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
jaumem@mat.upc.es, matcpl@mat.upc.es

Submitted: May 17, 2004; Accepted: Sep 22, 2004; Published: Oct 7, 2004
Mathematics Subject Classifications: 94A62, 94A60

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.

An access structure is said to be r-homogeneous if there are exactly r participants in every minimal qualified subset. A first approach to the characterization of the ideal 3-homogeneous access structures is made in this paper. We show that the results in the previously studied families can not be directly generalized to this one. Nevertheless, we prove that the equivalences above apply to the family of the sparse 3-homogeneous access structures, that is, those in which any subset of four participants contains at most two minimal qualified subsets. Besides, we give a complete description of the ideal 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 a secret value $k \in \mathcal{K}$ among a set of participants $\mathcal{P}$. Every participant $p \in \mathcal{P}$ receives a *share* $s_p \in \mathcal{S}_p$ in such a way that

*This work was partially supported by the Spanish *Ministerio de Ciencia y Tecnología* under projects TIC 2000-1044 and TIC 2003-00866. The material in this paper was presented in part at the *International Workshop on Coding and Cryptography WCC 2003*, Versailles, France. An earlier version of this paper appeared in the proceedings of this conference.

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 [22]. 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 increasing*, 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.

Due to efficiency reasons and the fact that the security of a system depends on the amount of information that must be kept secret, the size of the shares given to the participants is a key point in the design of secret sharing schemes. The *information rate* ρ of a secret sharing scheme is defined as the ratio between the length (in bits) of the secret and the maximum length of the shares given to the participants. Namely,

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

In any perfect secret sharing scheme, the size of the share of any participant is at least the size of the secret [22]. Hence, the information rate satisfies $0 < \rho \leq 1$. A secret sharing scheme is said to be *ideal* if its information rate is equal to one, that is, if all shares have the same size as the secret. The access structures that admit an ideal secret sharing scheme are called *ideal*. For instance, the threshold schemes proposed in the first works on secret sharing [1, 19] are ideal. Therefore, the (t,n)-*threshold access structure*, which consists of all subsets with at least t participants of a set of n participants, is ideal. Ito, Saito and Nishizeki [10] proved, in a constructive way, that there exists a secret sharing scheme for every access structure. The schemes constructed by the method in [10] are in general very inefficient, because the size of the shares is much larger than the size of the secret, that is, their information is, in most cases, very small.

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.

Matroids play an important role in the characterization of the ideal access structures.

Brickell and Davenport [6] gave a necessary condition in terms of matroids. 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 given by Brickell [5], who introduced the *vector space secret sharing schemes*, which are ideal schemes for a wide family of access structures, the *vector space access structures*. These structures are precisely the ones that are related to representable matroids and the ideal schemes are equivalent to the ones that are obtained from linear codes [15] and equivalent also to the ones obtained from monotone span programs [12]. As a consequence of the results by Simonis and Ashikhmin [21], this sufficient condition is not necessary. Namely, they proved that the access structures related to the non-Pappus matroid, which is not representable, are ideal but are not vector space.

Several techniques have been introduced in [4, 7, 17, 23] 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 improved 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 [22] and five [11] participants, access structures defined by graphs [2, 3, 4, 6, 7, 8, 23], 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 $2/3 < \rho^*(\Gamma) < 1$. Moreover, the ideal access structures in all these families have been completely characterized and described. 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 minimal qualified subsets have exactly r different participants. Notice that the access structures defined by graphs, one of the above-mentioned families, are precisely the 2-homogeneous ones.

Our first result, Proposition 3.1, is an example proving that the ideal 3-homogeneous access structures do not coincide with the vector space ones. Therefore, the results in the previously studied families do not apply to the family of the 3-homogeneous access structures. This example and the result in Proposition 3.2, lead us to study the *sparse* 3-homogeneous access structures, that is, the structures such that each set of four participants contains at most two minimal qualified subsets.

Our main results are gathered in Theorems 4.1 and 4.2. We prove in Theorem 4.1 that the vector space 3-homogeneous access structures over $\mathbb{Z}_2$ are sparse, while Theorem 4.2 provides a complete characterization and description of the ideal sparse 3-homogeneous access structures. We obtain for the sparse 3-homogeneous access structures similar results as in the previously studied families. Namely, we prove that the ideal sparse 3-homogenous access structures coincide with the vector space ones and that there is no access structure in this family with optimal information rate between 2/3 and 1. Besides, our results contain a characterization of the 3-homogeneous structures that are $\mathbb{Z}_2$-vector space access structures.

