New Results on Multipartite Access Structures

Javier Herranz[1] and Germán Sáez[2]

[1] Centrum voor Wiskunde en Informatica (CWI)
Kruislaan 413, P.O. Box 94079, NL-1090 GB Amsterdam, The Netherlands
Javier.Herranz@cwi.nl

[2] Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034-Barcelona, Spain
german@ma4.upc.edu

Abstract. In a multipartite access structure, the set of players is divided into K different entities, in such a way that all players of the same entity play the same role in the structure. Not many results are known about these structures, when $K \geq 3$.

Even if the total characterization of ideal multipartite access structures seems a very ambitious goal, we take a first step in this direction. On the one hand, we detect some conditions that directly imply that a multipartite structure cannot be ideal. On the other hand, we prove that three wide families of multipartite access structures are ideal. We believe that the techniques employed in these proofs are so general that they could be used to prove in the future more general results related to the characterization of ideal multipartite access structures.

Keywords: secret sharing schemes, multipartite access structures, information rate, ideal access structures.

1 Introduction

Distributed cryptography studies cryptographic schemes where the power to perform a specific task (as it could be signing or decrypting) is distributed among a set of players or servers. With this approach, the system improves its security and trustworthiness. A key tool in almost all these systems are secret sharing schemes. In these schemes, we start from a set of players and a family of authorized subsets (the so-called access structure). Then, an external figure (usually called dealer), takes a secret value and computes from it some shares that he sends secretly to the players. The system must withhold two properties: (1) the secret can be computed from the shares of any authorized subset in an unequivocal way; (2) any non-authorized subset does not obtain any information about the secret from the shares they hold.

The usual way to measure the efficiency of secret sharing schemes is by means of comparing the length of the shared secret with the length of the shares that players hold. This comparison is made using the information rate. This parameter takes its maximum value when the length of the shares is equal to that of the secret, the so-called ideal case. In general, figuring out if there exists or not an ideal secret sharing scheme realizing a given access structure, and even more, constructing it, is a very hard problem. For this reason, research in this area has focused on the study of specific families of access structures, such as threshold access structures [12], access structures defined by graphs [3], star access structures [7], those with at most 5 participants [8], the bipartite access structures [11], or weighted threshold access structures [1].

In this work we study some families of multipartite access structures: the set of players is divided into K disjoint entities, and all players in each entity play exactly the same role inside the access structure. These access structures can make a lot of sense in real life applications, where persons or machines are divided into different groups according to their position in a company, their responsibilities, their computational resources, or their probability to be corrupted by an attacker.

When $K = 1$, we recover threshold access structures, and when $K = 2$, we recover bipartite ones [11]. For $K = 3$ (tripartite access structures), some partial work has been done in [6, 1]. To the best of our knowledge, however, there are not many results involving multipartite access structures in general, for any value of K. This work is a first step in this direction.

We consider three families of multipartite access structures, and we prove that they are ideal. The two first families are multipartite for a general value of K, whereas the third one is tripartite ($K = 3$). The proofs of these results are not constructive, but existential. Furthermore, we believe that the mathematical techniques employed in the proofs are quite general and could be applied to prove that other general families of multipartite access structures are also ideal.

On the other hand, we also consider the question of detecting multipartite access structures that are not ideal. We prove that a list of different combinations of authorized/non-authorized subsets in a multipartite access structure directly imply that this structure cannot be ideal.

The rest of the paper is organized as follows. In Section 2 we recall the basic concepts related to secret sharing schemes, we give the definition of general multipartite access structures, we show that any access structure is a multipartite one and we mention some studied cases of such structures. We prove in Section 3 that three specific (but wide) families of multipartite access structures are ideal. In Section 4 we prove a result which allows to ensure that a multipartite access structure is not ideal, when some prohibited position is detected among the points which represent subsets of players in the space $(\mathbb{Z}^+)^K$. We give two simple examples of how to use this result to prove that some tripartite access structures are not ideal. Finally we conclude the work in Section 5, where we explain some possible future work to be done in this subject, by enunciating some conjectures related to the characterization of ideal multipartite access structures.

2 Secret Sharing Schemes

In this section we briefly introduce the necessary concepts about secret sharing schemes we need to understand the rest of our work.

In a *secret sharing schemes*, a dealer, that we will note as D, distributes shares of a secret value among a set of players $\mathcal{P} = \{P_1, \ldots, P_\ell\}$, in such a way that only authorized subsets of players (those in the so-called *access structure*, that we will note $\Gamma \subset 2^{\mathcal{P}}$) are able to obtain the secret from their shares. However, subsets that are not authorized (that is, those in the family $\overline{\Gamma} = 2^{\mathcal{P}} - \Gamma$) do not obtain any information on the secret. The family Γ must be *monotone increasing*, that is, if $A \in \Gamma$ and $A \subset B$, then $B \in \Gamma$. An access structure Γ is determined completely by its *basis* $\Gamma_0 = \{A \in \Gamma \mid A' \notin \Gamma,\ \forall A' \subsetneq A\}$, precisely by this monotone property. Analogously, the family of non-authorized subsets is determined by its basis $\overline{\Gamma}_0$, the family of maximal non-authorized subsets.

The parameter that is usually used to measure the efficiency of a secret sharing scheme is the *information rate* ρ, which is defined as the quotient between the length of the shared secret and the maximum length of the shares of the players. It can be easily proved that $\rho \leq 1$. The *ideal* case is when $\rho = 1$, that is, the length of the shares of every participant is equal to the length of the secret. We say that an access structure is *ideal* if there exists some ideal secret sharing scheme that realizes it. The *optimal information rate* $\rho^*(\Gamma)$ of an access structure Γ is the supremum of the information rates of all the secret sharing schemes that realize Γ.

Secret sharing schemes where independently introduced in 1979 by Shamir [12] and Blakley [2]. Shamir introduced a scheme realizing a *threshold* access structure: authorized subsets of players are those ones with at least t players.

Other works introduced secret sharing schemes realizing more general access structures. For example, *vector space* secret sharing schemes [5] realize access structures that include threshold access structures. These schemes are also ideal. Vector space access structures are defined by a public function $\psi : \mathcal{P} \cup \{D\} \to E$ (where E is a vector space over a finite field $GF(q)$), such that $A \in \Gamma$ if and only if $\psi(D) \in \langle \psi(A) \rangle$.

If the dealer wants to share a secret $s \in GF(q)$, he chooses a random vector $\mathbf{v} \in E$ such that $\mathbf{v} \cdot \psi(D) = s$. Then he computes and sends secretly to player P_i his share $s_i = \mathbf{v} \cdot \psi(P_i)$. If $A \in \Gamma$ is an authorized subset, then $\psi(D) = \sum_{P_i \in A} \lambda_i^A \psi(P_i)$, for some coefficients $\lambda_i^A \in GF(q)$. The players in A will be able to recover the secret s from their shares, as follows:

$$s = \mathbf{v} \cdot \psi(D) = \mathbf{v} \cdot \sum_{P_i \in A} \lambda_i^A \psi(P_i) = \sum_{P_i \in A} \lambda_i^A \mathbf{v} \cdot \psi(P_i) = \sum_{P_i \in A} \lambda_i^A s_i.$$

It can be proved that no information on the secret can be obtained from the shares of any non-authorized subset.

A generalization of vector space secret sharing schemes are *linear secret sharing schemes* [13]. It is proved that any access structure can be realized by a linear scheme.

2.1 Multipartite Access Structures

In this section we introduce multipartite access structures. We will mention some known works about this topic and we present some examples of structures of this family.

Let $\mathcal{P} = \{P_1, P_2, \ldots, P_\ell\}$ be the set of players that are distributed into different disjoint entities $X_1, X_2, \ldots, X_K$, where $K \geq 2$. Every entity X_j has ℓ_j players, therefore the whole set of players is $\ell = \sum_{i=1}^{K} \ell_j$. We will say that the access structure is multipartite when players in every entity play the same role. More formally: an access structure Γ defined in the set of players $\mathcal{P}$ is *multipartite* of partition $X_1, X_2, \ldots, X_K$ if $\sigma(\Gamma) = \Gamma$ for any permutation σ of $\mathcal{P}$ with $\sigma(X_1) = X_1, \ldots, \sigma(X_K) = X_K$. In this case we say that Γ is $(X_1, \ldots, X_K)$-multipartite, or that Γ is K-multipartite.

