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

One of the main open problems in secret sharing is the characterization of the ideal access structures. This problem has been studied for several families of access structures with similar results. Namely, in all these families, the ideal access structures coincide with the vector space ones and, besides, the optimal information rate of a non-ideal access structure is at most 2/3.

A first approach to the solution of that problem for the family of the 3-homogeneous access structures is made in this paper. First, we present an ideal 3-homogeneous access structure that is not vector space. Afterwards, we prove that the 3-homogeneous access structures that can be realized by a $\mathbb{Z}_2$-vector space secret sharing scheme are *sparse*, that is, any subset of four participants contains at most two minimal qualified subsets. Finally, we solve the characterization problem for the family of the sparse 3-homogeneous access structures. Specifically, we completely characterize the ideal access structures in this family, we prove that they coincide with the $\mathbb{Z}_2$-vector space ones and, besides, we demonstrate that there is no structure in this family having optimal information rate between 2/3 and 1. That is, we establish that the properties that were previously proved for several families also hold for the family of the sparse 3-homogeneous access structures.

Keywords. Cryptography; Secret sharing schemes; Information rate; Ideal secret sharing 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 [19]. A comprehensive introduction to this topic can be found in [21]. 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*, that is, 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 the qualified subsets, $\Gamma \subset 2^{\mathcal{P}}$. 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 Γ is determined by the family of the *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 first works about secret sharing [1, 19] 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 more general access structures and Ito, Saito and Nishizeki [10] 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 [10] 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* $\rho(\Sigma, \Gamma, \mathcal{K})$ 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.

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 $\Gamma \subset 2^{\mathcal{P}}$ is an *ideal access structure* if there exists an ideal secret sharing scheme for Γ. For instance, the threshold access structures are ideal.

Not all access structures are ideal. So, when designing a secret sharing scheme for a given access structure Γ, we may try to maximize the information rate. 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, more generally, to determine the optimal information rate of any access structure. Even though a number of results have been given, both problems are far from being solved.

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 [18], who proved that there is no ideal scheme for the access structures 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 [15] and equivalent also to the ones obtained from monotone span programs [12]. In fact, vector space access structures are exactly those related to representable matroids. Nevertheless, this sufficient condition is not necessary, because the existence of ideal access structures that are not vector space is deduced from the results by Simonis and

Ashikhmin [20] on the non-Pappus matroid.

Several techniques have been introduced in [4, 7, 17, 22] 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 [16]. However, 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 general results, these problems have been studied in several particular classes of access structures: access structures on sets of four [21] and five [11] participants, access structures defined by graphs [2, 3, 4, 6, 7, 8, 22], bipartite access structures [16], access structures with three or four minimal qualified subsets [13], and access structures with intersection number equal to one [14]. 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, besides, 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 to other families of access structures.

The aim of this paper is to present a first approximation to the characterization of the ideal 3-homogeneous access structures. An access structure is said to be *r-homogeneous* if all its minimal qualified subsets have exactly r different participants. Notice that the 2-homogeneous access structures are exactly those defined by graphs. As we said before, the ideal 2-homogeneous access structures coincide with the vector space ones. We prove that this fact can not be directly generalized to the family of the 3-homogeneous access structures by presenting a counterexample in Proposition 4.2. This counterexample leads us to restrict our study to the family of the *sparse 3-homogeneous access structures*. A 3-homogeneous access structure is said to be *sparse* if each set of four participants contains at most two minimal qualified subsets. On top of this, in Theorem 4.5 we prove that that any $\mathbb{Z}_2$-vector space 3-homogeneous access structure must be sparse. Both results, Proposition 4.2 and Theorem 4.5, make clear the relevance of the sparse access structures in the characterization of the ideal 3-homogeneous access structures.

The main result of this paper is the characterization of the ideal sparse 3-homogeneous access structures. We prove, in Theorem 5.1, that every ideal access structure in this family is a $\mathbb{Z}_2$-vector space access structure. Moreover, we show that there is no access structure with optimal information rate between $2/3$ and 1 in the family we consider. Besides, we present a complete description of the ideal sparse 3-homogeneous access structures in terms of their simple components.

The paper is organized as follows. In Section 2, the vector space access structures over the finite field $\mathbb{Z}_2$ are characterized in terms of a combinatorial property involving the dual access structure. We define in Section 3 the simple components of an access structure and present some basic facts on this concept. Our main results are given in the following two sections. Namely, general results on ideal 3-homogeneous access structures are presented in Section 4, while Section 5 deals with the characterization and description of the ideal sparse 3-homogeneous access structures. We conclude by showing some examples illustrating these results in Section 6.

2   On vector space access structures over $\mathbb{Z}_2$

Some definitions and basic facts on vector space secret sharing schemes and vector space access structures are recalled in this section. Besides, we present in Theorem 2.2 a characterization the $\mathbb{Z}_2$-vector space access structures that was given in [9]. As a corollary, we demonstrate that the access structures $\Gamma\langle S(p)\rangle$ defined by a 3-homogeneous star, the access structure Γ_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 3-homogeneous 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 [21] 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 $p \in A$.

Theorem 2.2, which is a characterization of $\mathbb{Z}_2$-vector space access structures, 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 $A \in \Gamma_0$.*

Proof. From the definition of Γ^*, we have that $B \in \Gamma^*$ if and only if $A \not\subset \mathcal{P} \setminus B$ for every $A \in \Gamma_0$. Thus, $B \in \Gamma^*$ if and only if $B \cap A \neq \emptyset$ for every $A \in \Gamma_0$. $\square$

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, $\psi(D) \in \langle \psi(p) : p \in A_0 \rangle \subset \langle \psi(p) : p \in A \rangle$.

