psi : \mathcal{P} \cup \{D\} \to \mathbb{K}^4$ be the map defined by $\psi(D) = (1,0,0,0)$, $\psi(p_1) = (1,0,1,0)$, $\psi(p_2) = (0,1,1,0)$, $\psi(p_3) = (0,1,0,0)$, $\psi(p_4) = (1,1,1,1)$, $\psi(p_5) = (0,0,1,1)$, $\psi(p_6) = (0,0,0,1)$, and $\psi(p_7) = (1,1,0,1)$. It is not hard to check that if $A \subset \mathcal{P}$ then, $A \in \Gamma_2$ is and only if the vector $\psi(D)$ can be expressed as a linear combination of the vectors in the set $\psi(A) = \{\psi(p) : p \in A\}$. So, Γ_2 is a vector space access structure over any finite field of characteristic two. □

Finally, we introduce some access structures related to the Fano plane that are also vector space access structures with intersection number equal to one.

Proposition 2.3 *Let $\Gamma_{2,1}$ 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 $(\Gamma_{2,1})_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_3, p_4, p_5\}\}$. Then, $\Gamma_{2,1}$ is a vector space access structure.*

Proof. Let Γ be an access structure on a set of participants $\mathcal{P}$. Let $p_0 \in \mathcal{P}$. On the set of participants $\mathcal{P} \setminus \{p_0\}$ we consider the access structure $\Gamma \,|\, p_0$ induced by Γ. That is, $\Gamma \,|\, p_0 = \{A \subset \mathcal{P} \setminus \{p_0\}$ such that $A \in \Gamma\}$. It is easy to show that if Γ is a $\mathbb{K}$-vector space access structure, then $\Gamma \,|\, p_0$ is so. In our case we have that $\Gamma_{2,1} = \Gamma_2 \,|\, p_7$. Hence, $\Gamma_{2,1}$ is a vector space access structure. □

Proposition 2.4 *Let $\Gamma_{2,2}$ 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 $(\Gamma_{2,2})_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}$, $\{p_3, p_4, p_5\}$, $\{p_1, p_4\}, \{p_2, p_5\}, \{p_3, p_6\}\}$. Then, $\Gamma_{2,2}$ is a vector space access structure.*

Proof. The dual Γ^* of an access structure Γ is the access structure $\Gamma^* = \{A \subset \mathcal{P} : \mathcal{P} \setminus A \notin \Gamma\}$. It is well known that an access structure Γ is a vector space access structure over a finite field $\mathbb{K}$ if and only if its dual Γ^* is so [11]. Therefore, since $\Gamma_{2,2} = (\Gamma_{2,1})^*$, hence $\Gamma_{2,2}$ is a vector space access structure. □

Proposition 2.5 *Let $\Gamma_{2,3}$ be the access structure on the set of five participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5\}$ with basis $(\Gamma_{2,3})_0 = \{\{p_1, p_2, p_3\}, \{p_3, p_4, p_5\}, \{p_1, p_4\}, \{p_2, p_5\}\}$. Then, $\Gamma_{2,3}$ is a vector space access structure.*

Proof. This proof works as the one of Proposition 2.3. Namely, since $\Gamma_{2,2}$ is a vector space access structure hence it follows that $\Gamma_{2,3} = \Gamma_{2,2} \,|\, p_6$ is so. □

Remark 2.6 Observe that no new vector space access structure can be obtained by duality from the Fano plane Γ_2 because $\Gamma_2^* = \Gamma_2$. Since $\Gamma_{2,3}^* \cong \Gamma_{2,3}$, the same occurs with the structure $\Gamma_{2,3}$.

Remark 2.7 It is well known that the access structure defined by a complete multipartite graph $K_{n_1,\ldots,n_\ell}$ is a vector space access structure over any finite field $\mathbb{K}$ with at least $\ell + 1$ elements. Besides, from the proofs of the above propositions it follows that $\Gamma\langle S(p_0)\rangle$ is a vector space access structure over any finite field, while the access structures Γ_2, $\Gamma_{2,1}$, $\Gamma_{2,2}$ and $\Gamma_{2,3}$ are vector space access structures over any finite field of characteristic two. Therefore, for any finite family $\Gamma_1, \ldots, \Gamma_r$, where every Γ_i is one of the above access structures, there exists a finite field $\mathbb{K}$ such that Γ_i is a $\mathbb{K}$-vector space access structures for any $i = 1, \ldots, r$. It is interesting to notice that, in fact, the access structure $\Gamma_{2,3}$ can also be realized as a vector space access structure over any finite field $\mathbb{K}$. Namely, if $\mathbb{K}$ is a finite field then the map $\psi : \mathcal{P} \cup \{D\} \to \mathbb{K}^3$ defined by $\psi(D) = (1,0,0)$, $\psi(p_1) = (1,0,1)$, $\psi(p_2) = (1,1,0)$, $\psi(p_3) = (1,1,1)$, $\psi(p_4) = (0,0,1)$, and $\psi(p_5) = (0,1,0)$, is a realization of $\Gamma_{2,3}$ as a $\mathbb{K}$-vector space access structure.

3 Characterization of ideal access structures

The aim of this section is to prove Theorem 3.1, which provides a complete characterization of ideal access structures with intersection number equal to one. Besides, this theorem states that ideal access structures coincide with the vector space ones and with those having optimal information rate greater than 2/3. Therefore, there does not exist any access structure with intersection number equal to one and optimal information rate between 2/3 and 1.

Let us introduce first some definitions. Let Γ be an access structure on a set of participants $\mathcal{P}$. We say that Γ is *connected* if for any pair of participants $p, q \in \mathcal{P}$ there exist $A_1, \ldots, A_\ell \in \Gamma_0$ such that $p \in A_1$, $q \in A_\ell$, and $A_i \cap A_{i+1} \neq \emptyset$ for any $1 \leq i \leq \ell - 1$. For any subset $\mathcal{Q} \subset \mathcal{P}$, the access structure *induced* by Γ on the subset $\mathcal{Q}$ is defined by $\Gamma(\mathcal{Q}) = \{A \in \Gamma : A \subset \mathcal{Q}\}$. It is clear that, for any access structure Γ on a set of participants $\mathcal{P}$, there exists an unique partition $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$ such that the induced access structures $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ are connected and $\Gamma = \Gamma(\mathcal{P}_1) \cup \cdots \cup \Gamma(\mathcal{P}_r)$. In this situation we say that $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ are the *connected components* of Γ.

Theorem 3.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$ with intersection number equal to one. 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. *Every connected component of Γ is either an access structure defined by a complete multipartite graph $\Gamma\langle K_{n_1,\ldots,n_\ell}\rangle$, or a star $\Gamma\langle S(p_0)\rangle$, or the access structure associated to the Fano plane Γ_2, or one of its related access structures $\Gamma_{2,1}$, $\Gamma_{2,2}$ or $\Gamma_{2,3}$.*

The rest of this section is devoted to prove this theorem. A vector space access structure is ideal and, hence, its optimal information rate is equal to one. Therefore we have that (1) implies (2) and that (2) implies (3). Furthermore, from the next lemma and the results in Section 2 it follows that (4) implies (1).

