Secret sharing schemes on sparse homogeneous access structures with rank three *

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. An access structure is said to be r-homogeneous whenever its minimal qualified subsets have exactly r different participants. It is well known that a 2-homogeneous access structures is ideal if and only if it is a vector space access structure and, besides, there is no 2-homogeneous access structure with optimal information rate between 2/3 and 1. The aim of this paper is to determine to which extent this result can be generalized for 3-homogeneous access structures.

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 some subsets of participants, the *qualified subsets*, are able to reconstruct the secret k from their shares. Secret sharing was introduced by Blakley [1] and Shamir [18]. A comprehensive introduction to this topic can be found in [20]. Only *perfect* secret sharing schemes are going to be considered in this paper, that is, schemes in which the shares of the participants in a *non-qualified subset* provide absolutely no information about the value of the secret. Besides, the reader must notice that we are dealing here with *unconditional security* because we are not making any assumption on the computational power of the participants.

The *access structure* of a secret sharing scheme is the family of qualified subsets, , $\subset 2^{\mathcal{P}}$. In general, access structures are considered to be *monotone*, that is, any subset of $\mathcal{P}$ containing a qualified subset is qualified. Then, the access structure , is determined by the family of *minimal qualified subsets*, , $_0$, which is called the *basis* of , . We assume that every participant belongs to at least one minimal qualified subset.

The first works about secret sharing [1, 18] considered only schemes with a (t, n)-*threshold access structure*, which is formed by all the subsets with at least t participants in a set of n participants. Further works considered the problem of finding secret sharing schemes for

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

more general access structures and Ito, Saito and Nishizeki [9] gave a method to construct a secret sharing scheme for any access structure. While in the threshold schemes the shares have the same size as the secret, the schemes constructed in [9] are very inefficient because the size of the shares is, in general, much larger than the size of the secret.

Actually, the size of the shares given to the participants is a key point in the design of secret sharing schemes. This is due to fact that the security of a system depends on the amount of information that must be kept secret. Therefore, one of the main parameters in secret sharing is the *information rate* $\rho(\Sigma, , , \mathcal{K})$ 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, $\rho(\Sigma, , , \mathcal{K}) = \log |\mathcal{K}| / \max_{p \in \mathcal{P}} \log |\mathcal{S}_p|$, where $\mathcal{S}_p$ is the set of all possible values of the share s_p corresponding to the participant p.

A high information rate is desirable. Since the size of any share can not be smaller than the size of the secret, the information rate of any secret sharing scheme is less than or equal to one. A secret sharing scheme is said to be *ideal* if its information rate is equal to one. An access structure , $\subset 2^{\mathcal{P}}$ is an *ideal access structure* if there exists an ideal secret sharing scheme for , . For instance, threshold access structures are ideal.

Not all access structures are ideal. So, when designing a secret sharing scheme for a given access structure , , we may try to maximize the information rate. The *optimal information rate* of an access structure , is defined by $\rho^*(,) = \sup(\rho(\Sigma, , , \mathcal{K}))$, 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 , 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, more generally, to determine the optimal information rate of any access structure.

A necessary condition for an access structure to be ideal was given by Brickell and Davenport [6] in terms of matroids. Namely, they proved that every ideal access structure induces a matroid. This necessary condition is not sufficient. A counterexample is obtained from the result by Seymour [17], who proved that there is no ideal scheme for the access structure related to the Vamos matroid.

A sufficient condition for an access structure to be ideal was introduced by Brickell [5] by means of the *vector space construction*. The vector space construction provides ideal secret sharing schemes for a wide family of access structures, the *vector space access structures*. The ideal secret sharing schemes that are obtained in this way are equivalent to the ones that are obtained from linear codes [14] and equivalent also to the ones obtained from monotone span programs [11]. In fact, vector space access structures are exactly those related to a representable matroid. Nevertheless, Simonis and Ashikhmin [19] presented an ideal access structure that is not a vector space access structure. Specifically, they proved that the access structure related to the non-Pappus matroid is ideal and it is not a vector space access structure.

Several techniques have been introduced in [4, 7, 16, 21] in order to construct secret sharing schemes for some families of access structures, which provide lower bounds on their 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, the *independent sequence method*, was given in [2] and was generalized in [15]. However, there exists a wide gap between the best known upper and lower bounds on the optimal information rate for most access structures.

Both problems, to characterize the ideal access structures as well as to determine the optimal information rate of any access structure, are far from being solved at present. Due to the difficulty of finding general results, these problems have been studied in several particular classes of access structures: access structures on sets of four [20] and five [10] participants, access structures defined by graphs [2, 3, 4, 6, 7, 8, 21], bipartite access structures [15], access structures with three or four minimal qualified subsets [12], and access structures with intersection number equal to one [13].

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 , whose optimal information rate is such that $2/3 < \rho^*(,) < 1$. A natural question that arises at this point is to determine to which extent these results can be generalized to other families of access structures.

The aim of this paper is to analyze this question for the family of the *sparse 3-homogeneous access structures*.