4

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 $A_0 \in (\Gamma^*)^* = \Gamma$ 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 theorem gives us an explicit realization for any $\mathbb{Z}_2$-vector space access structure Γ. For instance, let us consider the access structure Γ 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 Γ^* has basis $\Gamma_0^* = \{\{p_1, p_2, p_3, p_6\}, \{p_1, p_4, p_5, p_6\}, \{p_2, p_4\}, \{p_3, p_5\}\}$. Therefore, from Theorem 2.2 it follows that Γ 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 Γ 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 structures $\Gamma\langle S(p) \rangle$ defined by 3-homogeneous stars. That is, $\Gamma\langle S(p) \rangle$ is an access structure on a set of $2r+1$ participants $\mathcal{P} = \{p, a_1, \ldots, a_r, b_1, \ldots, b_r\}$ having basis $(\Gamma\langle S(p) \rangle)_0 = \{A_1, \ldots, A_r\}$ where $A_i = \{p, a_i, b_i\}$ for $i = 1, \ldots, r$.*

2. *The access structure Γ_2 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 $(\Gamma_2)_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_7\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_7\}, \{p_3, p_4, p_5\}, \{p_3, p_6, p_7\}\}$.*

3. *The access structure $\Gamma_{2,1}$ obtained from Γ_2 by removing one participant. That is, $\Gamma_{2,1}$ 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 $(\Gamma_{2,1})_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_3, p_4, p_5\}\}$.*

Proof. It is not hard to show that $(\Gamma\langle S(p) \rangle^*)_0 = \{\{p\}\} \cup \{\{c_1, \ldots, c_r\} : c_i \in \{a_i, b_i\}\}$, while $\Gamma_2^* = \Gamma_2$, and $(\Gamma_{2,1}^*)_0 = (\Gamma_{2,1})_0 \cup \{\{p_1, p_4\}, \{p_2, p_5\}, \{p_3, p_6\}\}$. Therefore, for each one of these access structures we have that $|A \cap A^*| = 1, 3$ whenever $A \in \Gamma_0$ and $A^* \in \Gamma_0^*$. Hence, applying Theorem 2.2 it follows that they are $\mathbb{Z}_2$-vector space access structures. $\square$

3   Simple components of an access structure

Let Γ 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 Γ on the set of participants $\mathcal{Q}$ as $\Gamma(\mathcal{Q}) = \{A \subset \mathcal{Q} : A \in \Gamma\}$. Hence the minimal qualified subsets of $\Gamma(\mathcal{Q})$ are exactly the subsets $A \subset \mathcal{Q}$ such that $A \in \Gamma_0$.

Let Γ be an access structure on a set of participants $\mathcal{P}$. We say that Γ is *connected* if for each 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 $A_i \cap A_{i+1} \neq \emptyset$ if $1 \leq i \leq \ell - 1$. It is clear that, for any access structure Γ 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 $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ 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.

Furthermore, related to the access structure Γ, 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 $A \in \Gamma_0$, and (2) if $A \subset \mathcal{P} \setminus \{p, q\}$ then, $A \cup \{p\} \in \Gamma_0$ if and only if $A \cup \{q\} \in \Gamma_0$.

We say that the access structure Γ 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 $\Gamma_\sim$ on the set $\mathcal{P}/\sim$ is obtained in a natural way from the access structure Γ by identifying equivalent participants. It is not difficult to check that $\Gamma_\sim$ is isomorphic to the induced access structure $\Gamma(\{p_1, \ldots, p_r\})$. The structure $\Gamma_\sim$ is called *the reduced access structure* of Γ. Notice that if Γ is reduced then $\Gamma = \Gamma_\sim$.

Let Γ be an access structure with connected components $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$. The reduced access structures $\Gamma(\mathcal{P}_1)_\sim, \ldots, \Gamma(\mathcal{P}_r)_\sim$ are called the *simple components* of Γ.

Lemma 3.1 *Let Γ be an access structure on a set of participants $\mathcal{P}$. Then, the following statements hold:*

1. *If Γ' is a simple component of Γ, then $\rho^*(\Gamma') \geq \rho^*(\Gamma)$.*

2. *If Γ is an ideal access structure, then all the simple components of Γ are so.*

3. *If $\mathbb{K}$ is a finite field then, Γ is a $\mathbb{K}$-vector space access structure if and only if every simple component of Γ is a $\mathbb{K}$-vector space access structure.*

Proof. Let $\mathcal{Q} \subset \mathcal{P}$ be a subset of participants. Any secret sharing scheme Σ with access structure Γ and set of secrets $\mathcal{K}$ induces, in a trivial way, a scheme $\Sigma_\mathcal{Q}$ for the induced access structure $\Gamma(\mathcal{Q})$ with the same set of secrets. Obviously, $\rho(\Sigma_\mathcal{Q}, \Gamma(\mathcal{Q}), \mathcal{K}) \geq \rho(\Sigma, \Gamma, \mathcal{K})$. Hence, $\rho^*(\Gamma(\mathcal{Q})) \geq \rho^*(\Gamma)$ and, besides, if Γ is an ideal access structure then $\Gamma(\mathcal{Q})$ is so. Since the simple components of Γ are induced access structures of Γ, hence the first two claims follow. We must demonstrate the last statement.

Let $\mathbb{K}$ be a finite field. Assume that Γ is a $\mathbb{K}$-vector space access structure. Let $\mathcal{Q} \subset \mathcal{P}$ be a subset of participants. It is clear that if $\psi : \mathcal{P} \cup \{D\} \longrightarrow E \setminus \{0\}$ is a realization of Γ as a $\mathbb{K}$-vector space access structure, then its restriction $\psi : \mathcal{Q} \cup \{D\} \longrightarrow E \setminus \{0\}$ is a realization of $\Gamma(\mathcal{Q})$ as a $\mathbb{K}$-vector space access structure. In particular, every simple component of Γ is a $\mathbb{K}$-vector space access structure. Conversely, let us assume that all the simple components $\Gamma(\mathcal{P}_1)_\sim, \ldots, \Gamma(\mathcal{P}_r)_\sim$ of Γ are $\mathbb{K}$-vector space access structures. We must demonstrate that, in such a case, Γ is a $\mathbb{K}$-vector space access structure too. It is not hard to check that a realization of $\Gamma(\mathcal{P}_i)$ as a $\mathbb{K}$-vector space access structure can be obtained from any realization of $\Gamma(\mathcal{P}_i)_\sim$ by assigning the same vector to equivalent participants. Hence, the connected components $\Gamma(\mathcal{P}_1), \ldots, \Gamma(\mathcal{P}_r)$ of Γ are $\mathbb{K}$-vector space access structures. For $1 \leq i \leq r$ let $\psi_i : \mathcal{P}_i \cup \{D_i\} \to E_i$ be a realization of $\Gamma(\mathcal{P}_i)$ as a $\mathbb{K}$-vector space access structure. 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 $\psi : \mathcal{P} \cup \{D\} \to E$ defined by $\psi(D) = (1, 0, \ldots, 0)$ and, if $p \in \mathcal{P}_i$, $\psi(p) = (\xi_p, 0, \ldots, v_p, \ldots, 0) \in \mathbb{K} \times E_1' \times \cdots \times E_i' \times \cdots \times E_r'$, where $\psi_i(p) = (\xi_p, v_p) \in \mathbb{K} \times E_i'$. It is not difficult to check that 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 $\psi(A) = \{\psi(p) \ : \ p \in A\}$. Therefore, ψ is a realization of Γ as a $\mathbb{K}$-vector space access structure. So, Γ is a $\mathbb{K}$-vector space access structure. $\square$