Lemma 3.2 *Let $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ be the connected components of an access structure Γ on a set of participants $\mathcal{P}$. Assume that $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ are vector space access structures over a finite field $\mathbb{K}$. Then, the access structure Γ is so.*

Proof. We assume that $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ are $\mathbb{K}$-vector space access structures. So, for $1 \leq i \leq r$ there exists a realization $\psi_i : \mathcal{P}_i \cup \{D_i\} \rightarrow E_i$ of $\Gamma(\mathcal{P}_i)$. We can suppose that $E_i = \mathbb{K} \times E_i'$ and that $\psi_i(D_i) = (1, 0) \in \mathbb{K} \times E_i'$. Let us consider the $\mathbb{K}$-vector space $E = \mathbb{K} \times E_1' \times \cdots \times E_r'$ and the map $\psi : \mathcal{P} \cup \{D\} \rightarrow E$ defined by $\psi(D) = (1, 0, \ldots, 0)$ and, if $p \in \mathcal{P}_i$, $\psi(p) = (\xi_p, 0, \ldots, v_p, \ldots, 0) \in \mathbb{K} \times E_1' \times \cdots \times E_i' \times \cdots \times E_r'$, where $\psi_i(p) = (\xi_p, v_p) \in \mathbb{K} \times E_i'$. It is not difficult to check that ψ is a realization of Γ as a $\mathbb{K}$-vector space access structure. □

Therefore, the proof of Theorem 3.1 will be concluded by proving that (3) implies (4). Let Γ be an access structure with connected components $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$. Observe that any secret sharing scheme Σ for Γ with set of secrets $\mathcal{K}$ induces, for every $i = 1, \ldots, r$, a secret sharing scheme Σ_i for $\Gamma(\mathcal{P}_i)$ with the same set of secrets and information rate $\rho(\Sigma_i, \Gamma(\mathcal{P}_i), \mathcal{K}) \geq \rho(\Sigma, \Gamma, \mathcal{K})$. Then, it is clear that $\rho^*(\Gamma) \leq \min\{\rho^*(\Gamma(\mathcal{P}_1)), \ldots, \rho^*(\Gamma(\mathcal{P}_r))\}$. Thus, to finish the proof of Theorem 3.1, it is enough to demonstrate that any connected access structure Γ on a set of participants $\mathcal{P}$ with intersection number equal to one and optimal information rate $\rho^*(\Gamma) > 2/3$ is either a complete multipartite graph $\Gamma\langle K_{n_1,\ldots,n_\ell}\rangle$, or a star $\Gamma\langle S(p_0)\rangle$, or the access structure associated to the Fano plane Γ_2, or one of its related access structures $\Gamma_{2,1}$, $\Gamma_{2,2}$ or $\Gamma_{2,3}$.

In order to prove it we distinguish two cases. The first one, which is solved in Subsection 3.1 by Proposition 3.6, deals with access structures with corank greater than two. The second one considers access structures with corank equal to two and is proved by Proposition 3.11 in Subsection 3.2.

Some lemmas, which determine several forbidden situations in an ideal access structure with intersection number equal to one, are needed to prove these propositions. The *independent sequence method* is a key point in the proof of these lemmas. This method was introduced by Blundo, De Santis, De Simone and Vaccaro in [2, Theorem 3.8] and was generalized by Padró and Sáez in [14, Theorem 2.1]. The independent sequence method works as follows. 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 $A \subset \mathcal{P}$, that is to say, 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. Then, $\rho^*(\Gamma) \leq |A|/(m+1)$ if $A \in \Gamma$, while $\rho^*(\Gamma) \leq |A|/m$ whenever $A \notin \Gamma$.

3.1 Ideal access structures with corank greater than two

The purpose of this subsection is to prove Proposition 3.6. In the following three lemmas, which are used in its proof, we assume that Γ is an access structure on a set of participants $\mathcal{P}$ having basis Γ_0, with intersection number equal to one, $\mathrm{corank}(\Gamma) \geq 3$, and optimal information rate $\rho^*(\Gamma) > 2/3$.

Lemma 3.3 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets and $p_{12}, p_{23}, p_{13} \in \mathcal{P}$ be three different participants such that $A_i \cap A_j = \{p_{ij}\}$ if $1 \leq i < j \leq 3$. Then, $(A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}, p_{13}\} \in \Gamma$.*

Proof. We are going to prove first that $(A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}\} \in \Gamma$. Let us suppose that it is false. In this case, we can consider the subsets $B_1 = (A_2 \cup \{p_{13}\}) \setminus \{p_{12}, p_{23}\}$, $B_2 = (A_1 \cup A_2) \setminus \{p_{12}, p_{23}\}$ and $B_3 = (A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}\}$. On one hand we have that the subsets $B_1 \cup \{p_{12}, p_{23}\}$, $B_2 \cup \{p_{12}\}$ and $B_3 \cup \{p_{23}\}$ are qualified because $A_2 \subset B_1 \cup \{p_{12}, p_{23}\}$, $A_1 \subset B_2 \cup \{p_{12}\}$ and $A_3 \subset B_3 \cup \{p_{23}\}$. On the other hand we claim that the subsets $B_1 \cup \{p_{12}\} = (A_2 \cup \{p_{13}\}) \setminus \{p_{23}\}$ and $B_2 \cup \{p_{23}\} = (A_1 \cup A_2) \setminus \{p_{12}\}$ are not qualified. In effect, since the intersection number of Γ is equal to one, any minimal qualified subset $C \in \Gamma_0$ such that $C \subset (A_2 \cup \{p_{13}\}) \setminus \{p_{23}\}$

or $C \subset (A_1 \cup A_2) \setminus \{p_{12}\}$ has at most two elements, which is a contradiction with $\mathrm{corank}(\Gamma) \geq 3$. Therefore, the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ is made independent by the set $A = \{p_{12}, p_{23}\} \notin \Gamma$ by taking $X_1 = \{p_{12}, p_{23}\}$, $X_2 = \{p_{12}\}$ and $X_3 = \{p_{23}\}$. Hence, by the independent sequence method it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Let us prove now that $(A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}, p_{13}\} \in \Gamma$. Let $A_4 \in \Gamma_0$ be a minimal qualified subset such that $A_4 \subset (A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}\}$. We only have to prove that $p_{13} \notin A_4$. If $p_{13} \in A_4$, then A_4 has at most two elements because $A_4 = \bigcup_{i=1}^{3}(A_4 \cap A_i)$, the intersection number of Γ is equal to one, and $p_{13} \in A_4 \cap A_1 \cap A_3$. But this is a contradiction with $\mathrm{corank}(\Gamma) \geq 3$. □

Lemma 3.4 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets and $p_{12}, p_{23}, p_{13} \in \mathcal{P}$ be three different participants such that $A_i \cap A_j = \{p_{ij}\}$ if $1 \leq i < j \leq 3$. Then, $|A_i| = 3$ for every $i = 1, 2, 3$.*

