On codes, matroids and secure multi-party computation from linear secret sharing schemes

Ronald Cramer* Vanesa Daza† Ignacio Gracia†
Jorge Jiménez Urroz† Gregor Leander‡ Jaume Martí-Farré†
Carles Padró†

September 23, 2004

Abstract

Error correcting codes and matroids have been widely used in the study of ordinary secret sharing schemes. In this paper, we study the connections between codes, matroids and a special class of secret sharing schemes, namely multiplicative linear secret sharing schemes (LSSSs). Such schemes are known to enable multi-party computation protocols secure against general (non-threshold) adversaries.

Two open problems related to the complexity of multiplicative LSSSs are considered in this paper.

The first one is to determine for which ideal $\mathcal{Q}_2$ access structures there exists an ideal multiplicative LSSS. To determine whether all self-dual vector space access structures are in this situation is an open problem we state in this paper. By the aforementioned connection, this in fact constitutes an open problem about matroid theory, since it can be re-stated in terms of representability of identically self-dual matroids by self-dual codes. We introduce a new concept, the flat-partition, that provides a useful classification of identically self-dual matroids. Uniform identically self-dual matroids, which are known to be representable by self-dual codes, form one of the classes. We prove that this property also holds for the family of matroids that, in a natural way, is the next class in the above classification: the identically self-dual bipartite matroids.

The second one deals with strongly multiplicative LSSSs. As opposed to the case of multiplicative LSSSs, it is not known whether there is an efficient method to transform an LSSS into a strongly multiplicative LSSS for the same access structure with a polynomial increase of the complexity. We prove a property of strongly multiplicative LSSSs that could be useful in solving this problem. Namely, using a suitable generalization of the well-known Berlekamp-Welch decoder, we show that all strongly multiplicative LSSSs enable efficient reconstruction of a shared secret in the presence of malicious faults.

Keywords: multi-party computation, multiplicative linear secret sharing schemes, identically self-dual matroids, self-dual codes, efficient error correction.

*CWI, Amsterdam & Mathematical Institute, Leiden University. cramer@cwi.nl

†Dept. of Applied Maths. IV, Technical University of Catalonia, Barcelona. {vdaza, ignacio, jjimenez, jaumem, matcpl}@ma4.upc.es

‡Maths. Dept., Ruhr-University Bochum. leander@itsc.ruhr-uni-bochum.de

1 Introduction

Two open problems on multiplicative linear secret sharing schemes are studied in this paper. Our results deal with the connections between linear codes, representable matroids and linear secret sharing schemes. Some Matroid Theory definitions are given in Section 3.1. The reader is referred to [23] for a general reference on this subject and to [4, 30, 29, 20] for more information about the relation between ideal secret sharing schemes and matroids.

Let $\mathcal{C}$ be a $[n+1, d]$-linear code over a finite field $\mathbb{K}$ and let M be a generator matrix of $\mathcal{C}$. Recall that M is a $d \times (n+1)$ matrix whose rows span the d-dimensional subspace $\mathcal{C} \subset \mathbb{K}^{n+1}$. The columns of M define a $\mathbb{K}$-representable matroid $\mathcal{M}$ on the set of points $Q = \{1, \ldots, n, n+1\}$. This matroid depends only on the code $\mathcal{C}$, that is, it does not depend on the choice of the generator matrix M. In this situation, we say that $\mathcal{M}$ is the matroid associated to the code $\mathcal{C}$ and also that the code $\mathcal{C}$ is a representation of the matroid $\mathcal{M}$. Several results on this relation between matroids and codes are given in [1, 5, 6] and other works.

Besides, the code $\mathcal{C}$ defines an ideal secret sharing scheme Σ_i for every $i \in Q$. Every codeword $(k_1, \ldots, k_i, \ldots, k_{n+1}) \in \mathcal{C}$ can be seen as a distribution of shares for the secret value $k_i \in \mathbb{K}$ between the players in $P_i = Q \backslash \{i\}$. A subset $A \subset P_i$ is a minimal qualified subset in the access structure of Σ_i if and only if $A \cup \{i\}$ is a circuit of the matroid $\mathcal{M}$. Therefore, the access structures of the schemes Σ_i are determined by the matroid $\mathcal{M}$. Any scheme defined in this way is called a $\mathbb{K}$-*vector space secret sharing scheme* and the access structure of such a scheme is called a $\mathbb{K}$-*vector space access structure*. These schemes were first considered in [3]. That connection between linear codes and secret sharing schemes has been considered in [19, 11].

The matroid $\mathcal{M}$ associated to a self-dual code is identically self-dual. Nevertheless, it is not known whether every representable identically self-dual matroid can by represented by a self-dual code. This is one of the open problems that are considered in this paper. Besides its theoretical interest, the relevance of this problem is mainly due to the fact that it is equivalent to an open problem on multiplicative linear secret sharing schemes. These schemes are a fundamental tool in general secure multi-party computation.

In a *linear secret sharing scheme* (LSSS) on the set of players $P = \{1, \ldots, n\}$, the share of every player $i \in P$ is a vector in a vector space E_i of finite dimension over a finite field $\mathbb{K}$, and is computed as a fixed linear function of the secret value $k \in \mathbb{K}$ and some random elements in $\mathbb{K}$. Observe that vector space secret sharing schemes are linear.

Linear secret sharing schemes are usually defined in a more general way by taking as the set of secrets a vector space not necessarily equal to $\mathbb{K}$. We do not need to consider such LSSSs in this paper. Therefore, in this paper, the ideal LSSSs coincide with the vector space secret sharing schemes.

The *complexity* of a LSSS Σ is defined as $\lambda(\Sigma) = \sum_{i=1}^{n} \dim E_i$, which corresponds to the total number of field elements that are distributed. Observe that $\lambda(\Sigma) \geq n$. For any finite field $\mathbb{K}$ and for any access structure Γ, there exists a $\mathbb{K}$-LSSS for Γ [14]. For an access structure Γ and a finite field $\mathbb{K}$, we define $\lambda_{\mathbb{K}}(\Gamma) = \min(\lambda(\Sigma))$, where the

minimum is taken over all $\mathbb{K}$-LSSSs with access structure Γ. Of course, Γ is a $\mathbb{K}$-vector space access structure if and only if $\lambda_{\mathbb{K}}(\Gamma) = n$.

The set of all possible distributions of shares $(k_1, \ldots, k_n, k)$ according to a $\mathbb{K}$-LSSS Σ is a subspace $\mathcal{C} \subset E_1 \times \cdots \times E_n \times \mathbb{K}$. This subspace can be seen as a $[\lambda(\Sigma)+1, d]$-linear code. Since $\mathcal{C}$ defines an ideal LSSS on a set of $\lambda(\Sigma)$ players, any LSSS can be seen as an ideal LSSS by changing the set of players.

Linear secret sharing schemes were first considered, only in the ideal case, in [3]. General Linear secret sharing schemes were introduced by Simmons [28], Jackson and Martin [15] and Karchmer and Wigderson [16] under other names such as geometric secret sharing schemes or monotone span programs.

In a LSSS, any linear combination of the shares of different secrets results in shares for the same linear combination of the secret values. Because of that, LSSSs are used as a building block of multi-party computation protocols. Nevertheless, if we require protocols computing any arithmetic circuit, a similar property is needed for the multiplication of two secrets, that is, the LSSS must be *multiplicative*.

We illustrate the multiplicative property of LSSSs by analyzing the Shamir's (d, n)-threshold scheme [27], which is an ideal LSSS. In this scheme, the secret $k \in \mathbb{K}$ and the shares $k_i \in \mathbb{K}$, where $i = 1, \ldots, n$, are the values of a random polynomial with degree at most $d-1$ in some given points. The secret is recovered by Lagrange interpolation. If $n \geq 2d-1$, the product kk' of the two secret values is a linear combination of any $2d-1$ values $c_i = k_i k'_i$. This linear combination is obtained by interpolating the product of the two random polynomials that were used to distribute the shares. This multiplicative property of the Shamir's scheme is used in [12, 2, 8, 7] to construct multi-party computation protocols that are secure against a threshold-based adversary.

In order to obtain efficient multi-party computation protocols for a general adversary structure, a generalization of the multiplicative property of the Shamir's scheme to any linear secret sharing scheme is proposed in [9].

Specifically, a linear secret sharing scheme over the finite field $\mathbb{K}$ is said to be *multiplicative* if every player $i \in P$ can compute, from his shares k_i, k'_i of two shared secrets $k, k' \in \mathbb{K}$, a value $c_i \in \mathbb{K}$ such that the product kk' is a linear combination of all the values $c_1, \ldots, c_n$. We say that a secret sharing scheme is *strongly multiplicative* if, for any subset $A \subset P$ such that $P \setminus A$ is not qualified, the product kk' can be computed using only values from the players in A.

Observe that the Shamir's (d, n)-secret sharing scheme is multiplicative if and only if $n \geq 2d-1$ and it is strongly multiplicative if and only if $n \geq 3d-2$. In general, as a consequence of the results in [13, 9], an access structure Γ can be realized by a (strongly) multiplicative LSSS if and only if it is $\mathcal{Q}_2$ ($\mathcal{Q}_3$), that is, if and only if the set of players is not the union of any two (three) unqualified subsets.

Cramer, Damgård and Maurer [9] presented a method to construct, from any $\mathbb{K}$-MLSSS Σ with $\mathcal{Q}_2$ access structure Γ, a multi-party computation protocol secure against a passive adversary which is able to corrupt any set of players $B \notin \Gamma$ and computing any arithmetic circuit C over $\mathbb{K}$. The complexity of this protocol is polynomial in the size of C, $\log |\mathbb{K}|$ and $\lambda(\Sigma)$. They prove a similar result for an active adversary. In this case, the resulting protocol is perfect with zero error probability if the LSSS is strongly multiplicative, with a $\mathcal{Q}_3$ access structure Γ.

One of the key results in [9] is a method to construct, from any $\mathbb{K}$-LSSS Σ with $\mathcal{Q}_2$ access structure Γ, a multiplicative $\mathbb{K}$-LSSS Σ' with the same access structure and complexity $\lambda(\Sigma') = 2\lambda(\Sigma)$. That is, if $\mu_{\mathbb{K}}(\Gamma)$ denotes the minimum complexity of all $\mathbb{K}$-MLSSSs with access structure Γ, the above result means that $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ for any finite field $\mathbb{K}$ and for any $\mathcal{Q}_2$ access structure Γ.

Therefore, in the passive adversary case, the construction of efficient multi-party computation protocols can be reduced to the search of efficient linear secret sharing schemes.

This is not the situation when an active adversary is considered, because it is not known whether it is possible to construct, for any $\mathcal{Q}_3$ access structure Γ, a strongly multiplicative LSSS whose complexity is polynomial on the complexity of the best LSSS for Γ.

2 Our Results

Two open problems are studied in this work. The first one is to determine the cases in which the factor 2 loss in the construction of MLSSSs is necessary, that is, to find out in which situations the bound $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ can be improved. For instance, if $n \geq 2d-1$ and Γ is the (d,n)-threshold structure, then $\mu_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma) = n$ for any finite field $\mathbb{K}$ with $|\mathbb{K}| > n$.

The second one deals with the strongly multiplicative case. As we said before, no efficient general reductions are known for it at all, except for some upper bounds on the minimal complexity of strongly multiplicative LSSSs in terms of certain threshold circuits. That is, the existence of a transformation that renders an LSSS strongly multiplicative at the cost of increasing its complexity at most polynomially is an unsolved question.

2.1 On the complexity of multiplicative linear secret sharing schemes

We study this problem in the ideal case, that is, we consider only access structures with $\lambda_{\mathbb{K}}(\Gamma) = n$ for some finite field $\mathbb{K}$. Specifically, we are interested in determining the $\mathcal{Q}_2$ access structures such that there exists a finite field $\mathbb{K}$ with $\mu_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma) = n$. In other words, we are trying to find out which $\mathcal{Q}_2$ vector space access structures can be realized by an ideal MLSSS.

Examples of access structures in this situation are obtained from self-dual codes. If $\mathcal{C}$ is a self-dual $[n+1, d]$-linear code over the finite field $\mathbb{K}$, all $\mathbb{K}$-vector space secret sharing schemes Σ_i, where $i \in Q$, are multiplicative. Then, $\mu_{\mathbb{K}}(\Gamma_i) = \lambda_{\mathbb{K}}(\Gamma_i) = n$, where Γ_i is the $\mathbb{K}$-vector space access structure corresponding to the scheme Σ_i.

On the other hand, we present in Example 9 a $\mathcal{Q}_2$ access structure Γ such that $\lambda_{\mathbb{K}}(\Gamma) = n$ for any finite field with characteristic greater than 3 while it does not admit any ideal MLSSS.

Self-dual access structures coincide with the *minimally* $\mathcal{Q}_2$ access structures, that is, with the $\mathcal{Q}_2$ access structures Γ such that any substructure $\Gamma' \subsetneq \Gamma$, on the same set of players, is not $\mathcal{Q}_2$. The results in this paper lead us to believe that any self-dual vector space access structure can be realized by an ideal multiplicative linear secret

sharing scheme and, hence, to state the following open problem. One of the goals of this paper is to move forward in the search of its solution.

Question 1. To determine whether there exists, for any self-dual $\mathbb{K}$-vector space access structure Γ, an ideal multiplicative $\mathbb{L}$-LSSS, being the finite field $\mathbb{L}$ an algebraic extension of $\mathbb{K}$.