Example 3.2 Let us consider the access structure Γ on the set of thirteen participants $\mathcal{P} = \{p_1, \ldots, p_7, q_1, \ldots, q_6\}$ whose minimal qualified subsets are $\{p_1, p_2, p_3\}$, $\{p_3, p_4, p_5\}$, $\{p_1, p_5, p_6\}$, $\{p_2, p_4, p_6\}$, $\{p_1, p_5, p_7\}$, $\{p_2, p_4, p_7\}$, $\{q_1, q_2, q_3\}$, $\{q_1, q_4, q_5\}$ and $\{q_1, q_2, q_6\}$. In this case Γ has two connected components $\Gamma_1 = \Gamma(\{p_1, \ldots, p_7\})$ and $\Gamma_2 = \Gamma(\{q_1, \ldots, q_6\})$. Besides, $p_7 \sim p_6$ and $q_6 \sim q_3$. Hence, the simple components of Γ are $\Gamma_{1,\sim} = \Gamma(\{p_1, \ldots, p_6\}) = \Gamma_{2,1}$ and $\Gamma_{2,\sim} = \Gamma(\{q_1, \ldots, q_5\})$ a 3-homogeneous star. From Corollary 2.4 it follows that both $\Gamma_{1,\sim}$ as well as $\Gamma_{2,\sim}$ are $\mathbb{Z}_2$-vector space access structures. Hence, applying Lemma 3.1, we conclude that the access structure Γ is so.

4 Homogeneous access structures with rank three

The next two sections contains our main results, which are a first approach to the characterization of the ideal 3-homogeneous access structures. Specifically, in this section we present some general results related to the ideal 3-homogeneous access structures. The main results in this section, Proposition 4.2 and Theorem 4.5, leads us to focus our attention on the family of the sparse 3-homogeneous access structures. The characterization of the ideal access structures in this family will be the aim of the next section.

An access structure Γ 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 Γ are, respectively, the maximum and the minimum number of participants in a minimal qualified subset. So, the 2-homogeneous access structures are exactly those that can be defined by a graph. Observe that the complete graph K_n represents a $(2, n)$-threshold access structure, which is the simple component of the access structure corresponding to a complete multipartite graph. Therefore, the characterization of ideal 2-homogeneous access structures, which is obtained from the results in [3, 4, 6, 8, 21], can be rewritten as follows:

Theorem 4.1 *Let Γ be a 2-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. *Every simple component of Γ is a $(2, n)$-threshold access structure.*

Our purpose is to examine to which extent this result can be generalized to the family of the 3-homogeneous access structures.

Let us show first that, in general, the equivalence between ideal an vector space access structures does not hold in the rank 3 case by presenting, in Proposition 4.2, an ideal 3-homogeneous access structure on a set of nine participants that is not vector space.

Simonis and Ashikhmin [20] proved that the non-Pappus matroid can be seen as the matroid of an almost affine code even though this matroid is not linearly representable over any finite field. From this result, and by means of the relationship between access structures

and matroids, it follows that there are ideal access structures that are not vector space access structures over any finite field. The access structures obtained in this way from the non-Pappus matroid are access structures defined on a set of eight participants that have corank equal to two and are not homogeneous. The ideal 3-homogeneous access structure showed in the next proposition is based in these results. Specifically, in order to obtain an ideal 3-homogeneous access structure from the above ones we must add a new participant in the non-Pappus matroid that will play the role of the dealer in the ideal scheme we propose. Besides, the ideal secret sharing scheme we present in the proof is obtained by means of suitable changes in the almost affine code in [20] for the non-Pappus matroid.