Proof. By symmetry, it is enough to prove that $|A_2| = 3$. From Lemma 3.3, there exists a minimal qualified subset $A \in \Gamma_0$ such that $A \subset (A_1 \cup A_2 \cup A_3) \setminus \{p_{12}, p_{23}, p_{13}\}$. Since Γ has intersection number one and its corank is at least three, $A = \{\alpha_1, \alpha_2, \alpha_3\}$ where $A \cap A_i = \{\alpha_i\}$. We can apply now Lemma 3.3 to the minimal qualified subsets A_1, A_2 and A. Then, there exists a minimal qualified subset $B \in \Gamma_0$ such that $B \subset (A_1 \cup A_2 \cup A) \setminus \{p_{12}, \alpha_1, \alpha_2\}$. As before, we have that $B = \{\beta_1, \beta_2, \alpha_3\}$, where $B \cap A_1 = \{\beta_1\}$, $B \cap A_2 = \{\beta_2\}$ and $B \cap A = \{\alpha_3\}$. We apply now Lemma 3.3 to the minimal qualified subsets A_1, A and B and we see that there exists a minimal qualified subset $C \in \Gamma_0$ such that $C \subset (A_1 \cup A \cup B) \setminus \{\alpha_1, \alpha_3, \beta_1\}$ and, then, $|C| = 3$. Observe that $C \cap A = \{\alpha_2\}$ and $C \cap B = \{\beta_2\}$ and, hence, $\alpha_2, \beta_2 \in A_2 \cap C$. Since $\alpha_2 \neq \beta_2$ and the intersection number of Γ is equal to one, we have that $A_2 = C$ and, then, A_2 has exactly three elements. □

Lemma 3.5 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets such that $A_1 \cap A_2 \neq \emptyset$, $A_3 \cap (A_1 \cup A_2) \neq \emptyset$ and $A_1 \cap A_3 \neq A_2 \cap A_3$. Then, $A_i \cap A_3 \neq \emptyset$ for every $i = 1, 2$.*

Proof. Since $A_3 \cap (A_1 \cup A_2) \neq \emptyset$, we can assume that $A_1 \cap A_3 \neq \emptyset$. We have to prove that $A_2 \cap A_3 \neq \emptyset$. By assumption, $A_1 \cap A_3 \neq A_2 \cap A_3$ and Γ has intersection number equal to one. Then, there exist two different participants $a, c \in \mathcal{P}$ such that $\{a\} = A_1 \cap A_2$ and $\{c\} = A_1 \cap A_3$. We have to prove that there exists a participant $b \neq a, c$ such that $\{b\} = A_2 \cap A_3$.

We are going to prove first that $(A_1 \cup A_2 \cup A_3) \setminus \{a, c\} \in \Gamma$. Let us suppose that this is false. In this case, we consider the subsets $B_1 = A_1 \setminus \{a, c\}$, $B_2 = (A_1 \cup A_2) \setminus \{a, c\}$ and $B_3 = (A_1 \cup A_2 \cup A_3) \setminus \{a, c\}$. It is clear that the subsets $B_1 \cup \{a, c\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{c\}$ are qualified, while the subset $B_1 \cup \{a\}$ is not qualified. Furthermore, since Γ has intersection number equal to one and its corank is at least three, $B_2 \cup \{c\} = (A_1 \cup A_2) \setminus \{a\}$ is not a qualified subset. Therefore, the set $\{a, c\}$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ by taking $X_1 = \{a, c\}$, $X_2 = \{a\}$ and $X_3 = \{c\}$. Hence, by the independent sequence method it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Let $A_4 \in \Gamma_0$ be a minimal qualified subset such that $A_4 \subset (A_1 \cup A_2 \cup A_3) \setminus \{a, c\}$. Since $\operatorname{corank}(\Gamma) \geq 3$ and the intersection number of Γ is equal to one, we have that $A_4 = \{\alpha_1, \alpha_2, \alpha_3\}$, where $\alpha_i \in A_i \setminus (A_j \cup A_k)$ if $\{i, j, k\} = \{1, 2, 3\}$. Observe that we can apply Lemma 3.4 to the subsets A_1, A_3 and A_4 and we get $|A_1| = |A_3| = 3$. Therefore $A_1 = \{a, c, \alpha_1\}$ and $A_3 = \{c, \alpha_3, b\}$ for some participant b. From Lemma 3.3, $\{a, \alpha_2, b\} = (A_1 \cup A_3 \cup A_4) \setminus \{c, \alpha_1, \alpha_3\} \in \Gamma$. Since $a, \alpha_2 \in A_2$ and the intersection number of Γ is equal to one, hence it follows that $A_2 = \{a, \alpha_2, b\}$ and, so, $\{b\} = A_2 \cap A_3$. □

Proposition 3.6 *Let Γ be a connected access structure on a set of participants $\mathcal{P}$ with intersection number equal to one,* $\operatorname{corank}(\Gamma) \geq 3$*, and optimal information rate $\rho^*(\Gamma) > 2/3$. Then, Γ is either a star $\Gamma\langle S(p_0)\rangle$, or the access structure associated to the Fano plane Γ_2, or the access structure $\Gamma_{2,1}$.*

Proof. Let us suppose that Γ is not a star. Then, there exist three minimal qualified subsets $A_1, A_2, A_3 \in \Gamma_0$ such that $A_1 \cap A_2 \neq \emptyset$, $A_1 \cap A_3 \neq \emptyset$ and $A_1 \cap A_2 \neq A_1 \cap A_3$. From Lemma 3.5, we have that $A_2 \cap A_3 \neq \emptyset$. Applying Lemmas 3.3 and 3.4, it follows that $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_3, p_4, p_5\}$ and $A_3 = \{p_1, p_5, p_6\}$ and, besides, $A_4 = \{p_2, p_4, p_6\} \in \Gamma_0$.

If $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$, then $\Gamma = \Gamma_{2,1}$. The proof is concluded by checking that $\Gamma = \Gamma_2$, the Fano plane, if $\Gamma_0 \neq \{A_1, A_2, A_3, A_4\}$.

Let us suppose that there exists a fifth minimal qualified subset $A_5 \in \Gamma_0$. Since Γ is connected, $A_5 \cap \{p_1, \ldots, p_6\} \neq \emptyset$. Without loss of generality, we can suppose that $p_1 \in A_5$. Observe that $p_2, p_3, p_5, p_6 \notin A_5$ because the intersection number of Γ is equal to one. We can apply Lemmas 3.5 and 3.4 to A_1, A_2 and A_5 and we get that $A_5 \cap A_2 \neq \emptyset$ and $|A_5| = 3$. Therefore, there exists a participant $p_7 \neq p_1, \ldots, p_6$ such that $A_5 = \{p_1, p_4, p_7\}$. Besides, from Lemma 3.3, $A_6 = \{p_2, p_5, p_7\} \in \Gamma_0$. Let us apply now Lemma 3.3 to the subsets, A_1, A_3 and A_6 to obtain that $A_7 = \{p_3, p_6, p_7\} \in \Gamma_0$. It is not difficult to check that $\{A_1, \ldots, A_7\} = (\Gamma_2)_0$, the basis of the access structure associated to the Fano plane. We finish by proving that $\Gamma_0 = \{A_1, \ldots, A_7\}$. In effect, let us suppose that there exists another minimal qualified subset $A_8 \in \Gamma_0$. As before, we can suppose that $p_1 \in A_8$ without loss of generality. Then, since the intersection number of Γ is equal to one, $p_i \notin A_8$ for any $i = 2, \ldots, 7$. A contradiction is obtained by applying Lemma 3.5 to A_1, A_2 and A_8. This completes the proof of the proposition. □

3.2 Ideal access structures with corank equal to two

The characterization of the ideal access structures with intersection number equal to one is concluded by Proposition 3.11. Its proof is obtained by a similar method as in the previous case. Namely, it is based on the following four lemmas determining some forbidden situations in such access structures. In these lemmas, we assume that Γ is an access structure on a set of participants $\mathcal{P}$ having basis Γ_0, with intersection number equal to one, $\mathrm{corank}(\Gamma) = 2$, and optimal information rate $\rho^*(\Gamma) > 2/3$.

