On Codes, Matroids, and Secure Multiparty Computation From Linear Secret-Sharing Schemes

Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró, *Member, IEEE*

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

Two open problems related to the complexity of multiplicative LSSSs are considered in this paper. The first 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. A property of strongly multiplicative LSSSs that could be useful in solving this problem is proved. Namely, using a suitable generalization of the well-known Berlekamp–Welch decoder, it is shown that all strongly multiplicative LSSSs enable efficient reconstruction of a shared secret in the presence of malicious faults. The second one is to characterize the access structures of ideal multiplicative LSSSs. Specifically, the considered open problem is to determine whether all self-dual vector space access structures are in this situation. By the aforementioned connection, this in fact constitutes an open problem about matroid theory, since it can be restated in terms of representability of identically self-dual matroids by self-dual codes. A new concept is introduced, 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. It is proved 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.

***Index Terms*—Efficient error correction, multiparty computation, multiplicative linear secret sharing schemes, self-dual codes, self-dual matroids.**

I. Introduction

Two open problems on multiplicative linear secret sharing schemes (LSSSs) are studied in this paper. Our results deal with the connections between linear codes, representable matroids, and linear secret sharing schemes. Some facts about these connections are recalled in Section I-C, while basic notions on matroid theory are given in Section I-B. The reader is referred to [25], [35] for general reference books on matroid theory and to [6], [22], [32], [33] for more information about the relation between secret sharing schemes and matroids.

A. Multiplicative Linear Secret Sharing Schemes and General Secure Multiparty Computation

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

More formally, every sequence $\Pi = (\pi_1,\ldots,\pi_n,\pi_{n+1})$ of surjective linear mappings $\pi_i\colon E \to E_i$, where E and E_i are vector spaces of finite dimension over $\mathbb{K}$ and $E_{n+1} = \mathbb{K}$, defines a $\mathbb{K}$-linear secret sharing scheme $\Sigma_{n+1}(\Pi)$ on the set $P = \{1,\ldots,n\}$ of players. For every vector $\boldsymbol{x} \in E$, the values $(\pi_i(\boldsymbol{x}))_{1\le i\le n}$ are *shares* of the *secret value* $k = \pi_{n+1}(\boldsymbol{x}) \in \mathbb{K}$. The *access structure* $\Gamma_{n+1}(\Pi)$ of this scheme, that is, the family of *qualified subsets*, consists of all subsets $A \subseteq P$ such that $\bigcap_{i\in A} \ker \pi_i \subseteq \ker \pi_{n+1}$.

LSSSs are usually defined in a more general way by considering that the vector space E_{n+1} corresponding to the secret value is not necessarily equal to $\mathbb{K}$. We do not consider such LSSSs in this paper.

The *complexity* of an LSSS Σ is defined as

$$\lambda(\Sigma) = \sum_{i=1}^{n} \dim E_i \ge n$$

which corresponds to the total number of field elements that are distributed. The schemes with complexity $\lambda(\Sigma) = n$ are called *ideal*. For every finite field $\mathbb{K}$ and for every access structure Γ, there exists a $\mathbb{K}$-LSSS for Γ[16]. The minimum complexity of the $\mathbb{K}$-LSSSs with access structure Γ is denoted by $\lambda_{\mathbb{K}}(\Gamma)$. If there exists an ideal $\mathbb{K}$-LSSS for Γ, that is, if $\lambda_{\mathbb{K}}(\Gamma) = n$, we say that Γ is a $\mathbb{K}$-vector space access structure.

LSSSs were first considered, only in the ideal case, in [5]. General linear secret sharing schemes were introduced by Simmons [31], Jackson and Martin [17], and Karchmer and

Manuscript received January 26, 2007; revised October 4, 2007. This work was supported in part by the Spanish Ministerio de Ciencia y Tecnología under Project TIC 2003-00866. The material in this paper was presented in part at CRYPTO 2005, Santa Barbara, CA and an earlier version of this paper was published in the *Proceedings of CRYPTO 2005*.

R. Cramer is with the CWI, Amsterdam, The Netherlands and with the Mathematical Institute, Leiden University, Leiden, The Netherlands (e-mail: ronald.cramer@cwi.nl).

V. Daza is with the Universitat Rovira i Virgili, 43006 Tarragona, Spain (e-mail: vanesa.daza@urv.cat).

I. Gracia, J. Jiménez Urroz, J. Martí-Farré, and C. Padró are with Universitat Politècnica de Catalunya, 08034 Barcelona, Spain (e-mail: ignacio@ma4.upc.edu; jjimenez@ma4.upc.edu; jaumem@ma4.upc.edu; cpadro@ma4.upc.edu).

G. Leander is with the Horst-Görtz Institute for IT-Security, Ruhr-University D-44780 Bochum, Germany (e-mail: gregor.leander@ruhr-uni-bochum.de).

Communicated by H. Imai, Guest Editor for Special Issue on Information Theoretic Security.

Digital Object Identifier 10.1109/TIT.2008.921692

0018-9448/$25.00 © 2008 IEEE

Wigderson [18] under other names such as geometric secret sharing schemes or monotone span programs.

Secure multiparty computation protocols deal with the scenario in which n players want to compute an agreed function of their secret inputs in such a way that the correct result is obtained but no additional information about the inputs is released. These requirements should be achieved even in the presence of an *adversary* who is able to corrupt some players. The power of a *passive* adversary is limited to see all internal data of the corrupted adversaries, while an *active* one can control their behavior.

Unconditionally secure multiparty computation protocols are based on the share–compute–reconstruct paradigm [4], [10], [11]. Namely, the secret inputs are distributed into shares according to a secret sharing scheme, and some computations are performed on the shares to obtain shares of the value of the function, which can be finally recovered. Since every function can be described as an arithmetic circuit, it is enough to find methods to compute, from shares of two secret values, shares of its sum and its product.

In an LSSS, every 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 building blocks of multiparty computation protocols. Nevertheless, if we require protocols computing every 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 Shamir's (k, n)-threshold scheme [30]. In this scheme, the secret $s \in \mathbb{K}$ and the shares $s_i \in \mathbb{K}$, where $i = 1, \ldots, n$, are the values of a random polynomial with degree at most $k-1$ in some given points. The secret is recovered by Lagrange interpolation. If $n \geq 2k-1$, the product ss' of two secret values is a linear combination of every $2k-1$ values $c_i = s_i s'_i$. This linear combination is obtained by interpolating the product of the two random polynomials that were used to distribute the shares. This product is a polynomial with degree at most $2k-2$, and hence it can be interpolated from its values in $2k-1$ points. This multiplicative property of the Shamir's scheme is used in [4], [9], [10], [13], and many other works to construct multiparty computation protocols that are secure against a threshold-based adversary.

To obtain efficient multiparty computation protocols for a general adversary structure, a generalization of the multiplicative property of Shamir's scheme to general linear secret sharing schemes is proposed in [11].

Specifically, in a *multiplicative* LSSS over the finite field $\mathbb{K}$ (or $\mathbb{K}$-MLSSS for short), every player $i \in P$ can compute, from his shares s_i, s'_i of two shared secrets $s, s' \in \mathbb{K}$, a value $c_i \in \mathbb{K}$ such that the product ss' is a linear combination of all the values $c_1, \ldots, c_n$. We say that an LSSS is *strongly multiplicative* if, for every subset $A \subseteq P$ such that $P - A$ is not qualified, the product ss' can be computed using only values from the players in A.

Observe that Shamir's (k, n)-secret sharing scheme is multiplicative if and only if $n \geq 2k-1$, and it is strongly multiplicative if and only if $n \geq 3k-2$. An access structure is said to be $\mathcal{Q}_2$, or $\mathcal{Q}_3$, if the set of players is not the union of any two, or, respectively, three, unqualified subsets. In general, as a consequence of the results in [11], [15], an access structure Γ can be realized by a multiplicative LSSS if and only if it is $\mathcal{Q}_2$, and Γ admits a strongly multiplicative LSSS if and only if it is $\mathcal{Q}_3$.

Cramer, Damgård, and Maurer [11] presented a method to construct, from every $\mathbb{K}$-MLSSS Σ with $\mathcal{Q}_2$ access structure Γ, an error-free multiparty computation protocol secure against a passive adversary which is able to corrupt any set of players $B \notin \Gamma$ and computing every 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 proved 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 [11] is a method to construct, from every $\mathbb{K}$-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 every finite field $\mathbb{K}$ and for every $\mathcal{Q}_2$ access structure Γ.

Therefore, in the passive adversary case, the construction of efficient multiparty computation protocols can be reduced to the search of efficient LSSSs. Specifically, a multiparty computation protocol computing every arithmetic circuit C over $\mathbb{K}$ and secure against a passive adversary which is able to corrupt any set of players $B \notin \Gamma$ can be efficiently constructed from every LSSS whose access structure Γ' is $\mathcal{Q}_2$ and $\Gamma' \subseteq \Gamma$.

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

Nevertheless, the active adversary case is also solved in [11] if an exponentially small error probability is allowed. A construction is given in [11] for the active adversary case that efficiently provides, from every LSSS with $\mathcal{Q}_3$ access structure Γ, a multiparty computation protocol with exponentially small error probability, secure against an active adversary which is able to corrupt any set of players not in Γ.

B. Matroid Theory Definitions

We recall here some definitions and basic facts about matroids. There exist many different equivalent definitions of matroid. The one we present here is based on the concept of *basis*.

Definition 1.1: A *matroid* $\mathcal{M} = (Q, \mathcal{B})$ consists of a finite set Q together with a family $\mathcal{B}$ of subsets of Q such that

1) $\mathcal{B}$ is nonempty, and
2) for every $B_1, B_2 \in \mathcal{B}$ and $i \in B_1 - B_2$, there exists $j \in B_2 - B_1$ such that $(B_1 - \{i\}) \cup \{j\}$ is in $\mathcal{B}$.

The set Q is the *ground set* of the matroid $\mathcal{M}$ and the sets in $\mathcal{B}$ are called the *bases* of $\mathcal{M}$. All sets in $\mathcal{B}$ have the same number of elements, which is $r(\mathcal{M})$, the *rank* of $\mathcal{M}$.

The concept of matroid is an abstraction of the relations of linear dependence among a finite set of vectors in a vector space. Actually, an important class of matroids, the representable ones, are defined from sets of vectors in a vector space. Consider a sequence of vectors $\Pi = (\pi_1, \ldots, \pi_n, \pi_{n+1})$ in a

$\mathbb{K}$-vector space F and suppose that those vectors span F. The sequence Π defines a matroid $\mathcal{M} = \mathcal{M}(\Pi) = (Q, \mathcal{B})$, where $Q = \{1, \ldots, n, n+1\}$ and $\{i_1, \ldots, i_k\} \in \mathcal{B}$ if and only if $\{\pi_{i_1}, \ldots, \pi_{i_k}\}$ is a basis of F. The matroids that can be defined in this way are called $\mathbb{K}$-*representable*.