An access structure , on a set of participants $\mathcal{P}$ is said to be *r-homogeneous* if its rank and its corank are equal to r, where the *rank* and the *corank* of , are, respectively, the maximum and the minimum number of participants in a minimal qualified subset. For instance, the 2-homogeneous access structures are exactly those defined by a graph.

For a subset of participants $\mathcal{Q} \subset \mathcal{P}$, we define $\omega(\mathcal{Q},,)$ as the number of minimal qualified subsets $A \in ,_0$ such that $A \subset \mathcal{Q}$. We consider also $\omega(s,,) = \max\{\omega(\mathcal{Q},,) : |\mathcal{Q}| = s\}$. Therefore, if , is a 3-homogeneous access structure then $1 \leq \omega(4,,) \leq 4$. A 3-homogeneous access structure is said to be *sparse* if $\omega(4,,) \leq 2$, that is, if each set of four participants contains at most two minimal qualified subsets.

Our main result is the characterization of the ideal sparse 3-homogeneous access structures. We prove, in Theorem 3.2, that every ideal access structure in this family is a vector space access structure over the finite field $\mathbb{Z}_2$. Moreover, we show that there is no access structure with optimal information rate between 2/3 and 1 in the family we consider. Besides, in Theorem 3.3, we present a complete description of the ideal access structures in this family in terms of their simplest components.

Therefore, our results are a first approach to the characterization of ideal 3-homogeneous access structures. Nevertheless, they can not be directly generalized to general 3-homogeneous access structures. Namely, by considering the ideal scheme presented in [19] for the non-Pappus matroid, we get that the equivalence between ideal and vector space access structures does not hold for general 3-homogeneous access structures. So, the characterization of ideal 3-homogeneous access structures with $\omega(4,,) \geq 3$ is still an open problem.

The paper is organized as follows. A general result on vector space access structures is given in Section 2. Specifically, we characterize the vector space access structures over the finite field $\mathbb{Z}_2$ by a combinatorial property involving the dual access structure. Our main results on the characterization of ideal sparse 3-homogeneous access structures, Theorems 3.2 and 3.3, are given in Section 3, together with some examples illustrating these results.

2 A characterization of vector space access structures over $\mathbb{Z}_2$

The aim of this section is to prove Theorem 2.2, which is a characterization of the $\mathbb{Z}_2$-vector space access structures. As corollary we demonstrate that the access structures , $\langle S(p) \rangle$ defined by a star, the access structure , $_2$ associated to the Fano plane (the finite projective plane

of order two), and its associated access structure $\Gamma_{2,1}$ are $\mathbb{Z}_2$-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 if $A \subset \mathcal{P}$ then, $A \in \Gamma$ 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 [20] for proofs). Namely, if Γ is a $\mathbb{K}$-vector space access structure then we can construct a secret sharing scheme for Γ with set of secrets $\mathcal{K} = \mathbb{K}$: given a secret value $k \in \mathbb{K}$, the dealer takes at random an element $v \in E$ such that $v \cdot \psi(D) = k$, and gives to the participant $p \in \mathcal{P}$ the share $s_p = v \cdot \psi(p)$. Observe that, a subset $A \subset \mathcal{P}$ is not qualified if and only if there exists a vector $v \in E$ such that $v \cdot \psi(D) \neq 0$ and $v \cdot \psi(p) = 0$ if $p \in A$.

Our characterization of $\mathbb{Z}_2$-vector space access structures, Theorem 2.2, involves the *dual access structure*. Recall that for a given access structure Γ on a set of participants $\mathcal{P}$, its dual access structure Γ^* is the access structure on $\mathcal{P}$ defined by $\Gamma^* = \{B \subset \mathcal{P} : \mathcal{P} \setminus B \notin \Gamma\}$. The following result will be used in several places in the paper.

Lemma 2.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$. Let $B \subset \mathcal{P}$. Then, $B \in \Gamma^*$ if and only if $B \cap A \neq \emptyset$ for every $A \in \Gamma_0$.*

Theorem 2.2 *Let Γ be an access structure on a set of participants $\mathcal{P}$. Then, Γ is a $\mathbb{Z}_2$-vector space access structure if and only if for every two subsets $A \in \Gamma_0$ and $A^* \in \Gamma_0^*$, the intersection $A \cap A^*$ has odd cardinal number.*

Proof. Let $\psi : \mathcal{P} \cup \{D\} \longrightarrow E \setminus \{0\}$ be a realization of Γ as a $\mathbb{Z}_2$-vector space access structure. Let $A \in \Gamma_0$ and $A^* \in \Gamma_0^*$. Since $\mathcal{P} \setminus A^*$ is a maximal non-qualified subset of the access structure Γ, there exists $v \in E$ such that $v \cdot \psi(D) = 1$, $v \cdot \psi(p) = 0$ if $p \in \mathcal{P} \setminus A^*$, and $v \cdot \psi(p) = 1$ if $p \in A^*$. Observe that, since $A \in \Gamma_0$ is a minimal qualified subset and $\mathbb{K} = \mathbb{Z}_2$, then $\psi(D) = \sum_{p \in A} \psi(p)$. Therefore, $1 = v \cdot \psi(D) = \sum_{p \in A} v \cdot \psi(p) = \sum_{p \in A \cap A^*} 1$ and, hence, $A \cap A^*$ has odd cardinal number.