Lemma 3.7 *Let $A_1, A_2 \in \Gamma_0$ be two minimal qualified subsets such that $|A_1| \geq 3$ and $|A_2| = 2$. Assume that $A_1 \cap A_2 \neq \emptyset$. Then, $(A_1 \cup A_2) \setminus (A_1 \cap A_2) \notin \Gamma$.*

Proof. Let us suppose that $(A_1 \cup A_2) \setminus (A_1 \cap A_2) \in \Gamma$. Let us consider the participants a, b such that $A_2 = \{a, b\}$ and $A_1 \cap A_2 = \{a\}$. Let $A_0 \in \Gamma_0$ be a minimal qualified subset such that $A_0 \subset (A_1 \cup A_2) \setminus (A_1 \cap A_2) = (A_1 \cup A_2) \setminus \{a\}$. Since the intersection number of Γ is equal to one, hence it follows that $A_0 = (A_0 \cap A_1) \cup (A_0 \cap A_2) = \{b, c\}$ where c is a participant in A_1. Let us consider the subsets $B_1 = \{c\}$ and $B_2 = A_1 \setminus \{a\}$. Observe that $B_1 \cup \{b\}$ and $B_2 \cup \{a\}$ are qualified subsets, while the subset $B_1 \cup \{a\}$ is not qualified because $|A_1| \geq 3$. Therefore, the sequence $\emptyset \neq B_1 \subset B_2 \notin \Gamma$ is made independent by the subset $\{a, b\} \in \Gamma$. Hence, by the independent sequence method, we have that $\rho^*(\Gamma) \leq 2/3$, a contradiction. □

Lemma 3.8 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets such that $|A_1| \geq 3$, $|A_2| = 2$ and $|A_3| \geq 2$. Assume that $\emptyset \neq A_1 \cap A_2 \neq A_2 \cap A_3 \neq \emptyset$. Then, $|A_1| = 3$, $|A_3| = 3$, $A_1 \cap A_3 \neq \emptyset$ and $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) \in \Gamma$.*

Proof. Let $A_2 = \{a, b\}$. We may assume that $\{a\} = A_1 \cap A_2$ and that $A_2 \cap A_3 = \{b\}$.

First we are going to prove that $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) \in \Gamma$. To do it let us consider the subsets $B_1 = A_1 \setminus \{a\}$ and $B_2 = (A_1 \cup A_3) \setminus A_2$. Notice that $B_1 \cup \{a\}$ and $B_2 \cup \{b\}$ are qualified subsets while, from Lemma 3.7, $B_1 \cup \{b\} = (A_1 \cup A_2) \setminus (A_1 \cap A_2)$ is not qualified. So, if $B_2 \notin \Gamma$, then the sequence $\emptyset \neq B_1 \subset B_2$ is made independent by the subset $\{a, b\} \in \Gamma$ and hence, by the independent sequence method, we have that $\rho^*(\Gamma) \leq 2/3$, a contradiction. Therefore $B_2 = (A_1 \cup A_3) \setminus A_2 \in \Gamma$. Since the intersection number of Γ is equal to one, $(A_1 \cup A_3) \setminus A_2 \in \Gamma$ if and only if $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) \in \Gamma$. Therefore, $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) \in \Gamma$ and, hence, there exist $a' \in A_1 \setminus (A_2 \cup A_3)$ and $b' \in A_3 \setminus (A_1 \cup A_2)$ such that $\{a', b'\} \in \Gamma_0$.

Now let us show that $|A_3| \geq 3$. We are going to prove that a contradiction holds if $|A_3| = 2$. If $|A_3| = 2$, then a $A_3 = \{b, b'\}$. In such a case we consider the subsets $B_1 = \{a\}$ and $B_2 = \{a, a'\}$. On one hand, $B_1 \cup \{b\}$ and $B_2 \cup \{b'\}$ are qualified subsets. On the other hand, from Lemma 3.7, $B_1 \cup \{b'\} = \{a, b'\} \subset (A_1 \cup \{a', b'\}) \setminus (A_1 \cap \{a', b'\}) \notin \Gamma$. Besides, $B_2 \notin \Gamma$ because $|A_1| \geq 3$. Therefore we have that the sequence $\emptyset \neq B_1 \subset B_2 \notin \Gamma$ is made independent by the subset $\{b, b'\} \in \Gamma$. Thus, $\rho^*(\Gamma) \leq 2/3$, a contradiction.

To finish the proof of the lemma we must demonstrate that $|A_1| = 3$, $|A_3| = 3$ and $A_1 \cap A_3 \neq \emptyset$. Notice that A_1 and A_3 play the same role. So, it is enough to show that $|A_3| = 3$ and that $A_1 \cap A_3 \neq \emptyset$.

In order to do it first we are going to prove that $(A_1 \cup \{b, b'\}) \setminus \{a, a'\} \in \Gamma$. Otherwise we consider the subsets $B_1 = A_1 \setminus \{a, a'\}$, $B_2 = (A_1 \cup \{b\}) \setminus \{a, a'\}$ and $B_3 = (A_1 \cup \{b, b'\}) \setminus \{a, a'\}$. It is clear that $B_1 \cup \{a, a'\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{a'\}$ are qualified subsets, while $B_1 \cup \{a\}$ is not qualified. Furthermore, applying Lemma 3.7 it follows that $B_2 \cup \{a'\} = (A_1 \cup A_2) \setminus (A_1 \cap A_2) \notin \Gamma$. Therefore $\{a, a'\} \notin \Gamma$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ by taking $X_1 = \{a, a'\}$, $X_2 = \{a\}$ and $X_3 = \{a'\}$. So, $\rho^*(\Gamma) \leq 2/3$, a contradiction.