Since $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ for any $\mathcal{Q}_2$ access structure Γ, to study this open problem seems to have a limited practical interest. Nevertheless, its theoretical interest can be justified by several reasons.

First, due to the minimality of the $\mathcal{Q}_2$ property, self-dual access structures are an extremal case in the theory of MLSSSs. Moreover, self-duality seems to be in the core of the multiplicative property. For instance, we prove in Section 3.6 that the construction in [9] providing the bound $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ is related to self-dual codes and, hence, to ideal MLSSSs for self-dual access structures.

Besides, we think that the results and techniques in this paper provide a better understanding of the multiplicative property and may be useful in the future to find new results on the existence of efficient strongly multiplicative LSSSs.

Finally, the interest of that problem is increased by the fact that, as we pointed out before, it can be stated in terms of an interesting open problem about the relation between Matroid Theory and Code Theory. Namely, by studying how the connection between codes, matroids and LSSSs applies to multiplicative LSSSs, we prove that Question 1 is equivalent to the following one.

Question 2. To determine whether every identically self-dual $\mathbb{K}$-representable matroid can be represented by a self-dual linear code over some finite field $\mathbb{L}$, an algebraic extension of $\mathbb{K}$.

We say that a matroid is *self-dually $\mathbb{K}$-representable* if it can be represented by a self-dual code over the finite field $\mathbb{K}$. Any self-dually representable matroid is identically self-dual and representable. The open problem we consider here is to decide whether the reciprocal of this fact is true.

The uniform matroids $U_{d,n}$ and the $\mathbb{Z}_2$-representable matroids are are the only families of matroids for which it is known that all identically self-dual matroids are self-dually representable.

There exist several methods to combine some given matroids into a new one. The *sum*, which is defined in Section 4, is one of them. We prove in Section 4 that the study of the above problem can be restricted to indecomposable matroids, that is, matroids that are not a non-trivial sum of two other matroids.

In order to take the first steps in solving Question 2, we introduce the concept of *flat-partition* of a matroid, which is defined in Section 4.

On one hand, we use the flat-partitions to characterize in Theorem 17 the indecomposable identically self-dual matroids.

On the other hand, the number of flat-partitions provide a useful classification of identically self-dual matroids. The identically self-dual matroids that do not admit any flat-partition are exactly the uniform matroids $U_{d,2d}$, which are self-dually representable.

One of the main results in this paper is to prove that the identically self-dual matroids with exactly one flat-partition are self-dually representable as well. These matroids are precisely the identically self-dual *bipartite* matroids. In a *bipartite matroid*, the set of points is divided in two parts and all points in each part are symmetrical. The access structures defined by these matroids are among the *bipartite access structures*, which were introduced in [24]. Bipartite matroids have been independently studied in [22, 21], where they are called *matroids with two uniform components*.

Theorem 3. *Let $\mathcal{M}$ be an identically self-dual bipartite matroid. Then, $\mathcal{M}$ can be represented by a self-dual linear code over some finite field $\mathbb{K}$. Equivalently, every self-dual bipartite vector space access structure can be realized by an ideal MLSSS over some finite field $\mathbb{K}$.*

Therefore, the bipartite matroids form another family of matroids for which all identically self-dual matroids are self-dually representable. Most of the identically self-dual matroids in this family are indecomposable. So, the existence of self-dual codes that represent them could not be derived from other matroids that were known to be self-dually representable.

2.2 On strongly multiplicative linear secret sharing schemes

By proving a new property of multiplicative LSSSs, we shed some light on the second problem, that is, whether there exists a transformation that renders an LSSS strongly multiplicative at the cost of increasing its complexity at most polynomially.

Using a suitable generalization of the well-known Berlekamp-Welch decoder for Reed-Solomon codes, we show that all strongly multiplicative LSSSs allow for efficient reconstruction of a shared secret in the presence of malicious faults. In this way, we find an interesting connection between the problem of the strong multiplication in LSSSs and the existence of codes with efficient decoding algorithms.

Theorem 4. *(*informal statement*) Let $\mathbf{s}$ be a full vector of shares for a secret s, computed according to a strongly multiplicative LSSS over a finite field $\mathbb{K}$, with access structure Γ on n players. Let $\mathbf{e}$ denote the all zero vector, except where it states the errors that a set of players $A \notin \Gamma$ have introduced in their respective shares. Define $\mathbf{c} = \mathbf{s} + \mathbf{e}$. Then the secret s can be recovered from $\mathbf{c}$ in time poly$(n, \log |\mathbb{K}|)$.*

2.3 Organization of the paper

Some definitions and basic facts on LSSSs, linear codes and matroids, as well as the notation we use in the paper, are given in Section 3. Besides, we study in that section the relation between MLSSSs, self-dual codes and identically self-dual matroids and prove the equivalence between Questions 1 and 2. Some results about the sum of matroids are given in Section 4, where we prove inthat the study of Question 2 can be restricted to indecomposable matroids. Besides, a characterization of indecomposable identically self-dual matroids in terms of their flat-partitions is presented. Some properties of identically self-dual bipartite matroids and the proof of Theorem 3 are given in Section 5. Theorem 4 is proved in Section 6.

3 Ideal multiplicative linear secret sharing shemes, self-dual linear codes and identically self-dual matroids

Some facts about the relation between linear codes, representable matroids and ideal linear secret sharing schemes are recalled in this section. We study this relation for ideal multiplicative LSSSs and we prove the equivalence between Question 1 and Question 2. The reader is referred to [23] for a general reference on Matroid Theory and to [4, 30] for more information about the relation between ideal secret sharing schemes and matroids.

3.1 Matroid Theory definitions

Let E be a $\mathbb{K}$-vector space and $Q = \{\mathbf{v}_1, \ldots, \mathbf{v}_{n+1}\} \subset E$ a finite set of vectors. The subsets of Q can be linearly independent or dependent, every subset spans a subspace of E with a certain dimension and some of them are basis of the subspace spanned by Q. A matroid is an abstraction of these concepts. Several axioms that fit in the situation above are given to define the matroids on a set of points $Q = \{1, \ldots, n, n+1\}$. See [23] for a general reference on Matroid Theory.

There exist many different equivalent definitions of matroid. The one we present here is based on the concept of *basis*.

Definition 5. A *matroid* $\mathcal{M}$ is a finite set Q together with a family $\mathcal{B}$ of subsets of Q such that:

1. $\mathcal{B}$ is nonempty,
2. if $B_1, B_2 \in \mathcal{B}$ and $B_1 \subset B_2$, then $B_1 = B_2$, and
3. for any $B_1, B_2 \in \mathcal{B}$ and $i \in B_1 \backslash B_2$, there exists $j \in B_2 \backslash B_1$ such that $(B_1 \backslash \{i\}) \cup \{j\}$ is in $\mathcal{B}$.

The set Q is the *set of points* of the matroid $\mathcal{M}$ and the sets in $\mathcal{B}$ are called the *basis* of $\mathcal{M}$. All sets in $\mathcal{B}$ have the same number of elements, which is the *dimension* of $\mathcal{M}$.

A subset $X \subset Q$ is said to be *independent* if there exists a basis $B \in \mathcal{B}$ with $X \subset B$. The *dependent* subsets are those that are not independent. A *circuit* is a minimally dependent subset and the maximally independent subsets coincide with the bases. The *rank* of $X \subset Q$ is the maximum cardinality of the subsets of X that are independent.

We say that $X \subset Q$ is a *flat* if $\mathrm{rank}(X \cup \{i\}) > \mathrm{rank}(X)$ for every $i \notin X$. The flat $\langle X \rangle = \{i \in Q : \mathrm{rank}(X \cup \{i\}) = \mathrm{rank}(X)\}$ is called the *flat spanned by* X. If X is a flat, any maximally independent subset $B \subset X$ is called a *basis* of the flat X.

If $\mathcal{M}$ is a matroid on the set Q, with family of bases $\mathcal{B}$, then $\mathcal{B}^* = \{Q \setminus B : B \in \mathcal{B}\}$ is the family of bases of a matroid $\mathcal{M}^*$ on the set Q, which is called the *dual* of $\mathcal{M}$. A *self-dual* matroid is isomorphic to its dual while an *identically self-dual* matroid is *equal* to its dual.

Let $\mathbb{K}$ be a finite field and M be a $d \times (n+1)$ matrix with entries in $\mathbb{K}$. A matroid $\mathcal{M}$ on the set $Q = \{1, \ldots, n, n+1\}$ is defined from the matrix M by considering that a subset $X = \{i_1, \ldots, i_r\} \subset Q$ is independent if and only if the corresponding columns

of M are linearly independent. In this situation, we say that the matrix M is a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. The matroids that can be defined in this way are called *representable*.

3.2 Ideal linear secret sharing schemes, linear codes and matroids

Let us take $Q = \{1, \ldots, n, n+1\}$ and $P_i = Q \setminus \{i\}$ for any $i \in Q$. This notation will be used all through the paper. Any sequence $\Pi = (\pi_1, \ldots, \pi_n, \pi_{n+1})$ of surjective linear mappings $\pi_i : E \to E_i$, where E and E_i are vector spaces of finite dimension over a finite field $\mathbb{K}$ and $E_{n+1} = \mathbb{K}$, defines a $\mathbb{K}$-*linear secret sharing scheme* ($\mathbb{K}$-LSSS) $\Sigma_{n+1}(\Pi)$ on the set of players $P_{n+1} = \{1, \ldots, n\}$. For any vector $\mathbf{x} \in E$, the values $(\pi_i(\mathbf{x}))_{1 \le i \le n}$ are shares of the secret value $k = \pi_{n+1}(\mathbf{x}) \in \mathbb{K}$. The access structure $\Gamma_{n+1}(\Pi)$ of this scheme consists of all subsets $A \subset P_{n+1}$ such that $\bigcap_{i \in A} \ker \pi_i \subset \ker \pi_{n+1}$. The *complexity* of the linear scheme $\Sigma_{n+1}(\Pi)$ is defined by $\lambda(\Sigma) = \sum_{i=1}^{n} \dim E_i$. We notate $\lambda_{\mathbb{K}}(\Gamma)$ for the minimum complexity of the LSSSs with access structure Γ.

If $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ is an *ideal* $\mathbb{K}$-LSSS, that is, if it has minimum complexity $\lambda(\Sigma) = n$, then $E_i = \mathbb{K}$ for every $i \in Q$. In this case, the linear mappings π_i are non-zero vectors in the dual space E^*. We are going to suppose always that the space E^* is spanned by the vectors $\pi_1, \ldots, \pi_n, \pi_{n+1}$. Let $\Pi \colon E \to \mathbb{K}^{n+1}$ be the linear mapping defined by $\Pi(\mathbf{x}) = (\pi_1(\mathbf{x}), \ldots, \pi_n(\mathbf{x}), \pi_{n+1}(\mathbf{x}))$. For every $i \in Q$, we obtain an ideal LSSS $\Sigma_i(\Pi)$ with access structure $\Gamma_i(\Pi)$ on the set of players P_i by taking the values $(\pi_j(\mathbf{x}))_{j \in P_i}$ as shares of the secret $\pi_i(\mathbf{x})$. Observe that a subset $A \subset P_i$ is in $\Gamma_i(\Pi)$ if and only if $\pi_i \in \langle \pi_j \,:\, j \in A \rangle$. The access structures that can be defined in this way are called $\mathbb{K}$-*vector space access structures*. Observe that an access structure Γ is a $\mathbb{K}$-vector space access structure if and only if $\lambda_{\mathbb{K}}(\Gamma) = n$.

From now on, vectors appearing in matrix operations will be considered as one-row matrices. Let us put $d = \dim E$. Once a basis of E is fixed, we can represent the linear mapping $\Pi \colon E \to \mathbb{K}^{n+1}$ by the $d \times (n+1)$ matrix $M = M(\Pi)$ such that $\Pi(\mathbf{x}) = \mathbf{x}M$, for all $\mathbf{x} \in E$, where the vector $\mathbf{x}$ is expressed as a row. Observe that $\operatorname{rank}(M) = d$ and that the i-th column of M corresponds to the linear form π_i. The matrix M can be seen as a generator matrix for the $[n+1, d]$-linear code $\mathcal{C}(\Pi) = \Pi(E) \subset \mathbb{K}^{n+1}$. The codewords in $\mathcal{C}(\Pi)$, which are the vectors in the subspace spanned by the rows of M, are exactly all possible distributions of shares according to any of the LSSSs $\Sigma_i(\Pi)$. Besides, the matrix M is a representation of a $\mathbb{K}$-representable matroid $\mathcal{M}(\Pi)$ on the set Q, which is the matroid associated to the code $\mathcal{C}(\Pi)$. The access structures $\Gamma_i(\Pi)$ are determined by the matroid $\mathcal{M}(\Pi)$: the minimal qualified subsets of $\Gamma_i(\Pi)$ are exactly the subsets $A \subset P_i$ such that $A \cup \{i\}$ is a circuit of $\mathcal{M}(\Pi)$. We notate $\Gamma_i(\mathcal{M})$ for the access structure on the set P_i defined in this way from the matroid $\mathcal{M}$.