For instance, consider a finite field $\mathbb{K}$ with characteristic greater than 3 and the sequence of vectors $\Pi = (\pi_1, \ldots, \pi_6)$ in $F = \mathbb{K}^3$ corresponding to the columns of the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{pmatrix}. \qquad (1)$$

Then the bases of the matroid $\mathcal{M} = \mathcal{M}(\Pi)$ are all subsets of $Q = \{1, \ldots, 6\}$ with three elements except $\{1, 2, 6\}$ and $\{3, 4, 6\}$.

Another interesting example of matroids are the *graphic* ones. For a connected graph G, consider the set E of its edges. The graphic matroid $\mathcal{M}$ defined by the graph G is $\mathcal{M} = (E, \mathcal{B})$, where $B \subseteq E$ is a basis of $\mathcal{M}$ if and only B is the set of edges of a spanning tree of G. Graphic matroids are representable over every finite field [25, Proposition 5.1.2].

We need to introduce more terminology on matroids. A subset $X \subseteq Q$ is said to be *independent* if there exists a basis $B \in \mathcal{B}$ with $X \subseteq B$. 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. A point $i \in Q$ is called a *loop* if $\{i\}$ is a dependent subset and a *coloop* is a point $i \in Q$ such that $i \in B$ for every basis $B \in \mathcal{B}$.

The *rank* of $X \subseteq Q$, which is denoted by $r(X)$, is the maximum cardinality of the subsets of X that are independent. Clearly, $r(\mathcal{M}) = r(Q)$. We say that $X \subseteq Q$ is a *flat* if $r(X \cup \{i\}) > r(X)$ for every $i \notin X$. The flat $\mathrm{cl}(X) = \{i \in Q : r(X \cup \{i\}) = r(X)\}$ is called the *closure* of X. If X is a flat, every maximally independent subset $B \subseteq X$ 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 $\mathcal{B}^* = \{Q - B : B \in \mathcal{B}\}$ 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.

C. Codes, Matroids, and Secret Sharing Schemes

In this section, we describe the connections between linear codes, representable matroids, and ideal LSSSs. We begin by introducing some notation. In particular, we introduce the notation Π for a sequence of linear forms, which will substantially simplify our work and will highlight even more the connections between the mentioned concepts.

Consider $Q = \{1, \ldots, n, n+1\}$ and $P_i = Q - \{i\}$ for every $i \in Q$. This notation will be used all through the paper. From now on, vectors appearing in matrix operations will be considered as one-row matrices.

Let E be a $\mathbb{K}$-vector space with $\dim E = k$ and let $\Pi = (\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a sequence of surjective linear mappings $\pi_i : E \rightarrow \mathbb{K}$, that is, nonzero vectors in the dual space E^*. We are going to suppose always that these vectors span E^*. Observe that Π can be seen as a linear mapping $\Pi : E \rightarrow \mathbb{K}^{n+1}$ and, once a basis of E is fixed, it can be represented by the $k \times (n+1)$ matrix $M = M(\Pi)$ such that $\Pi(\boldsymbol{x}) = \boldsymbol{x}M$ for all $\boldsymbol{x} \in E$. Observe that $\mathrm{rank}(M) = k$ and that the ith column of M corresponds to the linear form π_i.

The matrix M is a generator matrix of an $[n+1, k]$ linear code $\mathcal{C} = \mathcal{C}(\Pi)$. Actually

$$\mathcal{C}(\Pi) = \{(\pi_1(\boldsymbol{x}), \ldots, \pi_n(\boldsymbol{x}), \pi_{n+1}(\boldsymbol{x})) : \boldsymbol{x} \in E\}.$$

The columns of M define a $\mathbb{K}$-representable matroid $\mathcal{M} = \mathcal{M}(\Pi)$ on the set of points Q. For example, we described before the matroid defined by the matrix M in (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 $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. Observe that different codes can represent the same matroid.

Greene's theorem [14], which relates the weight enumerator of a code to the Tutte polynomial of its associated matroid, is the best known result about that connection between codes and matroids. Several works have appeared afterwards on that subject [1], [7], [8], [12].

In addition, the code $\mathcal{C}$ defines an ideal LSSS $\Sigma_i(\Pi)$ for every $i \in Q$. The codewords of $\mathcal{C}$ are precisely the vectors of $\mathbb{K}^{n+1}$ of the form $(\pi_1(\boldsymbol{x}), \ldots, \pi_i(\boldsymbol{x}), \ldots, \pi_{n+1}(\boldsymbol{x}))$ with $\boldsymbol{x} \in E$ and, for every $i \in Q$, they can be seen as distributions of shares for the secret value $\pi_i(\boldsymbol{x}) \in \mathbb{K}$ among the players in $P_i = Q - \{i\}$. Observe that the access structure $\Gamma_i(\Pi)$ of the scheme $\Sigma_i(\Pi)$, which is a $\mathbb{K}$-vector space access structure, consists of all subsets $A \subseteq P_i$ such that $\pi_i \in \langle \pi_j : j \in A \rangle$. Therefore, $A \subseteq P_i$ is a minimal qualified subset in that structure if and only if $A \cup \{i\}$ is a circuit of the matroid $\mathcal{M}(\Pi)$. As a consequence, the access structures $\Gamma_i(\Pi)$ are determined by the matroid $\mathcal{M}(\Pi)$. This connection between ideal secret sharing schemes and matroids, which applies to nonlinear schemes as well, was discovered by Brickell and Davenport [6] and has been studied afterwards by several authors [2], [21], [22], [32]. It plays a key role in one of the main open problems in secret sharing: the characterization of the access structures of ideal secret sharing schemes.

Example 1.2: Consider the sequence Π given by the matrix M in (1), which defines a matroid $\mathcal{M} = \mathcal{M}(\Pi)$ on the set $Q = \{1, \ldots, 6\}$. The circuits of the matroid $\mathcal{M}$ that contain the point 6 are $\{1,2,6\}$, $\{3,4,6\}$, $\{1,3,5,6\}$, $\{1,4,5,6\}$, $\{2,3,5,6\}$, and $\{2,4,5,6\}$. Therefore, the minimal qualified subsets of $\Gamma_6(\Pi)$ are $\{1,2\}$, $\{3,4\}$, $\{1,3,5\}$, $\{1,4,5\}$, $\{2,3,5\}$, and $\{2,4,5\}$. Analogously, one can check that the minimal qualified subsets of the access structure $\Gamma_5(\Pi)$ are all subsets of $P_5 = Q - \{5\}$ with three elements except $\{1,2,6\}$ and $\{3,4,6\}$.

Example 1.3: We describe next Shamir's secret sharing scheme by using our notation. Consider the sets $Q = \{1, \ldots, n, n+1\}$ and $P_{n+1} = Q - \{n+1\}$. For a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n+1$, we take the vector space E formed by all polynomials over $\mathbb{K}$ with degree at most $k-1$. We take as well $n+1$ different elements $x_1, \ldots, x_n, x_{n+1} \in \mathbb{K}$ and, for every $i \in Q$, we define the linear form $\pi_i : E \rightarrow \mathbb{K}$ by $\pi_i(f) = f(x_i)$. Clearly, the secret sharing scheme $\Sigma_{n+1}(\Pi)$

defined by the sequence $\Pi = (\pi_1, \dots, \pi_n, \pi_{n+1})$ is equivalent to Shamir's secret sharing scheme.

Actually, nonideal LSSSs can also be represented as linear codes. In the general case, several columns of the generator matrix are assigned to every player.

Error correction in linear codes is related to an important property of secret sharing schemes: the possibility of reconstructing the shared secret value even if some shares are not correct.

The different notions of *duality* that are defined for codes, for matroids, and for access structures are closely related.

Let N be a parity-check matrix for the code $\mathcal{C} = \mathcal{C}(\Pi)$. That is, N is an $(n-k+1)\times(n+1)$ matrix with $\operatorname{rank}(N) = n-k+1$ and $MN^\top = 0$, where $N^\top$ denotes the transpose of N. The matrix N is a generator matrix of an $[n+1, n-k+1]$ linear code $\mathcal{C}^\perp$, which is called the *dual code* of the code $\mathcal{C}$. The code $\mathcal{C}$ is said to be *self-dual* if $\mathcal{C}^\perp = \mathcal{C}$. In this case, $2k = n+1$ and $MM^\top = 0$ for every generator matrix M.

If the linear code $\mathcal{C}$ defines a (not necessarily ideal) LSSS with access structure Γ on the set P of players, then the dual code $\mathcal{C}^\perp$ defines an LSSS for the dual access structure $\Gamma^* = \{A \subseteq P : P - A \notin \Gamma\}$. As a consequence of this fact, $\lambda_{\mathbb{K}}(\Gamma^*) = \lambda_{\mathbb{K}}(\Gamma)$ for every access structure Γ and for every finite field $\mathbb{K}$.

The matroid $\mathcal{N}$ associated to the dual code $\mathcal{C}^\perp$ is the *dual matroid* of the matroid $\mathcal{M}$ corresponding to $\mathcal{C}$, that is, the family of bases of $\mathcal{N} = \mathcal{M}^*$ is $\mathcal{B}(\mathcal{M}^*) = \{B \subseteq Q : Q - B \in \mathcal{B}(\mathcal{M})\}$, where $\mathcal{B}(\mathcal{M})$ is the family of bases of $\mathcal{M}$. Moreover, for every $i \in Q$, 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.

Observe that the matroid $\mathcal{M}$ associated to a self-dual code is identically self-dual, that is, $\mathcal{M} = \mathcal{M}^*$. Nevertheless, it is not known whether every representable identically self-dual matroid can be represented by a self-dual code.

Duality plays an important role in the study of the multiplicative property of LSSSs. First of all, an access structure Γ is $\mathcal{Q}_2$ if and only if $\Gamma^* \subseteq \Gamma$. This fact and the aforementioned relation between duality in codes and LSSSs are the key points in the proof of the bound $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ given in [11]. In addition, all ideal LSSSs defined by self-dual codes are multiplicative and, hence, their access structures are such that $\mu_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma)$.

II. Our Results

A. *On Strongly Multiplicative LSSSs*

The first open problem we consider in this paper deals with the efficient construction of strongly multiplicative LSSSs. 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.

We shed some light on that problem by proving a new property of strongly multiplicative LSSSs. Using a suitable generalization of the well-known Berlekamp–Welch decoder for Reed–Solomon codes, we show (Theorem 1) 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 1: Let $\boldsymbol{s} = (s_1, \dots, s_n)$ be a full vector of shares for a secret $s \in \mathbb{K}$, computed according to a strongly multiplicative $\mathbb{K}$-LSSS with access structure Γ on n players. Let $\boldsymbol{e}$ 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 $\boldsymbol{c} = \boldsymbol{s} + \boldsymbol{e}$. Then the secret s can be recovered from $\boldsymbol{c}$ in time $\operatorname{poly}(n, \log|\mathbb{K}|)$.