Let $A_0 \in \Gamma_0$ such that $A_0 \subset (A_1 \cup \{b, b'\}) \setminus \{a, a'\}$. We have that $|A_3| \geq 3$ and that $\{b, b'\} \subset A_3$. Hence, since the intersection number of Γ is equal to one, it follows that $A_0 \cap A_1 \neq \emptyset$. Let $\{x\} = A_0 \cap A_1$. So $A_0 = \{x, b\}$, or $A_0 = \{x, b'\}$, or $A_0 = \{x, b, b'\}$. On one hand $\{x, b\} \subset (A_1 \cup A_2) \setminus (A_1 \cap A_2)$. On the other hand $\{x, b'\} \subset (A_1 \cup \{a', b'\}) \setminus (A_1 \cap \{a', b'\})$. Thus, applying Lemma 3.7 we conclude that $A_0 = \{x, b, b'\}$. Therefore $A_0 = A_3$. Hence, $|A_3| = 3$ and $A_1 \cap A_3 \neq \emptyset$, as we wanted to prove. □

Lemma 3.9 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets such that $|A_1| \geq 3$, $|A_2| = 2$ and $|A_3| = 2$. Assume that $\emptyset \neq A_1 \cap A_2 \neq A_1 \cap A_3 \neq \emptyset$. Then, $|A_1| = 3$, $A_2 \cap A_3 = \emptyset$ and $(A_1 \cup A_2 \cup A_3) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_3)) \in \Gamma$.*

Proof. Let $\{a\} = A_1 \cap A_2$ and $\{b\} = A_1 \cap A_3$. If $A_2 \cap A_3 \neq \emptyset$, then $A_3 \subset (A_1 \cup A_2) \setminus (A_1 \cap A_2)$. So $(A_1 \cup A_2) \setminus (A_1 \cap A_2) \in \Gamma$ which is a contradiction with Lemma 3.7. Therefore we have that $A_2 \cap A_3 = \emptyset$ and hence, $A_2 = \{a, x\}$ and $A_3 = \{b, y\}$ with $x \neq y$.

Now let us show that $(A_1 \cup \{x, y\}) \setminus \{a, b\} = (A_1 \cup A_2 \cup A_3) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_3)) \in \Gamma$. If not we consider the subsets $B_1 = A_1 \setminus \{a, b\}$, $B_2 = (A_1 \cup \{x\}) \setminus \{a, b\}$ and $B_3 = (A_1 \cup \{x, y\}) \setminus \{a, b\}$. Notice that $B_1 \cup \{a, b\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{b\}$ are qualified subsets, while $B_1 \cup \{a\}$ is not qualified. Furthermore, from Lemma 3.7, $B_2 \cup \{b\} = (A_1 \cup A_2) \setminus (A_1 \cap A_2) \notin \Gamma$. Therefore $\{a, b\} \notin \Gamma$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ by taking $X_1 = \{a, b\}$, $X_2 = \{a\}$ and $X_3 = \{b\}$. So, $\rho^*(\Gamma) \leq 2/3$, a contradiction.

To finish we must demonstrate that $|A_1| = 3$. Since $(A_1 \cup \{x, y\}) \setminus \{a, b\} \in \Gamma$, hence there exists $A_0 \in \Gamma_0$ such that $A_0 \subset (A_1 \cup \{x, y\}) \setminus \{a, b\}$. Without loss of generality we may assume that $x \in A_0$. Thus we have that $A_1, A_2, A_0 \in \Gamma_0$ are three different minimal qualified subsets such that $|A_1| \geq 3$, $|A_2| = 2$, $|A_0| \geq 2$ and such that $\{a\} = A_1 \cap A_2 \neq A_2 \cap A_0 = \{x\}$. So, from Lemma 3.8, we get that $|A_1| = 3$ as we wanted to prove. □

Lemma 3.10 *Let $A_1, A_2, A_3 \in \Gamma_0$ be three different minimal qualified subsets such that $|A_1| \geq 3$, $|A_2| = 2$ and $|A_3| \geq 3$. Assume that $\emptyset \neq A_1 \cap A_2 \neq A_1 \cap A_3 \neq \emptyset$. Then, $|A_1| = 3$, $|A_3| = 3$, $A_2 \cap A_3 \neq \emptyset$ and $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) \in \Gamma$.*

Proof. Let a, b, c be three different participants such that $A_2 = \{a, b\}$, $A_1 \cap A_2 = \{a\}$ and $A_1 \cap A_3 = \{c\}$.

We claim that $(A_1 \cup A_3 \cup \{b\}) \setminus \{a,c\}$ is a qualified subset. Let us show our claim. Assume that $(A_1 \cup A_2 \cup \{b\}) \setminus \{a,c\} \notin \Gamma$. In such a case we consider the subsets $B_1 = A_1 \setminus \{a,c\}$, $B_2 = (A_1 \cup \{b\}) \setminus \{a,c\}$ and $B_3 = (A_1 \cup A_3 \cup \{b\}) \setminus \{a,c\}$. It is clear that $B_1 \cup \{a,c\}$, $B_2 \cup \{a\}$ and $B_3 \cup \{c\}$ are qualified subsets, while $B_1 \cup \{a\}$ is not qualified. Furthermore, from Lemma 3.7, $B_2 \cup \{c\} = (A_1 \cup A_2) \setminus (A_1 \cap A_2) \notin \Gamma$. So, $\{a,c\} \notin \Gamma$ makes independent the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ by taking $X_1 = \{a,c\}$, $X_2 = \{a\}$ and $X_3 = \{c\}$. Hence, $\rho^*(\Gamma) \leq 2/3$, a contradiction. Therefore, our claim holds.

Let $A_0 \in \Gamma_0$ be a minimal qualified subset such that $A_0 \subset (A_1 \cup A_3 \cup \{b\}) \setminus \{a,c\}$. Since Γ has intersection number equal to one hence it follows that either $A_0 = \{a_1, a_3, b\}$, or $A_0 = \{a_1, b\}$, or $A_0 = \{a_3, b\}$, or $A_0 = \{a_1, a_3\}$, where $a_1 \in A_1$ and $a_3 \in A_3$. We are going to prove that $A_0 = \{a_1, a_3\}$. If $A_0 = \{a_1, a_3, b\}$ then, applying Lemma 3.8 to A_1, A_2 and A_0 we get that $\{c, a_3\} \in \Gamma$, so $A_3 = \{c, a_3\}$ which is a contradiction because $|A_3| \geq 3$. If $A_0 = \{a_1, b\}$ then a contradiction is obtained by applying Lemma 3.7 to A_1 and A_2. While, if $A_0 = \{a_3, b\}$ then a contradiction is obtained by applying Lemma 3.8 to A_1, A_2 and A_0 since $|A_0| \neq 3$. Therefore $A_0 = \{a_1, a_3\}$.

We apply now Lemma 3.9 to the minimal qualified subsets A_1, A_2 and A_0. Hence we get that $|A_1| = 3$ and that $(A_1 \cup A_2 \cup A_0) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_0)) \in \Gamma$. Therefore, $A_1 = \{a, a_1, c\}$ and $\{b, c, a_3\} \in \Gamma$. Since $c, a_3 \in A_3$, thus $A_3 = \{b, c, a_3\}$. So, $|A_3| = 3$, $A_2 \cap A_3 = \{b\} \neq \emptyset$ and $(A_1 \cup A_3) \setminus (A_2 \cup (A_3 \cap A_1)) = \{a_1, a_3\} \in \Gamma$. This completes the proof of the lemma. □

Proposition 3.11 *Let Γ be a connected access structure on a set of participants $\mathcal{P}$ with intersection number equal to one,* corank$(\Gamma) = 2$, *and optimal information rate $\rho^*(\Gamma) > 2/3$. Then, Γ is either a complete multipartite graph $\Gamma\langle K_{n_1,\ldots,n_\ell}\rangle$, or a star $\Gamma\langle S(p_0)\rangle$, or the access structure $\Gamma_{2,2}$, or the access structure $\Gamma_{2,3}$.*

Proof. The access structure Γ is defined by a graph if rank$(\Gamma) = 2$. In this case, $\Gamma = \Gamma\langle G\rangle$, where G is a complete multipartite graph [4, 6]. Therefore we must demonstrate that, if rank$(\Gamma) \geq 3$ then Γ is either an access structure defined by a star, or the access structure $\Gamma_{2,2}$, or the access structure $\Gamma_{2,3}$.