A matroid is said to be *connected* if any two points lie on a common circuit. An access structure Γ on a set of players P is *connected* if every player is in a minimal qualified subset. The access structure $\Gamma_{n+1}(\mathcal{M})$ is connected if and only if the matroid $\mathcal{M}$ is connected. In this case, all access structures $\Gamma_i(\mathcal{M})$, where $i \in Q$, are connected. A connected matroid is determined by the circuits through a single point. Then, if $\mathcal{M}$ is connected, it is univocally determined by the access structure $\Gamma_{n+1}(\mathcal{M})$. Therefore, if Γ is a connected access structure with $\Gamma = \Gamma_{n+1}(\Pi) = \Gamma_{n+1}(\Pi')$, the matroids $\mathcal{M}(\Pi)$

and $\mathcal{M}(\Pi')$ are identical and, hence, $\Gamma_i(\Pi) = \Gamma_i(\Pi')$ for every $i \in Q$.

Let N be a parity check matrix for the code $\mathcal{C}(\Pi)$. That is, N is a $(n-d+1)\times(n+1)$ matrix with $\mathrm{rank}(N) = n-d+1$ and $MN^\top = 0$, where $N^\top$ denotes the transpose of N. The rows of N span the subspace $\mathcal{C}(\Pi)^\perp \subset \mathbb{K}^{n+1}$, orthogonal to $\mathcal{C}(\Pi)$. The matrix N can be seen as a generator matrix of the $[n+1, n-d+1]$-linear code $\mathcal{C}(\Pi)^\perp$. This code is called the *dual code* of the code $\mathcal{C}(\Pi)$. A $[n+1, d]$-linear code $\mathcal{C}$ is said to be *self-dual* if $\mathcal{C}^\perp = \mathcal{C}$. In this case, $2d = n+1$ and a generator matrix M is also a parity check matrix, that is, $MM^\top = 0$. We say that a linear code $\mathcal{C}$ with generator matrix M is *almost self-dual* if there exists a non-singular diagonal matrix $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n, \lambda_{n+1})$ such that MD is a parity check matrix.

The *dual matroid* of the matroid $\mathcal{M}$ is the matroid $\mathcal{M}^*$ whose family of bases is $\mathcal{B}(\mathcal{M}^*) = \{B \subset Q : Q \setminus B \in \mathcal{B}(\mathcal{M})\}$, where $\mathcal{B}(\mathcal{M})$ is the family of bases of $\mathcal{M}$. A matroid is said to be *self-dual* if it is *isomorphic* to its dual and is said to be *identically self-dual* if it is *equal* to its dual.

Let Γ be an access structure on the set of participants P. The *dual* Γ^* of the access structure Γ is defined as $\Gamma^* = \{A \subset P : P \setminus A \notin \Gamma\}$. An access structure Γ is said to be *self-dual* if $\Gamma^* = \Gamma$. It is not difficult to check that an access structure is $\mathcal{Q}_2$ if and only if $\Gamma^* \subset \Gamma$ and that the minimally $\mathcal{Q}_2$ access structures coincide with the self-dual ones.

If $\mathcal{M}$ and $\mathcal{N}$ are the matroids associated, respectively, to a $[n+1, d]$-linear code $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$, then $\mathcal{N} = \mathcal{M}^*$. Besides, for any $i \in Q$, if Γ_i and Γ'_i are the access structures on the set P_i that are determined, respectively, by the matroids $\mathcal{M}$ and $\mathcal{M}^*$, then $\Gamma'_i = \Gamma_i^*$. Therefore, the dual of a $\mathbb{K}$-representable matroid is also $\mathbb{K}$-representable and the same applies to $\mathbb{K}$-vector space access structures. In fact, a more general result is known: $\lambda_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma^*)$ for any access structure Γ [15, 10].

If D is a $(n+1)\times(n+1)$ non-singular diagonal matrix, the columns of the matrices M and MD define the same matroid. Then, the matroid associated to an almost self-dual code is identically self-dual. Besides, the access structures $\Gamma_i(\mathcal{M})$ that are obtained from an identically self-dual matroid $\mathcal{M}$ are self-dual. Therefore, if a connected $\mathbb{K}$-vector space access structure $\Gamma_{n+1}(\Pi)$ is self-dual, all access structures $\Gamma_i(\Pi)$ are also self-dual and, in particular, $\mathcal{Q}_2$.

3.3 Multiplicative linear secret sharing schemes

Some definitions and basic results about multiplicative linear secret sharing schemes are given in the following.

We begin by recalling some notation and elementary facts about bilinear forms. If $\alpha, \beta \colon E \to \mathbb{K}$ are linear forms, $\alpha \otimes \beta$ denotes the bilinear form $\alpha \otimes \beta \colon E \times E \to \mathbb{K}$ defined by $(\alpha \otimes \beta)(\mathbf{x}, \mathbf{y}) = \alpha(\mathbf{x})\beta(\mathbf{y})$. These bilinear forms span the vector space of all bilinear forms on E, which is denoted by $E^* \otimes E^*$ and has dimension d^2, where $d = \dim E$. Actually, if $\{\mathbf{e}^1, \ldots, \mathbf{e}^d\}$ is a basis of E^*, then $\{\mathbf{e}^i \otimes \mathbf{e}^j : 1 \le i, j \le d\}$ is a basis of $E^* \otimes E^*$. Since $E^{**} = E$, the vector space of the bilinear forms on E^* is $E \otimes E$, which is spanned by $\{\mathbf{x} \otimes \mathbf{y} : \mathbf{x}, \mathbf{y} \in E\}$. Finally, observe that $(E \otimes E)^* = E^* \otimes E^*$. This is due to the fact that any bilinear form $\alpha \otimes \beta \in E^* \otimes E^*$ induces a linear form $\alpha \otimes \beta \colon E \otimes E \to \mathbb{K}$, determined by $(\alpha \otimes \beta)(\mathbf{x} \otimes \mathbf{y}) = \alpha(\mathbf{x})\beta(\mathbf{y})$.

The next two definitions deal with general (not necessarily ideal) LSSSs.

Definition 6. Let $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a $\mathbb{K}$-LSSS. The scheme Σ is said to be *multiplicative* if, for every $i \in P_{n+1} = \{1, \ldots, n\}$, there exists a bilinear form $\phi_i \colon E_i \times E_i \to \mathbb{K}$ such that $(\pi_{n+1} \otimes \pi_{n+1})(\mathbf{x}_1, \mathbf{x}_2) = \sum_{i=1}^{n} \phi_i(\pi_i(\mathbf{x}_1), \pi_i(\mathbf{x}_2))$ for any pair of vectors $\mathbf{x}_1, \mathbf{x}_2 \in E$.

If $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ is an LSSS and $A \subset P_{n+1}$, we notate Σ_A for the natural restriction of Σ to the players in A, that is, the scheme defined by the linear mappings $((\pi_i)_{i \in A}, \pi_{n+1})$.

Definition 7. Let $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a $\mathbb{K}$-LSSS with access structure Γ. We say that Σ is *strongly multiplicative* if the scheme $\Sigma_{P_{n+1} \setminus A}$ is multiplicative for every $A \subset P_{n+1}$ with $A \notin \Gamma$.

It is not difficult to check that the access structure of a multiplicative LSSS must be $\mathcal{Q}_2$. Equally, strongly multiplicative LSSSs only exist for $\mathcal{Q}_3$ access structures.

Let $\Sigma = \Sigma_{n+1}(\Pi)$ be an ideal LSSS. Every bilinear form $\phi \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ can be defined by $\phi(x, y) = \lambda xy$ for some $\lambda \in \mathbb{K}$. Therefore, Σ is multiplicative if and only if there exist values $\lambda_i \in \mathbb{K}$ such that $\pi_{n+1} \otimes \pi_{n+1} = \sum_{i=1}^{n} \lambda_i (\pi_i \otimes \pi_i)$. Equally, Σ is strongly multiplicative if and only if, for every $A \notin \Gamma_{n+1}(\Pi)$, there exist values $\lambda_{i,A} \in \mathbb{K}$ such that $\pi_{n+1} \otimes \pi_{n+1} = \sum_{i \in P_{n+1} \setminus A} \lambda_{i,A} (\pi_i \otimes \pi_i)$. The values λ_i or $\lambda_{i,A}$ form the *recombination vector* introduced in [9].

Since the bilinear forms $\pi_i \otimes \pi_i$ can be seen as vectors in $(E \otimes E)^*$, we can consider the LSSS $\Sigma^{\mu}_{n+1}(\Pi) = \Sigma_{n+1}(\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1})$, which has access structure $\Gamma^{\mu}_{n+1}(\Pi) = \Gamma_{n+1}(\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1})$. That is, $A \in \Gamma^{\mu}_{n+1}(\Pi)$ if and only if $\pi_{n+1} \otimes \pi_{n+1}$ is a linear combination of the vectors $\{\pi_i \otimes \pi_i \, : \, i \in A\}$.

Lemma 8. *Let $\Sigma = \Sigma_{n+1}(\Pi)$ be an ideal LSSS. Then, the following properties hold.*

1. $\Gamma^{\mu}_{n+1}(\Pi) \subset \Gamma_{n+1}(\Pi)$.
2. *Σ is multiplicative if and only if $\Gamma^{\mu}_{n+1}(\Pi) \neq \emptyset$.*
3. *Σ is strongly multiplicative if and only if $(\Gamma_{n+1}(\Pi))^* \subset \Gamma^{\mu}_{n+1}(\Pi)$.*

Proof: Let $A \subset P_{n+1}$ be a subset with $A \in \Gamma^{\mu}_{n+1}(\Pi)$. Then there exist $\lambda_i \in \mathbb{K}$ such that $\pi_{n+1} \otimes \pi_{n+1} = \sum_{i \in A} \lambda_i (\pi_i \otimes \pi_i)$. By taking a vector $\mathbf{x} \in E$ with $\pi_{n+1}(\mathbf{x}) = 1$, we obtain values $\lambda'_i \in \mathbb{K}$ such that $\pi_{n+1} = \sum_{i \in A} \lambda'_i \pi_i$, which implies that $A \in \Gamma_{n+1}(\Pi)$. The other statements follow from the previous observations. □

We present next an example of a $\mathcal{Q}_2$ (but not self-dual) vector space access structure $\Gamma_{n+1}(\Pi)$ that does not admit any ideal MLSSS. The proof exploits the fact that not all the access structures $\Gamma_i(\Pi)$ are $\mathcal{Q}_2$. Observe that this is not the case if the access structure $\Gamma_{n+1}(\Pi)$ is self-dual.

Example 9. We present a $\mathcal{Q}_2$ vector space access structure that does not admit an ideal MLSSS. Let Γ be the access structure on the set of participants $P_6 = \{1, 2, 3, 4, 5\}$

with minimal qualified subsets $\{\{1,2\},\{3,4\},\{1,3,5\},\{1,4,5\},\{2,3,5\},\{2,4,5\}\}$. The matrix

$$M = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 3 & 0 \end{pmatrix}$$

defines, over any finite field of characteristic greater than 3, an ideal LSSS with access structure Γ, where the last column corresponds to the dealer. Let us suppose that there exist a finite field $\mathbb{K}$ and a sequence of linear forms $\Pi = (\pi_1, \ldots, \pi_6)$ such that $\Gamma = \Gamma_6(\Pi)$ and $\Sigma_6(\Pi)$ is an ideal $\mathbb{K}$-MLSSS. In this case, there exist values $\lambda_1, \ldots, \lambda_5 \in \mathbb{K}$ such that $\pi_6 \otimes \pi_6 = \sum_{i=1}^{5} \lambda_i(\pi_i \otimes \pi_i)$. It is clear that for any subset $B \subset P_6$ with $B \neq P_6$, the induced substructure $\Gamma(B) = \{A \subset B : A \in \Gamma\}$ is not $\mathcal{Q}_2$. Observe that, if $\lambda_i = 0$, we would obtain a MLSSS for the induced access structure $\Gamma(P_6 \setminus \{i\})$, a contradiction. Then, $\lambda_i \neq 0$ for any $i = 1, \ldots, 5$. Let us consider now the access structure $\Gamma_5(\Pi)$ on the set $P_5 = \{1,2,3,4,6\}$. This access structure is not $\mathcal{Q}_2$ because $A_1 = \{1,2,6\} \notin \Gamma_5(\Pi)$, $A_2 = \{3,4\} \notin \Gamma_5(\Pi)$ and $A_1 \cup A_2 = P_5$. On the other hand, the LSSS $\Sigma_5(\Pi)$ is multiplicative because $\pi_5 \otimes \pi_5$ is a linear combination of the bilinear forms $\pi_i \otimes \pi_i$ with $i \in P_5$. This contradiction leads us to conclude that there is no ideal MLSSS with access structure Γ.

3.4 Equivalence between the two problems

We prove in this section that Question 1 and Question 2 are equivalent.