The paper is organized as follows. We recall in Section 2 some definitions and known results on vector space secret sharing schemes. Among them, we present a combinatorial property, related to the dual access structure, that characterizes the vector space access structures over the finite field $\mathbb{Z}_2$. Besides, we define in this section the simple components of an access structure and present some basic facts about this concept. Our main results are given in the following two sections. An ideal 3-homogeneous access structure that is not vector space is presented in Section 3, while Section 4 deals with the characterization and description of the ideal sparse 3-homogeneous access structures.

2 Preliminaries

Some definitions and the notation together with several general results that will be used in the following are given in this section. First we recall some basic facts on vector space secret sharing schemes and besides we present a characterization of the $\mathbb{Z}_2$-vector space access structures. Next, we recall some reduction methods that simplify the analysis of an access structure by decomposing it into simple components. Finally, we rewrite the well-known characterization of the ideal 2-homogeneous access structures in terms of those simple components. The goal of our paper is to find out to which extent this result can be generalized to the 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 [22] 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 $p \in A$. The schemes that can be defined in this way are called $\mathbb{K}$-*vector space secret sharing schemes*. They are a particular case of *linear* schemes, because the shares are obtained by linear maps applied to the secret and some random values and, hence, the secret is recovered also by linear maps applied to the shares of the qualified subsets. Vector space secret sharing schemes were introduced in [5], and general linear secret sharing schemes were first described in [20].

A characterization of the $\mathbb{Z}_2$-vector space access structures is presented in Theorem 2.2. This result was given in [9]. Nevertheless, since its proof is not long, we give it here for completeness' sake. It involves the *dual access structure* of an access structure Γ, which is the access structure Γ^* on the same set of participants $\mathcal{P}$ defined by $\Gamma^* = \{B \subset \mathcal{P} : \mathcal{P} \setminus B \notin \Gamma\}$. The following lemma on the dual access structure will be used in several places in the paper. Let us recall that Γ_0 denotes the basis of Γ, that is, the family of minimal qualified subsets.

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 converse. 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. The proof is concluded by checking that ψ is a realization of Γ as a $\mathbb{Z}_2$-vector space access structure. $\square$

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 $p_1, \ldots, p_m \in \mathcal{P}$ defining the set $\mathcal{P}/\sim$ of the equivalence classes given by the relation $\sim$, that is $\mathcal{P}/\!\sim =$

$\{[p_1], \dots, [p_m]\}$. 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 $\Gamma(\{p_1, \dots, p_m\})$. 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 $\Gamma(\mathcal{P}_1), \dots, \Gamma(\mathcal{P}_r)$. The reduced access structures $\Gamma(\mathcal{P}_1)_\sim, \dots, \Gamma(\mathcal{P}_r)_\sim$ are called the *simple components* of Γ. The proof of the following lemma is not difficult.

Lemma 2.3 *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.*

We conclude this section by stating the known results on the characterization of the ideal access structures that are defined by graphs in terms of their simple components.

An access structure Γ is said to be *r-homogeneous* if its rank and its min-rank are equal to r, where the *rank* and the *min-rank* 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, 22], can be rewritten as follows. The purpose of this paper is to examine to which extent this result can be generalized to the family of the 3-homogeneous access structures.

Theorem 2.4 *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.*

3 Two results on 3-homogeneous access structures

In this section we present two results related to the characterization of the ideal 3-homogeneous access structures. Namely, in Proposition 3.1, we prove that the equivalence between ideal and vector space access structures does not hold for the family of 3-homogeneous access structures. Meanwhile, in Proposition 3.2, we give a necessary condition for a 3-homogeneous access structure to have optimal information rate greater than 2/3 and, hence, to be ideal. From our propositions we get that the result in Theorem 2.4 for the family of 2-homogeneous access structures can not be directly generalized to the family of 3-homogeneous access structures. This fact leads us, in the next section, to focus our attention on the family of the sparse 3-homogeneous access structures.

Let us show, first, that there exists an ideal 3-homogeneous access structure that is not vector space. Simonis and Ashikhmin [21] presented the first examples of ideal access structures that are not $\mathbb{K}$-vector space access structures for any finite field $\mathbb{K}$. Namely, the access structures related to the non-Pappus matroid, which have rank 3 and min-rank 2 and, hence, are not homogeneous. Our goal is to point out an ideal 3-homogeneous access structure that is not vector space. This access structure is presented in the next proposition and arises from the results in [21] by means of suitable changes.