Assume that rank$(\Gamma) \geq 3$ and that Γ is not a star. We claim that then there exist five different participants $p_1, \ldots, p_5 \in \mathcal{P}$ such that the subsets $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_1, p_4\}$, $A_3 = \{p_3, p_4, p_5\}$ and $A_4 = \{p_2, p_5\}$ are minimal qualified subsets of the access structure Γ.

Let us show our claim. Since Γ is a connected access structure with rank$(\Gamma) \geq 3$ and corank$(\Gamma) = 2$, there exist minimal qualified subsets $A_1, A_2 \in \Gamma_0$ with $|A_1| \geq 3$, $|A_2| = 2$ and $A_1 \cap A_2 \neq \emptyset$. Due to the fact that Γ is not a star, there must exist a third minimal qualified subset $A_0 \in \Gamma_0$ such that $A_0 \cap A_1 \neq A_0 \cap A_2$. If $|A_0| \geq 3$ then, by Lemmas 3.8 and 3.10, it follows that $A_0 \cap A_i \neq \emptyset$ for $i = 1, 2$, that $|A_1| = |A_0| = 3$, and that $(A_1 \cup A_0) \setminus (A_2 \cup (A_1 \cap A_0)) \in \Gamma$. So, if $|A_0| \geq 3$ we define $A_3 = A_0$

and $A_4 = (A_1 \cup A_0) \setminus (A_2 \cup (A_1 \cap A_0)) \in \Gamma_0$. To finish the proof of our claim we must examine the case $|A_0| = 2$. If $|A_0| = 2$ then, by Lemma 3.8 it follows that $A_0 \cap A_2 = \emptyset$ and, hence, $A_0 \cap A_1 \neq \emptyset$. Now applying Lemma 3.9 we get that $|A_1| = 3$ and that $(A_1 \cup A_2 \cup A_0) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_0)) \in \Gamma$. Therefore, if $|A_0| = 2$ we define $A_3 = (A_1 \cup A_2 \cup A_0) \setminus ((A_1 \cap A_2) \cup (A_1 \cap A_0)) \in \Gamma_0$ and $A_4 = A_0$. This completes the proof of our claim.

Notice that, if $\Gamma_0 = \{A_1, A_2, A_3, A_4\}$ then $\Gamma = \Gamma_{2,3}$. Hence, to conclude the proof of the proposition we must demonstrate that if $\Gamma_0 \neq \{A_1, A_2, A_3, A_4\}$ then $\Gamma = \Gamma_{2,2}$.

Let us assume that $\Gamma_0 \neq \{A_1, A_2, A_3, A_4\}$. Since Γ is connected, there exists another minimal qualified subset $A_5 \in \Gamma_0$ with $A_5 \cap A_i \neq \emptyset$ for some $i = 1, 2, 3, 4$. We are going to distinguish two cases.

First we suppose that $p_3 \in A_5$. In this case, $p_1, p_2, p_4, p_5 \notin A_5$ because Γ has intersection number equal to one. If $|A_5| \geq 3$, we apply Lemma 3.10 to A_1, A_2 and A_5, and we have that $p_4 \in A_5$, a contradiction. Therefore $|A_5| = 2$. Hence, $A_5 = \{p_3, p_6\}$ where $p_6 \neq p_i$ if $1 \leq i \leq 5$. From Lemma 3.9 applied to A_1, A_2 and A_5, we have that $A_6 = \{p_2, p_4, p_6\} \in \Gamma_0$. Besides, we obtain that $A_7 = \{p_1, p_5, p_6\} \in \Gamma_0$ is also a minimal qualified subset by applying Lemma 3.9 to A_1, A_4 and A_5.

We assume now that $p_3 \notin A_5$. By symmetry, we can suppose that $p_1 \in A_5$. Observe that $p_2, p_3, p_4 \notin A_5$ because the intersection number of Γ is equal to one. Applying Lemma 3.8 to A_3, A_2 and A_5, we have that $|A_5| = 3$, $A_5 \cap A_3 \neq \emptyset$ and $(A_3 \cup A_5) \setminus (A_2 \cup (A_5 \cap A_3)) \in \Gamma$. Then $A_5 = \{p_1, p_5, p_6\}$ where $p_6 \neq p_i$ if $1 \leq i \leq 5$. Moreover, $A_6 = \{p_3, p_6\} = (A_3 \cup A_5) \setminus (A_2 \cup (A_5 \cap A_3)) \in \Gamma_0$. We apply now Lemma 3.9 to A_5, A_2 and A_4 and we obtain another minimal qualified subset $A_7 = \{p_2, p_4, p_6\}$.

In both cases we have that, if $\Gamma_0 = \{A_1, \ldots, A_7\}$ then $\Gamma = \Gamma_{2,2}$. Therefore we conclude the proof of the proposition by checking that $\Gamma_0 = \{A_1, \ldots, A_7\}$.

Let us suppose that there exists another minimal qualified subset $A_8 \in \Gamma_0$. Since Γ is connected and by symmetry among the participants, we may assume that $p_1 \in A_8$. Hence, $p_2, p_3, p_4, p_5, p_6 \notin A_8$ because the intersection number of Γ is equal to one. From Lemma 3.8 applied to A_3, A_2 and A_8, we have that $A_8 \cap A_3 \neq \emptyset$, a contradiction. This completes the proof of the proposition. □

4 Bounds on the optimal information rate

We present in Proposition 4.1 a bound on the optimal information rate for non-ideal access structures with intersection number equal to one. This result generalizes the one for access structures defined by graphs. Besides, we give in Proposition 4.2 a lower bound on the optimal information rate that holds to any access structure. To compare both bounds and to illustrate our results Some examples are given.

In order to prove our results we use the decomposition technique. A *decomposi-*

tion 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 [18] 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 [18, Theorem 2.1]. 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 $\mathbb{K}$. Then, the optimal information rate of Γ verifies $\rho^*(\Gamma) \geq \min\{\lambda_A : A \in \Gamma_0\} / \max\{r_p : p \in \mathcal{P}\}$, where $\lambda_A = |\{i \in \{1, \ldots, r\} : A \in \Gamma_{0,i}\}|$ and $r_p = |\{i \in \{1, \ldots, r\} : p \in \mathcal{P}_i\}|$.