Lemma 10. *Let $\Pi = (\pi_1, \ldots \pi_{2d})$ be a sequence of linear forms in $E^* = (\mathbb{K}^d)^*$ such that the matroid $\mathcal{M}(\Pi)$ is identically self-dual and connected. In the space $\mathcal{S}(E)$ of the symmetric bilinear forms on E, the vectors $\{\pi_j \otimes \pi_j : j \in Q \setminus \{i\}\}$ are linearly independent for any $i \in Q$.*

Proof: Let us suppose that the vectors $\{\pi_j \otimes \pi_j : 1 \leq j \leq 2d-1\}$ are linearly dependent. Then, we can suppose that

$$\pi_1 \otimes \pi_1 = \sum_{i=2}^{2d-1} \lambda_i(\pi_i \otimes \pi_i). \tag{1}$$

The access structure $\Gamma_1(\Pi)$ is self-dual and connected. Then, there exists a minimal qualified subset $A \subset P_1$ such that $2d \in A$. We can suppose that $A = \{r+1, \ldots, 2d-1, 2d\}$. Since $\Gamma_1(\Pi)$ is self-dual, $P_1 \setminus A = \{2, \ldots, r\}$ is not qualified. Then, there exists a vector $\mathbf{x} \in E$ such that $\pi_1(\mathbf{x}) = 1$ and $\pi_i(\mathbf{x}) = 0$ for every $i = 2, \ldots, r$. Therefore, from equation (1), $\pi_1 = \sum_{i=r+1}^{2d-1}(\lambda_i \pi_i(\mathbf{x}))\pi_i$, a contradiction with the fact that $A = \{r+1, \ldots, 2d-1, 2d\}$ is a *minimal* qualified subset of the access structure $\Gamma_1(\Pi)$. □

By taking into account that a non-connected matroid can be divided in connected components, the equivalence between Questions 1 and 2 is an immediate consequence of the following two propositions.

Proposition 11. *Let $\mathcal{M}$ be an identically self-dual representable connected matroid on the set of points $Q = \{1, \ldots, 2d\}$ and let $\Gamma_{2d}(\mathcal{M})$ be the access structure induced by $\mathcal{M}$*

on the set P_{2d}. Then $\Gamma_{2d}(\mathcal{M})$ can be realized by an ideal multiplicative $\mathbb{K}$-LSSS if and only if $\mathcal{M}$ can be represented by an almost self-dual code $\mathcal{C}$ over the field $\mathbb{K}$.

Proof: Let us suppose that $\mathcal{M}$ is represented, over the finite field $\mathbb{K}$, by an almost self-dual code $\mathcal{C} = \mathcal{C}(\Pi)$. Let $M = M(\Pi)$ be a generator matrix of this code and let $D = \text{diag}(\lambda_1, \ldots, \lambda_{2d-1}, \lambda_{2d})$ be the non-singular diagonal matrix such that MD is a parity check matrix of $\mathcal{C}$. Then, $\sum_{i=1}^{2d} \lambda_i(\pi_i \otimes \pi_i) = 0$ and, hence, $\Sigma_{2d}(\Pi)$ is an ideal multiplicative $\mathbb{K}$-LSSS with access structure $\Gamma_{2d}(\mathcal{M})$. Reciprocally, let us suppose that there exists an ideal multiplicative $\mathbb{K}$-LSSS, $\Sigma_{2d}(\Pi)$, with access structure $\Gamma_{2d}(\mathcal{M})$. Let us consider the matrices $M = M(\Pi)$ and $D = \text{diag}(\lambda_1, \ldots, \lambda_{2d-1}, -1)$, where $\pi_{2d} \otimes \pi_{2d} = \sum_{i=1}^{2d-1} \lambda_i(\pi_i \otimes \pi_i)$. By Lemma 10, D is a non-singular matrix. Then, M and MD are, respectively, the generator and parity check matrices of the code $\mathcal{C}(\Pi)$. Therefore, $\mathcal{C}(\Pi)$ is an almost self-dual code representing the matroid $\mathcal{M}$ over the finite field $\mathbb{K}$. □

Proposition 12. *Let $\mathcal{M}$ be an identically self-dual matroid that is represented, over the finite field $\mathbb{K}$, by an almost self-dual code. Then, there exists a finite field $\mathbb{L}$, which is an algebraic extension of $\mathbb{K}$, such that $\mathcal{M}$ is represented by a self-dual code over $\mathbb{L}$.*

Proof: Let $\mathcal{C}$ be an almost self-dual code over a finite field $\mathbb{K}$. Let M be a generator matrix and $D = \text{diag}(\lambda_1, \ldots, \lambda_{2d-1}, \lambda_{2d})$ the non-singular diagonal matrix such that MD is a parity check matrix. Let us consider, in an extension field $\mathbb{L} \supset \mathbb{K}$, the diagonal matrix $D_1 = \text{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_{2d-1}}, \sqrt{\lambda_{2d}})$. Then, the matrix $M_1 = MD_1$ is a generator matrix of a self-dual code $\mathcal{C}_1$. The matroids associated to $\mathcal{C}$ and to $\mathcal{C}_1$ are equal. □

3.5 Known families of self-dually representable matroids

There are two families of matroids for which it is known that all identically self-dual matroids are self-dually representable.

The uniform matroids are the first example. A uniform matroid $U_{d,n}$ is identically self-dual if and only if $n = 2d$. The access structure $\Gamma_{2d}(U_{d,2d})$ is the threshold structure $\Gamma_{d,2d-1}$, which can be realized by an ideal multiplicative $\mathbb{K}$-LSSS for any finite field $\mathbb{K}$ with $|\mathbb{K}| \geq 2d$. Namely, the Shamir's polynomial scheme. Therefore, the matroid $U_{d,2d}$ can be represented by an almost self-dual code over finite field $\mathbb{K}$ with $|\mathbb{K}| \geq 2d$.

The second family is formed by the $\mathbb{Z}_2$-representable matroids. For any of these matroids $\mathcal{M}$, there exists a unique $\mathbb{Z}_2$-representation. That is, there exists a unique linear code $\mathcal{C}$ over $\mathbb{Z}_2$ whose associated matroid is $\mathcal{M}$. If $\mathcal{M}$ is an identically self-dual $\mathbb{Z}_2$-representable matroid, the codes $\mathcal{C}$ and $\mathcal{C}^\perp$ are $\mathbb{Z}_2$-representations of $\mathcal{M}$ and, hence, $\mathcal{C} = \mathcal{C}^\perp$. Therefore, all identically self-dual $\mathbb{Z}_2$-representable matroids are self-dually $\mathbb{Z}_2$-representable. For instance, an identically self-dual binary matroid $\mathcal{M}$ on the set $Q = \{1, \ldots, 8\}$ is obtained from the eight vectors in the set $\{(v_1, v_2, v_3, v_4) \in \mathbb{Z}_2^4 : v_1 = 1\}$. All access structures that are obtained from $\mathcal{M}$ are isomorphic to the access structure defined by the Fano Plane by considering the points in the plane as the players and the lines as the minimal qualified subsets [18]. Therefore, this access structure can be realized by an ideal multiplicative $\mathbb{Z}_2$-LSSS.

3.6 Constructing efficient multiplicative linear secret sharing schemes

We present here an alternative description of the method given in [9] to construct, from any $\mathbb{K}$-LSSS Σ with $\mathcal{Q}_2$ access structure Γ, a $\mathbb{K}$-MLSSS Σ' with the same access structure and complexity $\lambda(\Sigma') = 2\lambda(\Sigma)$. We are going to consider only the ideal case, but the construction can be easily adapted to any LSSS. This alternative description shows that the construction in [9] is closely related to self-dual codes and, hence, to ideal MLSSSs with self-dual access structures.

We have to suppose that the characteristic of $\mathbb{K}$ is different from 2. Let $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ be an ideal $\mathbb{K}$-LSSS with $\mathcal{Q}_2$ access structure Γ. Let M be the $d \times (n+1)$ matrix associated to Σ, that is, a generator matrix of the corresponding code. Let N be the parity-check matrix of this code. Then N is a $(n+1-d) \times (n+1)$ matrix such that $MN^\top = 0$. Let us consider now the $(n+1) \times 2(n+1)$ matrix

$$\tilde{M} = \left(\begin{array}{c|c} M & M \\ \hline N & -N \end{array}\right)$$

Observe that $\tilde{M}$ is a generator matrix of an almost self-dual code. In fact, the diagonal matrix

$$D = \left(\begin{array}{c|c} I_{n+1} & 0 \\ \hline 0 & -I_{n+1} \end{array}\right)$$

is such that $\tilde{M}(\tilde{M}D)^\top = \tilde{M}D\tilde{M}^\top = 0$. Therefore, $\tilde{M}$ is the matrix of an ideal $\mathbb{K}$-MLSSS $\tilde{\Sigma} = \Sigma_{2n+2}(\gamma_1, \ldots, \gamma_{2n+1}, \gamma_{2n+2})$, where $\gamma_j \in (\mathbb{K}^{n+1})^*$ corresponds to the j-th column of $\tilde{M}$. Of course, the access structure of $\tilde{\Sigma}$ is self-dual.

We describe next how a non-ideal $\mathbb{K}$-MLSSS Σ' for Γ can be obtained from $\tilde{\Sigma}$. Let us consider $E = \ker \gamma_{2n+2} \subset \mathbb{K}^{n+1}$, the linear mapping $\phi_{n+1} : E \to \mathbb{K}$ defined by $\phi_{n+1}(\mathbf{x}) = \gamma_{n+1}(\mathbf{x})$ and, for every $j = 1, \ldots, n$, the linear mappings $\phi_j : E \to \mathbb{K}^2$ defined by $\phi_j(\mathbf{x}) = (\gamma_j(\mathbf{x}), \gamma_{n+1+j}(\mathbf{x}))$. Then, the $\mathbb{K}$-LSSS $\Sigma' = \Sigma_{n+1}(\phi_1, \ldots, \phi_n, \phi_{n+1})$ is multiplicative and its complexity is $\lambda(\Sigma') = 2n$. Since $\Gamma^* \subset \Gamma$, it has access structure Γ. Actually, this is essentially the same construction as in [9].

4 Flat-partitions and sum of matroids

The aim of this section is twofold. First, we prove that, to solve Question 2, it is enough to consider *indecomposable* identically self-dual matroids and, second, we present a useful characterization of such matroids. This characterization is based in a new concept we introduce in this paper: the *flat-partitions* of a matroid, which will be used also to classify identically self-dual matroids.

A matroid is said to be *indecomposable* if it is not the sum of smaller identically self-dual matroids. We recall next the definition and some properties of the sum of two matroids.

Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be connected matroids on the sets Q_1 and Q_2, respectively. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be their families of bases. Let us suppose that $Q_1 \cap Q_2 = \emptyset$ and let us take two points $q_1 \in Q_1$ and $q_2 \in Q_2$. The *sum of $\mathcal{M}_1$ and $\mathcal{M}_2$ at the points q_1 and q_2*, which will be denoted by $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$, is the matroid on the set of points $Q = (Q_1 \cup Q_2) \setminus \{q_1, q_2\}$ whose family of bases is $\mathcal{B} = \mathcal{B}'_1 \cup \mathcal{B}'_2$, where

- $\mathcal{B}'_1 = \{B_1 \cup C_2 \subset Q \,:\, B_1 \in \mathcal{B}_1, C_2 \cup \{q_2\} \in \mathcal{B}_2\}$,
- $\mathcal{B}'_2 = \{C_1 \cup B_2 \subset Q \,:\, C_1 \cup \{q_1\} \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}$.

It is not difficult to check that $\mathcal{B}$ verifies the axioms in Definition 5 and that $\mathcal{M}$ is a connected matroid with $\dim \mathcal{M} = \dim \mathcal{M}_1 + \dim \mathcal{M}_2 - 1$.

Proposition 13. *The matroid $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ is identically self-dual if and only if both $\mathcal{M}_1$ and $\mathcal{M}_2$ are identically self-dual.*

Proof: It is easy to prove that $\mathcal{M}^* = \mathcal{M}_1^* \oplus_{(q_1,q_2)} \mathcal{M}_2^*$. Hence, the sum of two identically self-dual matroids is identically self-dual.

Let us suppose now that $\mathcal{M}$ is identically self-dual. Let us consider $\dim \mathcal{M}_i = d_i$ and $|Q_i| = n_i + 1$, where $i = 1, 2$. We are going to prove now that, if B is a basis of $\mathcal{M}$ in the form $B = B_1 \cup C_2 \in \mathcal{B}'_1$, then $Q \setminus B \in \mathcal{B}'_2$. Otherwise, $Q \setminus B = \overline{B}_1 \cup \overline{C}_2 \in \mathcal{B}'_1$ and, hence, $n_1 = 2d_1$ and $n_2 = 2(d_2 - 1)$. Let us take now a basis $B' = C_1 \cup B_2 \in \mathcal{B}'_2$ and $Q \setminus B' = D_1 \cup D_2$, where $D_i \subset Q_i \setminus \{q_i\}$. Then, $|D_1| = n_1 - d_1 + 1 = d_1 + 1$ and, hence, $Q \setminus B'$ can not be a basis of $\mathcal{M}$, a contradiction. Equally, $Q \setminus B \in \mathcal{B}'_1$ for any basis $B \in \mathcal{B}'_2$.

Finally, let us prove that, for instance, $\mathcal{M}_1$ is identically self-dual. Let $B_1 \subset Q_1$ be a basis of $\mathcal{M}_1$. If $q_1 \notin B_1$, there is a basis of $\mathcal{M}$ in the form $B = B_1 \cup C_2 \in \mathcal{B}'_1$ and $Q \setminus B = C_1 \cup B_2 \in \mathcal{B}'_2$. Therefore, $Q_1 \setminus B_1 = C_1 \cup \{q_1\}$ is a basis of $\mathcal{M}_1$. Equally, $Q_1 \setminus B_1$ is a basis of $\mathcal{M}_1$ if B_1 is a basis of $\mathcal{M}_1$ with $q_1 \in B_1$. □

We say that a sum of matroids $\mathcal{M}_1 \oplus \mathcal{M}_2$ is *trivial* if one of the matroids $\mathcal{M}_i$ is the uniform matroid $U_{1,2}$. In this case, $\mathcal{M}_1 \oplus U_{1,2} \cong \mathcal{M}_1$. A matroid $\mathcal{M}$ is *indecomposable* if it is not isomorphic to any non-trivial sum of matroids.