In fact, any access structure is a multipartite one. In effect, let us denote as τ_{pq}, for two participants $p, q \in \mathcal{P}$, the transposition of two participants p, q in $\mathcal{P}$. In order to find participants with the same role in the structure we define the relation: $p \sim q$ if and only if $\tau_{pq}(\Gamma) = \Gamma$. It is not difficult to see that the binary relation $\sim$ is an equivalence relation. Therefore we can consider the quotient $\mathcal{P}/\sim\; = \{X_1, \ldots, X_K\}$, where $X_1, \ldots, X_K$ are the equivalence classes determined by the relation $\sim$.

Now one can prove that the structure Γ is $(X_1, \ldots, X_K)-$multipartite. In effect, let σ be a permutation of $\mathcal{P}$ with $\sigma(X_1) = X_1, \ldots, \sigma(X_K) = X_K$. It is easy to see that such a permutation can be seen as a composition of K permutations of the classes: $\sigma = \sigma_1 \circ \ldots \circ \sigma_K$ with $\sigma_i(X_i) = X_i$ and $\sigma_i(P_j) = P_j$ for any player $P_j \in \mathcal{P} - X_i$. Each σ_i can be expressed as a composition of transpositions between elements in X_i. So σ is a composition of transpositions between elements of the same class. This directly implies $\sigma(\Gamma) = \Gamma$, as desired. Therefore,

Proposition 1. *Any access structure is a multipartite access structure.*

Multipartite access structures were introduced in [11]. The only known results are the study of bipartite access structures (that is, when $K = 2$) in [11] and some partial results in the tripartite case ($K = 3$) in [6]. In [11], bipartite access structures are introduced, ideal bipartite structures are completely characterized, and the information rate of non-ideal ones is bounded and studied. In [6] some conditions for ideal tripartite access structures are introduced. Some particular families of tripartite access structures have been proved ideal in [1].

A subfamily of multipartite access structures that has been widely studied in literature is the family of access structures defined by weights. In this kind of access structure every participant $p \in \mathcal{P}$ has associated its own weight $\omega(p) \in \mathbb{R}^+$ and we will say that a subset $A \subset P$ is authorized if and only if $\omega(A) = \sum_{p \in A} \omega(p) \geq t$, where $t \geq 0$ is the threshold of the structure. These structures are a subfamily of multipartite ones by considering $X_i = \omega^{-1}(\omega_i)$ where $\omega_1, \ldots, \omega_K$ are the different weights derived from the mapping ω. A particular case studied in [11] are the structures with only two possible weights, which results in a bipartite access structure. The structures defined by weights and threshold were introduced by Shamir in [12]. Some results were given in [9] for the case when such structures are representable by a graph, while a total characterization of ideal weighted threshold access structures has been recently given in [1].

We use the notation $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$ for the set of non-negative integers. Given the partition $X_1, X_2, \ldots, X_K$ of the set of participants $\mathcal{P}$, for any subset $A \subset \mathcal{P}$ we consider the point $\pi(A) = (x_1(A), x_2(A), \ldots, x_K(A)) \in (\mathbb{Z}^+)^K$, where $x_i(A) = |A \cap X_i|$. We also consider the set of points

$$\pi(\Gamma) = \{\pi(A) \ : \ A \in \Gamma\} \subset (\mathbb{Z}^+)^K$$

defined by the structure Γ; or the set of points defined by the basis of the structure, $\pi(\Gamma_0) = \{\pi(A) \mid A \in \Gamma_0\} \subset (\mathbb{Z}^+)^K$. It is easy to prove that a multipartite structure Γ is completely determined by the set of points in $\pi(\Gamma)$, that is, $A \in \Gamma$ if and only if $\pi(A) \in \pi(\Gamma)$.

3 Some Families of Ideal Multipartite Access Structures

In this section we consider some wide families of multipartite access structures. We will prove that these access structures are ideal, by proving that they can be realized by a vector space secret sharing scheme.

In our results, we will use as a tool the following lemma, which is well known and can be proved by induction on the number of polynomial indeterminates.

Lemma 1. *Let $p(x_1, \ldots, x_\ell) \in \mathbb{Z}[x_1, \ldots, x_\ell]$ be a polynomial with integer coefficients in the ℓ variables $x_1, \ldots, x_\ell$. The polynomial $p(x_1, \ldots, x_\ell)$ is non null if and only if there exist integer numbers $\alpha_1, \ldots, \alpha_\ell$ such that $p(\alpha_1, \ldots, \alpha_\ell) \neq 0$.*

Recall that this result is not true for polynomials defined over finite fields (for example, the polynomial $p(x) = x^q - x \in \mathbb{Z}_q[x]$ is not the null polynomial, for any prime number q, but $p(\alpha) = 0$ for all $\alpha \in \mathbb{Z}_q$).

3.1 A First Family

Let $X_1, \ldots, X_K$ be a partition of $\mathcal{P}$. We define the mapping $\nu : \mathcal{P} \to \{1, 2, \ldots, K\}$ that assigns to every participant the entity he belongs to. We will use the notation $\nu_i = \nu(P_i)$, meaning that the participants P_i belongs to the entity X_{ν_i}. We also define, for a subset of players $A \subset \mathcal{P}$, the set of entities represented by A as $\nu(A) = \{\nu(P_i) \mid P_i \in A\}$.

We consider the multipartite access structure

$$\Gamma = \{A \subset \mathcal{P} \ : \ |A| \geq t \ \text{ and } \ |\nu(A)| \geq d\}$$

defined on the partition $X_1, \ldots, X_K$, for any $1 \leq d \leq t$ and $d \leq K$. That is, a subset is authorized if and only if it contains at least t players who come from at least d different entities.

In order to prove that these access structures are ideal we will prove that they are vector space access structures. The following lemma will be necessary in order to prove that the specific map $\psi : \mathcal{P} \cup \{D\} \longrightarrow GF(q)^t$ that we are going to construct actually realizes the considered access structure Γ.

Lemma 2. *Let $t, d \in \mathbb{Z}^+$ be integer numbers verifying $1 \leq d \leq t$ and let us consider the following polynomial in t variables, defined over the integers:*

$$Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t) = \begin{vmatrix} x_1 & x_1^2 & \ldots & x_1^{t-d} & r_1^{d-1} & \ldots & r_1^2 & r_1 & 1 \\ x_2 & x_2^2 & \ldots & x_2^{t-d} & r_2^{d-1} & \ldots & r_2^2 & r_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_t & x_t^2 & \ldots & x_t^{t-d} & r_t^{d-1} & \ldots & r_t^2 & r_t & 1 \end{vmatrix}.$$

The polynomial $Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t)$ is non null if and only if there exist d different numbers in $r_1,\ldots,r_t \in \mathbb{Z}^+$.

Proof. If $d = t$ the result is trivial. In order to prove that the polynomial $Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t)$ is not the null polynomial for $d < t$, we look for a coefficient different from zero. Let us suppose that $r_{t-d+1},\ldots,r_t$ are different. If not, it is easy to argue in the same way, exchanging some indeterminates and permuting some rows.