Let us prove now the reciprocal. We denote $\Gamma_0^* = \{B_1, \ldots, B_m\}$. Let $\psi : \mathcal{P} \cup \{D\} \longrightarrow \mathbb{Z}_2^m$ be the map defined by $\psi(D) = (1, \ldots, 1)$, and $\psi(p) = (\delta(p, B_1), \ldots, \delta(p, B_m))$ whenever $p \in \mathcal{P}$, where $\delta(p, B) = 1$ if $p \in B$ and $\delta(p, B) = 0$ otherwise. We claim that ψ is a realization of Γ as a $\mathbb{Z}_2$-vector space access structure. In order to prove our claim we must demonstrate that if $A \subset \mathcal{P}$ then, $A \in \Gamma$ if and only if the vector $\psi(D)$ can be expressed as a linear combination of the vectors in the set $\psi(A) = \{\psi(p) : p \in A\}$.

Assume that $A \in \Gamma$. So there exists $A_0 \in \Gamma_0$ such that $A_0 \subset A$. Therefore $\sum_{p \in A_0} \psi(p) = (\sum_{p \in A_0} \delta(p, B_1), \ldots, \sum_{p \in A_0} \delta(p, B_m)) = (|A_0 \cap B_1|, \ldots, |A_0 \cap B_m|) = (1, \ldots, 1) = \psi(D)$. Hence, $\psi(D) \in \langle \psi(p) : p \in A_0 \rangle \subset \langle \psi(p) : p \in A \rangle$.

Conversely, assuming that $\psi(D)$ is a linear combination of the vectors in the set $\psi(A) = \{\psi(p) : p \in A\}$, we must demonstrate that $A \in \Gamma$. Since $\psi(D) \in \langle \psi(p) : p \in A \rangle$, hence $\psi(D) = \sum_{p \in A} \lambda_p \psi(p) = \sum_{p \in A_0} \psi(p)$ where $A_0 = \{p \in A : \lambda_p \neq 0\}$. So, $(1, \ldots, 1) = \psi(D) = \sum_{p \in A_0} \psi(p) = (\sum_{p \in A_0} \delta(p, B_1), \ldots, \sum_{p \in A_0} \delta(p, B_m)) = (|A_0 \cap B_1|, \ldots, |A_0 \cap B_m|)$. Thus, for $i = 1, \ldots, m$ we have that $A_0 \cap B_i \neq \emptyset$. Therefore, from Lemma 2.1 it follows that $A_0 \in (\Gamma_0^*)^* = \Gamma_0$ and hence, $A \in \Gamma$ as we wanted to prove. $\square$

Remark 2.3 It is interesting to notice that the proof of the above proposition gives us an explicit realization for any $\mathbb{Z}_2$-vector space access structure Γ. For instance, let us consider

the access structure , on the set of six participants $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ having minimal qualified subsets $A_1 = \{p_1, p_2, p_3\}$, $A_2 = \{p_1, p_4, p_5\}$, $A_3 = \{p_2, p_3, p_6\}$, $A_4 = \{p_4, p_5, p_6\}$, $A_5 = \{p_2, p_5\}$ and $A_6 = \{p_3, p_4\}$. It is not hard to check that its dual access structure , * has basis $(, ^*)_0 = \{\{p_1, p_2, p_3, p_6\}, \{p_1, p_4, p_5, p_6\}, \{p_2, p_4\}, \{p_3, p_5\}\}$. Therefore, from Theorem 2.2 it follows that , is a vector space access structure. Furthermore, the map $\psi : \mathcal{P} \cup \{D\} \longrightarrow \mathbb{Z}_2^4$ defined by $\psi(D) = (1,1,1,1)$, $\psi(p_1) = (1,1,0,0)$, $\psi(p_2) = (1,0,1,0)$, $\psi(p_3) = (1,0,0,1)$, $\psi(p_4) = (0,1,1,0)$, $\psi(p_5) = (0,1,0,1)$ and $\psi(p_6) = (1,1,0,0)$, gives us a realization of , as a $\mathbb{Z}_2$-vector space access structure.