Let $\mathcal{M}$ be a matroid on a set of points Q and let (X_1, X_2) be a partition of Q. We say that (X_1, X_2) is a *flat-partition* of $\mathcal{M}$ if X_1 and X_2 are flats of $\mathcal{M}$.

Indecomposable identically self-dual matroids are characterized in Theorem 17 in terms of their flat-partitions. The following three lemmas are needed to prove that theorem.

Lemma 14. *Let $\mathcal{M}$ be a connected matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Then,* $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) > \dim(\mathcal{M})$ *and* $\mathrm{rank}(X_i) > 1$ *for* $i = 1, 2$.

Proof: Observe that $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) \geq \mathrm{rank}(X_1 \cup X_2) = \dim(\mathcal{M})$. Let us suppose that $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M})$. We are going to prove that, in this case, there does not exist any circuit C of $\mathcal{M}$ such that $C \cap X_i \neq \emptyset$ for $i = 1, 2$ and, hence, $\mathcal{M}$ is not connected. Let us suppose that there exists such a circuit C and let us take $C_i = C \cap X_i$. Since C is a minimal dependent subset, both sets C_1 and C_2 are independent and hence, for $i = 1, 2$, there is a basis B_i of the flat X_i with $C_i \subset B_i$. Observe that $\langle B_1 \cup B_2 \rangle = Q$ and that $|B_1 \cup B_2| = \mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M})$. Therefore, $B = B_1 \cup B_2$ is a basis of $\mathcal{M}$. But C is a circuit with $C \subset B$, a contradiction.

If (X_1, X_2) is a flat-partition with $\mathrm{rank}(X_1) = 1$, then $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) < 1 + \dim(\mathcal{M})$, a contradiction. □

Lemma 15. *Any set with exactly two points in a connected identically self-dual matroid $\mathcal{M}$ with* $\dim(\mathcal{M}) \geq 2$ *is independent.*

Proof: Let us suppose that $\{1,2\} \subset Q$ is a dependent subset and let us consider the flat $X_1 = \langle\{1,2\}\rangle$, whose rank is equal to 1. Since $\dim(\mathcal{M}) \geq 2$, we have that $X_2 = Q \setminus X_1 \neq \emptyset$. The proof is concluded by proving that X_2 is a flat and getting a contradiction from Lemma 14. If X_2 is not a flat, there exists $i \in X_1$ with $i \in \langle X_2\rangle$. Since $\mathcal{M}$ is connected, every set with one point is independent and, hence, $\langle\{i\}\rangle = X_1$. Therefore, $\langle X_2\rangle = Q$ and there is a basis B of $\mathcal{M}$ with $B \subset X_2$. Then, $\overline{B} = Q \setminus B$ is basis of $\mathcal{M}$ with $X_1 \subset \overline{B}$, a contradiction. □

Lemma 16. *Let $\mathcal{M}$ be a connected identically self-dual matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Let us take $d = \dim(\mathcal{M})$ and $r_i = \mathrm{rank}(X_i)$. Then,*

1. *$d - r_j \leq |B \cap X_i| \leq r_i$ if $B \subset Q$ is a basis of $\mathcal{M}$ and $\{i,j\} = \{1,2\}$, and*
2. *$|X_i| = d + r_i - r_j$ if $\{i,j\} = \{1,2\}$.*

Proof: Let $B \subset Q$ be a basis of $\mathcal{M}$. Since r_i is the maximum cardinality of an independent subset in X_i, it is clear that $|B \cap X_i| \leq r_i$. This proves the first statement by taking into account that $|B| = d$.

If $B_1 \subset X_1$ is a basis of the flat X_1, there exists a basis B of $\mathcal{M}$ such that $B_1 \subset B$ and, hence, $|B \cap X_2| = d - r_1$. Since $\mathcal{M}$ is identically self-dual, $Q \setminus B$ is also a basis of $\mathcal{M}$. Then, $|X_1| = |B \cap X_1| + |(Q \setminus B) \cap X_1| \geq r_1 + d - r_2$. Equally, there exists a basis B' of $\mathcal{M}$ such that $|B' \cap X_1| = d - r_2$ and, hence, $|X_1| = |B' \cap X_1| + |(Q \setminus B') \cap X_1| \leq d - r_2 + r_1$. Since $|Q| = 2d$, it is obvious that $|X_2| = d + r_2 - r_1$. □

Theorem 17. *Let $\mathcal{M}$ be a connected identically self-dual matroid. Then $\mathcal{M}$ is indecomposable if and only if there is no flat-partition (X_1, X_2) of $\mathcal{M}$ with* $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M}) + 1$.

Proof: Let us suppose that $\mathcal{M}$ is a non-trivial sum of two identically self-dual matroids, $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$. We are going to prove that (X_1, X_2), where $X_i = Q_i \setminus \{q_i\}$, is a flat-partition of $\mathcal{M}$ with $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M}) + 1$. Observe that $I \subset X_i$ is an independent set of the matroid $\mathcal{M}$ if and only if it is an independent subset of the matroid $\mathcal{M}_i$. Therefore, since the matroids $\mathcal{M}_i$ are connected, $\mathrm{rank}(X_i) = \dim(\mathcal{M}_i)$ and, hence, $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M}) + 1$. Besides, $\dim(\mathcal{M}_i) \geq 2$ because the sum is not trivial and $\mathcal{M}_i$ is identically self-dual. Let us suppose that X_1 is not a flat, that is, there exists $x \in X_2$ with $x \in \langle X_1\rangle$. By Lemma 15, $\{x, q_2\}$ is an independent set of $\mathcal{M}_2$. Then, there exists $C_2 \subset X_2$ such that $x \in C_2$ and $C_2 \cup \{q_2\}$ is a basis of $\mathcal{M}_2$. Let us consider a basis of $\mathcal{M}$ in the form $B = B_1 \cup C_2$, where $B_1 \subset X_1$ is a basis of $\mathcal{M}_1$. Observe that $x \in \langle X_1\rangle = \langle B_1\rangle$, a contradiction. Therefore, X_1 is a flat and, symmetrically, X_2 is a flat too.

Let us suppose now that there exists a flat-partition (X_1, X_2) of $\mathcal{M}$ with $\mathrm{rank}(X_1) + \mathrm{rank}(X_2) = \dim(\mathcal{M}) + 1$. From Lemma 16, $\mathrm{rank}(X_i) - 1 \leq |B \cap X_i| \leq \mathrm{rank}(X_i)$ for every basis B of $\mathcal{M}$ and $i = 1, 2$. Besides, if B is a basis of $\mathcal{M}$ with $|B \cap X_1| = \mathrm{rank}(X_1)$, then $B \cap X_1$ is a basis of the flat X_1, and $|B \cap X_2| = \mathrm{rank}(X_2) - 1$, and $B'_1 \cup (B \cap X_2)$ is a basis of $\mathcal{M}$ for every basis B'_1 of X_1. Obviously, the symmetrical properties equally hold.

Let us take $q_1, q_2 \notin Q$ and $Q_i = X_i \cup \{q_i\}$. Let $\mathcal{M}_1$ be the matroid on the set Q_1 defined by the set of basis $\mathcal{B}_1$, where $B_1 \in \mathcal{B}_1$ if and only if $|B_1| = \mathrm{rank}(X_1)$ and

- $q_1 \notin B_1$ and there exists $C_2 \subset X_2$ such that $B_1 \cup C_2$ is a basis of $\mathcal{M}$, or
- $q_1 \in B_1$ and there exists $B_2 \subset X_2$ such that $(B_1 \setminus \{q_1\}) \cup B_2$ is a basis of $\mathcal{M}$.

A matroid $\mathcal{M}_2$ on the set Q_2 is symmetrically defined. The proof is concluded by checking that these matroids are well defined and that $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$. Observe that, from Lemma 14, $\dim(\mathcal{M}_i) = \operatorname{rank}(X_i) \geq 2$ and, hence, the sum is not trivial. □

Proposition 18. *Let $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ be a non-trivial sum of two identically self-dual matroids. Then $\mathcal{M}$ is $\mathbb{K}$-representable if and only if both $\mathcal{M}_1$ and $\mathcal{M}_2$ are $\mathbb{K}$-representable.*

Proof: Let us suppose that $\mathcal{M}_1$ and $\mathcal{M}_2$ are $\mathbb{K}$-representable. We can suppose that $\mathcal{M}_1$ and $\mathcal{M}_2$ are represented by matrices in the form:

$$M_1 = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,m-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{d_1-1,1} & \cdots & a_{d_1-1,m-1} & 0 \\ \hline a_{d_1,1} & \cdots & a_{d_1,m-1} & 1 \end{array}\right) \quad \text{and} \quad M_2 = \left(\begin{array}{c|ccc} 1 & b_{1,2} & \cdots & b_{1,n} \\ \hline 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{d_2,2} & \cdots & b_{d_2,n} \end{array}\right)$$

where $d_i = \dim \mathcal{M}_i$, $|Q_1| = m$, $|Q_2| = n$ and the points q_1 and q_2 correspond, respectively, to the last column of M_1 and the first column of M_2. Then, the matrix

$$M = \left(\begin{array}{ccc|ccc} a_{1,1} & \cdots & a_{1,m-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{d_1-1,1} & \cdots & a_{d_1-1,m-1} & 0 & \cdots & 0 \\ \hline a_{d_1,1} & \cdots & a_{d_1,m-1} & b_{1,2} & \cdots & b_{1,n} \\ \hline 0 & \cdots & 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{d_2,1} & \cdots & b_{d_2,n} \end{array}\right)$$

is a $\mathbb{K}$-representation of the sum $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$.

Let us take $X_1 = Q_1 \setminus \{q_1\} = \{a_1, \ldots, a_{n-1}\}$ and $X_2 = Q_2 \setminus \{q_2\} = \{b_2, \ldots, b_n\}$. From Theorem 17, (X_1, X_2) is a flat-partition of $\mathcal{M}$ with $\operatorname{rank}(X_1) + \operatorname{rank}(X_2) = \dim(\mathcal{M}) + 1$. If $\mathcal{M}$ is $\mathbb{K}$-representable, there exists a sequence $\Pi = (\alpha_1, \ldots, \alpha_{m-1}, \beta_2, \ldots, \beta_n)$ of linear forms $\alpha_i, \beta_j \in E^* = (\mathbb{K}^d)^*$, where $d = \dim(\mathcal{M})$, such that $\mathcal{M} = \mathcal{M}(\Pi)$. Let us consider the subspaces $V_1, V_2 \subset E^*$ defined by $V_1 = \langle \alpha_1, \ldots, \alpha_{m-1} \rangle$ and $V_2 = \langle \beta_2, \ldots, \beta_n \rangle$. Clearly, $\dim(V_i) = \operatorname{rank}(X_i)$ and, hence, $\dim(V_1 \cap V_2) = 1$. Let $\pi \in E^*$ be a non-zero vector such that $V_1 \cap V_2 = \langle \pi \rangle$ and consider $\Pi_1 = (\alpha_1, \ldots, \alpha_{m-1}, \pi)$ and $\Pi_2 = (\pi, \beta_2, \ldots, \beta_n)$. Then, $\mathcal{M}_1 = \mathcal{M}(\Pi_1)$ and $\mathcal{M}_2 = \mathcal{M}(\Pi_2)$, where the linear form π correspond to the point q_1 in $\mathcal{M}_1$ and to the point q_2 in $\mathcal{M}_2$. □

Proposition 19. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids that are represented over a finite field $\mathbb{K}$ by almost self-dual codes. Then, the sum $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ can be represented over $\mathbb{K}$ by an almost self-dual code. Besides, if $\mathcal{M}_1$ and $\mathcal{M}_2$ are self-dually $\mathbb{K}$-representable, the sum $\mathcal{M}$ is self-dually $\mathbb{L}$-representable, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ with $(\mathbb{K} : \mathbb{L}) \leq 2$.*

Proof: Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be almost self-dual codes that represent $\mathcal{M}_1$ and $\mathcal{M}_2$ over $\mathbb{K}$, and let M_1 and M_2 be generator matrices of these codes. We can suppose that these matrices have the same form as the ones appearing in the proof of Proposition 18. Then, we construct in the same way a matrix M that is a $\mathbb{K}$-representation of the sum $\mathcal{M}$ and, besides, is a generator matrix of an almost self-dual code.

If $\mathcal{C}_1$ and $\mathcal{C}_2$ are self-dual codes, the matrix

$$\left(\begin{array}{ccc|ccc} a_{1,1} & \cdots & a_{1,m-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{d_1-1,1} & \cdots & a_{d_1-1,m-1} & 0 & \cdots & 0 \\ \hline a_{d_1,1} & \cdots & a_{d_1,m-1} & b_{1,2}\sqrt{-1} & \cdots & b_{1,n}\sqrt{-1} \\ \hline 0 & \cdots & 0 & b_{2,2}\sqrt{-1} & \cdots & b_{2,n}\sqrt{-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{d_2,1}\sqrt{-1} & \cdots & b_{d_2,n}\sqrt{-1} \end{array}\right)$$

is an $\mathbb{L}$-representation of $\mathcal{M}$, where $\mathbb{L} = \mathbb{K}(\sqrt{-1})$, and, besides, is the generator matrix of a self-dual code. □

From the previous results and taking into account that a self-dually $\mathbb{K}$-representable matroid is self-dually $\mathbb{L}$-representable whenever $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$, we get that Questions 1 and 2 are equivalent to the following one.