B. *On Ideal Multiplicative LSSSs*

The characterization of the access structures of ideal multiplicative LSSSs (MLSSSs) is the second open problem that is studied in this work. That is, we are interested in determining which $\mathcal{Q}_2$ vector space access structures can be realized by an ideal MLSSS or, equivalently, for which $\mathcal{Q}_2$ access structures there exists a finite field $\mathbb{K}$ with $\mu_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma) = n$.

This is a case of the more general problem of determining the cases in which the factor 2 loss in the construction of MLSSSs given in [11] 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.

The (k, n)-threshold structures with $n \geq 2k-1$ are examples of access structures that can be realized by an ideal LSSS. Other examples are obtained from self-dual codes. If the linear code $\mathcal{C}(\Pi)$ is self-dual, then the ideal LSSSs $\Sigma_i(\Pi)$, where $i \in Q$, are multiplicative. Therefore, for every $i \in Q$, the vector space access structure $\Gamma_i = \Gamma_i(\Pi)$ is such that $\mu_{\mathbb{K}}(\Gamma_i) = \lambda_{\mathbb{K}}(\Gamma_i) = n$. Observe that these access structures are self-dual, that is, $\Gamma_i^* = \Gamma_i$.

On the other hand, there exist examples of $\mathcal{Q}_2$ access structures Γ such that $\lambda_{\mathbb{K}}(\Gamma) = n$ for some finite field $\mathbb{K}$ but do not admit any ideal MLSSS over any finite field. The arguments that are used to prove this fact do not apply if a self-dual vector space access structure is considered. An infinite family of such examples is given in Section V.

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 every substructure $\Gamma' \subsetneq \Gamma$ is not $\mathcal{Q}_2$. The results in this paper, and the fact that no counterexample has been found, lead us to state the following open problem. One of the objectives of this paper is to move forward in the search of its solution.

Open Problem 1: Determine whether there exists, for every self-dual $\mathbb{K}$-vector space access structure Γ, an ideal multiplicative $\mathbb{L}$-LSSS, where $\mathbb{L}$ is some finite extension of $\mathbb{K}$.

Since $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ for every $\mathcal{Q}_2$ 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 at the core of the multiplicative property. For instance, the construction in [11] 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, the interest of Problem 1 is increased by the fact that 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 in Section V that Open Problem 1 is equivalent to the following one.

Open Problem 2: Determine whether every identically self-dual $\mathbb{K}$-representable matroid can be represented by a self-dual linear code over some finite extension of $\mathbb{K}$.

Finally, we think that the results and techniques in this paper, and the ones that possibly will be found in future research on that problem, can provide a better understanding of the multiplicative property and may be useful to find new results on the existence of efficient strongly multiplicative LSSSs. In particular, the study of the characterization of the access structures of ideal strongly multiplicative LSSSs, which should be also attacked by using matroid theory, may lead to interesting advances on that problem. For instance, one can observe a remarkable difference in the strong multiplicative case: the minimality of the $\mathcal{Q}_3$ property does not imply any important matroid property comparable to self-duality.

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 $\mathbb{K}$. Every 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 $U_{k,n}$ and the $\mathbb{Z}_2$-representable matroids are the only families of matroids for which it was known that all identically self-dual matroids are self-dually representable. It has been proved recently that this property also holds for the identically self-dual matroids on at most eight points [26].

There exist several methods to combine some given matroids into a new one. The *2-sum*, whose definition is recalled in Section VI, is one of them. We show in Section VI that the 2-sum of two self-dually representable matroids is equally self-dually representable and that Problem 2 can be restricted to indecomposable matroids, that is, matroids that are not a nontrivial 2-sum of smaller matroids.

To take the first steps in solving Problem 2, we introduce the concept of *flat-partition* of a matroid, which is defined in Section VI. On one hand, we use the flat-partitions to characterize in Proposition 6.5 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 $U_{k,2k}$, which, as we said before, are self-dually representable.

We prove in Theorem 2 that all 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 [27]. As a consequence of the results in [27], bipartite matroids are representable. Bipartite matroids have been independently studied in [23], [24], where they are called matroids with two uniform components.

Bipartite access structures are also interesting for their applications because they appear in a natural way in situations in which the players are divided into two different classes. They are closely related to other families of access structures that have practical interest as well: the hierarchical access structures [34] and the weighted threshold access structures [3], [30].

Theorem 2: Every identically self-dual bipartite matroid can be represented by a self-dual linear code over some finite field. Equivalently, every self-dual bipartite vector space access structure can be realized by an ideal MLSSS over some finite field.

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.

III. Multiplicative LSSSs

Some definitions and basic results about MLSSSs are given in the following.

We begin by recalling some notation and elementary facts about bilinear forms. A bilinear form on a $\mathbb{K}$-vector space E is a mapping $\omega: E \times E \to \mathbb{K}$ that is linear in both variables, that is,

- $\omega(\lambda_1 \boldsymbol{x}_1 + \lambda_2 \boldsymbol{x}_2, \boldsymbol{y}) = \lambda_1 \omega(\boldsymbol{x}_1, \boldsymbol{y}) + \lambda_2 \omega(\boldsymbol{x}_2, \boldsymbol{y})$ for every $\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y} \in E$ and $\lambda_1, \lambda_2 \in \mathbb{K}$, and
- $\omega(\boldsymbol{x}, \lambda_1 \boldsymbol{y}_1 + \lambda_2 \boldsymbol{y}_2) = \lambda_1 \omega(\boldsymbol{x}, \boldsymbol{y}_1) + \lambda_2 \omega(\boldsymbol{x}, \boldsymbol{y}_2)$ for every $\boldsymbol{x}, \boldsymbol{y}_1, \boldsymbol{y}_2 \in E$ and $\lambda_1, \lambda_2 \in \mathbb{K}$.

If $\alpha, \beta: E \to \mathbb{K}$ are linear forms, $\alpha \otimes \beta$ denotes the bilinear form $\alpha \otimes \beta: E \times E \to \mathbb{K}$ defined by $(\alpha \otimes \beta)(\boldsymbol{x}, \boldsymbol{y}) = \alpha(\boldsymbol{x})\beta(\boldsymbol{y})$. For instance, if $\pi_i: E \to \mathbb{K}$ is one of the linear forms we introduced in Example 1.3 to define Shamir's secret sharing scheme, the bilinear form $\pi_i \otimes \pi_i: E \times E \to \mathbb{K}$ satisfies that $\pi_i \otimes \pi_i(f, g) = f(x_i)g(x_i)$ for every pair of polynomials $f, g \in E$.

The bilinear forms $\alpha \otimes \beta$ span the vector space of all bilinear forms on E, which is denoted by $E^* \otimes E^*$ and has dimension k^2, where $k = \dim E$. Actually, if $\{\boldsymbol{e}^1, \ldots, \boldsymbol{e}^k\}$ is a basis of E^*, then $\{\boldsymbol{e}^i \otimes \boldsymbol{e}^j : 1 \leq i, j \leq k\}$ 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 $\{\boldsymbol{x} \otimes \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in E\}$. Finally, observe that $(E \otimes E)^* = E^* \otimes E^*$. This is due to the fact that every bilinear form $\alpha \otimes \beta \in E^* \otimes E^*$ induces a linear form $\alpha \otimes \beta: E \otimes E \to \mathbb{K}$, determined by $(\alpha \otimes \beta)(\boldsymbol{x} \otimes \boldsymbol{y}) = \alpha(\boldsymbol{x})\beta(\boldsymbol{y})$.

If $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ is an LSSS and $A \subseteq P_{n+1}$, we write Σ_A for the natural restriction of Σ to the players in A, that is, the scheme defined by the linear mappings $((\pi_i)_{i \in A}, \pi_{n+1})$. The next definition deals with general (not necessarily ideal) LSSSs.

Definition 3.1: Let $\Sigma = \Sigma_{n+1}(\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a $\mathbb{K}$-LSSS with access structure $\Gamma = \Gamma_{n+1}(\Pi)$. The scheme Σ is said to be *multiplicative* if, for every $i \in P_{n+1} = \{1, \dots, n\}$, there exists a bilinear form $\phi_i: E_i \times E_i \to \mathbb{K}$ such that

$$(\pi_{n+1} \otimes \pi_{n+1})(\boldsymbol{x}_1, \boldsymbol{x}_2) = \sum_{i=1}^{n} \phi_i(\pi_i(\boldsymbol{x}_1), \pi_i(\boldsymbol{x}_2))$$

for every pair of vectors $\boldsymbol{x}_1, \boldsymbol{x}_2 \in E$. We say that Σ is *strongly multiplicative* if the scheme $\Sigma_{P_{n+1}-A}$ is multiplicative for every $A \subseteq P_{n+1}$ 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 $\phi: \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ is of the form $\phi(x, y) = \lambda xy$ for some $\lambda \in \mathbb{K}$. Therefore, Σ is multiplicative if and only if there exist values $\lambda_i \in \mathbb{K}$ such that

$$\pi_{n+1} \otimes \pi_{n+1} = \sum_{i=1}^{n} \lambda_i(\pi_i \otimes \pi_i). \tag{2}$$

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

$$\pi_{n+1} \otimes \pi_{n+1} = \sum_{i \in P_{n+1}-A} \lambda_{i,A}(\pi_i \otimes \pi_i). \tag{3}$$

The values λ_i or $\lambda_{i,A}$ form the *recombination vector* introduced in [11].

Since the bilinear forms $\pi_i \otimes \pi_i$ can be seen as vectors in $(E \otimes E)^*$, we can consider the LSSS

$$\Sigma_{n+1}^{\mu}(\Pi) = \Sigma_{n+1}(\pi_1 \otimes \pi_1, \dots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1})$$

which has access structure

$$\Gamma_{n+1}^{\mu}(\Pi) = \Gamma_{n+1}(\pi_1 \otimes \pi_1, \dots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1}).$$

That is, $A \in \Gamma_{n+1}^{\mu}(\Pi)$ 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 3.2: Let $\Sigma = \Sigma_{n+1}(\Pi)$ be an ideal LSSS. Then the following properties hold.

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

Proof: Let $A \subseteq P_{n+1}$ be a subset with $A \in \Gamma_{n+1}^{\mu}(\Pi)$. 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 $\boldsymbol{x} \in E$ with $\pi_{n+1}(\boldsymbol{x}) = 1$, 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. □

IV. Reconstruction of a Secret in the Presence of Errors

Let $\boldsymbol{s} = (s_1, \dots, s_n)$ be a full vector of shares for a secret $s \in \mathbb{K}$, computed according to $\mathbb{K}$-LSSS with $\mathcal{Q}_3$ access structure Γ. Consider $\boldsymbol{c} = \boldsymbol{s} + \boldsymbol{e}$, where $\boldsymbol{e}$ denotes the errors that have been introduced in the shares by the participants in an unqualified set $A \notin \Gamma$, that is, $e_i = 0$ if $i \notin A$. Then the secret value s can be determined from the vector $\boldsymbol{c}$. This is proved by checking that, if $\boldsymbol{c} = \boldsymbol{s_1} + \boldsymbol{e_1} = \boldsymbol{s_2} + \boldsymbol{e_2}$ for some pair of collections of shares $\boldsymbol{s_1}$, $\boldsymbol{s_2}$, and some pair of error vectors $\boldsymbol{e_1}$, $\boldsymbol{e_2}$ corresponding, respectively, to unqualified subsets $A_1, A_2 \notin \Gamma$, then the shares in $\boldsymbol{s_1}$ and $\boldsymbol{s_2}$ correspond to the same secret value. Since the access structure Γ is $\mathcal{Q}_3$, the set $B = P - (A_1 \cup A_2)$ is qualified. In addition, $s_{1i} = s_{2i}$ for every $i \in B$, and hence $\boldsymbol{s_1}$ and $\boldsymbol{s_2}$ must be collections of shares for the secret $s \in \mathbb{K}$ that is determined by the shares $(s_{1i})_{i \in B} = (s_{2i})_{i \in B}$ corresponding to the qualified subset $B \in \Gamma$.