Proposition 4.2 *Let Γ be the 3-homogeneous access structure on the set $\mathcal{P} = \{p_1, \ldots, p_9\}$ of nine participants with basis $\Gamma_0 = \{A \subset \mathcal{P} : |A| = 3\} \setminus \mathcal{A}$, where $\mathcal{A} = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_7\}, \{p_1, p_6, p_8\}, \{p_2, p_4, p_7\}, \{p_2, p_6, p_9\}, \{p_3, p_4, p_8\}, \{p_3, p_5, p_9\}, \{p_4, p_5, p_6\}\}$. Then, Γ is not a vector space access structure but can be realized by an ideal secret sharing scheme.*
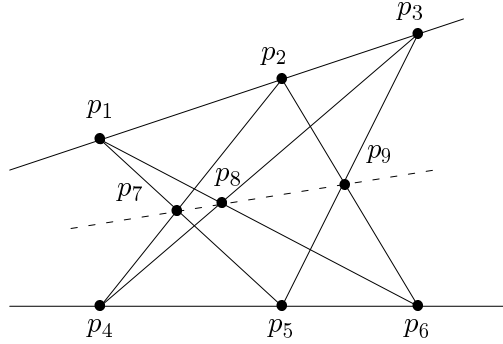
Proof. We prove first that Γ is not a $\mathbb{K}$-vector space access structure for any finite field $\mathbb{K}$. Let us suppose that there exists a realization $\psi : \mathcal{P} \cup \{D\} \to E \setminus \{0\}$ of Γ as a $\mathbb{K}$-vector space access structure. Let us denote $v_i = \psi(p_i)$ and $v_D = \psi(D)$. Since ψ is a realization of Γ hence, for any pair $p_i, p_j \in \mathcal{P}$ of different participants, we have that $\dim\langle v_i, v_j \rangle = 2$ while $\dim\langle v_i, v_j, v_D \rangle = 3$. We prove next that $\dim\langle v_1, \ldots, v_9, v_D \rangle = 3$. Let $i = 4, \ldots, 9$. Since $\{p_1, p_2, p_i\} \in \Gamma$ and Γ is a 3-homogeneous access structure, then there exist $\lambda_1, \lambda_2, \lambda_i \in \mathbb{K} \setminus \{0\}$ such that $v_D = \lambda_1 v_1 + \lambda_2 v_2 + \lambda_i v_i$. Hence it follows that $v_i \in \langle v_1, v_2, v_D \rangle$. In the same way, since $\{p_2, p_3, p_4\} \in \Gamma$, then $v_3 \in \langle v_2, v_4, v_D \rangle$, and thus $v_3 \in \langle v_1, v_2, v_D \rangle$. Therefore, $v_i \in \langle v_1, v_2, v_D \rangle$ for every $i = 3, \ldots, 9$, and so $\dim\langle v_1, \ldots, v_9, v_D \rangle = 3$. Besides, if $\{p_i, p_j, p_k\} \notin \Gamma$ is a non-qualified subset with three participants, then we have that $v_D \notin \langle v_i, v_j, v_k \rangle$, and hence $\dim\langle v_i, v_j, v_k \rangle = 2$ because $\dim\langle v_1, \ldots, v_9, v_D \rangle = 3$. In particular, $\dim\langle v_1, v_2, v_3 \rangle = 2$ and $\dim\langle v_4, v_5, v_6 \rangle = 2$ and, besides, $v_7 \in \langle v_1, v_5 \rangle \cap \langle v_2, v_4 \rangle$, $v_8 \in \langle v_1, v_6 \rangle \cap \langle v_3, v_4 \rangle$, $v_9 \in \langle v_3, v_5 \rangle \cap \langle v_2, v_6 \rangle$. By considering these nine vectors as points in the projective plane, and by applying the Theorem of Pappus, we conclude that $\dim\langle v_7, v_8, v_9 \rangle = 2$. Hence, the subset $\{p_7, p_8, p_9\}$ is not qualified, a contradiction.

Let us prove now that there exists an ideal secret sharing scheme for the access structure Γ. Let us consider the vector space $\mathbb{Z}_5^6$ and the subspaces $F_0 = \langle v_0, w_0 \rangle = \langle (1, 1, 1, 1, 0, 4), (3, 0, 2, 0, 1, 0) \rangle$. $F_1 = \langle v_1, w_1 \rangle = \langle (1, 0, 0, 0, 0, 0), (0, 1, 0, 0, 0, 0) \rangle$, $F_2 = \langle v_2, w_2 \rangle = \langle (1, 0, 0, 0, 1, 0), (0, 1, 0, 0, 0, 1) \rangle$, $F_3 = \langle v_3, w_3 \rangle = \langle (0, 0, 0, 0, 1, 0), (0, 0, 0, 0, 0, 1) \rangle$, $F_4 = \langle v_4, w_4 \rangle = \langle (1, 0, 1, 0, 0, 4), (0, 1, 0, 4, 1, 1) \rangle$, $F_5 = \langle v_5, w_5 \rangle = \langle (0, 0, 1, 0, 0, 0), (0, 0, 0, 1, 0, 0) \rangle$, $F_6 = \langle v_6, w_6 \rangle = \langle (1, 0, 4, 4, 0, 4), (0, 1, 1, 0, 1, 1) \rangle$, $F_7 = \langle v_7, w_7 \rangle = \langle (1, 0, 0, 1, 0, 0), (0, 1, 1, 4, 0, 0) \rangle$, $F_8 = \langle v_8, w_8 \rangle = \langle (1, 0, 1, 0, 1, 1), (0, 1, 0, 4, 1, 0) \rangle$,

$F_9 = \langle v_9, w_9 \rangle = \langle (0,0,1,0,1,0), (0,0,0,1,0,1) \rangle$. For any $A \subset \mathcal{P}$, we consider the subspace $F_A = \sum_{p_i \in A} F_i$. One can check that $\dim F_i = 2$ for every $i = 0, 1, \ldots, 9$ and that $F_0 \subset F_A$ if $A \in \Gamma$ while $F_0 \cap F_A = \{0\}$ whenever $A \notin \Gamma$. Then, an ideal secret sharing scheme with access structure Γ is obtained in the following way: for any secret value $k = (k_1, k_2) \in \mathcal{K} = \mathbb{Z}_5^2$, the dealer randomly chooses two vectors $u_1, u_2 \in \mathbb{Z}_5^6$ such that $v_0 \cdot u_1 = k_1$ and $w_0 \cdot u_2 = k_2$, and gives the share $s_i = (v_i \cdot u_1, w_i \cdot u_2) \in \mathbb{Z}_5^2$ to the participant p_i. The ideal scheme constructed in this way is an ideal linear secret sharing scheme. $\square$

The above proposition leads us to consider the family of the *sparse 3-homogenous access structures*. Let Γ be an access structure on a set of participants $\mathcal{P}$. For a subset of participants $\mathcal{Q} \subset \mathcal{P}$ we define $\omega(\mathcal{Q}, \Gamma)$ as the number of minimal qualified subsets $A \in \Gamma_0$ such that $A \subset \mathcal{Q}$. We consider also $\omega(s, \Gamma) = \max\{\omega(\mathcal{Q}, \Gamma) : |\mathcal{Q}| = s\}$. Therefore, if Γ is a 3-homogeneous access structure then $1 \leq \omega(4, \Gamma) \leq 4$. We say that a 3-homogeneous access structure Γ is *sparse* whenever $\omega(4, \Gamma) \leq 2$, that is, if each set of four participants contains at most two minimal qualified subsets. Observe that the access structure Γ in Proposition 4.2 is not sparse because it satisfies $\omega(\mathcal{Q}, \Gamma) \geq 3$ for every $\mathcal{Q} \subset \mathcal{P}$ with $|\mathcal{Q}| = 4$.