Corollary 2.4 *The following 3-homogeneous access structures are $\mathbb{Z}_2$-vector space access structures:*

1. *The access structure , $\langle S(p) \rangle$ defined by a 3-homogeneous star. That is, , $\langle S(p) \rangle$ is the access structure on the set of $2r+1$ participants $\mathcal{P} = \{p, a_1, \ldots, a_r, b_1, \ldots, b_r\}$ having basis $(, \langle S(p) \rangle)_0 = \{A_1, \ldots, A_r\}$ where $A_i = \{p, a_i, b_i\}$ for $i = 1, \ldots, r$.*

2. *The access structure , $_2$ associated to the Fano plane. That is, , $_2$ 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 $(, _2)_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_7\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_7\}, \{p_3, p_4, p_5\}, \{p_3, p_6, p_7\}\}$.*

3. *The access structure , $_{2,1}$ obtained from , $_2$ by removing one participant. That is, , $_{2,1}$ is the access structure on the set $\mathcal{P} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ of six participants with basis $(, _{2,1})_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_3, p_4, p_5\}\}$.*

Proof. It is not hard to show that $(, \langle S(p) \rangle^*)_0 = \{\{p\}\} \cup \{\{c_1, \ldots, c_r\}$ where $c_i \in \{a_i, b_i\}\}$, while , $^*_2 =$, $_2$, and $(, ^*_{2,1})_0 = (, _{2,1})_0 \cup \{\{p_1, p_4\}, \{p_2, p_5\}, \{p_3, p_6\}\}$. Therefore, for each one of these access structures we have that $|A \cap A^*| = 1, 3$ whenever $A \in , _0$ and $A^* \in , ^*_0$. Hence, applying Theorem 2.2 it follows that they are $\mathbb{Z}_2$-vector space access structures. □

3 Sparse homogeneous access structures with rank three

Let , be an access structure defined on a set of participants $\mathcal{P}$. For a subset $\mathcal{Q} \subset \mathcal{P}$ we define the *access structure induced* by , on the set of participants $\mathcal{Q}$ as , $(\mathcal{Q}) = \{A \subset \mathcal{Q} : A \in , \}$. Hence the minimal qualified subsets of , $(\mathcal{Q})$ are exactly the subsets $A \subset \mathcal{Q}$ such that $A \in , _0$. Let us denote $\omega(\mathcal{Q}, ,) = |, (\mathcal{Q})_0|$ and $\omega(s, ,) = \max\{\omega(\mathcal{Q}, ,) : |\mathcal{Q}| = s\}$. Notice that if , is a 3-homogeneous access structure then $1 \leq \omega(4, ,) \leq 4$. We say that a 3-homogeneous access structure , is *sparse* if $\omega(4, ,) \leq 2$.

We present in this section a characterization of the ideal sparse 3-homogeneous access structures. In Theorem 3.2 we prove that the ideal access structures in this family coincide with the vector space ones and, besides, that there is no sparse 3-homogeneous access structures whose optimal information rate verifies $2/3 < \rho^*(,) < 1$. Furthermore, a explicit description of the ideal sparse 3-homogeneous access structures is given in Theorem 3.3. The section will be finished by showing some examples of ideal and non ideal access structures.

The results in the previous section together with the independent sequence method are the key points in the proof of Theorem 3.2. The *independent sequence method* was introduced by Blundo, De Santis, De Simone and Vaccaro in [2, Theorem 3.8] and was generalized by Padró and Sáez in [15, Theorem 2.1]. This method works as follows. Let , be an access structure on a set of participants $\mathcal{P}$. Let $\emptyset \neq B_1 \subset \cdots \subset B_m \notin ,$ 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 every $i = 1, \ldots, m$ 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 $A \notin \Gamma$.

Lemma 3.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$, with corank* $\mathrm{corank}(\Gamma) \geq 3$*, and optimal information rate $\rho^*(\Gamma) > 2/3$. Let $p_1, p_2, p_3, p_4 \in \mathcal{P}$ be four different participants. Assume that $\{p_1, p_2, p_3\} \in \Gamma$ and that $\{p_1, p_2, p_4\} \in \Gamma$. Then, either $\{p_1, p_3, p_4\} \in \Gamma$, or $\{p_2, p_3, p_4\} \in \Gamma$, or $\{p_3, p_4, p\} \notin \Gamma$ for any participant $p \in \mathcal{P} \setminus \{p_1, p_2, p_3, p_4\}$.*

Proof. Let us assume that $\{p_1, p_3, p_4\}, \{p_2, p_3, p_4\} \notin \Gamma$. Let $p \in \mathcal{P} \setminus \{p_1, p_2, p_3, p_4\}$. We must demonstrate that $\{p_3, p_4, p\} \notin \Gamma$. In order to do it we distinguish two cases.

First let us suppose that $\{p_1, p_3, p\} \notin \Gamma$. In this case we can consider the subsets $B_1 = \{p_1\}$, $B_2 = \{p_1, p_3\}$ and $B_3 = \{p_1, p_3, p\}$. We have that $B_1 \cup \{p_2, p_4\} = \{p_1, p_2, p_4\} \in \Gamma$, $B_1 \cup \{p_2\} = \{p_1, p_2\} \notin \Gamma$ because $\mathrm{corank}(\Gamma) \geq 3$, $B_2 \cup \{p_2\} = \{p_1, p_2, p_3\} \in \Gamma$, and $B_2 \cup \{p_4\} = \{p_1, p_3, p_4\} \notin \Gamma$. Therefore, if $B_3 \cup \{p_4\} \in \Gamma$ then the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ is made independent by the set $A = \{p_2, p_4\} \notin \Gamma$ by taking $X_1 = \{p_2, p_4\}$, $X_2 = \{p_2\}$ and $X_3 = \{p_4\}$. Hence, by the independent sequence method it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction. Thus, $B_3 \cup \{p_4\} = \{p_1, p_3, p_4, p\} \notin \Gamma$. In particular, $\{p_3, p_4, p\} \notin \Gamma$ as we wanted to prove.