Developing this determinant by the first row we obtain:

$$Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t) = x_1 \begin{vmatrix} x_2^2 & x_2^3 & \ldots & x_2^{t-d} & r_2^{d-1} & \ldots & r_2^2 & r_2 & 1 \\ x_3^2 & x_3^3 & \ldots & x_3^{t-d} & r_3^{d-1} & \ldots & r_3^2 & r_3 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_t^2 & x_t^3 & \ldots & x_t^{t-d} & r_t^{d-1} & \ldots & r_t^2 & r_t & 1 \end{vmatrix} + p_1(x_1,\ldots,x_t)$$

where $p_1(x_1,\ldots,x_t)$ is a polynomial in which x_1^i appears with $i \neq 1$, that is, there are no terms of the form $x_1 x_2^{i_2} \cdot \ldots \cdot x_t^{i_t}$ in $p_1(x_1,\ldots,x_t)$. We can follow the development of the determinant obtaining:

$$Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t) = x_1 x_2^2 \begin{vmatrix} x_3^3 & x_3^4 & \ldots & x_3^{t-d} & r_3^{d-1} & \ldots & r_3^2 & r_3 & 1 \\ x_4^3 & x_4^4 & \ldots & x_4^{t-d} & r_4^{d-1} & \ldots & r_4^2 & r_4 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_t^3 & x_t^4 & \ldots & x_t^{t-d} & r_t^{d-1} & \ldots & r_t^2 & r_t & 1 \end{vmatrix} + p_2(x_1,\ldots,x_t)$$

where $p_2(x_1,\ldots,x_t)$ is a polynomial that does not contain terms of the form $x_1 x_2^2 x_3^{i_3} \cdot \ldots \cdot x_t^{i_t}$. Iterating the process we obtain:

$$Q_{r_1,\ldots,r_t}(x_1,\ldots,x_t) = x_1 x_2^2 x_3^3 \cdot \ldots \cdot x_{t-d}^{t-d} \begin{vmatrix} r_{t-d+1}^{d-1} & \ldots & r_{t-d+1}^2 & r_{t-d+1} & 1 \\ r_{t-d+2}^{d-1} & \ldots & r_{t-d+2}^2 & r_{t-d+2} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_t^{d-1} & \ldots & r_t^2 & r_t & 1 \end{vmatrix} + p_{t-d}(x_1,\ldots,x_t)$$

where $p_{t-d}(x_1, \ldots, x_t)$ is a polynomial that does not contain terms of the form $x_1 x_2^2 x_3^3 \cdot \ldots \cdot x_{t-d}^{t-d}$. Since the coefficient of the monomial $x_1 x_2^2 x_3^3 \cdot \ldots \cdot x_{t-d}^{t-d}$ is a non null Vandermonde determinant, the polynomial $Q_{r_1,\ldots,r_t}(x_1, \ldots, x_t)$ is non null.

Conversely, if there are not d different numbers among $r_1, \ldots, r_t \in \mathbb{Z}^+$, then any minor of order d of the last d columns is zero; therefore, these columns are linearly dependent and so the polynomial is null. $\square$

Theorem 1. *Let K, t, d be positive integer numbers with $1 \leq d \leq t$, $d \leq K$ and let $X_1, \ldots, X_K$ be a partition of $\mathcal{P}$. The multipartite access structure defined in the partition $X_1, \ldots, X_K$ by*

$$\Gamma = \{A \subset \mathcal{P} \ : \ |A| \geq t \ \ \text{and} \ \ |\nu(A)| \geq d\}$$

is ideal.

Proof. If $d = 1$ then Γ is a threshold access structure and thus ideal. For $d \geq 2$, we are going to prove that Γ is a vector space access structure, which directly implies that it is ideal.

Observe that this structure is defined by

$$\pi(\Gamma_0) = \{(a_1, \ldots, a_K) \in (\mathbb{Z}^+)^K : a_1 + \ldots + a_K = t \text{ with}$$

$$\text{at least } d \text{ numbers } a_i \neq 0\}.$$

Recall that the quantity of non null numbers a_i is the quantity of entities (or classes in the partition) that appear in the subset A represented by point $\pi(A) = (a_1, \ldots, a_K)$. Following the notation $X_i = \{P_{i1}, \ldots, P_{i\ell_i}\}$ for the entities, where $X_0 = \{P_{01}\}$, with $P_{01} = D$ (the dealer), we define the map $\psi : \mathcal{P} \cup \{D\} \longrightarrow GF(q)^t$ that will determine the structure Γ as a vector space access structure, as follows:

$$\psi(P_{ij}) = (0, \ldots, 0, i^{d-1}, i^{d-2}, \ldots, i, 1) + \alpha_{ij}(1, 0, \ldots, 0) + \alpha_{ij}^2(0, 1, 0, \ldots, 0) + \ldots +$$

$$+\alpha_{ij}^{t-d}(0, \ldots, 0, 1, 0, \ldots, 0) = (\alpha_{ij}, \alpha_{ij}^2, \ldots, \alpha_{ij}^{t-d}, i^{d-1}, i^{d-2}, \ldots, i, 1),$$

for some values α_{ij} to be determined. In order to find values α_{ij} and q such that the above map ψ defines the structure Γ we consider the polynomial:

$$Q(x_{01}, x_{11}, \ldots, x_{1\ell_1}, \ldots, x_{K1}, \ldots, x_{K\ell_K}) = \prod_{\{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \mathcal{I}} Q_{r_1,\ldots,r_t}(x_{r_1 i_1}, \ldots, x_{r_t i_t})$$

with $\mathcal{I} = \Gamma_0 \cup \{\{P_{01}\} \cup A \ : \ A \subset \mathcal{P}, \ \nu(A) \geq d-1, \ |A| = t-1\}$ and where the factors of the polynomial are defined as in Lemma 2. We will justify that $Q(x_{01}, x_{11}, \ldots, x_{1\ell_1}, \ldots, x_{K1}, \ldots, x_{K\ell_K})$ is a non null polynomial applying Lemma 2 to every factor. The first kind of factors in polynomial Q are $Q_{r_1,\ldots,r_t}(x_{r_1 i_1}, \ldots, x_{r_t i_t})$ for $\{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \Gamma_0$. These factors are non null because there are at least d different numbers among $r_1, \ldots, r_t$. The second kind of factors is $Q_{0,r_1,\ldots,r_{t-1}}(x_{01}, x_{r_1 i_1}, \ldots, x_{r_{t-1} i_{t-1}})$ for $A = \{P_{r_1 i_1}, \ldots, P_{r_{t-1} i_{t-1}}\}$

with $\nu(A) \geq d-1$, then $\{P_{01}\} \cup A$ has at least d different numbers in $0, r_1, \ldots, r_{t-1}$. From the integrity of integer polynomial product we obtain that Q is non null. Then using Lemma 1 we can ensure the existence of $\alpha_{01}, \alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{K1}, \ldots, \alpha_{K\ell_K} \in \mathbb{Z}$ such that

$$Q(\alpha_{01}, \alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{K1}, \ldots, \alpha_{K\ell_K}) \neq 0.$$

Let $p > K$ be a prime such that:

$$p > max_{\{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \mathcal{I}} |Q_{r_1, \ldots, r_t}(\alpha_{r_1 i_1}, \ldots, \alpha_{r_t i_t})|.$$

Let us suppose that map ψ defined above determines an access structure Γ_ψ. Now we prove that $\Gamma_\psi = \Gamma$ for any field $GF(q)$ with q a power of the prime p.

First we justify that $\Gamma \subset \Gamma_\psi$. Let $A \in \Gamma$ be a subset with $|A| = t$. Then $A \in \Gamma_0$, that is $A \in \mathcal{I}$ and by definition of polynomial Q, the t vectors in $\psi(A)$ are linearly independent because their determinant is different from zero. So these vectors form a basis of $GF(q)^t$ and then $\psi(D) \in \langle \psi(A) \rangle$. That is, we have justified that $A \in \Gamma_\psi$ when $|A| = t$. For any subset $A \in \Gamma$, we have $|A| \geq t$, and, of course, the assert is also true taking into account that $d \leq t$.

Secondly we show that $\Gamma_\psi \subset \Gamma$. Equivalently we prove that if $A \notin \Gamma$ then $A \notin \Gamma_\psi$. Let us suppose that $A \notin \Gamma$, then two possible cases can occur. If $|\nu(A)| < d$ we have $A \notin \Gamma_\psi$. This fact is true because if $A \in \Gamma_\psi$ then $\psi(P_{01}) = \sum_{p \in A} \beta_p \psi(p)$ for some scalars $\beta_p \in GF(q)$, then using the last d coordinates of this expression we have $(0, \ldots, 0, 1) = \sum_{i \in \nu(A)} \beta'_i (i^{d-1}, i^{d-2}, \ldots, i^2, i, 1)$ for some scalars $\beta'_i \in GF(q)$, so $|\nu(A)| \geq d$ for the properties of Vandermonde vectors. Then for $A \notin \Gamma$ with $|\nu(A)| < d$ we have $A \notin \Gamma_\psi$. In the second case $A \notin \Gamma$ is such that $|\nu(A)| \geq d$, then $|A| < t$. If $|A| = t-1$ with $|\nu(A)| \geq d$ we have $A \notin \Gamma_\psi$. This is true because in this case $\{P_{01}\} \cup A \in \mathcal{I}$, then vectors $\psi(D)$ and $\psi(A)$ are linearly independent by definition of polynomial Q, so $\psi(D) \notin \langle \psi(A) \rangle$, that is $A \notin \Gamma_\psi$. Of course from this case it can be deduced that for any $A \subset \mathcal{P}$ with $|A| < t$, $|\nu(A)| \geq d$ we also have $A \notin \Gamma_\psi$. □

3.2 A Second Family

Now we present a different result, proving that multipartite access structures defined by $\Gamma = \{A \subset \mathcal{P} \ : \ |A| \geq t \ \text{ and } \ x_1(A) \geq n_1, \ldots, \ x_K(A) \geq n_K\}$ (where $x_i(A) = |A \cap X_i|$) are also ideal for any values $0 \leq n_1, \ldots, n_K \leq t$ satisfying $n_1 + \ldots + n_K \leq t$. We will proceed in a similar way as before: we will prove first a lemma that helps us to define the map expressing the structure as a vector space access structure.