Proposition 3.1 *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 $\mathcal{A} = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_7\}, \{p_1, p_6, p_8\}, \{p_2, p_4, p_7\}, \{p_2, p_6, p_9\}, \{p_3, p_4, p_8\}, \{p_3, p_5, p_9\}, \{p_4, p_5, p_6\}\}$, (the sets in $\mathcal{A}$ correspond to the lines in Figure 1). Then, Γ is not a vector space access structure but can be realized by an ideal secret sharing scheme.*

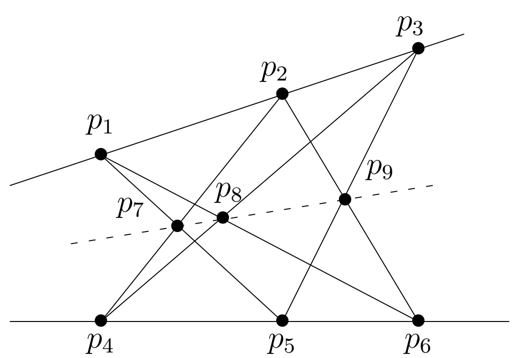

Figure 1: A representation of the access structure in Proposition 3.1.

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 $\dim\langle v_1, \ldots, v_9, v_D\rangle = 3$ as we wanted to prove. Notice that, if $\{p_i, p_j, p_k\} \notin \Gamma$ is a non-qualified subset with three participants, then $v_D \notin \langle v_i, v_j, v_k\rangle$, 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, $v_7 \in \langle v_1, v_5\rangle \cap \langle v_2, v_4\rangle$, $v_8 \in \langle v_1, v_6\rangle \cap \langle v_3, v_4\rangle$, $v_9 \in \langle v_3, v_5\rangle \cap \langle v_2, v_6\rangle$. If we consider these nine vectors as points in the projective plane, their relative position is depicted in Figure 1 and, hence, by applying the Theorem of Pappus, we conclude that $\dim\langle v_7, v_8, v_9\rangle = 2$. Therefore, $v_D \notin \langle v_7, v_8, v_9\rangle$ and so $\{p_7, p_8, p_9\}$ is not a minimal qualified subset, 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 $F_i = \langle v_i, w_i\rangle$, where

$$
\begin{aligned}
&v_0 = (1,1,1,1,0,4),\ w_0 = (3,0,2,0,1,0),\ v_1 = (1,0,0,0,0,0),\ w_1 = (0,1,0,0,0,0),\\
&v_2 = (1,0,0,0,1,0),\ w_2 = (0,1,0,0,0,1),\ v_3 = (0,0,0,0,1,0),\ w_3 = (0,0,0,0,0,1),\\
&v_4 = (1,0,1,0,0,4),\ w_4 = (0,1,0,4,1,1),\ v_5 = (0,0,1,0,0,0),\ w_5 = (0,0,0,1,0,0),\\
&v_6 = (1,0,4,4,0,4),\ w_6 = (0,1,1,0,1,1),\ v_7 = (1,0,0,1,0,0),\ w_7 = (0,1,1,4,0,0),\\
&v_8 = (1,0,1,0,1,1),\ w_8 = (0,1,0,4,1,0),\ v_9 = (0,0,1,0,1,0),\ w_9 = (0,0,0,1,0,1).
\end{aligned}
$$

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. $\square$

Observe that the ideal scheme we have presented for the access structure Γ in Proposition 3.1 is not a vector space secret sharing scheme but it is a linear secret sharing scheme, because the shares are computed by means of linear maps.

A necessary condition for a 3-homogeneous access structure to have optimal information rate greater than $2/3$ and, hence, to be ideal is presented in the next proposition. This necessary condition will be used in several places in the following section. The *independent sequence method* is a key point in its proof. This method works as follows, (see [2, Theorem 3.8] and [16, Theorem 2.1]). 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 $A \notin \Gamma$.