Now we assume that $\{p_1, p_3, p\} \in \Gamma$. In such a case we consider the subsets $B_1 = \{p_3\}$, $B_2 = \{p_3, p_4\}$ and $B_3 = \{p_2, p_3, p_4\}$. Notice that $B_1 \cup \{p_1, p\} = \{p_1, p_3, p\} \in \Gamma$, $B_1 \cup \{p\} = \{p_3, p\} \notin \Gamma$ because $\mathrm{corank}(\Gamma) \geq 3$, $B_2 \cup \{p_1\} = \{p_1, p_3, p_4\} \notin \Gamma$, and $B_3 \cup \{p_1\} = \{p_1, p_2, p_3, p_4\} \in \Gamma$. Thus, if $B_2 \cup \{p\} \in \Gamma$, then the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ is made independent by the set $A = \{p_1, p\} \notin \Gamma$ by taking $X_1 = \{p_1, p\}$, $X_2 = \{p\}$ and $X_3 = \{p_1\}$. Therefore, by the independent sequence method it follows that $\rho^*(\Gamma) \leq 2/3$, a contradiction. Hence, $\{p_3, p_4, p\} = B_2 \cup \{p\} \notin \Gamma$. This completes the proof of the lemma. □

Theorem 3.2 *Let Γ be a sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$. 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. *If $A \in \Gamma_0$ and $A^* \in \Gamma_0^*$, then the intersection $A \cap A^*$ has odd cardinal number.*

Proof. 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 Theorem 2.2 it follows that (4) implies (1). So, the proof of theorem will be concluded by proving that (3) implies (4).

Let us assume that $\rho^*(\Gamma) > 2/3$ and that there exist $A = \{p_1, p_2, p_3\} \in \Gamma_0$ and $A^* \in \Gamma_0^*$ such that the intersection $A \cap A^*$ has even cardinal number. We are going to prove that a contradiction holds in this case.

From Lemma 2.1 we have that $A \cap A^* \neq \emptyset$. Therefore $|A \cap A^*| = 2$. Without loss of generality we can suppose that $p_1, p_2 \in A^*$ and that $p_3 \notin A^*$. Since $A^* \in \Gamma_0^*$, hence it follows that $A^* \setminus \{p_i\} \notin \Gamma^*$ whenever $i = 1, 2$. Therefore, from Lemma 2.1, we get that there exists $\{p_i, q_{i,1}, q_{i,2}\} \in \Gamma_0$ such that $q_{i,1}, q_{i,2} \notin A^*$. Let us consider the subsets $B_1 = \{p_3\}$, $B_2 = \{p_3, q_{1,1}, q_{1,2}\}$ and $B_3 = \{p_3, q_{1,1}, q_{1,2}, q_{2,1}, q_{2,2}\}$. Observe that $B_3 \cap A^* = \emptyset$. Hence,

applying Lemma 2.1 it follows that $B_3 \notin (,^*)^* = ,$. We claim that the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin ,$ is made independent by the set $A = \{p_1, p_2\} \notin ,$ by taking the subsets $X_1 = \{p_1, p_2\}$, $X_2 = \{p_1\}$ and $X_3 = \{p_2\}$. Therefore, from our claim and by applying the independent sequence method it follows that $\rho^*(,) \leq 2/3$, a contradiction. Hence, the proof will be completed by proving our claim. Let us demonstrate it.

On one hand, we have that the subsets $B_3 \cup X_3$, $B_2 \cup X_2$ and $B_1 \cup X_1$ are qualified subsets for the access structure , because $\{p_2, q_{2,1}, q_{2,2}\} \subset B_3 \cup X_3$, $\{p_1, q_{1,1}, q_{1,2}\} \subset B_2 \cup X_2$ and $\{p_1, p_2, p_3\} = B_1 \cup X_1$. On the other hand, $B_1 \cup X_2 = \{p_1, p_3\}$ is not a qualified subset since , is a 3-homogeneous access structure. Therefore, in order to prove our claim we only must to check that $B_2 \cup X_3 \notin ,$. Since $B_2 \cup X_3 = \{p_2, p_3, q_{1,1}, q_{1,2}\}$ and , is 3-homogeneous, hence it follows that it is enough to show that the subsets $\{p_2, p_3, q_{1,1}\}$, $\{p_2, p_3, q_{1,2}\}$, $\{p_2, q_{1,1}, q_{1,2}\}$ and $\{p_3, q_{1,1}, q_{1,2}\}$ are not qualified.