Proposition 4.1 *Let Γ be an access structure with intersection number equal to one on a set of participants $\mathcal{P}$. For every $p \in \mathcal{P}$, we define $n_\Gamma(p)$ as the number of participants $q \in \mathcal{P}$ such that $p, q \in A$ for some minimal qualified subset $A \in \Gamma_0$. We define also the degree of p in the access structure Γ as the number of minimal qualified subsets it belongs to, that is $\deg_\Gamma(p) = |\{A \in \Gamma_0 : p \in A\}|$. Assume that Γ is not realizable by an ideal secret sharing scheme. Then,*

$$\frac{2}{3} \geq \rho^*(\Gamma) \geq \frac{\mathrm{corank}(\Gamma)}{\max\{n_\Gamma(p) : p \in \mathcal{P}\}} \geq \frac{\mathrm{corank}(\Gamma)}{(\mathrm{rank}(\Gamma) - 1)\max\{\deg_\Gamma(p) : p \in \mathcal{P}\} + 1}.$$

Proof. We assume that Γ is not realizable by an ideal secret sharing scheme. Hence applying Theorem 3.1 it follows that $\rho^*(\Gamma) \leq 2/3$. Next we prove the lower bound by using a suitable decomposition of Γ. Let us denote $\mathcal{P} = \{p_1, \ldots, p_n\}$. For every $i = 1, \ldots, n$, let us consider $\Gamma_{0,i} = \{A \in \Gamma_0 : p_i \in A\}$ and $\mathcal{P}_i = \bigcup_{A \in \Gamma_{0,i}} A$. Since the intersection number of Γ is equal to one, $\Gamma_{0,i}$ is a star $S(p_i)$ for any $i = 1, \ldots, n$. Then, from Proposition 2.1 the access structure Γ_i on $\mathcal{P}_i$ having basis $\Gamma_{0,i}$ is a vector space access structure. It is clear that the substructures $\Gamma_{0,i}$ form a decomposition of Γ. Hence, $\rho^*(\Gamma) \geq \min\{\lambda_A : A \in \Gamma_0\} / \max\{r_p : p \in \mathcal{P}\}$. On one hand we have that $\lambda_A = |\{i \in \{1, \ldots, n\} : A \in \Gamma_{0,i}\}| = |A|$ for every $A \in \Gamma_0$. On the other hand it is not difficult to check that, for every participant $p \in \mathcal{P}$, $r_p = |\{i \in \{1, \ldots, n\} : p \in \mathcal{P}_i\}| = n_\Gamma(p) \leq (\mathrm{rank}(\Gamma) - 1)\deg_\Gamma(p) + 1$. Therefore, the lower bounds follow. □

Notice the last inequality in the previous proposition is an equality, whenever Γ is *homogeneous*, that is, whenever $\mathrm{rank}(\Gamma) = \mathrm{corank}(\Gamma)$. Hence, we get the lower bound

$$\frac{2}{3} \geq \rho^*(\Gamma) \geq \frac{r}{(r-1)d + 1}$$

for any non-ideal homogeneous access structure Γ with rank r, intersection number equal to one, and maximum degree $d = \max\{\deg_\Gamma(p) : p \in \mathcal{P}\}$.

We apply this result to the access structures defined by graphs. Let $\Gamma = \Gamma\langle G\rangle$ be the access structure defined by a graph G. Then, Γ is a homogeneous access structure of rank $r = 2$, with intersection number equal to one and maximum degree d equal to the maximum degree of the graph G. If G is a complete multipartite graph, then $\Gamma\langle G\rangle$ is an ideal access structure. While, if G is not a complete multipartite graph, then $2/3 \geq \rho^*(\Gamma\langle G\rangle) \geq 2/(d+1)$. This lower bound on the optimal information rate of access structures defined by graphs was given by Stinson in [18]. Besides, Blundo et al. [2] proved that this lower bound is tight.

Let us apply now this result to the access structures associated to finite projective projective planes. Let $\Gamma = \Gamma_n$ be the access structure associated to the finite projective plane of order n. Then, Γ_n is a homogeneous access structure of rank $r = n + 1$, with intersection number equal to one, and maximum degree $d = n + 1$. If $n = 2$ then the access structure is defined by the Fano plane and so it is ideal, while $2/3 \geq \rho^*(\Gamma_n) \geq (n + 1)/(n^2 + n + 1)$ whenever $n \geq 3$.

We present next a lower bound on the optimal information rate that applies to any access structure. This lower bound improves in some cases the one in Proposition 4.1.

Proposition 4.2 *Let Γ be an access structure on a set of participants $\mathcal{P}$. Let $m = |\Gamma_0|$ and let $d = \max\{\deg_\Gamma(p) : p \in \mathcal{P}\}$. Then,*

$$\rho^*(\Gamma) \geq \frac{2(m-1)}{d(2m-d-1)}.$$

Proof. Let $\Gamma_0 = \{A_1, \ldots, A_m\}$. For every pair of different minimal qualified subsets A_i, A_j, we consider $\Gamma_{0,\{i,j\}} = \{A_i, A_j\}$. It is not difficult to prove that any access structure with exactly two minimal qualified subsets is a vector space access structure over any finite field $\mathbb{K}$. Then, we can apply the λ-decomposition method to the decomposition given by the substructures $\Gamma_{0,\{i,j\}}$, where $1 \leq i < j \leq m$, and we obtain $\rho^*(\Gamma) \geq \min\{\lambda_A : A \in \Gamma_0\}/\max\{r_p : p \in \mathcal{P}\}$. On one hand, it is clear that $\lambda_A = m - 1$ for any $A \in \Gamma_0$. On the other hand, for every participant $p \in \mathcal{P}$,

$$r_p = \deg_\Gamma(p)(m - \deg_\Gamma(p)) \left(\begin{array}{c} \deg_\Gamma(p) \\ 2 \end{array} \right) = \frac{1}{2}\deg_\Gamma(p)(2m - \deg_\Gamma(p) - 1).$$

Notice that the function $f(x) = x(2m - x - 1)$ is monotone increasing if $x \leq m - 1/2$ and that $f(m - 1) = f(m) = m^2 - m$. Then, since $d = \max\{\deg_\Gamma(p) : p \in \mathcal{P}\} \leq m$, it follows that $r_p = f(\deg_\Gamma(p))/2 \leq f(d)/2 = d(2m - d - 1)/2$ for any $p \in \mathcal{P}$. □

The lower bounds given in Propositions 4.1 and 4.2 are easily comparable for homogeneous access structures with intersection number equal to one. In effect, let Γ be an homogeneous access structure with rank r and intersection number equal to one. In this case, applying Propositions 4.1 and 4.2, we obtain

$$\rho^*(\Gamma) \geq \max\left\{\frac{r}{(r-1)d+1}, \frac{2(m-1)}{d(2m-d-1)}\right\} = \begin{cases} \dfrac{r}{(r-1)d+1} & \text{if } 2m \geq rd+2 \\ \\ \dfrac{2(m-1)}{d(2m-d-1)} & \text{if } 2m < rd+2 \end{cases}$$

Notice that, if $\Gamma = \Gamma\langle G\rangle$ is an access structure defined by a graph G, then $r = 2$, $m \geq d$, and $m = d$ if and only if Γ is a star and, hence, Γ is ideal. Then, for non-ideal access structures defined by graphs, the bound given by Proposition 4.1 is always better than the one obtained from Proposition 4.2.

Besides, if $\Gamma = \Gamma_n$ is the access structure associated to the finite projective plane of order n, then $m = n^2 + n + 1$ and $r = d = n + 1$. So, in this case, $2m \geq rd + 2$. In this case, the bound given by Proposition 4.1 is also better than the one given by Proposition 4.2.