Example 4.3 A wide family of sparse 3-homogeneous access structures are those with intersection number equal to one. That is, those with at most one participant in the intersection of any two different minimal qualified subsets. For instance, the access structure $\Gamma\langle S(p) \rangle$ defined by a 3-homogeneous star, the access structure Γ_2 associated to the Fano plane and its related access structure $\Gamma_{2,1}$. Nevertheless, there are sparse 3-homogeneous access structures with intersection number not equal to one. For example, the access structure Γ on the set of six participants $\mathcal{P} = \{p_1, \ldots, p_6\}$ whose minimal qualified subsets are $\{p_1, p_2, p_3\}$, $\{p_3, p_4, p_5\}$, $\{p_1, p_5, p_6\}$ and $\{p_4, p_5, p_6\}$.

Example 4.4 It is not difficult to check that, a 3-homogeneous access structure Γ is sparse if and only if its reduced access structure $\Gamma_\sim$ is so. Therefore, new sparse access structures can be obtained from old by adding equivalent participants. Namely, let Γ be a sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$ with basis Γ_0. Let $p \in \mathcal{P}$ and let $p' \notin \mathcal{P}$ be a new participant. Then, the 3-homogeneous access structure Γ' on $\mathcal{P}' = \mathcal{P} \cup \{p'\}$ having basis $\Gamma_0' = \Gamma_0 \cup \{(A \setminus \{p\}) \cup \{p'\} : p \in A \in \Gamma_0\}$ is sparse. For instance, the access structure Γ on $\mathcal{P} = \{p_1, \ldots, p_6\}$ with minimal qualified subsets $\{p_1, p_2, p_3\}$, $\{p_3, p_4, p_5\}$ and $\{p_1, p_5, p_6\}$ is sparse. Hence, so is the access structure Γ' on $\mathcal{P}' = \mathcal{P} \cup \{p_7\}$ having minimal qualified subsets $\{p_1, p_2, p_3\}$, $\{p_3, p_4, p_5\}$, $\{p_1, p_5, p_6\}$, $\{p_7, p_2, p_3\}$ and $\{p_7, p_5, p_6\}$.

One of the main results in this paper is to prove that Theorem 4.1 can be generalized to the family of the sparse 3-homogeneous access structures. Specifically, in the next section we demonstrate that the ideal access structures in this family coincides with the vector space ones and, besides, there is no access structure in this family with optimal information rate between $2/3$ and 1. Furthermore, we present a complete description of the ideal sparse 3-homogeneous access structures in terms of their simple components.

Besides, the importance of the sparse access structures is also pointed up with Theorem 4.5. This theorem states that any $\mathbb{Z}_2$-vector space 3-homogeneous access structure must be sparse. The existence of vector space 3-homogeneous access structures that are not vector space over $\mathbb{Z}_2$ is showed in Proposition 4.6.

Theorem 4.5 *Let Γ be a 3-homogeneous access structure on a set of participants $\mathcal{P}$. Assume that Γ is a $\mathbb{Z}_2$-vector space access structure. Then, Γ is sparse.*

Proof. Let us suppose that Γ is not sparse. So there exist four different participants $p_1, p_2, p_3, p_4 \in \mathcal{P}$ such that $\omega(\{p_1, p_2, p_3, p_4\}, \Gamma) \geq 3$. Without loss of generality we may assume that the subsets $\{p_1, p_2, p_3\}$, $\{p_1, p_2, p_4\}$ and $\{p_1, p_3, p_4\}$ are minimal qualified subsets. Since Γ is 3-homogeneous, hence $\{p_1, p_2\} \notin \Gamma = (\Gamma^*)^*$ and so, from Lemma 2.1, it follows that there exists $B \in \Gamma_0^*$ such that $p_1, p_2 \notin B$. Besides, since $\{p_1, p_2, p_3\}$ and $\{p_1, p_2, p_4\}$ are minimal qualified subsets then, applying again Lemma 2.1, we conclude that $p_3, p_4 \in B$. Therefore $\{p_1, p_3, p_4\} \cap B = \{p_3, p_4\}$ has even cardinal number. Thus, from Theorem 2.2, it follows that Γ is not a $\mathbb{Z}_2$-vector space access structure, a contradiction. $\square$

Proposition 4.6 *Let Γ be a 3-homogeneous access structure on a set of participants $\mathcal{P}$ such that every simple component of Γ is a $(3, n)$-threshold access structure. Then, Γ is a vector space access structure but it is not a $\mathbb{Z}_2$-vector space access structure.*

Proof. Let $\mathbb{K}$ be a finite field with $|\mathbb{K}| > |\mathcal{P}|$. Let Γ' be a simple component of Γ. By assumption Γ' is a $(3, n')$-threshold access structure. So it is a vector space access structure over any finite field $\mathbb{K}'$ with $|\mathbb{K}'| > n'$ [21]. In particular, Γ' is a $\mathbb{K}$-vector space access structure. Thus, applying Lemma 3.1, Γ is a $\mathbb{K}$-vector space access structure. Besides, since Γ is not sparse hence, from Theorem 4.5, it is not a $\mathbb{Z}_2$-vector space access structure. $\square$

5 Sparse homogeneous access structures with rank three

This section is devoted to prove Theorem 5.1. This theorem states that, even though the results in Theorem 4.1 for the family of the 2-homogeneous access structures can not be directly generalized to 3-homogeneous access structures, they can be extended to the family of the sparse 3-homogeneous access structures.