Firstly let us show that $\{p_3, q_{1,1}, q_{1,2}\} \notin ,$. Since $p_3, q_{1,1}, q_{1,2} \notin A^*$, hence $\{p_3, q_{1,1}, q_{1,2}\} \cap A^* = \emptyset$. Thus, from Lemma 2.1, $\{p_3, q_{1,1}, q_{1,2}\} \notin (,^*)^* = ,$.

Now we are going to prove that $\{p_2, p_3, q_{1,1}\}, \{p_2, p_3, q_{1,2}\} \notin ,$. By symmetry we only need to show that $\{p_2, p_3, q_{1,1}\} \notin ,$. If $\{p_2, p_3, q_{1,1}\} \in ,$, then $p_1, p_2, p_3, q_{1,1} \in \mathcal{P}$ are four different participants. On one hand we have that $\{p_1, p_2, p_3\} \in ,$. Hence $\omega(\{p_1, p_2, p_3, q_{1,1}\}, ,) \geq 2$, and then $\omega(\{p_1, p_2, p_3, q_{1,1}\}, ,) = 2$ because , is sparse. On the other hand we have that $\{p_1, q_{1,1}, q_{1,2}\} \in ,$. Therefore, a contradiction follows by applying Lemma 3.1.

To finish we must demonstrate that $\{p_2, q_{1,1}, q_{1,2}\} \notin ,$. Otherwise, $p_1, p_2, q_{1,1}, q_{1,2} \in \mathcal{P}$ are four different participants and $\omega(\{p_1, p_2, q_{1,1}, q_{1,2}\}, ,) \geq 2$. So $\omega(\{p_1, p_2, q_{1,1}, q_{1,2}\}, ,) = 2$. Since $\{p_1, p_2, p_3\} \in ,$, hence from Lemma 3.1 we get a contradiction. This completes the proof of our claim and so the proof of the theorem. □

Next, in Theorem 3.3, we present a description of the ideal sparse 3-homogeneous access structures. This theorem states that the ideal, *reduced* and *connected*, access structures in the family that we consider are exactly those given in Corollary 2.4. The previous theorem together with the results given in [13] and the independent sequence method are the key points in its proof.

Let , be an access structure on the set of participants $\mathcal{P}$. We say that , is *connected* if for each pair of participants $p, q \in \mathcal{P}$ there exist $A_1, \ldots, A_\ell \in ,_0$ such that $p \in A_1$, $q \in A_\ell$, and $A_i \cap A_{i+1} \neq \emptyset$ if $1 \leq i \leq \ell - 1$. It is clear that, for any access structure , on a set of participants $\mathcal{P}$, there exists a unique partition $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_r$ such that the induced access structures $,(\mathcal{P}_1), \ldots, ,(\mathcal{P}_r)$ are connected and $, = ,(\mathcal{P}_1) \cup \cdots \cup ,(\mathcal{P}_r)$. In this situation we say that $,(\mathcal{P}_1), \ldots, ,(\mathcal{P}_r)$ are the *connected components* of ,.

Furthermore, related to the access structure , we define the equivalence relation $\sim$ in $\mathcal{P}$ as follows. Two participants $p, q \in \mathcal{P}$ are said to be *equivalent* if either $p = q$ or $p \neq q$ and the following two conditions are satisfied: (1) $\{p, q\} \not\subset A$ if $A \in ,_0$, and (2) if $A \subset \mathcal{P} \setminus \{p, q\}$, then $A \cup \{p\} \in ,_0$ if and only if $A \cup \{q\} \in ,_0$. We say that the access structure , is *a reduced access structure* if there is no pair of different equivalent participants. Otherwise, we consider participants $p_1, \ldots, p_r \in \mathcal{P}$ defining the set $\mathcal{P}/\sim$ of the equivalence classes given by the relation $\sim$, that is $\mathcal{P}/\sim = \{[p_1], \ldots, [p_r]\}$. An access structure $,_\sim$ on the set $\mathcal{P}/\sim$ is obtained in a natural way from the access structure , by identifying equivalent participants. It is not difficult to check that $,_\sim$ is isomorphic to the induced access structure $,(\{p_1, \ldots, p_r\})$. The structure $,_\sim$ is called *the reduced access structure* of ,.

Theorem 3.3 *Let , be a sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$.*

Then, the following conditions are equivalent:

1. , *is an ideal access structure.*
2. *Every connected component of the reduced access structure* , $\sim$ *of* , *is either an access structure* , $\langle S(p_0)\rangle$ *defined by a 3-homogeneous star, or the access structure associated to the Fano plane* , $_2$*, or its related access structure* , $_{2,1}$.

Proof. First we are going to prove that (2) implies (1). It is not hard to show that if , is an access structure on a set of participants $\mathcal{P}$ such that each connected component of its reduced access structure , $\sim$ is a $\mathbb{K}$-vector space access structure, then , is a $\mathbb{K}$-vector space access structure. In our case, from Corollary 2.4 we have that the access structures , $\langle S(p_0)\rangle$, , $_2$ and , $_{2,1}$ are $\mathbb{Z}_2$-vector space access structures. Therefore, , is a $\mathbb{Z}_2$-vector space access structure and so it is ideal.