Question 20. To determine whether all indecomposable identically self-dual $\mathbb{K}$-representable matroids can be represented by a self-dual linear code over some finite field $\mathbb{L}$, an algebraic extension of $\mathbb{K}$.

That is, we can restrict ourselves to indecomposable matroids when trying to solve Question 2.

The sum of matroids is related to a well known method to compose access structures. Let Γ^1 and Γ^2 be connected access structures on the sets of participants P^1 and P^2 and let us consider a participant $p \in P^1$. The qualified subsets in the composed access structure $\Gamma = \Gamma^1[\Gamma^2; p]$ on the set of participants $P = (P^1 \setminus \{p\}) \cup P^2$ are the subsets $A \subset P^1 \setminus \{p\}$ with $A \in \Gamma^1$ and the subsets $A \subset P$ such that $A \cap P^2 \in \Gamma^2$ and $(A \cap P^1) \cup \{p\} \in \Gamma^1$. If $\mathcal{M}_1$ and $\mathcal{M}_2$ are matroids on the sets Q_1 and Q_2 such that $\Gamma^1 = \Gamma_{q_1}(\mathcal{M}_1)$ and $\Gamma^2 = \Gamma_{q_2}(\mathcal{M}_2)$, where $q_i \in Q_i$, then the composition $\Gamma^1[\Gamma^2; p\,]$ is related to a sum of the matroids $\mathcal{M}_1$ and $\mathcal{M}_2$. Namely, $\Gamma^1[\Gamma^2; p\,] = \Gamma_{q_1}(\mathcal{M}_1 \oplus_{(p,q_2)} \mathcal{M}_2)$.

It follows from Propositions 13 and 18 that the composition $\Gamma = \Gamma^1[\Gamma^2; p\,]$ of two self-dual $\mathbb{K}$-vector space access structures is also a self-dual $\mathbb{K}$-vector space access structure. Besides, from Proposition 19, if both Γ^1 and Γ^2 are self-dual access structures admitting an ideal multiplicative $\mathbb{K}$-LSSS, the same applies to the composed access structure Γ.

5 A new family of identically self-dual matroids that are representable by self-dual codes

5.1 Identically self-dual bipartite matroids

It is not hard to see that the uniform matroid $U_{d,2d}$ on the set $Q = \{1, \ldots, 2d\}$ does not admit any flat-partition. As a direct cosequence of the next lemma, any non-uniform identically self-dual matroid admits a flat partition.

Lemma 21. *Let $\mathcal{M}$ be an identically self-dual matroid and let $C \subset Q$ be a circuit of $\mathcal{M}$ with* $\mathrm{rank}(C) < \dim(\mathcal{M})$. *Let us consider the flat $X_1 = \langle C \rangle$ and $X_2 = Q \setminus X_1$. Then, (X_1, X_2) is a flat-partition of $\mathcal{M}$.*

Proof: We have to prove that X_2 is a flat. Otherwise, there exists $x \in X_1 \cap \langle X_2 \rangle$. Since C is a circuit, there exists a basis B_1 of X_1 with $x \notin B_1$. Besides, there exists $C_2 \subset X_2$ such that $B = B_1 \cup C_2$ is a basis of $\mathcal{M}$. Let us consider the basis $B' = Q \setminus B$ and $B_2 = B' \cap X_2$.

We are going to prove that $\langle B_2 \rangle = X_2$. If not, there exists $y \in X_2 \setminus \langle B_2 \rangle$. Observe that $y \in C_2$ and that $B_2 \cup \{y\}$ is an independent set. Therefore, $Q \setminus (B_2 \cup \{y\}) = X_1 \cup (C_2 \setminus \{y\})$ is a spanning set. Since $\langle B_1 \rangle = X_1$, we have that $B'' = B_1 \cup (C_2 \setminus \{y\})$ is equally a spanning set, a contradiction with $B'' \subsetneq B$.

Therefore, $x \in \langle B_2 \rangle$, a contradiction with $B_2 \cup \{x\} \subset B'$. □

As said before, any identically self-dual uniform matroid $U_{d,2d}$ can be represented by a self-dual code $\mathcal{C}$ over some finite field $\mathbb{K}$. By the above observation, this means that the answer to Question 2 is affirmative for the identically self-dual matroids that do not admit any flat-partition.

A natural question arising at this point is whether the same occurs with the identically self-dual matroids that admit exactly *one* flat-partition. Proposition 23 shows that these matroids coincide with the identically self-dual bipartite matroids.

Let d, r_1 and r_2 be any integers such that $1 < r_i < d < r_1 + r_2$. Let us take $Q = \{1, \ldots, n, n+1\}$ and a partition (X_1, X_2) of Q with $|X_i| \geq r_i$. We define the matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ by determining its basis: $B \subset Q$ is a basis of $\mathcal{M}$ if and only if $|B| = d$ and $d - r_j \leq |B \cap X_i| \leq r_i$, where $\{i, j\} = \{1, 2\}$. Observe that (X_1, X_2) is a flat-partition of Q with $\mathrm{rank}(X_i) = r_i$. Any matroid in this form is said to be *bipartite*.

The access structures defined by these bipartite matroids were first considered in [24], where the authors proved that they are vector space access structures, that is, they admit an ideal LSSS. As a direct consequence of this fact, any bipartite matroid is representable. Independently, the bipartite matroids have also been studied in [22, 21], where they are called *matroids with two uniform components*.

Theorem 3, which is proved in the following, extends this result of [24] by showing that, additionally, the identically self-dual bipartite matroids are self-dually representable. This is done by a refinement of the approach of [24] based on techniques from Algebraic Geometry.

From Theorem 17 and Propositions 22 and 23, the identically self-dual bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ is indecomposable whenever $r_1 + r_2 - d > 1$. There-

fore, we found a new large family of identically self-dual matroids giving an affirmative answer to Question 2 and, hence, a new large family of self-dual vector space access structures for which Question 1 has a positive answer.

Proposition 22. *Let $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ be a bipartite matroid. Then, $\mathcal{M}$ is identically self-dual if and only if $|Q| = 2d$ and $|X_1| = d + r_1 - r_2$.*

Proof: Let us suppose that $|Q| = 2d$ and $|X_1| = d + r_1 - r_2$. Let $B \subset Q$ be a basis of B. It is not difficult to check that $d - r_j \leq |(Q \setminus B) \cap X_i| \leq r_i$ whenever $\{i, j\} = \{1, 2\}$. Then, $Q \setminus B$ is a basis of $\mathcal{M}$. The reciprocal is a direct consequence of Lemma 16. □

Proposition 23. *Let $\mathcal{M}$ be a connected identically self-dual matroid. Then, $\mathcal{M}$ is bipartite if and only if it admits exactly one flat-partition.*

Proof: Let us suppose that $\mathcal{M}$ is bipartite, that is, $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$. We have to prove that (X_1, X_2) is the only flat-partition of $\mathcal{M}$. Let (Y_1, Y_2) be a flat-partition of $\mathcal{M}$. We can suppose that $|Y_1| \geq d = \dim(\mathcal{M})$. If $|Y_1 \cap X_i| \geq d - r_j$ for all $\{i, j\} = \{1, 2\}$, there exists $B \subset Y_1$ such that $|B| = d$ and $d - r_j \leq |B \cap X_i| \leq r_i$. Since Y_1 does not contain any basis of $\mathcal{M}$, we get $|Y_1 \cap X_1| < d - r_2$ or $|Y_1 \cap X_2| < d - r_1$. Without loss of generality, we assume that $|Y_1 \cap X_2| < d - r_1$. Then, $|Y_1 \cap X_1| > r_1$ because $d \geq |Y_1 \cap X_1| + |Y_1 \cap X_2|$. Besides, since $d + r_2 - r_1 = |Y_1 \cap X_2| + |Y_2 \cap X_2|$, we have that $|Y_2 \cap X_2| > r_2$. Observe that, for $i = 1, 2$, any subset of r_i points in X_i is independent and, hence, $X_i \subset Y_i$ because Y_i is a flat and contains a basis of X_i. Therefore, $(X_1, X_2) = (Y_1, Y_2)$.

Let us suppose now that (X_1, X_2) is the only flat-partition of $\mathcal{M}$. We are going to prove that $\mathcal{M}$ is the bipartite matroid $\mathcal{M}(X_1, X_2, r_1, r_2, d)$, where $r_i = \text{rank}(X_i)$ and $d = \dim(\mathcal{M})$. From Lemma 14, $1 < r_i < d < r_1 + r_2$. From Lemma 16, $d - r_j \leq |B \cap X_i| \leq r_i$ if B is a basis of $\mathcal{M}$ and $\{i, j\} = \{1, 2\}$. We only have to prove that any set $B \subset Q$ such that $|B| = d$ and $d - r_j \leq |B \cap X_i| \leq r_i$ for $\{i, j\} = \{1, 2\}$ is a basis of $\mathcal{M}$. Let us suppose that, on the contrary, there exists such a subset B that is not a basis. Then, there exists a circuit $C \subset B$. Let us consider $Y_1 = \langle C \rangle$ and $Y_2 = Q \setminus Y_1$. From Lemma 21, (Y_1, Y_2) is a flat-partition of $\mathcal{M}$. The proof is concluded by showing that this flat-partition is different from (X_1, X_2). If $Y_1 = X_i$ for some $i = 1, 2$, we have $C \subset X_i$. Since $|C| \leq r_i$ and C is a circuit, $\text{rank}(Y_1) < r_i$, a contradiction. □

5.2 Proof of Theorem 3

This section is devoted to the proof of Theorem 3, which is divided in several partial results.

Let $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ be an identically self-dual bipartite matroid on the set of points $Q = \{1, \ldots, 2d\}$, where $1 < r_i < d < r_1 + r_2$. Let us consider $s_1 = d - r_2$ and $s_2 = d - r_1$. From Proposition 22, $|X_i| = r_i + s_i$. Let us suppose that $X_1 = \{1, \ldots, r_1 + s_1\}$ and $X_2 = Q \setminus X_1$.

Theorem 3 is proved if we are able to demonstrate that there exist a finite field $\mathbb{K}$ and a sequence $\Pi = (\pi_1, \ldots, \pi_{2d})$ of linear forms $\pi_i \in E^*$, where $E = \mathbb{K}^d$, satisfying the following two properties.

1. For any set $B = \{i_1, \ldots, i_d\} \subset Q$ with $s_1 \leq |B \cap X_1| \leq r_1$, the vectors $\{\pi_{i_1}, \ldots, \pi_{i_d}\}$ form a basis of E^*. That is, $\mathcal{M} = \mathcal{M}(\Pi)$.

2. $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2d} \otimes \pi_{2d} \rangle = 2d - 1$, that is, the code $\mathcal{C}(\Pi)$ is almost self-dual.

Let us take $n_i = r_i + s_i$ and $t = r_1 + r_2 - d = r_i - s_i$. Since $\mathrm{rank}(X_i) = r_i$, the vectors $\{\pi_1, \ldots, \pi_{n_1}\}$ must be in a subspace $V_1 \subset E^*$ with $\dim V_1 = r_1$, and the vectors $\{\pi_{n_1+1}, \ldots, \pi_{2d}\}$ must be in a subspace $V_2 \subset E^*$ with $\dim V_2 = r_2$. Since $V_1 + V_2 = E^*$, we have that $\dim(V_1 \cap V_2) = t$.

We can suppose that

$$V_1 = \{(v_1, \ldots, v_d) \in E^* \,:\, v_{r_1+1} = \cdots = v_d = 0\}$$

and

$$V_2 = \{(v_1, \ldots, v_d) \in E^* \,:\, v_{t+1} = \cdots = v_{r_1} = 0\}$$

Let us consider now the mappings $\mathbf{v} : \mathbb{K} \to V_1$ and $\mathbf{w} : \mathbb{K} \to V_2$ defined, respectively, by

$$\begin{array}{rcl} \mathbf{v}(x) & = & (1, \ \ldots, \ x^{t-1}, \ x^t, \ \ldots, \ x^{r_1-1}, \ 0, \ \ldots, \ 0) \\ \mathbf{w}(x) & = & (1, \ \ldots, \ x^{t-1}, \ 0, \ \ldots, \ 0, \ x^t, \ \ldots, \ x^{r_2-1}) \end{array}$$

At this point, it is enough to prove the existence of a finite field $\mathbb{K}$ containing n_1 pairwise different values $\alpha_1, \ldots, \alpha_{n_1} \in \mathbb{K} \setminus \{0\}$ and n_2 pairwise different values $\beta_1, \ldots, \beta_{n_2} \in \mathbb{K} \setminus \{0\}$ such that the vectors $\pi_i = \mathbf{v}(\alpha_i^{-1})$, where $1 \leq i \leq n_1$, and $\pi_i = \mathbf{w}(\beta_{i-n_1}^{-1})$, where $n_1 + 1 \leq i \leq 2d$, satisfy the following conditions:

1. Any set in the form $\{\mathbf{v}(\alpha_{i_1}^{-1}), \ldots, \mathbf{v}(\alpha_{i_{s_1+k}}^{-1}), \mathbf{w}(\beta_{j_1}^{-1}), \ldots, \mathbf{w}(\beta_{j_{r_2-k}}^{-1})\}$, where $0 \leq k \leq t$, is a basis of E^*.