Proposition 3.2 *Let Γ be a 3-homogeneous access structure on a set of participants $\mathcal{P}$ with 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 Γ is 3-homogeneous, $B_2 \cup \{p_2\} = \{p_1, p_2, p_3\} \in \Gamma$, 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 Γ is 3-homogeneous, $B_2 \cup \{p_1\} = \{p_1, p_3, p_4\} \notin \Gamma$, 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 proposition. $\square$

4 Sparse 3-homogeneous access structures

From the results in the previous section it follows that the equivalences in Theorem 2.4 for the family of the 2-homogeneous access structures can not be directly generalized to the family of the 3-homogeneous access structures. We wonder if this equivalence applies if we consider some subfamily of 3-homogeneous structures. One of the main results of this section is to give a positive answer to this question by considering the family of the *sparse* 3*-homogeneous access structures*, that is 3-homogeneous access structures such that each set of four participants contains at most two minimal qualified subsets. Namely in Theorem 4.2 we demonstrate that the ideal access structures in this family coincides with the vector space ones and, besides, we prove that there is no access structure in this family with optimal information rate between 2/3 and 1. Moreover, we present a complete description of the ideal sparse 3-homogeneous access structures in terms of their simple components. In addition, our results provide also a complete characterization of the 3-homogeneous $\mathbb{Z}_2$-vector space access structures.

Before doing it, let us show how the sparse 3-homogeneous access structures arise from the results in the previous section in a natural way.

Let Γ be a 3-homogeneous access structure on a set of participants $\mathcal{P}$. The necessary condition in Proposition 3.2 on Γ to have optimal information rate greater than 2/3 involves the number of minimal qualified subsets contained in a subset $\{p_1, p_2, p_3, p_4\} \subset \mathcal{P}$ of four participants. This leads us to consider, for a subset of participants $\mathcal{Q} \subset \mathcal{P}$, the number $\omega(\mathcal{Q}, \Gamma)$ of minimal qualified subsets $A \in \Gamma_0$ such that $A \subset \mathcal{Q}$. Besides, we consider $\omega(4, \Gamma) = \max\{\omega(\mathcal{Q}, \Gamma) : |\mathcal{Q}| = 4\}$. On one hand, $1 \leq \omega(4, \Gamma) \leq 4$ if Γ is a 3-homogeneous access structure. On the other hand, the ideal and not vector space 3-homogeneous access structure in Proposition 3.1 is such that any subset of four participants contains at least three minimal qualified subsets. These facts leads us to focus our attention on the family of 3-homogeneous access structures satisfying $\omega(4,\Gamma) \leq 2$, that is on the family of 3-homogeneous access structures such that each set of four participants contains at most two minimal qualified subsets. These access structures are called *sparse*.

On top of this, the importance of the sparse 3-homogeneous access structures is also pointed to by Theorem 4.1. This theorem states that the vector space 3-homogeneous access structures over $\mathbb{Z}_2$ are exactly the ideal and sparse ones. A complete characterization and description of these access structures will be given in Theorem 4.2.

Theorem 4.1 *Let Γ be a 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 sparse and has optimal information rate $\rho^*(\Gamma) > 2/3$.*

Proof. First let us show that (1) implies (2). Let Γ be a $\mathbb{Z}_2$-vector space 3-homogeneous access structure. Since Γ is a vector space access structure, then it is ideal and so $\rho^*(\Gamma) = 1 > 2/3$. We must prove that Γ is sparse. Otherwise there exist four different participants $p_1, p_2, p_3, p_4 \in \mathcal{P}$ such 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. This completes the proof of this implication.

Conversely, assuming (2) we must demonstrate (1). Let us assume that Γ is a sparse 3-homogeneous access structure with optimal information rate $\rho^*(\Gamma) > 2/3$. If 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 Γ is a 3-homogeneous access structure. Therefore, in order to prove our claim we only must 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 it follows that $\{p_3, q_{1,1}, q_{1,2}\} \cap A^* = \emptyset$. 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 Proposition 3.2.

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 Proposition 3.2 we get a contradiction. This completes the proof of our claim and so the proof of the theorem. $\square$

The above theorem makes clear the relevance of the sparse access structures in the characterization of the ideal 3-homogeneous access structures: the $\mathbb{Z}_2$-vector space 3-homogeneous access structures are exactly the ideal and sparse ones.

Our next goal is to give a complete characterization and description of the ideal sparse 3-homogeneous access structures. We obtain for this the same equivalences as the ones established in Theorem 2.4 for the family of the 2-homogeneous access structures. That is, the vector space access structures in both families coincide with the ideal ones and with those having optimal information rate greater than 2/3.

It is easy to check that the simple components of a sparse 3-homogeneous access structure is also a sparse 3-homogeneous access structure. Therefore, new sparse 3-homogeneous access structures can be obtained from old by adding or cutting off equivalent participants. We describe now the reduced and connected sparse 3-homogeneous access structures that will be proved to be the only ideal access structures with these properties.