Lemma 3. *Let $t, d \in \mathbb{Z}^+$ be positive integer numbers with $1 \leq d \leq t$, let $\mathbf{v}_1, \ldots, \mathbf{v}_t \in \mathbb{Z}^d$ be integer vectors, and consider the polynomial $Q_{\mathbf{v}_1, \ldots, \mathbf{v}_t}(x_1, \ldots, x_t) \in \mathbb{Z}[x_1, \ldots, x_t]$ in t variables defined by*

$$Q_{\mathbf{v}_1, \ldots, \mathbf{v}_t}(x_1, \ldots, x_t) = \begin{vmatrix} x_1 & x_1^2 & \ldots & x_1^{t-d} & \mathbf{v}_1 \\ x_2 & x_2^2 & \ldots & x_2^{t-d} & \mathbf{v}_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_t & x_t^2 & \ldots & x_t^{t-d} & \mathbf{v}_t \end{vmatrix}.$$

The polynomial $Q_{\mathbf{v}_1,\ldots,\mathbf{v}_t}(x_1,\ldots,x_t)$ is non null if and only if there exists d linearly independent vectors among vectors $\mathbf{v}_1,\ldots,\mathbf{v}_t$.

Proof. If $d=t$ the result is trivial. As in the previous lemma, in order to prove that the polynomial $Q_{\mathbf{v}_1,\ldots,\mathbf{v}_t}(x_1,\ldots,x_t)$ with $d<t$ is not the null polynomial, we look for a coefficient different from zero. Let us suppose without loss of generality that $\mathbf{v}_{t-d+1},\ldots,\mathbf{v}_t$ are linearly independent (if necessary, exchanging some indeterminates and permuting some rows).

Developing this determinant as in Lemma 2 we have

$$Q_{\mathbf{v}_1,\ldots,\mathbf{v}_t}(x_1,\ldots,x_t) = x_1x_2^2x_3^3\cdot\ldots\cdot x_{t-d}^{t-d}\cdot\det(\mathbf{v}_{t-d+1},\ldots,\mathbf{v}_t)+p(x_1,\ldots,x_t)$$

where $p(x_1,\ldots,x_t)$ is a polynomial that does not contain terms of the form $x_1x_2^2x_3^3\cdot\ldots\cdot x_{t-d}^{t-d}$. Since coefficient of monomial $x_1x_2^2x_3^3\cdot\ldots\cdot x_{t-d}^{t-d}$ is a non null determinant, the polynomial $Q_{\mathbf{v}_1,\ldots,\mathbf{v}_t}(x_1,\ldots,x_t)$ is non null.

Reciprocally, if every subset of d vectors among vectors $\mathbf{v}_1,\ldots,\mathbf{v}_t$ are linearly dependent then the last d columns of the determinant are linearly dependent, and so $Q_{\mathbf{v}_1,\ldots,\mathbf{v}_t}(x_1,\ldots,x_t)$ is null. □

Note that Lemma 2 is a particular case of Lemma 3 taking the corresponding vectors $\mathbf{v}_1,\ldots,\mathbf{v}_t$. Using Lemma 1 and Lemma 3 we prove the following result.

Theorem 2. *Let $K,t,n_1,\ldots,n_K$ be non-negative integer numbers with $n_1+\ldots+n_K\leq t$ and let $X_1,\ldots,X_K$ be a partition of $\mathcal{P}$ verifying $n_i\leq|X_i|=\ell_i$. The multipartite access structure defined in the partition $X_1,\ldots,X_K$ by*

$$\Gamma=\{A\subset\mathcal{P}\ :\ |A|\geq t\ \ \text{and}\ \ |x_1(A)|\geq n_1,\ldots,\ |x_K(A)|\geq n_K\}$$

is ideal.

Proof. Observe that the structure is defined by

$$\pi(\Gamma_0)=\{(a_1,\ldots,a_K)\in(\mathbb{Z}^+)^K : a_1+\ldots+a_K=t, a_1\geq n_1,\ldots,a_K\geq n_K\}.$$

Let $\ell_i=|X_i|$ be the cardinalities of the partition classes. The family of associated points for maximal non-authorized subsets is:

$$\pi(\overline{\Gamma}_0)=\{(a_1,\ldots,a_K)\in(\mathbb{Z}^+)^K : a_1+\ldots+a_K=t-1, a_1\geq n_1,\ldots,a_K\geq n_K\}\cup$$

$$\cup\{(n_1-1,\ell_2,\ldots,\ell_K),(\ell_1,n_2-1,\ldots,\ell_K),\ldots,(\ell_1,\ldots,\ell_{K-1},n_K-1)\}.$$

Let d be the positive integer number $d=n_1+\ldots+n_K$. Let us define the map $\psi:\mathcal{P}\cup\{D\}\longrightarrow GF(q)^t$ that will determine the structure Γ as a vector space access structure. For any $P_{ij}\in X_i$, where $X_0=\{P_{01}\}$ and $P_{01}=D$ (the dealer), we define for some values α_{ij} (not determined, by the moment):

$$\psi(P_{ij})=(0,\ldots,0,\mathbf{v}_{ij})+\alpha_{ij}(1,0,\ldots,0)+\alpha_{ij}^2(0,1,0,\ldots,0)+\ldots+$$

$$+\alpha_{ij}^{t-d}(0,\ldots,0,1,0,\ldots,0)=(\alpha_{ij},\alpha_{ij}^2,\ldots,\alpha_{ij}^{t-d},\mathbf{v}_{ij})$$

where the d-dimensional vectors $\mathbf{v}_{ij}$ are defined as

$$\mathbf{v}_{01} = (V_{n_1}(0), \ldots, V_{n_K}(0)) \in \mathbb{Z}^d$$

$$\mathbf{v}_{ij} = (0_{n_1}, \ldots, 0_{n_{i-1}}, V_{n_i}(j), 0_{n_{i+1}}, \ldots, 0_{n_K}) \in \mathbb{Z}^d, \text{ for } P_{ij} \in \mathcal{P}.$$

Here 0_{n_j} denotes the n_j-dimensional null vector, and $V_{n_i}(j) = (1, j, j^2, \ldots, j^{n_i-1})$ denotes a n_i-dimensional Vandermonde vector.

Observe that if $t = d$ the result is true for any power $q = p^r$ of a prime p satisfying $p > \ell_i$, for every $i = 1, \ldots, K$.