Theorem 5.1 *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 $\mathbb{Z}_2$-vector space access structure.*

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

3. *Γ is an ideal access structure.*

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

5. *Every simple component of Γ is either an access structure $\Gamma\langle S(p) \rangle$ defined by a 3-homogeneous star, or the access structure associated to the Fano plane Γ_2, or its related access structure $\Gamma_{2,1}$.*

The results in the previous sections, together with the independent sequence method, are the key points in the proof of Theorem 5.1. The *independent sequence method* was introduced by Blundo, De Santis, De Simone and Vaccaro [2, Theorem 3.8] and was generalized by Padró and Sáez [16, Theorem 2.1]. This method works as follows. Let Γ be an access structure on a set of participants $\mathcal{P}$. We say that a sequence $\emptyset \neq B_1 \subset \cdots \subset B_m \notin \Gamma$ of subsets of $\mathcal{P}$ is *made independent* by a subset $A \subset \mathcal{P}$ if there exist subsets $X_1, \ldots, X_m \subset A$ 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. If there exists such a sequence, then $\rho^*(\Gamma) \leq |A|/(m+1)$ if $A \in \Gamma$, while $\rho^*(\Gamma) \leq |A|/m$ whenever $A \notin \Gamma$.

First we are going to prove that Conditions 1–4 in Theorem 5.1 are equivalent. A vector space access structure is ideal and, hence, its optimal information rate is equal to one. Thus, we only have to demonstrate that (4) implies (1). This implication is given in Proposition 5.3. We need a previous lemma that works for more general access structures.

Lemma 5.2 *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 $\mathrm{corank}(\Gamma) \geq 3$, $B_2 \cup \{p_2\} = \{p_1, p_3, p_2\} \in \Gamma$, 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. $\square$

Proposition 5.3 *Let Γ be a sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$ with optimal information rate $\rho^*(\Gamma) > 2/3$. Then, Γ is a $\mathbb{Z}_2$-vector space access structure.*

Proof. Let us assume that $\rho^*(\Gamma) > 2/3$ and that Γ is not a $\mathbb{Z}_2$-vector space access structure. Then, from Theorem 2.2, 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 $B_3 \notin (\Gamma^*)^* = \Gamma$. We claim that the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ is made independent by the set $A = \{p_1, p_2\} \notin \Gamma$ 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 $\rho^*(\Gamma) \leq 2/3$, 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 Γ 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

11

Γ is a 3-homogeneous access structure. Therefore, in order to prove our claim we only must to check that $B_2 \cup X_3 \notin \Gamma$. Since $B_2 \cup X_3 = \{p_2, p_3, q_{1,1}, q_{1,2}\}$ and Γ 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 $\{p_3, q_{1,1}, q_{1,2}\} \notin \Gamma$. 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, $\{p_3, q_{1,1}, q_{1,2}\} \notin (\Gamma^*)^* = \Gamma$.

Now we are going to prove that $\{p_2, p_3, q_{1,1}\}, \{p_2, p_3, q_{1,2}\} \notin \Gamma$. By symmetry we only need to show that $\{p_2, p_3, q_{1,1}\} \notin \Gamma$. If $\{p_2, p_3, q_{1,1}\} \in \Gamma$, then $p_1, p_2, p_3, q_{1,1} \in \mathcal{P}$ are four different participants. On one hand we have that $\{p_1, p_2, p_3\} \in \Gamma$. Hence $\omega(\{p_1, p_2, p_3, q_{1,1}\}, \Gamma) \geq 2$, and then $\omega(\{p_1, p_2, p_3, q_{1,1}\}, \Gamma) = 2$ because Γ is sparse. On the other hand we have that $\{p_1, q_{1,1}, q_{1,2}\} \in \Gamma$. Therefore, a contradiction follows by applying Lemma 5.2.

To finish we must demonstrate that $\{p_2, q_{1,1}, q_{1,2}\} \notin \Gamma$. Otherwise, $p_1, p_2, q_{1,1}, q_{1,2} \in \mathcal{P}$ are four different participants and $\omega(\{p_1, p_2, q_{1,1}, q_{1,2}\}, \Gamma) \geq 2$. So $\omega(\{p_1, p_2, q_{1,1}, q_{1,2}\}, \Gamma) = 2$. Since $\{p_1, p_2, p_3\} \in \Gamma$, hence from Lemma 5.2 we get a contradiction. This completes the proof of our claim and so the proof of the proposition. $\square$

From the proposition above, we get that Conditions 1–4 in Theorem 5.1 are equivalent. Then, we only have to show the equivalence of those conditions with Condition 5 to conclude the proof of Theorem 5.1. By applying Corollary 2.4 and Lemma 3.1 we get that (5) implies (1). The proof will be finished by showing that (3) implies (5). This is done in the following proposition.

Proposition 5.4 *Let Γ be an ideal sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$. Then, every simple component of Γ is either an access structure $\Gamma\langle S(p)\rangle$ defined by a 3-homogeneous star, or the access structure associated to the Fano plane Γ_2, or its related access structure $\Gamma_{2,1}$.*

Proof. The simple components of Γ are induced substructures of Γ. Then the simple components of a sparse 3-homogeneous access structures are also sparse 3-homogeneous access structures. Besides, from Lemma 3.1 the simple components of Γ are ideal. Therefore, we only have to prove that: if Γ is an ideal, reduced and connected sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$, then Γ is either an access structure $\Gamma\langle S(p)\rangle$ defined by a 3-homogeneous star, or the access structure associated to the Fano plane Γ_2, or its related access structure $\Gamma_{2,1}$. From the results in [14] it follows that $\Gamma\langle S(p)\rangle$, Γ_2 and $\Gamma_{2,1}$ 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 Γ is an ideal, reduced and connected sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$, then Γ has intersection number equal to one.

It is clear that a 3-homogeneous access structures Γ has intersection number equal to one if and only if $\omega(\{a, b, c, d\}, \Gamma) \leq 1$ 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 $\omega(\{a, b, c, d\}, \Gamma) \geq 2$. Since Γ is sparse, hence we can assume that $\{a, c, d\}, \{b, c, d\} \in \Gamma$ and that $\{a, b, c\}, \{a, b, d\} \notin \Gamma$. We are going to prove that, in this situation, a and b are equivalent participants and, hence, Γ is not a reduced access structure, a contradiction.