Therefore, in every 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 1, 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 $t < n/3$, 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, as we explain in the following.

Let p be a polynomial of degree at most t, and define $p(0) = s$. Let $\boldsymbol{s}$ be the vector with $s_i = p(i)$, $i = 1, \dots, n$, and let $\boldsymbol{e}$ be a vector of Hamming weight at most t. Write $\boldsymbol{c} = \boldsymbol{s} + \boldsymbol{e}$. Given $\boldsymbol{c}$ only, compute nonzero polynomials F and E with $\deg(F) \leq 2t$ and $\deg(E) \leq t$, such that $F(i) = c_i \cdot E(i)$, for $i = 1, \dots, n$. This is in fact a system of linear equations in the coefficients of F and E, and it has a nontrivial solution. Actually, for every polynomial E such that $E(i) = 0$ whenever the ith share is corrupted, that is, $c_i \neq s_i$, 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 ith share is corrupted. The corrupted shares are then deleted by removing all c_i with $E(i) = 0$ from $\boldsymbol{c}$. All that remains are uncorrupted shares, that is, $c_j = s_j$, and there will be more than t of those left.

In the following, 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. Technically, our generalization bears some similarity to the decoding algorithm proposed by Pellikaan [28].

Strong multiplication was first considered in [11] and was used to construct efficient multiparty computation protocols with zero error probability 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 1. Let $\Pi = (\pi_1, \dots, \pi_n, \pi_{n+1})$ be a sequence of linear forms $\pi_i : E \to \mathbb{K}$ such that $\Sigma = \Sigma_{n+1}(\Pi)$ is a strongly multiplicative LSSS with $\mathcal{Q}_3$ access structure $\Gamma = \Gamma_{n+1}(\Pi)$. Consider also the scheme

$$\Sigma^\mu = \Sigma^\mu_{n+1}(\Pi) = \Sigma_{n+1}(\pi_1 \otimes \pi_1, \dots, \pi_n \otimes \pi_n, \pi_{n+1} \otimes \pi_{n+1}).$$

From Lemma 3.2, the access structure of this scheme, $\Gamma^\mu = \Gamma^\mu_{n+1}(\Pi)$ is such that $\Gamma^* \subseteq \Gamma^\mu$.

Take 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 $k = \dim E$, the matrix M has k rows and $n+1$ columns while $\widehat{M}$ has k^2 rows and $n+1$ columns.

If $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^m$, then $\boldsymbol{u} * \boldsymbol{v}$ denotes the vector $(u_1 v_1, \dots, u_m v_m)$. Observe that

$$\begin{aligned}(\boldsymbol{x} \otimes \boldsymbol{y})\widehat{M} &= ((\pi_i \otimes \pi_i)(\boldsymbol{x} \otimes \boldsymbol{y}))_{1 \le i \le n+1} \\ &= (\pi_i(\boldsymbol{x})\pi_i(\boldsymbol{y}))_{1 \le i \le n+1} \\ &= (\boldsymbol{x}M) * (\boldsymbol{y}M) \end{aligned} \tag{4}$$

every pair of vectors $\boldsymbol{x}, \boldsymbol{y} \in E$.

Consider $\boldsymbol{s}' = (s_1, \dots, s_n, s_{n+1}) = \boldsymbol{x}M$. Then $\boldsymbol{s} = (s_1, \dots, s_n)$ is a full set of shares for the secret $s_{n+1} = \pi_{n+1}(\boldsymbol{x})$. Let $A \subseteq P_{n+1}$ be a nonqualified subset, that is, $A \notin \Gamma$. Let $\boldsymbol{e} = (e_1, \dots, e_n)$ be a vector with $e_i = 0$ for every $i \notin A$. Write $\boldsymbol{c} = (c_1, \dots, c_n) = \boldsymbol{s} + \boldsymbol{e}$. Given only $\boldsymbol{c}$, 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 $\boldsymbol{c} = \boldsymbol{x}N + \boldsymbol{e}$. Consider the system of linear equations

$$\begin{cases} \widehat{\boldsymbol{y}}\widehat{N} = \boldsymbol{c} * (\boldsymbol{y}N) \\ \pi_{n+1}(\boldsymbol{y}) = 1 \end{cases} \tag{5}$$

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

This is argued as follows. We prove first that $(\widehat{\boldsymbol{y}}, \boldsymbol{y})$ is a solution of (5) if and only if $(\widehat{\boldsymbol{y}} - \boldsymbol{x} \otimes \boldsymbol{y})\widehat{N} = \boldsymbol{e} * (\boldsymbol{y}N)$ and $\pi_{n+1}(\boldsymbol{y}) = 1$. Effectively, $(\boldsymbol{x}N) * (\boldsymbol{y}N) = (\boldsymbol{x} \otimes \boldsymbol{y})\widehat{N}$ by (4), and hence

$$\begin{aligned}\boldsymbol{c} * (\boldsymbol{y}N) &= (\boldsymbol{x}N + \boldsymbol{e}) * (\boldsymbol{y}N) \\ &= (\boldsymbol{x} \otimes \boldsymbol{y})\widehat{N} + \boldsymbol{e} * (\boldsymbol{y}N).\end{aligned}$$

that, since $A \notin \Gamma$, there exists a vector $\boldsymbol{z} \in E$ such that $\pi_{n+1}(\boldsymbol{z}) = 1$ while $\pi_i(\boldsymbol{z}) = 0$ for every $i \in A$. Then $(\boldsymbol{x} \otimes \boldsymbol{z}, \boldsymbol{z})$ is a solution of (5) for every vector $\boldsymbol{z} \in E$ in that situation. Indeed, $\boldsymbol{e} * (\boldsymbol{z}N) = 0$, because $\boldsymbol{z}N$ is zero where $\boldsymbol{e}$ is nonzero. Let $(\widehat{\boldsymbol{y}}, \boldsymbol{y})$ be an arbitrary solution and consider $(\widehat{\boldsymbol{y}} - \boldsymbol{x} \otimes \boldsymbol{y})\widehat{M} = (t_1, \dots, t_n, t_{n+1})$. Then $(t_1, \dots, t_n)$ are shares of the secret t_{n+1} according to the LSSS Σ^μ. Since $(t_1, \dots, t_n) = \boldsymbol{e} * (\boldsymbol{y}N)$, we get that $t_i = 0$ for every $i \in P_{n+1} - A$ and, hence, $t_{n+1} = 0$ because $P_{n+1} - A \in \Gamma^* \subseteq \Gamma^\mu$. Finally

$$(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\boldsymbol{y}} - \boldsymbol{x} \otimes \boldsymbol{y}) = t_{n+1} = 0$$

and

$$\begin{aligned}(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\boldsymbol{y}}) &= (\pi_{n+1} \otimes \pi_{n+1})(\boldsymbol{x} \otimes \boldsymbol{y}) \\ &= \pi_{n+1}(\boldsymbol{x})\pi_{n+1}(\boldsymbol{y}) = s_{n+1}.\end{aligned}$$

A positive application of Theorem 1 is as follows. Using a strongly multiplicative LSSS, the Commitment Multiplication Protocol from [11] is directly a verifiable secret sharing scheme. This saves a multiplicative factor n in the volume of communication needed, since the general reduction from verifiable secret sharing scheme to the Commitment Multiplication Protocol is not needed in this case.

V. Ideal Multiplicative LSSSs, Self-Dual Linear Codes, and Identically Self-dual Matroids

The aim of this section is to explain in detail the connections between ideal multiplicative LSSSs, self-dual linear codes, and identically self-dual matroids. We prove the equivalence between Open Problem 1 and Open Problem 2.

A. Ideal LSSSs, Linear Codes, and Matroids

Let E be a vector space with $\dim E = k$ over a finite field $\mathbb{K}$ and consider a sequence $\Pi = (\pi_1, \dots, \pi_n, \pi_{n+1})$ of linear forms in E^*. Recall that we are assuming that those vectors span E^*. As we saw before, Π defines an $[n+1, k]$ linear code $\mathcal{C} = \mathcal{C}(\Pi)$ that consists of the codewords of the form $(\pi_1(\boldsymbol{x}), \dots, \pi_n(\boldsymbol{x}), \pi_{n+1}(\boldsymbol{x}))$ for some $\boldsymbol{x} \in E$. The matroid $\mathcal{M} = \mathcal{M}(\Pi)$ is the matroid associated to the code $\mathcal{C}$, which is said to be a $\mathbb{K}$-representation of $\mathcal{M}$.

In addition, the sequence Π defines an ideal secret sharing scheme $\Sigma_i(\Pi)$ on the set of players $P_i = Q - \{i\}$ for every $i \in Q = \{1, \dots, n, n+1\}$. Observe that the access structure $\Gamma_i(\Pi)$ of the scheme $\Sigma_i(\Pi)$, which is a $\mathbb{K}$-vector space access structure, is determined by the $\mathbb{K}$-representable matroid $\mathcal{M} = \mathcal{M}(\Pi)$. Actually, $A \subseteq P_i$ is in $\Gamma_i(\Pi)$ if and only if $r(A \cup \{i\}) = r(A)$, where we are considering the rank function of $\mathcal{M}$. Then $A \subseteq P_i$ is a minimal qualified subset of $\Gamma_i(\Pi)$ if and only if $A \cup \{i\}$ is a circuit of $\mathcal{M}$. Therefore, we can write $\Gamma_i(\Pi) = \Gamma_i(\mathcal{M})$. The access structures that can be defined in this way from a matroid are called *matroid-related*. One of the most important results in secret sharing is that the access structure of every ideal (not necessarily linear) secret sharing scheme is matroid-related [6].