Now, let us show that (1) implies (2). If , is ideal, then it is easy to check that all the connected components of the reduced access structure , $\sim$ are also ideal. Besides, since , $\sim \cong$, $(\{p_1, \ldots, p_r\})$, these connected components are also sparse 3-homogeneous access structures. Therefore, we only have to prove that: if , is an ideal, reduced and connected sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$, then , is either an access structure , $\langle S(p_0)\rangle$ defined by a 3-homogeneous star, or the access structure associated to the Fano plane , $_2$, or its related access structure , $_{2,1}$. From the results in [13] it follows that , $\langle S(p_0)\rangle$, , $_2$ and , $_{2,1}$ are the only ideal and 3-homogeneous connected access structures with intersection number equal to one (that is to say, there is at most one participant in the intersection of any two different minimal qualified subsets). Hence, the proof is concluded by checking that: if , is an ideal, reduced and connected sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$, then , has intersection number equal to one.

It is clear that a 3-homogeneous access structures , has intersection number equal to one if and only if $\omega(\{a, b, c, d\}, ,) \leq 1$ for every four different participants $a, b, c, d \in \mathcal{P}$. Let us suppose that there exist four different participants $a, b, c, d \in \mathcal{P}$ such that $\omega(\{a, b, c, d\}, ,) \geq 2$. Since , is sparse, hence we can assume that $\{a, c, d\}, \{b, c, d\} \in$, and that $\{a, b, c\}, \{a, b, d\} \notin$, . We are going to prove that, in this situation, a and b are equivalent participants and, hence, , is not a reduced access structure.

From Lemma 3.1, the set $\{a, b, p\}$ is not qualified for any $p \in \mathcal{P}$. Then, $\{a, b\} \not\subset A$ if $A \in$, $_0$. Let us prove now that, if $A \subset \mathcal{P} \setminus \{a, b\}$, then $A \cup \{a\} \in$, $_0$ if and only if $A \cup \{b\} \in$, $_0$. Obviously, we can suppose that $|A| = 2$. We distinguish two cases.

Case 1: $A \cap \{c, d\} \neq \emptyset$. Since both $\{a, c, d\}$ and $\{b, c, d\}$ are minimal qualified subsets, we can suppose that $A = \{c, x\}$ with $x \neq d$. Let us show that, if $\{a, c, x\} \in$, $_0$, then $\{b, c, x\} \in$, $_0$, being the reciprocal proved in the same way. We consider the subsets $B_1 = \{c\}$, $B_2 = \{b, c\}$ and $B_3 = \{b, c, x\}$, and $X_1 = \{a, d\}$, $X_2 = \{d\}$ and $X_3 = \{a\}$. If $\{b, c, x\} \notin$, , then the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin$, is made independent by $\{a, d\}$ and, hence $\rho^*(,) \leq 2/3$, a contradiction. Therefore, $\{b, c, x\} \in$, $_0$.

Case 2: $A \cap \{c, d\} = \emptyset$. Hence, $A = \{x, y\} \subset \mathcal{P} \setminus \{a, b, c, d\}$. As before, it is enough to prove that $\{b, x, y\} \in$, $_0$ if $\{a, x, y\} \in$, $_0$. So, let us assume that $\{a, x, y\} \in$, $_0$. Notice that, in such a case we have that $\{b, c, x, y\} \in$, , because otherwise a contradiction is obtained by applying the independent sequence method to the subsets $B_1 = \{c\}$, $B_2 = \{b, c\}$ and $B_3 = \{b, c, x, y\}$, and $X_1 = \{a, d\}$, $X_2 = \{d\}$ and $X_3 = \{a\}$. Let us suppose that $\{b, x, y\} \notin$, . Hence, at least one of the subsets $\{b, c, x\}$, $\{b, c, y\}$, $\{c, x, y\}$ is qualified. If $\{c, x, y\} \in$, , we can apply Lemma 3.1 to the minimal qualified subsets $\{c, x, y\}$ and $\{a, x, y\}$ and, since $\{a, c, d\} \in$, ,

we obtain that $\omega(\{a,c,x,y\},,) > 2$, a contradiction. Then, without loss of generality, we can suppose that $\{b,c,x\} \in ,_0$, and so, from Case 1, we get that $\{a,c,x\} \in ,_0$. Since $\{b,x,y\} \notin ,,$ from Lemma 2.1, there exists $A^* \in ,_0^*$ such that $\{b,x,y\} \cap A^* = \emptyset$. Applying again Lemma 2.1, $\{b,c,x\} \cap A^* \neq \emptyset$ and $\{a,x,y\} \cap A^* \neq \emptyset$. Hence, $\{a,c,x\} \cap A^* = \{a,c\}$ has an even number of elements, a contradiction with Theorem 3.2. This completes the proof. □

To finish we point out some examples in order to illustrate our results. In the following examples , is a 3-homogeneous access structure on a set $\mathcal{P} = \{p_1,p_2,p_3,p_4,p_5,p_6\}$ of six participants. The first two are sparse access structure, while the last two satisfy $\omega(4,,) \geq 3$.