From Lemma 5.2, the set $\{a, b, p\}$ is not qualified for any $p \in \mathcal{P}$. Then, $\{a, b\} \not\subset A$ if $A \in \Gamma_0$. Let us prove now that, if $A \subset \mathcal{P} \setminus \{a, b\}$, then $A \cup \{a\} \in \Gamma_0$ if and only if $A \cup \{b\} \in \Gamma_0$. 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 $\{a, c, x\} \in \Gamma_0$, then $\{b, c, x\} \in \Gamma_0$, 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 $\{b, c, x\} \notin \Gamma$, then the sequence $\emptyset \neq B_1 \subset B_2 \subset B_3 \notin \Gamma$ is made independent by $\{a, d\}$ and, hence $\rho^*(\Gamma) \leq 2/3$, a contradiction. Therefore, $\{b, c, x\} \in \Gamma_0$.

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 $\{b, x, y\} \in \Gamma_0$ if $\{a, x, y\} \in \Gamma_0$. So, let us assume that $\{a, x, y\} \in \Gamma_0$. Notice that, in such a case we have that $\{b, c, x, y\} \in \Gamma$, 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 $\{b, x, y\} \notin \Gamma$. Hence, at least one of the subsets $\{b, c, x\}$, $\{b, c, y\}$, $\{c, x, y\}$ is qualified. If $\{c, x, y\} \in \Gamma$, we can apply Lemma 5.2 to the minimal qualified subsets $\{c, x, y\}$ and $\{a, x, y\}$ and, since $\{a, c, d\} \in \Gamma$, we obtain that $\omega(\{a, c, x, y\}, \Gamma) > 2$, a contradiction. Then, without loss of generality, we can suppose that $\{b, c, x\} \in \Gamma_0$, and so, from Case 1, we get that $\{a, c, x\} \in \Gamma_0$. Since $\{b, x, y\} \notin \Gamma = (\Gamma^*)^*$ then, from Lemma 2.1, there exists $A^* \in \Gamma_0^*$ 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. Therefore, from Theorem 2.2 it follows that Γ is not a $\mathbb{Z}_2$-vector space access structure. This leads us to a contradiction with Proposition 5.3 because, by assumption, Γ is an ideal sparse 3-homogeneous access structure. This completes the proof of the proposition. □

6   Examples

To finish, in this section we point out some examples in order to illustrate our results. Specifically, we analyze several examples of 3-homogeneous access structures in order to decide whether they are ideal or not by applying some of the results in this paper. While in the first ones the access structures are sparse, in the last examples the access structures we consider satisfy $\omega(4, \Gamma) \geq 3$.

Let us start with the sparse case. In order to check whenever a sparse 3-homogeneous access structure is ideal or not we will use either the characterization of $\mathbb{Z}_2$-vector space access structures given in Theorem 2.2 or we compute its simple components.

Example 6.1 Let Γ be the access structure on a set $\mathcal{P} = \{p_1, \ldots, p_6\}$ of six participants 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 $\omega(4, \Gamma) = 2$, and hence Γ is a sparse 3-homogeneous access structure. From Lemma 2.1 it follows that $\{p_1, p_5\} \in \Gamma_0^*$. Since $|\{p_1, p_5\} \cap \{p_1, p_5, p_6\}| = 2$ hence, from Theorem 2.2, Γ is not a $\mathbb{Z}_2$-vector space access structure. Now, by applying Theorem 5.1 we conclude that Γ is not ideal and has optimal information rate $\rho^*(\Gamma) \leq 2/3$. We could also prove that $\rho^*(\Gamma) \leq 2/3$ by checking that Γ is a connected and reduced access structure and it is neither a star nor Γ_2 nor $\Gamma_{2,1}$.

Example 6.2 Now we consider the 3-homogeneous access structure Γ on $\mathcal{P} = \{p_1, \ldots, p_6\}$ 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 $\omega(4, \Gamma) = 2$ and so Γ is sparse. It is not hard to check that $\Gamma_0^* = \{\{p_1, p_6\}, \{p_2, p_4\}, \{p_2, p_5\}, \{p_3, p_4\}, \{p_3, p_5\}\}$. So $|A \cap A^*| = 1$ if $A \in \Gamma_0$ and $A^* \in \Gamma_0^*$. Hence, from Theorem 2.2, it follows that Γ is a vector space access structure.

Notice that Γ is connected and, besides, the participants p_1 and p_6 are equivalent. Thus, the simple component of Γ is $\Gamma_\sim = \Gamma(\{p_1, \ldots, p_5\})$ a 3-homogeneous star access structure and so, by applying Theorem 5.1, it follows that Γ is a vector space access structure.

Example 6.3 On the set $\mathcal{P} = \{p_1, \ldots, p_7, q_1, \ldots, q_7\}$ of fourteen participants let us consider the 3-homogeneous access structure Γ whose minimal qualified subsets are $\{p_1, p_2, p_3\}$, $\{p_3, p_4, p_5\}$, $\{p_1, p_5, p_6\}$, $\{p_2, p_4, p_6\}$, $\{p_1, p_5, p_7\}$, $\{p_2, p_4, p_7\}$, $\{q_1, q_2, q_3\}$, $\{q_1, q_4, q_5\}$, $\{q_1, q_6, q_7\}$, $\{q_2, q_4, q_6\}$ and $\{q_3, q_5, q_7\}$. Notice that Γ is sparse. In this case Γ has two connected components $\Gamma_1 = \Gamma(\{p_1, \ldots, p_7\})$ and $\Gamma_2 = \Gamma(\{q_1, \ldots, q_7\})$ and there exist only one pair of equivalent participants $p_7 \sim p_6$. Hence, the simple components of Γ are $\Gamma_{1,\sim} = \Gamma(\{p_1, \ldots, p_6\})$ and $\Gamma_{2,\sim} = \Gamma(\{q_1, \ldots, q_7\})$. On one hand $\Gamma(\{p_1, \ldots, p_6\}) = \Gamma_{2,1}$. On the other hand, $\Gamma(\{q_1, \ldots, q_7\})$ is neither a 3-homogeneous star, nor Γ_2 nor $\Gamma_{2,1}$. Thus, from Theorem 5.1, we conclude that $\rho^*(\Gamma) \leq 2/3$.