Moreover, a connected matroid $\mathcal{M}$ is uniquely determined by any one of the access structures $\Gamma_i(\mathcal{M})$. A matroid is said to be *connected* if every 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. As a consequence of [25, Proposition 4.1.2], for every $i \in Q$, the access structure $\Gamma_i(\mathcal{M})$ is connected if and only if the matroid $\mathcal{M}$ is connected. A connected matroid is determined by the circuits through a single point. Then every connected matroid $\mathcal{M}$ is univocally determined by any one of the access structures $\Gamma_i(\mathcal{M})$. Therefore, if Γ is a connected vector space access structure with $\Gamma = \Gamma_{n+1}(\Pi) =$

$\Gamma_{n+1}(\Pi')$, then 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 M and N be, respectively, a generator matrix and a parity-check matrix for the code $\mathcal{C} = \mathcal{C}(\Pi)$. Recall that the matrix N is the generator matrix of the dual code $\mathcal{C}^\perp$ and, hence, $MN^\top = 0$. An $[n+1, k]$ linear code $\mathcal{C}$ is said to be *self-dual* if $\mathcal{C}^\perp = \mathcal{C}$. In this case, $2k = n+1$ and every generator matrix M is also a parity-check matrix. We say that a linear code $\mathcal{C}$ with generator matrix M is *almost self-dual* if there exists a nonsingular diagonal matrix $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n, \lambda_{n+1})$ such that MD is a parity-check matrix. Of course, the equality $2k = n+1$ holds for almost self-dual codes as well. Clearly, the matrices M and MD represent the same matroid. Therefore, the matroid $\mathcal{M}(\Pi)$ associated to an almost self-dual code $\mathcal{C}(\Pi)$ is identically self-dual, and hence the access structures $\Gamma_i(\Pi)$ are self-dual.

B. Equivalence Between the Two Problems

We prove in the following that Open Problem 1 and Open Problem 2 are equivalent. Recall that, since we are dealing with identically self-dual matroids, $n+1 = 2k$.

Lemma 5.1: Let $\Pi = (\pi_1, \ldots \pi_{2k})$ be a sequence of linear forms in E^* such that the matroid $\mathcal{M}(\Pi)$ is identically self-dual and connected. In the space $E^* \otimes E^*$ of the bilinear forms on E, the set of vectors $\{\pi_j \otimes \pi_j : j \in Q - \{i\}\}$ is linearly independent for every $i \in Q$.

Proof: Suppose that the set $\{\pi_j \otimes \pi_j : 1 \leq j \leq 2k-1\}$ is linearly dependent. Then we can suppose that

$$\pi_1 \otimes \pi_1 = \sum_{i=2}^{2k-1} \lambda_i (\pi_i \otimes \pi_i). \tag{6}$$

The access structure $\Gamma_1(\Pi)$ is self-dual and connected. Then there exists a minimal qualified subset $A \subseteq P_1$ such that $2k \in A$. We can suppose that $A = \{r+1, \ldots, 2k-1, 2k\}$. Since $\Gamma_1(\Pi)$ is self-dual, $P_1 - A = \{2, \ldots, r\}$ is not qualified. Then there exists a vector $\boldsymbol{x} \in E$ such that $\pi_1(\boldsymbol{x}) = 1$ and $\pi_i(\boldsymbol{x}) = 0$ for every $i = 2, \ldots, r$. Therefore, from (6), $\pi_1 = \sum_{i=r+1}^{2k-1} (\lambda_i \pi_i(\boldsymbol{x}))\pi_i$, a contradiction with the fact that A is a minimal qualified subset of the access structure $\Gamma_1(\Pi)$. □

Corollary 5.2: Let $\Pi = (\pi_1, \ldots, \pi_{2k})$ be a sequence of linear forms in E^* such that the matroid $\mathcal{M}(\Pi)$ is identically self-dual and connected. The code $\mathcal{C}(\Pi)$ is almost self-dual if and only if $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2k} \otimes \pi_{2k} \rangle = 2k-1$.

Proof: Consider the generator matrix $M = M(\Pi)$ of the code $\mathcal{C} = \mathcal{C}(\Pi)$. From Lemma 5.1, $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2k} \otimes \pi_{2k} \rangle = 2k-1$ if and only if there exist values $\lambda_1, \ldots, \lambda_{2k} \in \mathbb{K} - \{0\}$ such that $\sum_{i=1}^{2k} \lambda_i (\pi_i \otimes \pi_i) = 0$. This is equivalent to the existence of a nonsingular diagonal matrix $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_{2k})$ such that MD is a parity-check matrix of $\mathcal{C}$. □

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

Proposition 5.3: Let $\mathcal{M}$ be an identically self-dual representable connected matroid with ground set $Q = \{1, \ldots, 2k\}$ and let $\Gamma_{2k}(\mathcal{M})$ be the access structure induced by $\mathcal{M}$ on the set P_{2k}. Then $\Gamma_{2k}(\mathcal{M})$ 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: Suppose that there exists an ideal multiplicative $\mathbb{K}$-LSSS $\Sigma_{2k}(\Pi)$ with access structure $\Gamma_{2k}(\mathcal{M})$. Then, by (2), the vectors $\{\pi_1 \otimes \pi_1, \ldots, \pi_{2k} \otimes \pi_{2k}\}$ are linearly dependent, and hence the code $\mathcal{C}(\Pi)$, which represents the matroid $\mathcal{M}$, is almost self-dual by Corollary 5.2. Conversely, if $\mathcal{M}$ is represented by an almost self-dual code $\mathcal{C} = \mathcal{C}(\Pi)$ over the finite field $\mathbb{K}$, then the linear forms π_i satisfy (2), and hence $\Sigma_{2k}(\Pi)$ is an ideal multiplicative $\mathbb{K}$-LSSS with access structure $\Gamma_{2k}(\mathcal{M})$. □

Proposition 5.4: 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 $\mathcal{M}$ can be represented by a self-dual code over some finite extension $\mathbb{L}$ of $\mathbb{K}$ with $[\mathbb{L} : \mathbb{K}] \leq 2k$.

Proof: Let $\mathcal{C}$ be an almost self-dual code over a finite field $\mathbb{K}$. Let M be a generator matrix and $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_{2k-1}, \lambda_{2k})$ the nonsingular diagonal matrix such that MD is a parity-check matrix. Consider, in an extension field $\mathbb{L} \supset \mathbb{K}$, the diagonal matrix $D_1 = \operatorname{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_{2k-1}}, \sqrt{\lambda_{2k}})$. 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. □

C. Known Families of Self-Dually Representable Matroids

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

The second family is formed by the $\mathbb{Z}_2$-representable matroids. Let $\mathcal{M} = (Q, \mathcal{B})$ be a matroid that is represented over $\mathbb{Z}_2$ by an $[n+1, k]$ linear code $\mathcal{C}$. For every circuit $C \subseteq Q$ of the dual matroid $\mathcal{M}^*$, the code $\mathcal{C}$ must contain the codeword $(x_1, \ldots, x_n, x_{n+1})$ determined by $x_i = 1$ if and only if $i \in C$. Moreover, the code $\mathcal{C}$ is the one spanned by these codewords, and hence $\mathcal{C}$ is determined by $\mathcal{M}$. Therefore, for every $\mathbb{Z}_2$-representable matroid $\mathcal{M}$ there exists a *unique* binary linear code representing $\mathcal{M}$. 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 [20]. Therefore, this access structure can be realized by an ideal multiplicative $\mathbb{Z}_2$-LSSS.

Finally, all identically self-dual matroids with rank at most four, that is, on at most eight points, are self-dually representable [26].

D. A Family of Counterexamples

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

For every given integer $k \geq 3$, consider the set of players $P = \{1, \ldots, 2k-1\}$ and the subsets $X_1 = \{1, \ldots, k-1\}$ and $X_2 = \{k, \ldots, 2k-2\}$. Consider on P the access structure Γ whose minimal qualified subsets are X_1, X_2, and all subsets $A \subseteq P$ with $|A| = k$ and $X_i \not\subseteq A$. By using the techniques in [27], it can be proved that Γ is a $\mathbb{K}$-vector space access structure if the finite field $\mathbb{K}$ is large enough. Specifically, given two different subspaces $V_1, V_2 \subseteq E^*$, where $E = \mathbb{K}^k$ and $\dim V_i = k-1$, we can find vectors $\pi_1, \ldots, \pi_{k-1} \in V_1$, and $\pi_k, \ldots, \pi_{2k-2} \in V_2$, and $\pi_{2k-1} \in E^* - (V_1 \cup V_2)$, and $\pi_{2k} \in V_1 \cap V_2$ such that $\Gamma = \Gamma_{2k}(\Pi) = \Gamma_{2k}(\pi_1, \ldots, \pi_{2k-1}, \pi_{2k})$. For instance, if the characteristic of $\mathbb{K}$ is large enough, the columns of the matrix M in (1) provide the sequence Π for the case $k = 3$, while for $k = 4$ we can consider the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 0 & 0 & 0 & -2 & 0 \\ 1 & 4 & 9 & -1 & -2 & -3 & 4 & 0 \\ 0 & 0 & 0 & 1 & 4 & 9 & -5 & 0 \end{pmatrix}.$$

Clearly, the access structure Γ is $\mathcal{Q}_2$. We claim that, for every Π with $\Gamma = \Gamma_{2k}(\Pi)$, the LSSS $\Sigma_{2k}(\Pi)$ is not multiplicative. Suppose that, on the contrary, there exist a sequence Π such that $\pi_{2k} \otimes \pi_{2k} = \sum_{i=1}^{2k-1} \lambda_i (\pi_i \otimes \pi_i)$. Since the induced substructure $\Gamma(P - j) = \{A \in \Gamma : A \subseteq P - j\}$ on the set $P - j$ is not $\mathcal{Q}_2$, we get that $\lambda_j \neq 0$ for every $j = 1, \ldots, 2k-1$. Therefore, $\pi_{2k-1} \otimes \pi_{2k-1}$ is a linear combination of the bilinear forms $(\pi_i \otimes \pi_i)_{i \neq 2k-1}$ and, hence, the scheme $\Sigma_{2k-1}(\Pi)$ is multiplicative. Because of the election of the vectors π_i, it is clear that $X_1 \cup \{2k\}, X_2 \notin \Gamma_{2k-1}(\Pi)$, and hence this access structure is not $\mathcal{Q}_2$, a contradiction with the fact that $\Sigma_{2k-1}(\Pi)$ is multiplicative. Notice that, since Γ is connected, the access structure $\Gamma_{2k-1}(\Pi)$ is determined by Γ, that is, it does not depend on the choice of Π.

VI. Flat-Partitions and Sum of Matroids

We present in the following the definition and some properties of the 2-*sum* of two matroids. More information about this operation can be found in [25, Chs. 7 and 8]. A matroid is said to be *indecomposable* if it is not the 2-sum of smaller matroids. The aim of this section is twofold. First, we prove that, to solve Open Problem 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 on *flat-partitions* of matroids, a concept that is introduced here. It will be used also to classify the identically self-dual matroids.

Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be matroids on the sets Q_1 and Q_2, respectively. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be their families of bases. Suppose that $Q_1 \cap Q_2 = \{p\}$ and that p is neither a loop nor a co-loop of $\mathcal{M}_i$. The 2-sum of $\mathcal{M}_1$ and $\mathcal{M}_2$ at the point p, which will be denoted by $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$, is the matroid with ground set $Q = (Q_1 \cup Q_2) - \{p\}$ whose family of bases is $\mathcal{B} = \mathcal{B}'_1 \cup \mathcal{B}'_2$, where

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

It is not difficult to check that $\mathcal{B}$ satisfies the axioms in Definition 1.1 and that $r(\mathcal{M}) = r(\mathcal{M}_1) + r(\mathcal{M}_2) - 1$. The matroid $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$ is connected if and only if both $\mathcal{M}_1$ and $\mathcal{M}_2$ are connected [25, Proposition 7.1.20].

Observe that, if $\mathcal{M}_2$ is the uniform matroid $U_{1,2}$, then $\mathcal{M}_1 \oplus_2 U_{1,2} \cong \mathcal{M}_1$. Effectively, $U_{1,2} = (Q_2, \mathcal{B}_2)$ with $Q_2 = \{p, q\}$ and $\mathcal{B}_2 = \{\{p\}, \{q\}\}$. Then the family of bases of $\mathcal{M}_1 \oplus_2 U_{1,2}$ is $\mathcal{B} = \mathcal{B}'_1 \cup \mathcal{B}'_2$, where

- $\mathcal{B}'_1 = \{B_1 \cup C_2 \subseteq Q : B_1 \in \mathcal{B}_1, C_2 = \emptyset\}$,
- $\mathcal{B}'_2 = \{C_1 \cup B_2 \subseteq Q : C_1 \cup \{p\} \in \mathcal{B}_1, B_2 = \{q\}\}$.

Clearly, the bijection $\varphi : Q_1 \to Q$ defined by $\varphi(p) = q$ and $\varphi(x) = x$ for every $x \in Q_1 - \{p\}$ proves that the matroid $\mathcal{M}_1$ is isomorphic to $\mathcal{M}_1 \oplus_2 U_{1,2}$. This is said to be a *trivial* 2-sum. A connected matroid is said to be *indecomposable* if it is not isomorphic to any nontrivial 2-sum of matroids.

Proposition 6.1: The matroid $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$ is identically self-dual if and only if both $\mathcal{M}_1$ and $\mathcal{M}_2$ are identically self-dual.

Proof: Since $\mathcal{M}^* = \mathcal{M}_1^* \oplus_2 \mathcal{M}_2^*$[25, Proposition 7.1.20], the 2-sum of two identically self-dual matroids is identically self-dual.

Suppose now that $\mathcal{M}$ is identically self-dual. Take $r(\mathcal{M}_i) = r_i$ and $|Q_i| = n_i + 1$, where $i = 1, 2$. Consider a basis of $\mathcal{M}$ of the form $B^1 = B_1 \cup C_2 \in \mathcal{B}'_1$. Since $\mathcal{M}$ is identically self-dual, $B^2 = Q - B^1$ is also a basis of B. Observe that $B^2 \cap Q_1 = Q_1 - (B_1 \cup \{p\})$, and hence $|B^2 \cap Q_1| = n_1 - r_1$. On the other hand, $B^2 \cap Q_2 = Q_2 - (C_2 \cup \{p\})$, which implies that $|B^2 \cap Q_2| = n_2 - r_1 + 1$. Therefore, B^2 must be of the form $B^2 = C_1 \cup B_2 \in \mathcal{B}'_2$. Analogously, $Q - B \in \mathcal{B}'_1$ if $B \in \mathcal{B}'_2$. We prove that, for instance, $\mathcal{M}_1$ is identically self-dual. Let B_1 be a basis of $\mathcal{M}_1$ with $p \notin B_1$, and let B be a basis of $\mathcal{M}$ of the form $B = B_1 \cup C_2 \in \mathcal{B}'_1$. Then $Q - B = C_1 \cup B_2 \in \mathcal{B}'_2$, Therefore, $Q_1 - B_1 = C_1 \cup \{p\}$ is a basis of $\mathcal{M}_1$. Analogously, $Q_1 - B_1$ is a basis of $\mathcal{M}_1$ if B_1 is a basis of $\mathcal{M}_1$ with $p \in B_1$. □

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 nonempty flats of $\mathcal{M}$. Indecomposable identically self-dual matroids are characterized in Proposition 6.5 in terms of their flat-partitions. The next three lemmas are needed to prove that result.

Lemma 6.2: Let $\mathcal{M}$ be a connected matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Then $r(X_1) + r(X_2) > r(\mathcal{M})$ and $r(X_i) > 1$ for $i = 1, 2$.

Proof: If $\mathcal{M}$ is connected and $\emptyset \neq X \subsetneq Q$, then $r(X) + r(Q - X) > r(\mathcal{M})$[25, Proposition 4.2.1]. Since $r(X_i) < r(\mathcal{M})$ and $r(X_1) + r(X_2) > r(\mathcal{M})$, we get that $r(X_i) > 1$ for $i = 1, 2$. □

A *cyclic flat* of a matroid is a flat that is a union of circuits. It is easy to show that X is a cyclic flat of a matroid on Q if and only if $Q - X$ is a cyclic flat of the dual matroid [25, Exercise 2.1.13]. In addition, the closure of any circuit is a cyclic flat. Applying these ideas to identically self-dual matroids gives the following lemma.

Lemma 6.3: Let $\mathcal{M}$ be an identically self-dual matroid with ground set Q and let C be a circuit of $\mathcal{M}$ with $0 < r(C) < r(\mathcal{M})$. Then $\big(\mathrm{cl}(C), Q - \mathrm{cl}(C)\big)$ is a flat-partition of $\mathcal{M}$. As a consequence, $r(C) \geq 2$ if $\mathcal{M}$ is connected.

Lemma 6.4: Let $\mathcal{M}$ be a connected identically self-dual matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Take $k = r(\mathcal{M})$ and $r_i = r(X_i)$. Then

1) $|B \cap X_1| \leq r_1$ and $|B \cap X_2| \leq r_2$ for every basis B of $\mathcal{M}$, and
2) $|X_1| = k + r_1 - r_2$ and $|X_2| = k + r_2 - r_1$.

Proof: Let $B \subseteq Q$ be a basis of $\mathcal{M}$. Since r_i is the maximum cardinality of an independent subset in X_i, it is clear that $|B \cap X_i| \leq r_i$. The second statement is a direct consequence of the fact that $r^*(X) = |X| - r(\mathcal{M}) + r(Q - X)$ for every matroid $\mathcal{M}$ and for every subset $X \subseteq Q$, where $r^*(X)$ is the rank of X in the dual matroid [25, Proposition 2.1.9]. □

The next proposition provides a characterization of indecomposable identically self-dual matroids in terms of their flat-partitions.

Proposition 6.5: Let $\mathcal{M}$ be a connected identically self-dual matroid. If $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$, where $r(\mathcal{M}_i) \geq 2$, then $(X_1, X_2) = (Q_1 - \{p\}, Q_2 - \{p\})$ is a flat-partition of $\mathcal{M}$ with $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$. Moreover, if there exists a flat-partition (X_1, X_2) of $\mathcal{M}$ with $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$, then there exist two connected identically self-dual matroids $\mathcal{M}_1$, $\mathcal{M}_2$, with $r(\mathcal{M}_i) = r(X_i)$ and ground sets $Q_i = X_i \cup \{p\}$, such that $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$. As a consequence, $\mathcal{M}$ is indecomposable if and only if there is no flat-partition (X_1, X_2) of $\mathcal{M}$ with $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$.

Proof: Suppose that $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$, where $r(\mathcal{M}_i) \geq 2$. Then the matroids $\mathcal{M}_1$ and $\mathcal{M}_2$ are connected and identically self-dual. Consider $X_i = Q_i - \{p\}$ and suppose that there exists $x \in X_2 \cap \mathrm{cl}(X_1)$. By Lemma 6.3, there is no circuit C with $r(C) = 1$ in $\mathcal{M}_2$, and hence, $\{x, p\}$ is an independent set of $\mathcal{M}_2$. Therefore, there exists a $C_2 \subseteq X_2$ such that $x \in C_2$ and $C_2 \cup \{p\}$ is a basis of $\mathcal{M}_2$. Then $B_1 \cup C_2$ is a basis of $\mathcal{M}$ if B_1 is a basis of $\mathcal{M}_1$. But $x \in \mathrm{cl}(X_1) = \mathrm{cl}(B_1)$, a contradiction. Therefore, (X_1, X_2) is a flat-partition of $\mathcal{M}$ and, clearly, $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$.

We prove now that the matroid $\mathcal{M}$ is a nontrivial 2-sum if there exist a flat-partition (X_1, X_2) with $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$. Take $r_i = r(X_i)$. Consider a point $p \notin Q$ and $Q_i = X_i \cup \{p\}$. From Lemma 6.2, $r_1 \geq 2$. We claim that $r_1 - 1 \leq |B \cap X_1| \leq r_1$ for every basis B of $\mathcal{M}$. Actually, from Lemma 6.4, $|B \cap X_i| \leq r_i$ for $i = 1, 2$, and $|B \cap X_1| = r(\mathcal{M}) - |B \cap X_2| \geq r(\mathcal{M}) - r_2 = r_1 - 1$. Consider the matroid $\mathcal{M}_1 = (Q_1, \mathcal{B}_1)$, where $B_1 \subseteq Q_1$ is in $\mathcal{B}_1$ if and only if $|B_1| = r_1$ and there exists a basis B of $\mathcal{M}$ with $B \cap X_1 = B_1 - \{p\}$. It is not difficult to check that $\mathcal{B}_1$ satisfies the axioms in Definition 1.1. Equally, consider the matroid $\mathcal{M}_2 = (Q_2, \mathcal{B}_2)$ that is defined symmetrically. The proof is concluded by checking that $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$. □

Once we have obtained a characterization of indecomposable identically self-dual matroids, our next goal is to prove that, when trying to solve Open Problem 2, we can restrict ourselves to indecomposable matroids. The next proposition deals with the representability of the sum of matroids. It is a direct consequence of [25, Proposition 7.1.21], but we give here its proof because it will be useful to prove Proposition 6.7.

Proposition 6.6: Let $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$ be a nontrivial 2-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: 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, respectively, by matrices of the form

$$M_1 = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,m-1} & 0 \\ \vdots & & \vdots & \vdots \\ a_{r_1-1,1} & \cdots & a_{r_1-1,m-1} & 0 \\ \hline a_{r_1,1} & \cdots & a_{r_1,m-1} & 1 \end{array}\right)$$

and

$$M_2 = \left(\begin{array}{c|ccc} 1 & b_{1,2} & \cdots & b_{1,n} \\ \hline 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ 0 & b_{r_2,2} & \cdots & b_{r_2,n} \end{array}\right)$$

where $r_i = r(\mathcal{M}_i)$, $|Q_1| = m$, $|Q_2| = n$, and the point $p \in Q_1 \cap Q_2$ correspond to the last column of M_1 and the first column of M_2. Then the matrix

$$M = \left(\begin{array}{ccc|ccc} a_{1,1} & \cdots & a_{1,m-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r_1-1,1} & \cdots & a_{r_1-1,m-1} & 0 & \cdots & 0 \\ \hline a_{r_1,1} & \cdots & a_{r_1,m-1} & b_{1,2} & \cdots & b_{1,n} \\ \hline 0 & \cdots & 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{r_2,1} & \cdots & b_{r_2,n} \end{array}\right)$$

is a $\mathbb{K}$-representation of the 2-sum $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$.