Example 3.4 Let , be the access structure on $\mathcal{P}$ with minimal qualified subsets $A_1 = \{p_1,p_2,p_3\}$, $A_2 = \{p_1,p_2,p_6\}$, $A_3 = \{p_1,p_5,p_6\}$ and $A_4 = \{p_3,p_4,p_5\}$. So $\omega(4,,) = 2$, and hence , is sparse. From Lemma 2.1 it follows that $\{p_1,p_5\} \in ,_0^*$. Since $|\{p_1,p_5\} \cap \{p_1,p_5,p_6\}| = 2$ hence, from Theorem 3.2, we conclude that , is not ideal and has optimal information rate $\rho^*(,) \leq 2/3$. Observe that , is a connected and reduced access structure.

Example 3.5 Now we consider the access structure , on $\mathcal{P}$ whose minimal qualified subsets are $A_1 = \{p_1,p_2,p_3\}$, $A_2 = \{p_4,p_5,p_6\}$, $A_3 = \{p_1,p_4,p_5\}$ and $A_4 = \{p_2,p_3,p_6\}$. Hence we have that $\omega(4,,) = 2$ and so , is sparse. It is not hard to check that $,_0^* = \{\{p_1,p_6\},\{p_2,p_4\},\{p_2,p_5\},\{p_3,p_4\},\{p_3,p_5\}\}$. So $|A \cap A^*| = 1$ if $A \in ,_0$ and $A^* \in ,_0^*$. Hence, from Theorem 3.2, it follows that , is a vector space access structure. Notice that , $\sim$ is a star access structure.

Example 3.6 Next we consider the access structure , on $\mathcal{P}$ having minimal qualified subsets $A_1 = \{p_1,p_2,p_3\}$, $A_2 = \{p_1,p_2,p_4\}$, $A_3 = \{p_3,p_4,p_5\}$, $A_4 = \{p_3,p_4,p_6\}$, and $A_5 = \{p_4,p_5,p_6\}$. Notice that , is not sparse because $\omega(\{p_3,p_4,p_5,p_6\},,) = 3$. Nevertheless we can apply Lemma 3.1. Namely, we have that $\{p_1,p_2,p_3\},\{p_1,p_2,p_4\} \in ,,$ that $\{p_1,p_3,p_4\},\{p_2,p_3,p_4\} \notin ,,$ and that $\{p_3,p_4,p_5\} \in ,,$. Therefore applying Lemma 3.1 we conclude that $\rho^*(,) \leq 2/3$.

Example 3.7 Finally, let , be the access structure on $\mathcal{P}$ with minimal qualified subsets $A_1 = \{p_1,p_2,p_3\}$, $A_2 = \{p_1,p_2,p_4\}$, $A_3 = \{p_1,p_3,p_4\}$, $A_4 = \{p_2,p_3,p_4\}$, $A_5 = \{p_1,p_2,p_5\}$, $A_6 = \{p_1,p_3,p_6\}$ and $A_7 = \{p_1,p_4,p_6\}$. Notice that for any $i = 0,1,2,3,4$ there exists a subset $C_i \subset \mathcal{P}$ with $|C_i| = 4$ and $\omega(C_i,,) = i$. In particular, , is not sparse. However we are going to prove that , is not ideal by applying our results to a suitable substructure. Namely, let $,(\mathcal{P}_4)$ be the access structure induced by , on $\mathcal{P}_4 = \mathcal{P} \setminus \{p_4\}$. So, $(,(\mathcal{P}_4))_0 = \{A_1,A_5,A_6\}$. Hence, $,(\mathcal{P}_4)$ is a sparse 3-homogeneous access structure on $\mathcal{P}_4$. From Lemma 2.1 we get that $\{p_2,p_3\} \in (,(\mathcal{P}_4))_0^*$ and thus we conclude that $\rho^*(,(\mathcal{P}_4)) \leq 2/3$ by applying Theorem 3.2. It is clear that any secret sharing scheme for , induce a secret sharing scheme for $,(\mathcal{P}_4)$ with the same set of secrets. Hence $\rho^*(,) \leq \rho^*(,(\mathcal{P}_4))$. Therefore, $\rho^*(,) \leq 2/3$.

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. LNCS* 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. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography* 9 (1996), 267–286.

[11] M. Karchmer, A. Wigderson. On span programs. *Proceedings of the Eighth Annual Structure in Complexity Theory Conference* (San Diego, CA, 1993), 102–111.

[12] J. Martí-Farré, C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, to appear.

[13] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Proceedings of the Third Conference on Security in Communication Networks* (Amalfi, Italy, 2002) *LNCS*, to appear.

[14] J.L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, 1993, 276–279.

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

[16] C. Padró, G. Sáez. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. *Information Processing Letters* 83 (2002), 345-351.

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

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

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

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

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