The 3-*homogeneous star* $\Gamma\langle S(p)\rangle$ 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 $(\Gamma\langle S(p)\rangle)_0 = \{A_1, \ldots, A_r\}$, where $A_i = \{p, a_i, b_i\}$ for $i = 1, \ldots, r$.

We notate Γ_2 for the access structure associated to the Fano plane, in which the participants and the minimal qualified subsets are, respectively, the points and the lines of the finite projective plane of order 2. Namely, Γ_2 is the access structure on the set $\mathcal{P} = \{p_1, \ldots, p_7\}$ with basis $(\Gamma_2)_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_7\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_7\}, \{p_3, p_4, p_5\}, \{p_3, p_6, p_7\}\}$.

Finally, $\Gamma_{2,1}$ will denote the access structure obtained from Γ_2 by removing one participant. That is, the set of participants of $\Gamma_{2,1}$ is $\mathcal{P} = \{p_1, \ldots, p_6\}$ and its basis is $(\Gamma_{2,1})_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_5, p_6\}, \{p_2, p_4, p_6\}, \{p_3, p_4, p_5\}\}$.

Theorem 4.2 *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. *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. Any vector space access structure is ideal and, hence, its optimal information rate is greater than $2/3$. Besides, from Theorem 4.1 we get that (3) implies (1). Hence, conditions (1), (2) and (3) are equivalent.

Now let us prove that (4) implies (1). It is not hard to show that the dual access structure of a 3-homogeneous star has basis $(\Gamma\langle S(p)\rangle^*)_0 = \{\{p\}\} \cup \{\{c_1, \ldots, c_r\} : c_i \in \{a_i, b_i\}\}$, 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 $A^* \in \Gamma_0^*$ and hence, by applying Theorem 2.2, we conclude that they are $\mathbb{Z}_2$-vector space access structures. The proof of this implication is completed by applying Lemma 2.3.

In order to finish the proof of the theorem it is enough to demonstrate that (2) implies (4). That is, assuming that Γ is an ideal sparse 3-homogeneous access structure on a set of participants $\mathcal{P}$, we must prove that every simple component of Γ is either a 3-homogeneous star, or Γ_2 or $\Gamma_{2,1}$.

On one hand, the simple components of Γ are also sparse 3-homogeneous access structures because they are induced substructures of Γ. On the other hand, from Lemma 2.3 it follows that the simple components of Γ are ideal. Therefore, we may assume that Γ is an ideal, reduced and connected sparse 3-homogeneous access structure. Besides, 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 structure 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 Proposition 3.2, 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 converse 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 Proposition 3.2 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 $\{b,c,x\} \in \Gamma_0$. Hence, 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. The proof of the theorem is completed by noticing that there is a contradiction with Theorem 4.1 because, by assumption, Γ is an ideal sparse 3-homogeneous access structure. $\square$

We conclude the section by showing three examples in order to illustrate our result.

Example 4.3 On the set $\mathcal{P} = \{p_1,\ldots,p_6\}$ of six participants we consider the access structure Γ with minimal qualified subsets $\{p_1,p_2,p_3\}$, $\{p_1,p_2,p_6\}$, $\{p_1,p_5,p_6\}$ and $\{p_3,p_4,p_5\}$. This access structure is sparse, reduced and connected. Besides, the structure Γ is neither a 3-homogeneous star, nor Γ_2 nor $\Gamma_{2,1}$. Thus, from Theorem 4.2, Γ is not ideal. Moreover, $\rho^*(\Gamma) \leq 2/3$.

Example 4.4 Next, let Γ be the access structure on $\mathcal{P} = \{p_1,\ldots,p_7\}$ whose minimal qualified subsets are $\{p_1,p_2,p_3\}$, $\{p_1,p_4,p_5\}$, $\{p_1,p_4,p_7\}$, $\{p_2,p_3,p_6\}$, $\{p_4,p_5,p_6\}$ and $\{p_4,p_6,p_7\}$. Now, Γ is sparse and connected. Besides, the participants p_1 and p_6 are equivalent as well as the participants p_5 and p_7. Thus, the simple component of Γ is $\Gamma_\sim = \Gamma(\{p_1,\ldots,p_5\})$ a 3-homogeneous star and so, by applying Theorem 4.2, Γ is a vector space access structure.