In order to find values α_{ij} and q such that the above map ψ defines the structure Γ for $t \geq d$ we consider the polynomial:

$$Q(x_{01}, x_{11}, \ldots, x_{1\ell_1}, \ldots, x_{K1}, \ldots, x_{K\ell_K}) = \prod_{\{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \mathcal{I}} Q_{\mathbf{v}_{r_1 i_1}, \ldots, \mathbf{v}_{r_t i_t}}(x_{r_1 i_1}, \ldots, x_{r_t i_t})$$

with $\mathcal{I} = \Gamma_0 \cup \{\{P_{01}\} \cup A : A \in \overline{\Gamma}_0,\ |A| = t-1\}$ and where the factors of the polynomial are the ones defined in Lemma 3. We will justify that $Q(x_{01}, x_{11}, \ldots, x_{1\ell_1}, \ldots, x_{K1}, \ldots, x_{K\ell_K})$ is a non null polynomial applying Lemma 3 to every factor. The first kind of factors in polynomial Q are $Q_{r_1, \ldots, r_t}(x_{r_1 i_1}, \ldots, x_{r_t i_t})$ for $A = \{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \Gamma_0$, then $|A| \geq t$ with $|x_1(A)| \geq n_1, \ldots, |x_K(A)| \geq n_K$. The last d coordinates of vectors in $\psi(A)$ contain at least n_i vectors corresponding to users in X_i for $i = 1, \ldots, K$, then these $n_1 + \ldots + n_K = d$ vectors are linearly independent because their determinant is

$$\begin{vmatrix} W_1 & 0 & \ldots & 0 \\ 0 & W_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & W_K \end{vmatrix} = |W_1| \cdot \ldots \cdot |W_K| \neq 0$$

where in this block diagonal determinant, every block determinant $|W_i|$ has Vandermonde form. Using Lemma 3 we have that these factors $Q_{r_1, \ldots, r_t}(x_{r_1 i_1}, \ldots, x_{r_t i_t})$ are non null. The second kind of factors are $Q_{0, r_1, \ldots, r_{t-1}}(x_{01}, x_{r_1 i_1}, \ldots, x_{r_{t-1} i_{t-1}})$ for $A = \{P_{r_1 i_1}, \ldots, P_{r_{t-1} i_{t-1}}\}$ with $A \in \overline{\Gamma}_0$, then the subset of t vectors determined by $\{P_{01}\} \cup A$ has at least d linearly independent vectors determined by the last d coordinates in the same way as above. So, by Lemma 3 the polynomial factors determined by $\{P_{01}\} \cup A$ are non null. From the integrity of integer polynomial product we obtain that Q is non null. Then using Lemma 1 we can deduce the existence of $\alpha_{01}, \alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{K1}, \ldots, \alpha_{K\ell_K} \in \mathbb{Z}$ such that

$$A(\alpha_{01}, \alpha_{11}, \ldots, \alpha_{1\ell_1}, \ldots, \alpha_{K1}, \ldots, \alpha_{K\ell_K}) \neq 0.$$

Let $p > K$ be a prime such that:

$$p > max_{\{P_{r_1 i_1}, \ldots, P_{r_t i_t}\} \in \mathcal{I}} |Q_{\mathbf{v}_{r_1 i_1}, \ldots, \mathbf{v}_{r_t i_t}}(\alpha_{r_1 i_1}, \ldots, \alpha_{r_t i_t})|.$$

In order to prove that the map ψ determines Γ if we consider any field $GF(q)$ with q a power of p, let us denote by Γ_ψ the access structure defined by the map ψ. Now we show that $\Gamma_\psi = \Gamma$.

First we justify that $\Gamma \subset \Gamma_\psi$. Let $A \in \Gamma$ be a subset with $|A| = t$. This subset A satisfies $|A| = t$ and $|x_1(A)| \geq n_1, \ldots, |x_K(A)| \geq n_K$, and so $A \in \Gamma_0$. Therefore $A \in \mathcal{I}$ and by definition of polynomial Q the t vectors in $\psi(A)$ are linearly independent because their determinant is different from zero. So these vectors form a basis of $GF(q)^t$ and then $\psi(D) \in \langle\psi(A)\rangle$. That is, we have justified that $A \in \Gamma_\psi$ when $|A| = t$. The assert is also true for any subset $A \in \Gamma$ because since $|A| \geq t$, and $n_1 + \ldots + n_K = d \leq t$ we can take t users with at least n_i users from X_i, for every $i = 1, \ldots, K$.

Secondly we prove that $\Gamma_\psi \subset \Gamma$. Equivalently we see that if $A \notin \Gamma$ then $A \notin \Gamma_\psi$. Assume that $A \notin \Gamma$, then two possible cases can occur. If for some $i = 1, \ldots, K$ we have $|x_i(A)| < n_i$, then $A \notin \Gamma_\psi$. In effect, if $A \in \Gamma_\psi$ then $\psi(P_{01}) = \sum_{P_{ij} \in A} \beta_{P_{ij}} \psi(P_{ij})$ for some scalars $\beta_{P_{ij}} \in GF(q)$. Using the corresponding block of n_i coordinates of this expression we have $V_{n_i}(0) = \sum_{P_{ij} \in A \cap X_i} \beta_{P_{ij}} V_{n_i}(j)$, so $|A \cap X_i| \geq n_i$ for the properties of Vandermonde vectors. Therefore, $|x_i(A)| \geq n_i$ for every $i = 1, \ldots, K$.

In the second case $A \notin \Gamma$ is such that $|x_1(A)| \geq n_1, \ldots, |x_K(A)| \geq n_K$, but $|A| < t$. If $|A| = t - 1$ with $|x_1(A)| \geq n_1, \ldots, |x_K(A)| \geq n_K$ we have $A \notin \Gamma_\psi$. This is true because in this case $\{P_{01}\} \cup A \in \mathcal{I}$, then vectors $\psi(D)$ and $\psi(A)$ are linearly independent by definition of polynomial Q, so $\psi(D) \notin \langle\psi(A)\rangle$, that is $A \notin \Gamma_\psi$. Of course from this case it can be deduced that for any $A \subset \mathcal{P}$ with $|A| < t$, $|x_1(A)| \geq n_1, \ldots, |x_K(A)| \geq n_K$ we also have $A \notin \Gamma_\psi$. □

It is possible to obtain many other families of ideal multipartite access structures following the same techniques as in the proof of this Theorem 2, but defining the vector $\psi(D)$ assigned to the dealer in more general and different ways. As an example, we will see in next section how to construct many different families of ideal tripartite access structures by changing the position of the vector of the dealer.

3.3 A Third Family: Tripartite Access Structures

In this section we deal with tripartite access structures. The participants are divided into three disjoint entities X_1, X_2, X_3 such that $X_1 \cup X_2 \cup X_3 = \mathcal{P}$. To simplify the notation, given a subset A of participants, we will use x_i to refer to the value $x_i(A) = |A \cap X_i|$, for $i = 1, 2, 3$. We identify a wide family of ideal tripartite access structures, as stated in the following theorem, whose proof is only sketched, for clarity and by lack of space.

Theorem 3. *Let Γ be a tripartite access structure. Assume that there exist non-negative integer numbers $d_1, d_2, d_3, d_{12}, d_{13}, d_{23}, t$, verifying*

(i) $0 \leq d_i \leq t$, *for all* $i = 1, 2, 3$,
(ii) $d_1 + d_2 + d_3 - d_{ij} - d_{jk} \geq t \geq d_1 + d_2 + d_3 - (d_{12} + d_{13} + d_{23})$, *for all values of* $i, j, k \in \{1, 2, 3\}$, $i \neq j$, $i \neq k$, $j \neq k$,
(iii) and $0 \leq d_{ij} \leq min(d_i, d_j)$, *for all values of* $i, j \in \{1, 2, 3\}$, $i < j$,

such that Γ can be expressed as $\pi(\Gamma) = A_1 \cup A_2 \cup A_3 \cup A_{12} \cup A_{13} \cup A_{23} \cup T$, *where:*

– $A_i = \emptyset$ *or* $A_i = \{\ (x_1, x_2, x_3) : x_i \geq d_i\ \}$ *for* $i = 1, 2, 3$,

– $A_{ij} = \emptyset$ *or* $A_{ij} = \left\{ \begin{array}{ll} (x_1, x_2, x_3) : x_i + x_j \geq d_i + d_j - d_{ij} \ \wedge & x_i \geq d_i - d_{ij} \\ & x_j \geq d_j - d_{ij} \end{array} \right\}$ *for* $i, j \in \{1, 2, 3\}$, $i < j$

– $T = \left\{ \begin{array}{lll} & x_1 \geq t - (d_2 + d_3 - d_{23}) & x_1 + x_2 \geq t - d_3 \\ (x_1, x_2, x_3) : \ x_1 + x_2 + x_3 \geq t \ \wedge & x_2 \geq t - (d_1 + d_3 - d_{13}) \ \wedge & x_1 + x_3 \geq t - d_2 \\ & x_3 \geq t - (d_1 + d_2 - d_{12}) & x_2 + x_3 \geq t - d_1 \end{array} \right\}$

Then Γ is a vector space access structure, and so ideal.