We prove now the converse. Take $X_1 = Q_1 - \{p\} = \{a_1, \ldots, a_{m-1}\}$ and $X_2 = Q_2 - \{p\} = \{b_2, \ldots, b_n\}$. From Proposition 6.5, (X_1, X_2) is a flat-partition of $\mathcal{M}$ with $r(X_1) + r(X_2) = r(\mathcal{M}) + 1$. 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 $\alpha_i, \beta_j \in E^* = (\mathbb{K}^k)^*$, where $k = r(\mathcal{M})$, such that $\mathcal{M} = \mathcal{M}(\Pi)$. Consider the subspaces $V_1, V_2 \subseteq E^*$ defined by $V_1 = \langle \alpha_1, \ldots, \alpha_{m-1} \rangle$ and $V_2 = \langle \beta_2, \ldots, \beta_n \rangle$. Clearly, $\dim(V_i) = r(X_i)$ and $\dim(V_1 \cap V_2) = 1$. Let $\pi \in E^*$ be a nonzero 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 p for both $\mathcal{M}_1$ and $\mathcal{M}_2$. □

Proposition 6.7: 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 2-sum $\mathcal{M} = \mathcal{M}_1 \oplus_2 \mathcal{M}_2$ can be represented over $\mathbb{K}$ by an almost self-dual code. Moreover, 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 extension of $\mathbb{K}$ with $[\mathbb{L} : \mathbb{K}] \leq 2$.

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 6.6. 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

$$\left(\begin{array}{ccc|ccc} a_{1,1} & \cdots & a_{1,m-1} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r_1-1,1} & \cdots & a_{r_1-1,m-1} & 0 & \cdots & 0 \\ \hline a_{r_1,1} & \cdots & a_{r_1,m-1} & b_{1,2}\sqrt{-1} & \cdots & b_{1,n}\sqrt{-1} \\ \hline 0 & \cdots & 0 & b_{2,2}\sqrt{-1} & \cdots & b_{2,n}\sqrt{-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{r_2,1}\sqrt{-1} & \cdots & b_{r_2,n}\sqrt{-1} \end{array}\right)$$

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. Notice that we need to multiply the second matrix by $\sqrt{-1}$ because the dot product of the central row by itself must be zero. □

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 Open Problems 1 and 2 are equivalent to the following one.

Open Problem 3: To determine whether all indecomposable identically self-dual $\mathbb{K}$-representable matroids can be represented by a self-dual linear code over some finite extension of $\mathbb{K}$.

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

The 2-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 two disjoint sets P^1 and P^2 and consider a player $p \in P^1$. The qualified subsets in the composed access structure $\Gamma = \Gamma^1[\Gamma^2; p]$ on the set of players $P = (P^1 - \{p\}) \cup P^2$ are the subsets $A \subseteq P^1 - \{p\}$ with $A \in \Gamma^1$ and the subsets $A \subseteq P$ such that $A \cap P^2 \in \Gamma^2$ and $(A \cap P^1) \cup \{p\} \in \Gamma^1$. Suppose that there exist matroids $\mathcal{M}_1$ and $\mathcal{M}_2$, with ground sets Q_1 and Q_2, respectively, such that $Q_1 \cap Q_2 = \{p\}$, and $\Gamma^1 = \Gamma_q(\mathcal{M}_1)$ for some $q \in Q_1 - \{p\}$, and $\Gamma^2 = \Gamma_p(\mathcal{M}_2)$. Then the composition $\Gamma^1[\Gamma^2; p]$ is related to the 2-sum at the point p of the matroids $\mathcal{M}_1$ and $\mathcal{M}_2$. Namely, $\Gamma^1[\Gamma^2; p] = \Gamma_q(\mathcal{M}_1 \oplus_2 \mathcal{M}_2)$.

It follows from Propositions 6.1 and 6.6 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 6.7, 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.

VII. All Identically Self-Dual Bipartite Matroids are Representable by Self-Dual Codes

A. Identically Self-Dual Bipartite Matroids

It is not hard to see that the uniform matroid $U_{k,2k}$ does not admit any flat-partition. As a direct consequence of Lemma 6.3, every nonuniform identically self-dual matroid admits a flat-partition.

As stated earlier, every identically self-dual uniform matroid $U_{k,2k}$ can be represented by a self-dual code $\mathcal{C}$ over every finite field $\mathbb{K}$ with $|\mathbb{K}| \geq 2k$. By the above observation, this means that the answer to Open Problem 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 7.2 shows that these matroids coincide with the identically self-dual bipartite matroids.

Let k, r_1, and r_2 be integers such that $1 < r_i < k < r_1 + r_2$. 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 $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ by determining its bases: $B \subseteq Q$ is a basis of $\mathcal{M}$ if and only if $|B| = k$ and $|B \cap X_i| \leq r_i$ for $i = 1, 2$. Every matroid of this form is said to be *bipartite*. Observe that (X_1, X_2) is a flat-partition of $\mathcal{M}$ with $r(X_i) = r_i$.

The access structures defined by these bipartite matroids were first considered in [27], where the authors proved that they are vector space access structures, that is, they admit an ideal LSSS. As a consequence of the results in [27], for every bipartite matroid $\mathcal{M}$ and for every prime p, there exists a finite extension $\mathbb{K}$ of $\mathbb{Z}_p$ such that $\mathcal{M}$ is representable over $\mathbb{K}$.

Theorem 2, which is proved in the following, extends this result of [27] by showing that, additionally, the identically self-dual bipartite matroids are self-dually representable. This is done by a refinement of the approach of [27] based on techniques from algebraic geometry.

From Propositions 6.5, 7.1, and 7.2, the identically self-dual bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ is indecomposable whenever $r_1 + r_2 - k > 1$. Therefore, we found a new large family of self-dually representable matroids and, hence, a new large family of self-dual vector space access structures that admit an ideal MLSSS.

Proposition 7.1: Let $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ be a bipartite matroid. Then $\mathcal{M}$ is identically self-dual if and only if $|Q| = 2k$ and $|X_1| = k + r_1 - r_2$.

Proof: We only have to prove that the dual of a bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ is the bipartite matroid $\mathcal{M}^* = \mathcal{M}(X_1, X_2, r_1^*, r_2^*, k^*)$, where $r_1^* = |X_1| - k + r_2$ and $r_2^* = |X_2| - k + r_1$, and $k^* = |Q| - k$. A set $B \subseteq Q$ is a basis of $\mathcal{M}^*$ if and only if $Q - B$ is a basis of $\mathcal{M}$, that is, if and only if $|Q - B| = k$ and $|(Q - B) \cap X_i| = |X_i - (B \cap X_i)| \leq r_i$. Therefore, $B \subseteq Q$ is a basis of $\mathcal{M}^*$ if and only if $|B| = |Q| - k$ and $|B \cap X_i| = |B| - |B \cap X_j| \leq |Q| - k - |X_j| + r_j = |X_i| - k + r_j$ if $\{i, j\} = \{1, 2\}$. Therefore, $k^* = |Q| - k$, and $r_i^* = |X_i| - k + r_j$ if $\{i, j\} = \{1, 2\}$. □

Proposition 7.2: 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: We prove first that (X_1, X_2) is the only flat-partition of the bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$. Let (Y_1, Y_2) be a flat-partition of $\mathcal{M}$. We can suppose that $|Y_1| \geq k = r(\mathcal{M})$. If $|Y_1 \cap X_i| \geq k - r_j$ for all $\{i, j\} = \{1, 2\}$, there exists $B \subseteq Y_1$ such that $|B| = k$ and $|B \cap X_i| \leq r_i$ for $i = 1, 2$. Since Y_1 does not contain any basis of $\mathcal{M}$, we get $|Y_1 \cap X_1| < k - r_2$ or $|Y_1 \cap X_2| < k - r_1$. Without loss of generality, we assume that $|Y_1 \cap X_2| < k - r_1$. Then $|Y_1 \cap X_1| > r_1$ because $k \geq |Y_1 \cap X_1| + |Y_1 \cap X_2|$. In addition, $k + r_2 - r_1 = |Y_1 \cap X_2| + |Y_2 \cap X_2|$ implies that $|Y_2 \cap X_2| > r_2$. Observe that, for $i = 1, 2$, every subset of r_i points in X_i is independent, and hence, $X_i \subseteq Y_i$ because Y_i is a flat that contains a basis of X_i. Therefore, $(X_1, X_2) = (Y_1, Y_2)$.

Suppose now that (X_1, X_2) is the only flat-partition of $\mathcal{M}$. We prove that $\mathcal{M}$ is the bipartite matroid $\mathcal{M}(X_1, X_2, r_1, r_2, k)$ with $r_i = r(X_i)$ and $k = r(\mathcal{M})$. From Lemma 6.2, $1 < r_i < k < r_1 + r_2$ while, from Lemma 6.4, $|B \cap X_i| \leq r_i$ for $i = 1, 2$ if B is a basis of $\mathcal{M}$. We only have to prove that every subset $B \subseteq Q$ with $|B| = k$ and $|B \cap X_i| \leq r_i$ for $i = 1, 2$ is a basis of $\mathcal{M}$. Suppose that, on the contrary, there exists such a subset B that is not a basis. Then there exists a circuit $C \subseteq B$. The proof is concluded by showing that $(\mathrm{cl}(C), Q - \mathrm{cl}(C))$, which is a flat-partition by Lemma 6.3, is different from (X_1, X_2). If, for instance, $\mathrm{cl}(C) = X_1$, we have $C \subseteq B \cap X_1$, and hence $|C| \leq r_1$. Since C is a circuit, $r(C) < r_1 = r(X_1)$, a contradiction. □

B. Proof of Theorem 2

This section is devoted to the proof of Theorem 2, which is divided into several partial results.

Our proof uses a special class of evaluation codes that is described in the following. Consider the quotient ring $\mathbb{K}[x, y]/I$ of the ring $\mathbb{K}[x, y]$ (the polynomials on two variables over the finite field $\mathbb{K}$) modulo the ideal I spanned by the polynomial xy. The ring $\mathbb{K}[x, y]/I$ is a vector space over $\mathbb{K}$. Consider a subspace $E \subset \mathbb{K}[x, y]/I$ with $\dim E = k$. Given $2k$ points $p_1, \ldots, p_{2k} \in \mathcal{X} = \{(x, y) \in \mathbb{K}^2 : xy = 0\}$, consider, for every $i = 1, \ldots, 2k$, the linear form $\pi_i \colon E \to \mathbb{K}$ defined by $\pi_i(f) = f(p_i)$. The sequence $\Pi = (\pi_1, \ldots, \pi_{2k})$ defines a linear code $\mathcal{C}(\Pi)$, whose codewords are of the form $(f(p_1), \ldots, f(p_{2k}))$ for some $f \in E$. Consider the subspace $\widehat{E} = \langle fg : f, g \in E \rangle \subset \mathbb{K}[x, y]/I$ and the linear mapping $\widehat{\Pi} \colon \widehat{E} \to \mathbb{K}^{2k}$ defined by $\widehat{\Pi}(h) = (h(p_1), \ldots, h(p_{2k}))$.