Nevertheless, the following example points out a homogeneous access structure with intersection number one, in which the lower bound given by Proposition 4.2 is better than the one given by Proposition 4.1.

Example 4.3 Let us consider the set of $3(n+1)$ participants $\mathcal{P} = \{x, y, z, a_1, \ldots, a_n, b_1, \ldots, b_n, c_1, \ldots, c_n\}$, where $n \geq 1$, and the access structure Γ having basis $\Gamma_0 = \{A_1, A_2, A_3\}$, where $A_1 = \{x, y, a_1, \ldots, a_n\}$, $A_2 = \{y, z, b_1, \ldots, b_n\}$ and $A_3 = \{x, z, c_1, \ldots, c_n\}$. It is clear that Γ is a homogeneous access structure with rank $r = n+2$, intersection number equal to one and maximum degree $d = 2$. From Theorem 3.1 and Propositions 4.1 and 4.2 we get that $2/3 \geq \rho^*(\Gamma) \geq \max\{(n+2)/(2n+3), 2/3\} = 2/3$. Therefore, $\rho^*(\Gamma) = 2/3$.

We conclude the section by studying, in the following examples, the optimal information rates of two non-homogeneous access structures. In the first example we find bounds improving the ones obtained from the results in this section. While in the second one we find bounds on the optimal information rate of an access structure with intersection number different from one by considering its dual.

Example 4.4 Let us consider now the access structure Γ on a set of eight participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}$ having minimal qualified subsets $A_1 = \{p_1, p_2, p_4\}$, $A_2 = \{p_1, p_5, p_6\}$, $A_3 = \{p_2, p_6, p_7\}$, $A_4 = \{p_3, p_7, p_8\}$ and $A_5 = \{p_2, p_3\}$. This access structure has intersection number equal to one, rank equal to three and corank equal to two. From Theorem 3.1 and Propositions 4.1 and 4.2, we get that $2/3 \geq \rho^*(\Gamma) \geq \max\{1/3, 4/9\} = 4/9$. In this case we can improve both the upper and the lower bounds. Namely, we are going to prove that $3/5 \geq \rho^*(\Gamma) \geq 1/2$. The new upper bound is obtained by means of the independent sequence method. Let us consider the subsets $B_1 = \{p_4\}$, $B_2 = \{p_4, p_5, p_6\}$, $B_3 = \{p_4, p_5, p_6, p_7\}$ and

$B_4 = \{p_4, p_5, p_6, p_7, p_8\}$. Equally, we take the subsets $X_1 = \{p_1, p_2\}$, $X_2 = \{p_1\}$, $X_3 = \{p_2\}$ and $X_4 = \{p_3\}$. It is not difficult to check that the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \subset B_4 \notin \Gamma$ is made independent by the set $A = \{p_1, p_2, p_3\}$. Since $A \in \Gamma$, we have that $\rho^*(\Gamma) \leq 3/5$. In order to find the new lower bound, we consider the decomposition $\{\Gamma_1, \Gamma_2\}$ of Γ defined by $(\Gamma_1)_0 = \{A_1, A_3, A_5\}$ and $(\Gamma_1)_0 = \{A_2, A_4\}$. Since Γ_1 is a star and Γ_2 has two minimal qualified subsets, both are ideal access structures. This decomposition implies that $\rho^*(\Gamma) \geq 1/2$.

Example 4.5 Let Γ be the access structure on $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$ defined by $\Gamma_0 = \{\{p_1, p_2, p_3, p_4\}, \{p_1, p_2, p_7\}, \{p_1, p_3, p_6\}, \{p_1, p_6, p_7\}, \{p_2, p_3, p_5\}, \{p_2, p_5, p_7\}, \{p_3, p_5, p_6\}, \{p_5, p_6, p_7\}\}$. Notice that Γ has intersection number equal to two, rank equal to four and corank equal to three. The dual access structure Γ^* of Γ has basis $(\Gamma^*)_0 = \{A_1, A_2, A_3, A_4\}$ where $A_1 = \{p_1, p_5\}$, $A_2 = \{p_2, p_6\}$, $A_3 = \{p_3, p_7\}$ and $A_4 = \{p_4, p_5, p_6, p_7\}$. Therefore Γ^* has intersection number equal to one, rank equal to four and corank equal to two. From Theorem 3.1 it follows that Γ^* is not an ideal access structure. Hence, Γ is not an ideal access structure. Furthermore, from Propositions 4.1 and 4.2, we get that $2/3 \geq \rho^*(\Gamma^*) \geq \max\{2/5, 3/5\} = 3/5$. Therefore, $2/3 \geq \rho^*(\Gamma) \geq 3/5$.

5 Conclusion and open problems

This paper deals with the characterization of ideal access structures and the search for bounds on the optimal information rate for the access structures with intersection number equal to one. Then, our results generalize the previously obtained ones for access structures defined by graphs [3, 6, 8, 18].

Theorem 3.1 is the main result in this paper. It contains the complete characterization of the ideal access structures with intersection number equal to one. Namely, we prove that the complete multipartite graphs, the stars and the access structure associated to the Fano plane, together with three other access structures related to it, are the only ideal connected access structures with intersection number equal to one. Besides, Theorem 3.1 states also that the ideal access structures in that family coincide with the vector space ones and with those having optimal information rate greater than 2/3. That is, there is no access structure with intersection number equal to one such that its optimal information rate verifies $2/3 < \rho^*(\Gamma) < 1$.

Apart from the access structures defined by graphs, similar results had been previously obtained for several families of access structures: access structures on sets of four [17] and five [12] participants, bipartite access structures [14], and access structures with three or four minimal qualified subsets [13]. These coincidences lead to the following two questions:

1. Is there any ideal access structure that is not a vector space access structure?

2. Is there any access structure Γ such that $2/3 < \rho^*(\Gamma) < 1$?

As far as we know, the second question remains open. A negative answer to the first question is given in [16]. Namely, by using the Theorem of Pappus, the authors present an ideal access structure that does not admit a vector space realization. Nevertheless, this access structure can be realized by an ideal linear secret sharing scheme. So, the following question seems to be still without answer:

1'. Is there any ideal access structure that is not realized by any ideal linear secret sharing scheme?

Besides the characterization of the ideal access structures with intersection number equal to one, we give some lower bounds on the optimal information rate for the non-ideal case. These bounds are obtained from decomposition techniques. When applied to the access structures defined by graphs, our bounds become the well known bound $\rho^*(\Gamma\langle G\rangle) \geq 2/(d+1)$ given by Stinson [18], which Blundo et al. [2] proved to be tight. The tightness of the bounds we present here is an open problem, both in the general case of access structures with intersection number equal to one or considering only the homogeneous structures with rank greater than 2. Another open question is the search of new techniques to construct secret sharing schemes for the access structures with intersection number equal to one. In this way, better lower bounds on their optimal information rate could be found.

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] P. Dembowski. *Finite geometries. Reprint of the 1968 original.* Classics in Mathematics. Springer-Verlag, Berlin, 1997.

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

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

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

[13] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. Preprint.

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

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

[16] J. Simonis, A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography.* 14 (1998), 179–197.

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

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