2. $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2d} \otimes \pi_{2d} \rangle = 2d - 1$.

We take the inverses of α_i and β_j just because the proofs are more easily written in this way.

In the following, we briefly describe how the proof of Theorem 3 is concluded. Lemma 24 states that the second condition above is fulfilled if the values α_i, β_j satisfy certain polynomial equations. On the other hand, Lemma 25 affirms that the first condition holds if the values α_i, β_j are not solutions of some other polynomial equations. By using Algebraic Geometry techniques, we prove that such values exist in the infinite field $\overline{\mathbb{Z}}_p$, the algebraic closure of the finite field $\mathbb{Z}_p$, where p is a large enough prime. Therefore, there exists a finite field $\mathbb{K} \supset \mathbb{Z}_p$, which is an algebraic extension of $\mathbb{Z}_p$, containing the values α_i, β_j that satisfy the required conditions.

For any integer $n \geq 1$, we consider the symmetric polynomials on n variables $S_{n,i} = S_{n,i}(x_1, \ldots, x_n)$, where $i = 1, \ldots, n$, defined by $(x - x_1)(x - x_2) \cdots (x - x_n) = x^n + S_{n,1}x^{n-1} + S_{n,2}x^{n-2} + \cdots + S_{n,n-1}x + S_{n,n}$.

Lemma 24. *If $S_{n_1,i}(\alpha_1, \ldots, \alpha_{n_1}) = S_{n_2,i}(\beta_1, \ldots, \beta_{n_2}) = 0$ for every $i = 1, \ldots, t-1$, then $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2d} \otimes \pi_{2d} \rangle = 2d - 1$.*

Proof: The vectors $\pi_i \otimes \pi_i$ are in $\mathcal{S}(E)$, the space of the symmetric bilinear forms on E. Every symmetric bilinear form $\Lambda \in \mathcal{S}(E)$ can be represented by the symmetric $d \times d$ matrix $M(\Lambda) = (\lambda_{ij})$ such that $\Lambda(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{x}_1 M(\Lambda) \mathbf{x}_2^\top$ for every $\mathbf{x}_1, \mathbf{x}_2 \in E$. One can prove that $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2d} \otimes \pi_{2d} \rangle = 2d - 1$ by proving that the coefficients $(\lambda_{ij})_{1 \leq i \leq j \leq d}$ of those bilinear forms satisfy $\dim \mathcal{S}(E) - (2d-1) = (d-1)(d-2)/2$ linearly independent linear equations in the form $\sum_{1 \leq i \leq j \leq d} c_{ij} \lambda_{ij} = 0$. Observe that, if $\pi = (v_1, \ldots, v_d) \in E^*$, the coefficients of the bilinear form $\pi \otimes \pi$ are $\lambda_{ij} = v_i v_j$. Then, we have to prove that the vectors $\{\pi_1, \ldots, \pi_{2d}\}$ satisfy $(d-1)(d-2)/2$ linearly independent quadratic equations in the form $\sum_{1 \leq i \leq j \leq d} c_{ij} v_i v_j = 0$..

Any vector $\pi = (v_1, \ldots, v_d) \in E^*$ in the form $\mathbf{v}(x)$ or $\mathbf{w}(x)$ fulfills the quadratic equations in Table 1. Then, we have presented $(d-1)(d-2)/2 - (t-1)$ linearly independent quadratic equations that are fulfilled by any vector in the form $\mathbf{v}(x)$ or $\mathbf{w}(x)$.

We are going to present $t-1$ new equations that will be fulfilled by the vectors $\mathbf{v}(\alpha_i^{-1})$, $\mathbf{w}(\beta_j^{-1})$ whenever $S_{n_1,i}(\alpha_1, \ldots, \alpha_{n_1}) = S_{n_2,i}(\beta_1, \ldots, \beta_{n_2}) = 0$ for every $i = 1, \ldots, t-1$. Let us consider the polynomials

$$p_1(x) = (x - \alpha_1) \cdots (x - \alpha_{n_1}) = x^{n_1} + a_t x^{2s_1} + \cdots + a_{n_1 - 1} x + a_{n_1}$$

and

$$p_2(x) = (x - \beta_1) \cdots (x - \beta_{n_2}) = x^{n_2} + b_t x^{2s_2} + \cdots + b_{n_2 - 1} x + b_{n_2}.$$

We consider also the polynomials $q_1(x) = x^{n_1} p_1(1/x) = 1 + a_t x^t + \cdots + a_{n_1} x^{n_1}$ and $q_2(x) = x^{n_2} p_2(1/x) = 1 + b_t x^t + \cdots + b_{n_2} x^{n_2}$. Let us consider, for any $\ell = 0, 1, \ldots, t-2$, the polynomial $x^\ell q_1(x) = x^\ell + a_t x^{t+\ell} + \cdots + a_{n_1} x^{n_1 + \ell}$. Observe that, since $q_1(\alpha_i^{-1}) = 0$ for any $i = 1, \ldots, n_1$, the vector $\pi_i = \mathbf{v}(\alpha_i^{-1})$ verifies, for any $\ell = 0, 1, \ldots, t-2$, a quadratic equation in the form

$$v_{\ell+1} v_1 + \sum_{k=t+\ell}^{n_1+\ell} a_{k-\ell} v_{i_k} v_{j_k} = 0$$

where, for every $k = t + \ell, \ldots, n_1 + \ell$, we choose i_k, j_k with $i_k \leq j_k \leq r_1$, $i_k + j_k = k + 2$ and $j_k \geq t + 1$. Since $j_k \geq t + 1$, we have that $v_{i_k} v_{j_k} = 0$ for any vector in V_2. Equally, we consider the $t-1$ polynomials $x^\ell q_2(x) = x^\ell + b_t x^{t+\ell} + \cdots + b_{n_2} x^{n_2 + \ell}$, where $\ell = 0, 1, \ldots, t-2$. For any $i = n_1 + 1, \ldots, 2d$, the vectors $\pi_i = \mathbf{w}(\beta_{i-n_1}^{-1})$ verify, for any $\ell = 0, 1, \ldots, t-2$, a quadratic equation in the form

$$v_{\ell+1} v_1 + \sum_{k=t+\ell}^{n_2+\ell} b_{k-\ell} v_{i'_k} v_{j'_k} = 0$$

where, for every $k = t + \ell, \ldots, n_2 + \ell$, we take i'_k, j'_k such that $j'_k \geq r_1 + 1$ and $i'_k \in \{1, \ldots, t-1, r_1 + 1, \ldots, d\}$. Observe that, in this case, the vectors in V_1 are such that $v_{i'_k} v_{j'_k} = 0$. Therefore, all vectors π_i fulfill the $t-1$ quadratic equations

$$v_{\ell+1} v_1 + \sum_{k=t+\ell}^{n_1+\ell} a_{k-\ell} v_{i_k} v_{j_k} + \sum_{k=t+\ell}^{n_2+\ell} b_{k-\ell} v_{i'_k} v_{j'_k} = 0,$$

Equations	Ranges of the indices		Number of equations
$v_iv_j = 0$	$t+1 \le i \le r_1$	$r_1+1 \le j \le d$	s_1s_2
$v_iv_j = v_{i-1}v_{j+1}$	$2 \le i \le j \le t-1$		$(t-1)(t-2)/2$
	$2 \le i \le t$	$t+1 \le j \le r_1-1$	$(t-1)(s_1-1)$
	$2 \le i \le t$	$r_1+1 \le j \le d-1$	$(t-1)(s_2-1)$
	$t+2 \le i \le j \le r_1-1$		$(s_1-1)(s_1-2)/2$
	$r_1+2 \le i \le j \le d-1$		$(s_2-1)(s_2-2)/2$
	$i = t+1$	$t+1 \le j \le r_1-1$	s_1-1
$v_{r_1+1}v_j = v_tv_{j+1}$	$r_1+1 \le j \le d-1$		s_2-1
$v_iv_t = v_{i-1}v_{t+1} + v_{i-1}v_{r_1+1}$	$2 \le i \le t$		$t-1$

Table 1: Quadratic equations that are fulfilled by the vectors $\mathbf{v}(x)$, $\mathbf{w}(x)$

where $\ell = 0, 1, \ldots, t-2$. The proof is concluded by checking that the $(d-1)(d-2)/2$ quadratic equations we have presented are linearly independent. □

Lemma 25. *For every $k = 0, \ldots, t$, the function $\delta_k(x_1, \ldots, x_{s_1+k}, y_1, \ldots, y_{r_2-k}) = \det(x_1^{r_1-1}\mathbf{v}(x_1^{-1}), \ldots, x_{s_1+k}^{r_1-1}\mathbf{v}(x_{s_1+k}^{-1}), y_1^{r_2-1}\mathbf{w}(y_1^{-1}), \ldots, y_{r_2-k}^{r_2-1}\mathbf{w}(y_{r_2-k}^{-1}))$ is a polynomial on the variables $x_1, \ldots, x_{s_1+k}, y_1, \ldots, y_{r_2-k}$. Let us consider s_1+k pairwise different elements $\alpha_1, \ldots, \alpha_{s_1+k} \in \mathbb{K} \setminus \{0\}$ and r_2-k pairwise different elements $\beta_1, \ldots, \beta_{r_2-k} \in \mathbb{K} \setminus \{0\}$. Then, the set of vectors $\{\mathbf{v}(\alpha_1^{-1}), \ldots, \mathbf{v}(\alpha_{s_1+k}^{-1}), \mathbf{w}(\beta_1^{-1}), \ldots, \mathbf{w}(\beta_{r_2-k}^{-1})\}$ is a basis of $(\mathbb{K}^d)^*$ if and only if $\delta_k(\alpha_1, \ldots, \alpha_{s_1+k}, \beta_1, \ldots, \beta_{r_2-k}) \neq 0$.*

Let us consider now the (infinite) field $\overline{\mathbb{Z}}_p$, the algebraic closure of the finite field $\mathbb{Z}_p$, where p is large enough. Let $\alpha_1, \ldots, \alpha_{n_1}$ be the n_1-th roots of unity in $\overline{\mathbb{Z}}_p$. Observe that $S_{n_1,i}(\alpha_1, \ldots, \alpha_{n_1}) = 0$ for any $i = 1, \ldots, t-1$. We consider the algebraic variety M in the space $\overline{\mathbb{Z}}_p^{n_2}$ defined by $M = \{(y_1, \ldots, y_{n_2}) \in \overline{\mathbb{Z}}_p^{n_2} : S_{n_2,i}(y_1, \ldots, y_{n_2}) = 0 \text{ for every } i = 1, \ldots, t-1\}$. As a consequence of [26, Lemma 9.4], the variety M is irreducible. This fact is proved in [26] for a field with characteristic zero, but the proof can be easily adapted to our case if the characteristic p of our field is large enough. For every election of indices $1 \le i_1 < i_2 < \cdots < i_{s_1+k} \le n_1$ and $1 \le j_1 < j_2 < \cdots < j_{r_2-k} \le n_2$, where $0 \le k \le t$, we consider in $\overline{\mathbb{Z}}_p^{n_2}$ the algebraic variety $V_{i_1,\ldots,i_{s_1+k}}^{j_1,\ldots,j_{r_2-k}} = \left\{(y_1, \ldots, y_{n_2}) \in \overline{\mathbb{Z}}_p^{n_2} : \delta_k(\alpha_{i_1}, \ldots, \alpha_{i_{s_1+k}}, y_{j_1}, \ldots, y_{j_{r_2-k}}) = 0\right\}$. Finally, for every $i = 1, \ldots, n_1$ and for every pair i, j with $1 \le i < j \le n_1$, we consider the algebraic varieties $V_i, V_{ij} \subset \overline{\mathbb{Z}}_p^{n_2}$ defined, respectively, by $y_i = 0$ and $y_i = y_j$.