Proof. (Sketch.) Let $d = t + d_{12} + d_{13} + d_{23} - (d_1 + d_2 + d_3)$. We have that $d \geq 0$. We will consider a vector space L with dimension equal to t. In this space, we will construct three vector subspaces L_1, L_2, L_3 such that $\dim(L_i) = d_i$, $\dim(L_i \cap L_j) = d_{ij}$ and $\dim(L_1 \cap L_2 \cap L_3) = d$. The idea is that vectors assigned to participants in the entity X_i will be in the subspace L_i. Recall that we use ℓ_i to denote the total number of participants in each entity X_i.

Intuitively, given a vector in the space L, we will think it as

$$(*_{123} \parallel *_{12} \parallel *_{13} \parallel *_{23} \parallel *_1 \parallel *_2 \parallel *_3),$$

where $*_{123}$ is the part of the vector (the first d coordinates) generated by a basis of $L_1 \cap L_2 \cap L_3$; we consider the most simple basis, formed by $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_d$, where $\boldsymbol{e}_i$ is the vector in $\mathbb{Z}^t$ which has 1 in the i-th position and 0 in the rest of positions. Then, $*_{12}$ is the part of the vector ($d_{12} - d$ coordinates) corresponding to $(L_1 \cap L_2) - L_3$, $*_1$ is the part of the vector ($d_1 - d_{12} - d_{13} + d$ coordinates) corresponding to $L_1 - L_2 - L_3$, and so on.

For users P_{1j} in the first entity X_1, we define $\psi(P_{1j})$ as a linear combination of the vectors which generate L_1, in such a way that $\psi(P_{1j}) \notin L_2 + L_3$. That is,

$$\psi(P_{1j}) = (\alpha_j^{d_1-1}, \ldots, \alpha_j^{d_1-d} \parallel \alpha_j^{d_1-(d+1)}, \ldots, \alpha_j^{d_1-d_{12}} \parallel \alpha_j^{d_1-(d_{12}+1)}, \ldots, \alpha_j^{d_1-(d_{12}+d_{13}-d)} \parallel$$

$$0, \ldots, 0 \parallel \alpha_j^{d_1-(d_{12}+d_{13}-d)-1}, \ldots, \alpha_j^2, \alpha_j, 1 \parallel 0, \ldots, 0 \parallel 0, \ldots, 0),$$

for some integer values α_j which will be determined later.

Analogously, for users P_{2k} in the second entity X_2, we define $\psi(P_{2k})$ as a linear combination of the vectors which generate L_2, in such a way that $\psi(P_{2k}) \notin L_1 + L_3$. That is,

$$\psi(P_{2k}) = (\beta_k^{d_2-1}, \ldots, \beta_k^{d_2-d} \parallel \beta_k^{d_2-(d+1)}, \ldots, \beta_k^{d_2-d_{12}} \parallel 0, \ldots, 0 \parallel$$

$$\beta_k^{d_2-(d_{12}+1)}, \ldots, \beta_k^{d_2-(d_{12}+d_{23}-d)} \parallel 0, \ldots, 0 \parallel \beta_k^{d_2-(d_{12}+d_{23}-d)-1}, \ldots, \beta_k^2, \beta_k, 1 \parallel 0, \ldots, 0),$$

for some integer values β_k to be determined later.

Finally, for users P_{3m} in the third entity X_3, we define $\psi(P_{3m})$ as a linear combination of the vectors which generate L_3, in such a way that $\psi(P_{3m}) \notin L_1 + L_2$. Namely,

$$\psi(P_{3m}) = (\gamma_m^{d_3-1}, \ldots, \gamma_m^{d_3-d} \parallel 0, \ldots, 0 \parallel \gamma_m^{d_3-(d+1)}, \ldots, \gamma_m^{d_3-d_{13}} \parallel$$

$\gamma_m^{d_3-(d_{13}+1)}, \ldots, \gamma_m^{d_3-(d_{13}+d_{23}-d)} \parallel 0, \ldots, 0 \parallel 0, \ldots, 0 \parallel \gamma_m^{d_3-(d_{13}+d_{23}-d)-1}, \ldots, \gamma_m^2, \gamma_k, 1),$

for some integer values γ_m to be determined later.

With respect to the vector $\psi(D)$, depending on where we place it, we will obtain the different possibilities listed in the statement of this theorem. For example, if $\psi(D) \notin L_i + L_j$, for all $i, j \in \{1, 2, 3\}$, $i < j$ then we will have $A_i = A_{ij} = \emptyset$, for all $i, j \in \{1, 2, 3\}$, $i < j$. In this case, we will define

$$\psi(D) = (\mu^{t-1}, \mu^{t-2}, \ldots, \mu^2, \mu, 1) \in \mathbb{Z}^t$$

for some indeterminate integer value μ. The case on the other extreme happens if we impose $\psi(D) \in L_1 \cap L_2 \cap L_3$. In this case we have $A_i \neq \emptyset$ and $A_{ij} \neq \emptyset$, for all $i, j \in \{1, 2, 3\}$, $i < j$, and then we define

$$\psi(D) = (\mu^{d-1}, \mu^{d-2}, \ldots, \mu^2, \mu, 1, 0, \ldots, 0) \in \mathbb{Z}^t$$

again for some indeterminate integer μ (that is, the vector $\psi(D)$ has coordinates equal to 0 anywhere but in the first d coordinates $*_{123}$, which correspond to $L_1 \cap L_2 \cap L_3$).

There are many intermediate cases, and each one leads to a different family of tripartite access structure. As a matter of example, if $\psi(D) \in L_1$ but $\psi(D) \notin L_2 + L_3$, then we have that $A_2 = A_3 = A_{23} = \emptyset$, but A_1, A_{12} and A_{13} are not empty. In this case, the vector $\psi(D)$ has exactly the same form as a vector $\psi(P_{1j})$ corresponding to the first entity X_1, obviously for some indeterminate μ different from the indeterminates $\{\alpha_j\}_{1 \leq j \leq \ell_1}$.

To show that there exist specific values for q and for the values μ, $\{\alpha_j\}_{1 \leq j \leq \ell_1}$, $\{\beta_k\}_{1 \leq k \leq \ell_2}$ and $\{\gamma_m\}_{1 \leq m \leq \ell_3}$ such that the map ψ, defined as above over $GF(q)^t$, determines exactly the access structure Γ, we proceed as in Theorems 1 and 2. That is, we define a very big polynomial

$$Q\left(\mu, \{\alpha_j\}_{1 \leq j \leq \ell_1}, \{\beta_k\}_{1 \leq k \leq \ell_2}, \{\gamma_m\}_{1 \leq m \leq \ell_3}\right) =$$

$$\prod_{A \in \mathcal{I}} Q_A\left(\mu, \{\alpha_j\}_{P_{1j} \in A}, \{\beta_k\}_{P_{2k} \in A}, \{\gamma_m\}_{P_{3m} \in A}\right),$$

where each polynomial Q_A consists of some maximal minor of the matrix whose rows are the vectors $\psi(P)$ for all $P \in A$. The composition of the family $\mathcal{I}$ will depend on the specific position of the vector $\psi(D)$, but typically it will contain Γ_0 and subsets of the form $A = \{D\} \cup B$, where B is some maximal non-authorized subset of the structure Γ (we omit the details for simplicity).

The idea is that one can prove that the polynomial Q is not the null polynomial, by proving that each polynomial factor Q_A is not null (using the same techniques as in Lemmas 2 and 3, showing that there exists some monomial of the polynomials whose coefficient cannot be 0). Therefore, there will exist specific integer values $\tilde{\mu}, \{\tilde{\alpha}_j\}_{1 \leq j \leq \ell_1}, \{\tilde{\beta}_k\}_{1 \leq k \leq \ell_2}, \{\tilde{\gamma}_m\}_{1 \leq m \leq \ell_3}$ such that

$$Q\left(\tilde{\mu}, \{\tilde{\alpha}_j\}_{1 \leq j \leq \ell_1}, \{\tilde{\beta}_k\}_{1 \leq k \leq \ell_2}, \{\tilde{\gamma}_m\}_{1 \leq m \leq \ell_3}\right) \neq 0.$$

Taking a large enough value of q, one can prove that the access structure Γ_ψ defined by the resulting map ψ is exactly Γ, by proving $\Gamma_\psi \subset \Gamma$ and $\Gamma \subset \Gamma_\psi$. □

Note that this family of ideal tripartite access structures is quite more general than the tripartite families proved ideal in [1]. An open problem is to completely characterize ideal tripartite access structures; that is, are there more ideal tripartite access structures, other than the ones listed in the statement of Theorem 3?