Next, in the following examples, we are going to consider 3-homogeneous access structures that are not sparse. Even though the characterization of the ideal and non-sparse 3-homogeneous access structures is still an open problem, by means of the following examples we show that sometimes our results work whenever $\omega(4, \Gamma) \geq 3$.

Example 6.4 Let Γ be the access structure on $\mathcal{P} = \{p_1, \ldots, p_6\}$ having minimal qualified subsets $\{p_1, p_2, p_3\}$, $\{p_1, p_2, p_4\}$, $\{p_3, p_4, p_5\}$, $\{p_3, p_4, p_6\}$ and $\{p_4, p_5, p_6\}$. Notice that $\omega(4, \Gamma) = 3$. Nevertheless we can apply Lemma 5.2 in order to conclude that $\rho^*(\Gamma) \leq 2/3$. Namely, we have that $\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\} \in \Gamma$, that $\{p_1, p_3, p_4\}, \{p_2, p_3, p_4\} \notin \Gamma$, and that $\{p_3, p_4, p_5\} \in \Gamma$. Therefore, from Lemma 5.2 it follows that $\rho^*(\Gamma) \leq 2/3$.

Example 6.5 On the set of participants $\mathcal{P} = \{p_1, \ldots, p_5\}$ we consider the 3-homogeneous access structure with minimal qualified subsets $\{p_1, p_2, p_3\}$, $\{p_1, p_2, p_4\}$, $\{p_1, p_3, p_4\}$, $\{p_2, p_3, p_4\}$, $\{p_1, p_2, p_5\}$, $\{p_1, p_3, p_5\}$ and $\{p_2, p_3, p_5\}$. Now we have that $\omega(4, \Gamma) = 4$. Nevertheless in this case we have that Γ is connected and the participants p_4 and p_5 are equivalent. So Γ has only one simple component $\Gamma_\sim = \Gamma(\{p_1, p_2, p_3, p_4\})$, and it is the $(3, 4)$-threshold access structure. Hence, from Proposition 4.6, it follows that Γ is a vector space access structure.

Example 6.6 Finally, let Γ be the access structure on $\mathcal{P} = \{p_1, \ldots, p_6\}$ 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 $\omega(C_i, \Gamma) = i$. In particular, Γ is not sparse. However we are going to prove that Γ is not ideal by applying our results to a suitable substructure. Namely, let $\Gamma(\mathcal{P}_4)$ be the access structure induced by Γ on $\mathcal{P}_4 = \mathcal{P} \setminus \{p_4\}$. So, $(\Gamma(\mathcal{P}_4))_0 = \{A_1, A_5, A_6\}$. Hence, $\Gamma(\mathcal{P}_4)$ is a sparse 3-homogeneous access structure on $\mathcal{P}_4$. From Lemma 2.1 we get that $\{p_2, p_3\} \in (\Gamma(\mathcal{P}_4))_0^*$ and thus we conclude that $\rho^*(\Gamma(\mathcal{P}_4)) \leq 2/3$ by applying Theorem 2.2 and Theorem 5.1. On the other hand, it is clear that any secret sharing scheme for Γ induce a secret sharing scheme for $\Gamma(\mathcal{P}_4)$ with the same set of secrets. Hence $\rho^*(\Gamma) \leq \rho^*(\Gamma(\mathcal{P}_4))$. Therefore, $\rho^*(\Gamma) \leq 2/3$.

7 Conclusion and open problems

The characterization of ideal access structures and the search for bounds on the optimal information rate are two important problems in secret sharing. The results we present in

this paper are a first approach to the characterization of the ideal 3-homogeneous access structures.

One of the main results in this paper is a complete characterization of the ideal access structures in the family of the sparse 3-homogeneous access structures. Namely, we prove that the vector space access structures in this family coincide with the ideal ones and with those having optimal information rate greater than 2/3. Besides, we present a complete description of the ideal access structures in this family by means of their simple components.

Similar results had been previously obtained for other families of access structures: access structures on sets of four and five participants, access structures defined by graphs, bipartite access structures, access structures with three or four minimal qualified subsets and access structures with intersection number equal to one.

Nevertheless, we prove that this result can not be directly generalized to the family of the 3-homogeneous access structures. Specifically, we demonstrate that the equivalence between ideal and vector space access structures does not hold for general 3-homogeneous access structures. To do it we present a 3-homogeneous access structures that is not vector space even though it can be realized by an ideal linear secret sharing scheme.

Actually, the characterization of the ideal 3-homogeneous access structures is far from being solved. As a further step, an interesting open problem is to find out to which this result can be generalized to other families of access structures. For instance, other families of 3-homogeneous access defined in terms of the value of $\omega(4, \Gamma)$, (recall that $1 \leq \omega(4, \Gamma) \leq 4$, and that the sparse access structures are exactly those with $\omega(4, \Gamma) \leq 2$).

Besides, the characterization of ideal access structures provides some interesting open problems: is there any ideal access structure that is not realized by any ideal linear secret sharing scheme? and, is there any access structure Γ such that $2/3 < \rho^*(\Gamma) < 1$?.

References

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

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

[3] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. On the information rate of secret sharing schemes. *Advances in Cryptology CRYPTO'92. Lecture Notes in Computer Science* 740, 148–167.

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

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

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

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

[8] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro. On the size of shares of secret sharing schemes. *J. Cryptology* 6 (1993), 157–168.

[9] M. van Dijk. Secret Key Sharing and Secret Key Generation. *Ph.D. Thesis*, 1997, TU Eindhoven.

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

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

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

[14] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. *Proceedings of the Third International Conference on Security in Communication Networks SCN'02, Lecture Notes in Computer Science* 2576 (2003) 354–363.

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

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

[17] 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.

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

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

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

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

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