Lemma 26. *There exists a point $(\beta_1, \ldots, \beta_{n_2}) \in M$ that is not in any of the varieties $V_{i_1,\ldots,i_{s_1+k}}^{j_1,\ldots,j_{r_2-k}}$, V_i and V_{ij}.*

Proof: By applying an elementary result in Algebraic Geometry (see [17], for instance), since M is irreducible, it is enough to prove that M is not a subset of any of those varieties. Let θ be a primitive n_2-th root of unity. It is clear that the point $(\gamma_1, \gamma_2, \ldots, \gamma_{n_2}) = (1, \theta, \ldots, \theta^{n_2-1})$ is in M and is not in any of the varieties V_i, V_{ij}. We only have to check that $M \not\subset V_{i_1,\ldots,i_{s_1+k}}^{j_1,\ldots,j_{r_2-k}}$ for any election of

$1 \leq i_1 < i_2 < \cdots < i_{s_1+k} \leq n_1$ and $1 \leq j_1 < j_2 < \cdots < j_{r_2-k} \leq n_2$. Observe that $(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \ldots, \gamma_{\sigma n_2}) \in M$ for any permutation σ on the set $\{1, \ldots, n_2\}$. We are going to prove that there exists a permutation σ such that $(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \ldots, \gamma_{\sigma n_2}) \notin V_{i_1,\ldots,i_{s_1+k}}^{j_1,\ldots,j_{r_2-k}}$. It is not difficult to check that the vectors $\{\mathbf{v}(\alpha_{i_1}^{-1}), \ldots, \mathbf{v}(\alpha_{i_{s_1}}^{-1}), \mathbf{w}(\gamma_1^{-1}), \ldots, \mathbf{w}(\gamma_{r_2}^{-1})\}$ form a basis of E^*. Since $s_1 + k \leq r_1$, the vectors $\mathbf{v}(\alpha_{i_1}^{-1}), \ldots, \mathbf{v}(\alpha_{i_{s_1}}^{-1}), \ldots, \mathbf{v}(\alpha_{i_{s_1+k}}^{-1})$ are linearly independent. Then, by repeatedly applying Steinitz's Exchange Theorem, we obtain a basis of E^* in the form $\{\mathbf{v}(\alpha_{i_1}^{-1}), \ldots, \mathbf{v}(\alpha_{i_{s_1+k}}^{-1}), \mathbf{w}(\gamma_{\ell_1}^{-1}), \ldots, \mathbf{w}(\gamma_{\ell_{r_2-k}}^{-1})\}$. Therefore, $\delta_k(\alpha_{i_1}, \ldots, \alpha_{i_{s_1+k}}, \gamma_{\ell_1}, \ldots, \gamma_{\ell_{r_2-k}}) \neq 0$ and we obtain a point $(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \ldots, \gamma_{\sigma n_2}) \notin V_{i_1,\ldots,i_{s_1+k}}^{j_1,\ldots,j_{r_2-k}}$ by considering a suitable permutation σ. □

Let $\alpha_1, \ldots, \alpha_{n_1} \in \overline{\mathbb{Z}}_p$ be the values we considered before, that is, the n_1-th roots of unity, and let $\beta_1, \ldots, \beta_{n_2} \in \overline{\mathbb{Z}}_p$ be the values whose existence is assured by Lemma 26. Let us consider the finite field $\mathbb{K} = \mathbb{Z}_p(\alpha_1, \ldots, \alpha_{n_1}, \beta_1, \ldots, \beta_{n_2})$, that is, an algebraic extension of $\mathbb{Z}_p$ containing all values α_i, β_j. At this point, it is clear that the proof of Theorem 3 is concluded by considering the finite field $\mathbb{K}$ and the vectors $\pi_i = \mathbf{v}(\alpha_i^{-1})$, where $1 \leq i \leq n_1$, and $\pi_i = \mathbf{w}(\beta_{i-n_1}^{-1})$, where $n_1 + 1 \leq i \leq 2d$.

6 Reconstruction of a secret in the presence of errors

In any LSSS with a $\mathcal{Q}_3$ access structure Γ, unique reconstruction of the secret from the full set of n shares is possible, even if the shares corresponding to an unqualified set $A \notin \Gamma$ are corrupted. Nevertheless, it is not known how to do that efficiently. In this section we prove Theorem 4, which implies that, if the LSSS is strongly multiplicative, there exists an efficient reconstruction algorithm.

We only consider here the *ideal* LSSS case. Proofs extend easily to the general case, at the cost of some notational headaches.

First we review the familiar case of Shamir's secret sharing scheme, where $t + 1$ or more shares jointly determine the secret, and at most t shares do not even jointly contain any information about the secret. Exactly when $t < \frac{n}{3}$, unique reconstruction of the secret from the full set of n shares is possible, even if at most t shares are corrupted. This can be done efficiently, for instance by the Berlekamp-Welch decoding algorithm for Reed-Solomon codes.

Let p be a polynomial of degree at most t, and define $p(0) = s$. Let $\mathbf{s}$ be the vector with $s_i = p(i)$, $i = 1, \ldots, n$, and let $\mathbf{e}$ be a vector of Hamming-weight at most t. Write $\mathbf{c} = \mathbf{s} + \mathbf{e}$. Given $\mathbf{c}$ only, compute non-zero polynomials F and E with $\deg(F) \leq 2t$ and $\deg(E) \leq t$, such that $F(i) = c_i \cdot E(i)$, for $i = 1, \ldots, n$. This is in fact a system of linear equations in the coefficients of F and E, and it has a non-trivial solution. Actually, for every polynomial E such that $E(i) = 0$ whenever the i-th share is corrupted, that is, $c_i \neq e_i$, the polynomials $F = pE$ and E are a solution to the system. Moreover, from Lagrange's Interpolation Theorem, all solutions are in this form. Therefore, for all F, E that satisfy the system, it holds that $E(i) = 0$ if the i-th share is corrupted. The corrupted shares are then deleted by removing all c_i with $E(i) = 0$ from $\mathbf{c}$. All that remains are incorrupted shares, that is, $c_j = s_j$, and there will be more than t of those

left.

Below we present an efficient reconstruction algorithm for the more general situation where the secret is shared according to a strongly multiplicative LSSS with a $\mathcal{Q}_3$ access structure Γ. We do this by appropriately generalizing the Berlekamp-Welch algorithm. Note that such generalizations cannot generally rely on Lagrange's Interpolation Theorem, since LSSSs are not in general based on evaluation of polynomials.

Pellikaan [25] has previously generalized the Berlekamp-Welch algorithm and has shown that his generalized decoding algorithm applies to a much wider class of error correcting codes. Technically, our generalization bears some similarity to that of [25].

Strong multiplication was first considered in [9] and was used to construct efficient multi-party computation protocols with zero error in the active adversary model. More precisely it is used in the *Commitment Multiplication Protocol* to ensure that commitments for a, b and c are consistent in the sense that $ab = c$ with zero probability to cheat.

We now prove Theorem 4. Let $\Pi = (\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a sequence of linear forms $\pi_i \colon E \to \mathbb{K}$ such that $\Sigma = \Sigma_{n+1}(\Pi)$ is a strongly multiplicative LSSS with $\mathcal{Q}_3$ access structure $\Gamma = \Gamma_{n+1}(\Pi)$. Let us consider also the scheme $\Sigma^\mu = \Sigma^\mu_{n+1}(\Pi) = \Sigma_{n+1}(\pi_1 \otimes \pi_1, \ldots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1})$. From Lemma 8, the access structure of this scheme, $\Gamma^\mu = \Gamma^\mu_{n+1}(\Pi)$, is such that $\Gamma^* \subset \Gamma^\mu$.

Let us fix a basis for E and the induced basis of $E \otimes E$. Let M and $\widehat{M}$ be the matrices associated, respectively, to the schemes Σ and Σ^μ. Observe that, if $d = \dim E$, the matrix M has d rows and $n+1$ columns while $\widehat{M}$ has d^2 rows and $n+1$ columns.

If $\mathbf{u}, \mathbf{v} \in \mathbb{K}^k$, then $\mathbf{u} * \mathbf{v}$ denotes the vector $(u_1 v_1, \ldots, u_k v_k)$. Observe that $(\mathbf{x} \otimes \mathbf{y})\widehat{M} = ((\pi_i \otimes \pi_i)(\mathbf{x} \otimes \mathbf{y}))_{1 \le i \le n+1} = (\pi_i(\mathbf{x})\pi_i(\mathbf{y}))_{1 \le i \le n+1} = (\mathbf{x}M) * (\mathbf{y}M)$ for every pair of vectors $\mathbf{x}, \mathbf{y} \in E$.

Let us consider $\mathbf{s}' = (s_1, \ldots, s_n, s_{n+1}) = \mathbf{x}M$. Then, $\mathbf{s} = (s_1, \ldots, s_n)$ is a full set of shares for the secret $s_{n+1} = \pi_{n+1}(\mathbf{x})$. Let $A \subset P_{n+1}$ be a non-qualified subset, that is, $A \notin \Gamma$. Let $\mathbf{e} = (e_1, \ldots, e_n)$ be a vector with $e_i = 0$ for every $i \notin A$. Write $\mathbf{c} = (c_1, \ldots, c_n) = \mathbf{s} + \mathbf{e}$. Given only $\mathbf{c}$, the secret s_{n+1} is recovered efficiently as follows.

Let $\widehat{N}$ and N be the matrices that are obtained, respectively, from $\widehat{M}$ and M by removing the last column. Observe that $\mathbf{c} = \mathbf{x}N + \mathbf{e}$. Let us consider the system of linear equations

$$\begin{cases} \widehat{\mathbf{y}}\widehat{N} = \mathbf{c} * (\mathbf{y}N) \\ \pi_{n+1}(\mathbf{y}) = 1 \end{cases}$$

where the unknowns are the d^2 coordinates of the vector $\widehat{\mathbf{y}} \in E \otimes E$ and the d coordinates of the vector $\mathbf{y} \in E$. We claim that this system of linear equations always has a solution and that $s_{n+1} = (\pi_{n+1} \otimes \pi_{n+1})(\widehat{\mathbf{y}})$ for every solution $(\widehat{\mathbf{y}}, \mathbf{y})$. Therefore, the secret s_{n+1} can be obtained from $\mathbf{c}$ by solving that system of linear equations.

This is argued as follows. Note that $(\widehat{\mathbf{y}}, \mathbf{y})$ is a solution if and only if

$$(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y})\widehat{N} = \mathbf{e} * (\mathbf{y}N).$$

Since $A \notin \Gamma$, there exists a vector $\mathbf{z} \in E$ such that $\pi_{n+1}(\mathbf{z}) = 1$ while $\pi_i(\mathbf{z}) = 0$ for every $i \in A$. Observe that $(\mathbf{x} \otimes \mathbf{z}, \mathbf{z})$ is a solution for every vector $\mathbf{z} \in E$ in that situation. Indeed, $\mathbf{e} * (\mathbf{z}N) = 0$, because $\mathbf{z}N$ is zero where $\mathbf{e}$ is non-zero. Let $(\widehat{\mathbf{y}}, \mathbf{y})$ be an arbitrary

solution and consider $(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y})\widehat{M} = (t_1, \ldots, t_n, t_{n+1})$. Then, $(t_1, \ldots, t_n)$ are shares of the secret t_{n+1} according to the LSSS Σ^μ. Since $(t_1, \ldots, t_n) = \mathbf{e} * (\mathbf{y}N)$, we get that $t_i = 0$ for every $i \in P_{n+1} \setminus A$ and, hence, $t_{n+1} = 0$ because $P_{n+1} \setminus A \in \Gamma^* \subset \Gamma^\mu$. Finally, $(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y}) = t_{n+1} = 0$ and $(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\mathbf{y}}) = (\pi_{n+1} \otimes \pi_{n+1})(\mathbf{x} \otimes \mathbf{y}) = \pi_{n+1}(\mathbf{x})\pi_{n+1}(\mathbf{y}) = s_{n+1}$. □

A positive application of our latter result is as follows. Using a strongly multiplicative LSSS, the Commitment Multiplication Protocol (CMP) from [9] is directly a Verifiable Secret Sharing scheme (VSS). This saves a multiplicative factor n in the volume of communication needed, since the general reduction from VSS to CMP is not needed in this case.

References

[1] A. Barg. On some polynomials related to weight enumerators of linear codes. *SIAM J. Discrete Math.* **15** (2002) 155–164.

[2] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proc. ACM STOC'88* (1988) 1–10.

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

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

[5] T. Britz. MacWilliams identities and matroid polynomials. *Electron. J. Combin.* **9** (2002), Research Paper 19, 16 pp.

[6] P.J. Cameron. Cycle index, weight enumerator, and Tutte polynomial. *Electron. J. Combin.* **9** (2002), Note 2, 10 pp.

[7] R. Canetti, U. Feige, O. Goldreich, M. Naor. Adaptively secure multi-party computation. *Proc. ACM STOC'96* (1996) 639–648.

[8] D. Chaum, C. Crépeau, I. Damgård. Multi-party unconditionally secure protocols. *Proc. ACM STOC'88* (1988) 11–19.

[9] R. Cramer, I. Damgård, U. Maurer. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Comput. Sci.* **1807** (2000) 316–334.

[10] R. Cramer, S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups. *Advances in Cryptology - CRYPTO 2002, Lecture Notes in Comput. Sci.* **2442** (2002) 272–287.

[11] M. van Dijk. A linear construction of secret sharing schemes. *Des. Codes Cryptogr.* **12** (1997) 161–201.

[12] O. Goldreich, M. Micali, A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. *Proc.19th ACM Symposium on the Theory of Computing STOC'87* (1987) 218–229.

[13] M. Hirt and U. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation. *Proc. 16th Symposium on Principles of Distributed Computing PODC '97* (1997) 25–34.

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

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

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

[17] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, Boston, 1985.

[18] J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. In *Proceedings of the Third Conference on Security in Communication Networks '02, Lecture Notes in Comput. Sci.* **2576** (2003) 354–363. Amalfi, Italy, 2002.

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

[20] F. Matúš. Matroid representations by partitions. *Discrete Mathematics* **203** (1999) 169–194.

[21] S.-L. Ng. A Representation of a Family of Secret Sharing Matroids. *Des. Codes Cryptogr.* **30** (2003) 5-19.

[22] S.-L. Ng, M. Walker. On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptogr.* **24** (2001) 49-67.

[23] J.G. Oxley. *Matroid theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[24] C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory.* **46** (2000) 2596–2604. A previous version appeared in *Advances in Cryptology - EUROCRYPT'98, Lecture Notes in Comput. Sci.* **1403** (1998) 500-511.

[25] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.* **106/107** (1992) 369–381.

[26] Z. Reichstein, B. Youssin. Essential dimensions of algebraic groups and a resolution theorem for G-varieties. With an appendix by János Kollár and Endre Szabó. *Canad. J. Math.* **52** (2000) 1018–1056.

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

[28] G.J. Simmons. An introduction to shared secret and/or shared control schemes and their application. *Contemporary Cryptology. The Science of Information Integrity.* IEEE Press (1991), 441-497.

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

[30] D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.