4 Detecting Non-Ideal Multipartite Access Structures

In this section we present some results related to the optimal information rate of multipartite access structures. A necessary tool which appears in the proofs of these results is the concept of independent sequence of subsets, due to Blundo *et al.* [4] and slightly generalized in [11]. Let Γ be an access structure on a set of participants $\mathcal{P}$. We say that a sequence $B_1, B_2, \ldots, B_m$, where $\emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_m \subset \mathcal{P}$, is *independent* if

1. $B_m \notin \Gamma$.
2. For all $i = 1, 2, \ldots, m$, there exists a set $X_i \subset \mathcal{P}$ such that $B_i \cup X_i \in \Gamma$ and $B_{i-1} \cup X_i \notin \Gamma$, where $B_0 = \emptyset$.

We say that a set $A \supset X_1 \cup \ldots \cup X_m$ makes the sequence $B_1, B_2, \ldots, B_m$ independent. The use of independent sequences of subsets is very useful to find upper bounds on the optimal information rates because the following result holds (Theorem 3.8 in [4], generalized in Theorem 2.1 of [11]):

– If $A \in \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|A|}{m+1}$.
– If $A \notin \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|A|}{m}$.

The following theorem expresses some prohibited positions in ideal multipartite access structures, since the optimal information rate of access structures satisfying the stated conditions cannot be greater than 2/3.

Theorem 4. *Consider a K-multipartite access structure Γ and non-negative integers $x_1, \ldots, x_K, Y_1, \ldots, Y_{K-1}$ satisfying $x_K \geq 1$ and $Y_i \geq x_i$ for all $i = 1, \ldots, K-1$, such that $(x_1, \ldots, x_K) \in \pi(\Gamma)$ and $(Y_1, \ldots, Y_{K-1}, x_K - 1) \in \pi(\Gamma)$, and such that there exists at least one index $i_* \in \{1, \ldots, K-1\}$ such that the following conditions hold:*

(i) $Y_{i_*} > x_{i_*} \geq 1$.
(ii) $(x_1, \ldots, x_{i_*-1}, x_{i_*} - 1, x_{i_*+1}, \ldots, x_{K-1}, x_K) \notin \pi(\Gamma)$.
(iii) $(Y_1, \ldots, Y_{i_*-1}, Y_{i_*} - 1, Y_{i_*+1}, \ldots, Y_{K-1}, x_K - 1) \notin \pi(\Gamma)$.

If $Y_1 + \ldots + Y_{K-1} + x_K - 1 \neq x_1 + \ldots + x_K$ then $\rho^*(\Gamma) \leq 2/3$.

Proof. Let us assume first that $Y_1 + \ldots + Y_{K-1} + x_K - 1 < x_1 + \ldots + x_K$. Then, from the condition $Y_i \geq x_i$ for $i = 1, \ldots, K-1$ we obtain $x_1 + \ldots + x_K - 1 \leq Y_1 + \ldots + Y_{K-1} + x_K - 1 < x_1 + \ldots + x_K$. Therefore we conclude that $Y_i = x_i$ for any $i = 1, \ldots, K-1$, which gives us a contradiction with the existence of an index i_* such that $Y_{i_*} > x_{i_*}$. Thus we can concentrate on the case $Y_1 + \ldots + Y_{K-1} + x_K - 1 > x_1 + \ldots + x_K$.

We have two possible cases: there are at least two different indexes $i_*, j_* \in \{1, \ldots, K-1\}$ satisfying conditions $(i), (ii), (iii)$, or there is a unique index $i_* \in \{1, \ldots, K-1\}$ satisfying such conditions. We are going to consider the two cases in a separate way.

1. In the first case, we assume for simplicity $i_* = 1$ and $j_* = 2$; so we have $Y_1 > x_1 \geq 1$ and $Y_2 > x_2 \geq 1$. We can consider two sub-cases, depending on whether the point $(1, 0, \ldots, 0, 1)$ belongs to $\pi(\Gamma)$ or not.

   – If $(1, 0, \ldots, 0, 1) \notin \pi(\Gamma)$, then we construct an independent sequence with subsets $B_1 \subset B_2 \subset B_3$ and X_1, X_2, X_3 such that:

$$\begin{aligned}
\pi(B_1) &= (x_1 - 1, x_2, \ldots, x_{K-1}, x_K - 1),\\
\pi(X_1) &= (1, 0, \ldots, 0, 1),\\
\pi(B_2) &= (Y_1 - 1, Y_2 - 1, Y_3, \ldots, Y_{K-1}, x_K - 1),\\
\pi(X_2) &= (0, 0, \ldots, 0, 1),\\
\pi(B_3) &= (Y_1 - 1, Y_2, Y_3, \ldots, Y_{K-1}, x_K - 1),\\
\pi(X_3) &= (1, 0, \ldots, 0, 0).
\end{aligned}$$

   In this case we have $A = X_1 \cup X_2 \cup X_3 \notin \Gamma$, with $|A| = 2$ and $m = 3$, so the result $\rho^*(\Gamma) \leq 2/3$ holds.

   – If $(1, 0, \ldots, 0, 1) \in \pi(\Gamma)$, then the appropriate independent sequence is composed by subsets $B_1 \subset B_2$ and X_1, X_2 such that:

$$\begin{aligned}
\pi(B_1) &= (1, 0, \ldots, 0, 0),\\
\pi(X_1) &= (0, 0, \ldots, 0, 1),\\
\pi(B_2) &= (Y_1 - 1, Y_2, \ldots, Y_{K-1}, x_K - 1),\\
\pi(X_2) &= (1, 0, \ldots, 0, 0).
\end{aligned}$$

   Now we have $A = X_1 \cup X_2 \in \Gamma$, with $|A| = 2$ and $m = 2$, and so the result $\rho^*(\Gamma) \leq 2/3$ holds again.

2. In the second case, we assume for simplicity $i_* = 1$, and so we have $Y_1 > x_1 \geq 1$. Note that if $Y_1 = x_1 + 1$, then there must be another index j_* (for simplicity, $j_* = 2$) such that $Y_{j_*} > x_{j_*}$ (even if $x_{j_*} = 0$), because of the condition $Y_1 + \ldots + Y_{K-1} + x_K - 1 > x_1 + \ldots + x_K$. If this happens we can apply the first case, above, to $i_* = 1$ and $j_* = 2$; note that in the independent sequences above, $x_2 > 0$ is not assumed at any time.

   Therefore, we can concentrate on the situation where $Y_1 > x_1 + 1$. Again we consider two sub-cases, depending on whether the point $(1, 0, \ldots, 0, 1)$ is in $\pi(\Gamma)$ or not.

– If $(1,0,\ldots,0,1) \notin \pi(\Gamma)$, then we define an independent sequence with subsets $B_1 \subset B_2 \subset B_3$ and X_1, X_2, X_3 such that:

$$\begin{aligned}
\pi(B_1) &= (x_1 - 1, x_2, \ldots, x_{K-1}, x_K - 1),\\
\pi(X_1) &= (1, 0, \ldots, 0, 1),\\
\pi(B_2) &= (x_1, x_2, \ldots, x_{K-1}, x_K - 1),\\
\pi(X_2) &= (0, 0, \ldots, 0, 1),\\
\pi(B_3) &= (Y_1 - 1, Y_2, \ldots, Y_{K-1}, x_K - 1),\\
\pi(X_3) &= (1, 0, \ldots, 0, 0).
\end{aligned}$$

In this case we have $A = X_1 \cup X_2 \cup X_3 \notin \Gamma$, with $|A| = 2$ and $m = 3$, so the result $\rho^*(\Gamma) \leq 2/3$ holds.