Example 4.5 Finally, on the set $\mathcal{P} = \{p_1,\ldots,p_7,q_1,\ldots,q_7\}$ of fourteen participants let Γ be the sparse access structure with minimal qualified subsets $\{p_1,p_2,p_3\}$, $\{p_3,p_4,p_5\}$, $\{p_1,p_5,p_6\}$, $\{p_2,p_4,p_6\}$, $\{p_1,p_5,p_7\}$, $\{p_2,p_4,p_7\}$, $\{q_1,q_2,q_3\}$, $\{q_1,q_5,q_6\}$, $\{q_1,q_6,q_7\}$, $\{q_3,q_4,q_5\}$ and $\{q_3,q_4,q_7\}$. 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 the equivalent participants are $p_7 \sim p_6$ and $q_7 \sim q_5$. Hence, the simple components of Γ are $\Gamma_{1,\sim} = \Gamma(\{p_1,\ldots,p_6\})$ and $\Gamma_{2,\sim} = \Gamma(\{q_1,\ldots,q_6\})$. Notice that $\Gamma_{1,\sim} = \Gamma_{2,1}$, while $\Gamma_{2,\sim}$ is neither a 3-homogeneous star, nor Γ_2 nor $\Gamma_{2,1}$. Thus, from Theorem 4.2 we conclude that Γ is a non-ideal access structure and $\rho^*(\Gamma) \leq 2/3$.

5 Conclusion and open problems

The characterization of ideal access structures and the search for bounds on the optimal information rate are two of the main open problems in secret sharing. The results we present in this paper are a first approach to the characterization of the ideal 3-homogeneous access structures.

The main result 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, in this family, the vector space access structures coincide with the ideal ones and also with those having optimal information rate greater than 2/3. Besides, a complete description of the ideal and sparse access structures is given. Moreover, our results provide also a characterization of the $\mathbb{Z}_2$-vector space 3-homogeneous access structures, because we demonstrate that those structures are sparse.

Nevertheless, a similar characterization of the ideal access structures can not be found for the family of the 3-homogeneous access structures. Specifically, we demonstrate that the equivalence between ideal and vector space access structures does not hold in that family.

Actually, the characterization of the ideal 3-homogeneous access structures is far from being solved. On one hand, to characterize the $\mathbb{K}$-vector space access structures in that family is still an open problem, which have been solved in this paper only in the case $\mathbb{K} = \mathbb{Z}_2$. On the other hand, the other open problem is to characterize the ideal 3-homogeneous access structures that are not vector space, whose existence have been proved in Section 3.

As a further step, one could try to find other families of 3-homogeneous access structures in which similar properties as in the sparse case are obtained when characterizing the ideal access structures. For instance, other families of 3-homogeneous access structures defined in terms of $\omega(4,\Gamma)$, (recall that $1 \leq \omega(4,\Gamma) \leq 4$ and that the sparse are those with $\omega(4,\Gamma) \leq 2$).

In general, matroids play a key role in the characterization of the ideal access structures. Brickell and Davenport [6] proved that, if Γ is an ideal access structure on a set of participants $\mathcal{P}$, there exists a matroid $\mathcal{M}$ on the set $\mathcal{P} \cup \{D\}$ such that $A \subset \mathcal{P}$ is a minimal qualified subset of Γ if and only if $A \cup \{D\}$ is a circuit of $\mathcal{M}$. Besides, for every participant $p \in \mathcal{P}$, the circuits of $\mathcal{M}$ containing p equally determine the minimal qualified subsets of an ideal access structure on the set of participants $(\mathcal{P} \cup \{D\}) \setminus \{p\}$. The matroids that are related in that way to ideal access structures are called *secret sharing matroids*.

Seymour [18] proved the existence of non-secret sharing matroids. Specifically, they proved that the access structures that are obtained from the Vamos matroid are not ideal. The vector space construction by Brickell [5] implies that all representable matroids are secret sharing matroids. Nevertheless, Simonis and Ashikhmin [21] proved that the non-Pappus matroid, which is not representable, is a secret sharing matroid.

Therefore, the main open problem in relation to the characterization of ideal access structures is to determine which non-representable matroids are secret sharing matroids. The non-Pappus matroid and the matroid related to the access structure in Proposition 3.1 are two examples. The ideal schemes realizing these access structures are linear (but not vector space). An interesting open problem appears here: is there any secret sharing matroid that is not realized by any ideal linear secret sharing scheme?

Finally, the gap between 2/3 and 1 appearing in the values of the optimal information rates of several families access structures suggests the following question: 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 (1993), 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] G.J. Simmons, W. Jackson and K. Martin. The geometry of secret sharing schemes. *Bulletin of the ICA* 1 (1991) 71–88.

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

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

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