– If $(1,0,\ldots,0,1) \in \pi(\Gamma)$, then we define an independent sequence with subsets $B_1 \subset B_2$ and X_1, X_2 such that:

$$\begin{aligned}
\pi(B_1) &= (1, 0, \ldots, 0, 0),\\
\pi(X_1) &= (0, 0, \ldots, 0, 1),\\
\pi(B_2) &= (Y_1 - 1, Y_2, \ldots, Y_{K-1}, x_K - 1),\\
\pi(X_2) &= (1, 0, \ldots, 0, 0).
\end{aligned}$$

Now we have $A = X_1 \cup X_2 \in \Gamma$, with $|A| = 2$ and $m = 2$, and so the result $\rho^*(\Gamma) \leq 2/3$ holds again. □

The following corollary is immediately derived from the result above.

Corollary 1. *Consider a K-multipartite access structure Γ and non-negative integers $x_1, \ldots, x_K, Y_1, \ldots, Y_{K-1}$ satisfying $x_K \geq 1$ and $Y_i \geq x_i$ for all $i = 1, \ldots, K-1$, such that $(x_1, \ldots, x_K) \in \pi(\Gamma_0)$ and $(Y_1, \ldots, Y_{K-1}, x_K - 1) \in \pi(\Gamma_0)$, and such that there exists at least one index $i_* \in \{1, \ldots, K-1\}$ such that $Y_{i_*} > x_{i_*} \geq 1$. If $Y_1 + \ldots + Y_{K-1} + x_K - 1 \neq x_1 + \ldots + x_K$ then $\rho^*(\Gamma) \leq 2/3$.*

4.1 Some Examples

In this section we show some simple examples of how the result of Theorem 4 can be used in practice to detect that a given multipartite access structure is not ideal. We are going to consider two tripartite access structures. Given such a tripartite access structure, one can first try to write it as one of the structures listed in the statement of Theorem 3; if this can be done, then the access structure will be ideal. Otherwise, one can suspect that the access structure may not be ideal, and so one can look for some of the prohibited positions described in the statements of Theorem 4 and Corollary 1, in order to conclude that the access structure is not ideal.

Let us first consider the tripartite access structure Γ defined by

$$\pi(\Gamma) = \{(x_1, x_2, x_3) : \; x_1 + x_2 + x_3 \geq 4 \; \wedge \; x_3 \geq 1\} \; \cup \; \{(x_1, x_2, x_3) : \; x_1 \geq 4\}.$$

We can apply the result of Theorem 4 to subsets represented by points $(x_1, x_2, x_3) = (2, 1, 1)$ and $(Y_1, Y_2, x_3 - 1) = (4, 1, 0)$. Note that in this case we have $i_* = 1$, because $Y_1 > x_1 \geq 1$. All the conditions stated in the Theorem are satisfied: $(x_1, x_2, x_3) \in \pi(\Gamma)$, $(Y_1, Y_2, x_3 - 1) \in \pi(\Gamma)$, $(Y_1 - 1, Y_2, x_3 - 1) = (3, 1, 0) \notin \pi(\Gamma)$ and $(x_1 - 1, x_2, x_3) = (1, 1, 1) \notin \pi(\Gamma)$. Therefore, we conclude that $\rho^*(\Gamma) \leq 2/3$ and so this access structure is not ideal.

In the second example, we take a different tripartite access structure Γ defined by

$$\pi(\Gamma) = \{(x_1, x_2, x_3) : \ x_1 + x_2 + x_3 \geq 6\} \cup \{(x_1, x_2, x_3) : \ x_2 + x_3 \geq 4 \wedge x_3 \geq 1\} \cup$$

$$\cup \ \{(x_1, x_2, x_3) : \ x_1 + x_2 \geq 5\}.$$

Again, it is possible to see that this access structure cannot be written as one of the ideal tripartite ones listed in the statement of Theorem 3. The following step would be then to look for a prohibited position on it. In effect, we can apply in this case Corollary 1 to subsets corresponding to points $(x_1, x_2, x_3) = (0, 3, 1)$ and $(Y_1, Y_2, x_3 - 1) = (1, 4, 0)$. These two points belong to $\pi(\Gamma_0)$ as required; furthermore, we have $Y_1 \geq x_1$ and $Y_2 > x_2 \geq 1$ (so $i_* = 2$). Therefore, we can apply the result of the corollary, to claim that this access structure cannot either be ideal, because $\rho^*(\Gamma) \leq 2/3$.

5 Conclusions and Future Work

In this work we have studied general multipartite access structures, where players are divided into K disjoint entities in such a way that players in an entity play all the same role in the access structure. To remark the importance of these structures, we have first shown that any access structure is a multipartite one. Then we have proved that three wide families of multipartite access structures are ideal, by showing in an existential way that a vector space secret sharing scheme realizing them can be constructed. The mathematical techniques employed in these proofs are quite general, and so we expect that other general families of multipartite access structure could be proved ideal in the future, by using similar ideas.

We have also proved a result (Theorem 4) which gives some necessary conditions on a multipartite access structure to be ideal. Other necessary conditions were already known [6]: if we define the slice of a K-multipartite structure Γ as

$$\Gamma^{(x_i = a_i)} = \{A \subset \mathcal{P} - X_i : A \cup A_i \in \Gamma\}$$

where $A_i \subset X_i$ with $|A_i| = a_i$, then $\Gamma^{(x_i = a_i)}$ is a $(K - 1)$-multipartite access structure over $\mathcal{P} - X_i$. It is not difficult to see that any slice of an ideal multipartite access structure must be also ideal. This gives a sort of recurrence, which ends at $K = 2$, because ideal bipartite access structures are completely characterized (see [11]). Using this idea, one could maybe prove some result such as:

$$\Gamma \text{ is ideal } \Leftrightarrow \ \Gamma \text{ satisfies condition } C \ \wedge \ \text{any slice of } \Gamma \text{ is ideal.}$$

The problem is, obviously, to find the proper condition C which makes this result true. To do this, possible tools to be used are independent sequences, geometric and algebraic arguments (as in the characterization of ideal bipartite structures in [11]), or the relation between matroids and ideal secret sharing (for example, this relation has been exploited in [10] for the case of bipartite access structures). We have the intuition that a good candidate for condition C is that, if Γ is a K-multipartite access structure, then $x_1 + \ldots + x_K = t$, for some constant positive integer t, and for all points $(x_1, \ldots, x_K) \in \pi(\Gamma_0)$ satisfying $x_i \geq 1$, for all $i = 1, \ldots, K$. But up to this moment we have not been able even to prove that this is a necessary condition for Γ to be ideal, for general values of K. This has been proved for the case $K = 3$, by Collins [6], and by ourselves in a different way. Summing up, there is a lot of work to do in the domain of multipartite access structures.

References

1. A. Beimel, T. Tassa and E. Weinreb. Characterizing ideal weighted threshold secret sharing. *Proceedings of TCC'05*, LNCS **3378**, Springer-Verlag, pp. 600–619 (2005).
2. G.R. Blakley. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference, American Federation of Information*, Processing Societies Proceedings, **48**, pp. 313–317 (1979).
3. C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology*, Vol. **8**, No. **1**, pp. 39–64 (1995).
4. C. Blundo, A. De Santis, L. Gargano, U. Vaccaro. Tight bounds on the information rate of secret sharing schemes. *Designs, Codes and Cryptography*, **11**, pp. 107–122 (1997).
5. E.F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, **9**, pp. 105–113 (1989).
6. M.J. Collins. A note on ideal tripartite access structures. Manuscript available at `http://eprint.iacr.org/2002/193/` (2002).
7. G. Di Crescenzo and C. Galdi. Hypergraph decomposition and secret sharing. *Proceedings of ISAAC'03*, LNCS **2906**, Springer-Verlag, pp. 645–654 (2003).
8. W.A. Jackson and K.M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, **9**, pp. 267–286 (1996).
9. P. Morillo, C. Padró, G. Sáez and J.L. Villar. Weighted threshold secret sharing schemes. *Information Processing Letters*, **70**, pp. 211–216 (1999).
10. S.L. Ng and M. Walker. On the composition of matroids and ideal secret sharing schemes. *Designs, Codes and Cryptography*, Vol. **24**, No. **1**, pp. 49–67 (2001).
11. C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, Vol. **46**, No. **7**, pp. 2596–2604 (2000).
12. A. Shamir. How to share a secret. *Communications of the ACM*, **22**, pp. 612–613 (1979).
13. G. J. Simmons, W. A. Jackson and K. M. Martin. The geometry of secret sharing schemes. *Bulletin of the ICA*, **1**, pp. 71–88 (1991).