Lemma 7.3: If the matroid $\mathcal{M}(\Pi)$ associated with $\mathcal{C}(\Pi)$ is connected and identically self-dual, then $\mathcal{C}(\Pi)$ is almost self-dual if and only if $\mathrm{rank}(\widehat{\Pi}) = 2k - 1$.

Proof: Consider the linear mapping $\Psi \colon E \otimes E \to \mathbb{K}^{2k}$ defined by

$$\Psi(f \otimes g) = ((\pi_1 \otimes \pi_1)(f \otimes g), \ldots, (\pi_{2k} \otimes \pi_{2k})(f \otimes g)).$$

Clearly, $\Psi(f \otimes g) = (fg(p_1), \ldots, fg(p_{2k}))$, and hence the linear mappings Ψ and $\widehat{\Pi}$ have the same image. Therefore,

$$\mathrm{rank}(\widehat{\Pi}) = \mathrm{rank}\Psi = \dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_{2k} \otimes \pi_{2k} \rangle.$$

The proof is concluded by applying Corollary 5.2. □

Let $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$, where $1 < r_i < k < r_1 + r_2$, be an identically self-dual bipartite matroid with ground set $Q = \{1, \ldots, 2k\}$. Our goal is to prove that, for some finite field $\mathbb{K}$, there exist a subspace $E \subset \mathbb{K}[x, y]/I$ and points $p_1, \ldots, p_{2k} \in \mathcal{X}$ such that the code $\mathcal{C}(\Pi)$ is almost self-dual and represents the matroid $\mathcal{M}$.

Consider $s_1 = k - r_2$ and $s_2 = k - r_1$. From Proposition 7.1, $|X_i| = r_i + s_i$. Suppose that $X_1 = \{1, \ldots, r_1 + s_1\}$ and $X_2 = Q - X_1$. Take $n_i = r_i + s_i$ and $t = r_1 + r_2 - k = r_i - s_i$. Observe that $B \subseteq Q$ is a basis of $\mathcal{M}$ if and only if $|B| = k$ and $s_1 \leq |B \cap X_1| \leq r_1$.

For a field $\mathbb{K}$, let $E \subset \mathbb{K}[x, y]/I$ be the subspace formed by the polynomials of the form

$$\begin{aligned} &a_0 + a_1(x + y) + \cdots + a_{t-1}(x^{t-1} + y^{t-1}) \\ &\quad + b_t x^t + \cdots + b_{r_1 - 1} x^{r_1 - 1} \\ &\quad + c_t y^t + \cdots + c_{r_2 - 1} y^{r_2 - 1}. \end{aligned}$$

is, E is the subspace of $\mathbb{K}[x, y]/I$ spanned by

$$\{1, x + y, \ldots, x^{t-1} + y^{t-1}, x^t, \ldots, x^{r_1 - 1}, y^t, \ldots, y^{r_2 - 1}\}.$$

Observe that $\dim E = k$. Given n_1 distinct values $\alpha_1, \ldots, \alpha_{n_1} \in \mathbb{K} - \{0\}$, and n_2 distinct values $\beta_1, \ldots, \beta_{n_2} \in \mathbb{K} - \{0\}$, consider the points $p_1, \ldots, p_{2k} \in \mathcal{X}$ given by $p_i = (\alpha_i^{-1}, 0)$ if $1 \leq i \leq n_1$ and $p_{n_1 + j} = (0, \beta_j^{-1})$ if $1 \leq j \leq n_2$.

For every integer $n \geq 1$, 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

$$\begin{aligned} &(x - x_1)(x - x_2) \cdots (x - x_n) \\ &\quad = x^n + S_{n,1} x^{n-1} + S_{n,2} x^{n-2} + \cdots + S_{n,n-1} x + S_{n,n}. \end{aligned}$$

Lemma 7.4: 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 $\mathrm{rank}(\widehat{\Pi}) \leq 2k - 1$.

Proof: The subspace $\widehat{E} \subset \mathbb{K}[x, y]/I$ is spanned by

$$\{1, x + y, \ldots, x^{t-1} + y^{t-1}, x^t, \ldots, x^{2r_1 - 2}, y^t, \ldots, y^{2r_2 - 2}\}.$$

Then $\dim \widehat{E} = t + 2r_1 - t - 1 + 2r_2 - t - 1 = 2k + t - 2$. Therefore, $\mathrm{rank}(\widehat{\Pi}) \leq 2k - 1$ if and only if $\dim \ker \widehat{\Pi} \geq t - 1$, that is, if and only if there exist a linearly independent set of polynomials $\{h_1, \ldots, h_{t-1}\} \subset \widehat{E}$ such that $h_\ell(p_i) = 0$ for every $\ell = 1, \ldots, t-1$ and for every $i = 1, \ldots, 2k$.

Consider the polynomials

$$\begin{aligned} f_1(x) &= (x - \alpha_1) \ldots (x - \alpha_{n_1}) \\ &= x^{n_1} + a_t x^{2s_1} + \cdots + a_{n_1 - 1} x + a_{n_1} \\ f_2(y) &= (y - \beta_1) \ldots (y - \beta_{n_2}) \\ &= y^{n_2} + b_t y^{2s_2} + \cdots + b_{n_2 - 1} y + b_{n_2}, \end{aligned}$$

also the polynomials

$$g_1(x) = x^{n_1} f_1(1/x) = 1 + a_t x^t + \cdots + a_{n_1} x^{n_1}$$

and

$$g_2(y) = y^{n_2} f_2(1/y) = 1 + b_t y^t + \cdots + b_{n_2} y^{n_2}.$$

In addition, we take

$$\begin{aligned} h_1(x, y) &= g_1(x) + g_2(y) - 1 \\ &= 1 + a_t x^t + \cdots + a_{n_1} x^{n_1} + b_t y^t + \cdots + b_{n_2} y^{n_2} \end{aligned}$$

for every $\ell = 2,\dots,t-1$

$$\begin{aligned} h_\ell(x,y) &= x^{\ell-1}g_1(x) + y^{\ell-1}g_2(y) \\ &= x^{\ell-1} + y^{\ell-1} \\ &\quad + a_t x^{t+\ell-1} + \cdots + a_{n_1} x^{n_1+\ell-1} \\ &\quad + b_t y^{t+\ell-1} + \cdots + b_{n_2} y^{n_2+\ell-1}. \end{aligned}$$

$\{h_1,\dots,h_{t-1}\} \subset \widehat{E}$ is a linearly independent set of vectors and $h_\ell(p_i) = 0$ for every $\ell = 1,\dots,t-1$ and for every $i = 1,\dots,2k$. □

Lemma 7.5: If a subset $B \subset Q$ is a basis of the matroid $\mathcal{M}(\Pi)$, then B is a basis of the bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ we are considering.

Proof: Clearly, if $f \in E$ is such that $f(p_i) = 0$ for every $i \in Q$, then $f = 0$. This implies that the rank of the matroid $\mathcal{M}(\Pi)$ is equal to $k = \dim E$. In addition, it is not difficult to check that, for $i = 1, 2$, the rank of the set X_i in the matroid $\mathcal{M}(\Pi)$ is equal to r_i. Therefore, every basis B of $\mathcal{M}(\Pi)$ satisfies $|B| = k$ and $|B \cap X_i| \le r_i$ for $i = 1, 2$. □

Lemma 7.6: If B is a basis of $\mathcal{M}$ with $|B \cap X_1| = r_1$ or $|B \cap X_2| = r_2$, then B is a basis of $\mathcal{M}(\Pi)$.

Proof: Let B be a basis of $\mathcal{M}$ with $|B \cap X_1| = r_1$. Without loss of generality, we can suppose that $B = \{1,\dots,r_1, n_1+1,\dots,n_1+s_2\}$. This set is a basis of $\mathcal{M}(\Pi)$ if there does not exist any $f \in E - \{0\}$ such that $f(p_i) = 0$ for every $i \in B$. Consider $f \in E$ with $f(p_i) = 0$ for every $i \in B$. Then f is a polynomial of the form

$$\begin{aligned} f(x,y) &= a_0 + a_1(x+y) + \cdots + a_{t-1}(x^{t-1} + y^{t-1}) \\ &\quad + b_t x^t + \cdots + b_{r_1-1} x^{r_1-1} \\ &\quad + c_t y^t + \cdots + c_{r_2-1} y^{r_2-1}. \end{aligned}$$

If $1 \le i \le r_1$

$$\begin{aligned} 0 = f(p_i) &= f\left(\alpha_i^{-1}, 0\right) \\ &= a_0 + a_1\alpha_i^{-1} + \cdots + a_{t-1}\left(\alpha_i^{-1}\right)^{t-1} \\ &\quad + b_t\left(\alpha_i^{-1}\right)^t + \cdots + b_{r_1-1}\left(\alpha_i^{-1}\right)^{r_1-1}. \end{aligned}$$

Then the coefficients a_i, b_j are all 0. If $1 \le j \le s_2$

$$\begin{aligned} 0 = f(p_{n_1+j}) &= f\left(0, \beta_j^{-1}\right) \\ &= c_t\left(\beta_j^{-1}\right)^t + \cdots + c_{r_2-1}\left(\beta_j^{-1}\right)^{r_2-1} \\ &= \left(\beta_j^{-1}\right)^t \left(c_t + \cdots + c_{r_2-1}\left(\beta_j^{-1}\right)^{s_2-1}\right). \end{aligned}$$

This implies that $c_t = \cdots = c_{r_2-1} = 0$. □

Assume now that the field $\mathbb{K}$ contains all n_1th roots of unity, and fix the values $\alpha_1,\dots,\alpha_{n_1}$ to be these roots. Observe that $S_{n_1,i}(\alpha_1,\dots,\alpha_{n_1}) = 0$ for every $i = 1,\dots,t-1$.

Lemma 7.7: For every basis B of the matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$, there exists a polynomial δ_B on n_2 variables over $\mathbb{K}$ such that B is a basis of $\mathcal{M}(\Pi)$ if and only if $\delta_B(\beta_1,\dots,\beta_{n_2}) \neq 0$.

Proof: Consider the generator matrix M of the code $\mathcal{C}(\Pi)$ that is obtained by taking the basis

$$\{1, x+y, \dots, x^{t-1} + y^{t-1}, x^t, \dots, x^{r_1-1}, y^t, \dots, y^{r_2-1}\}$$

of the subspace $E \subset \mathbb{K}[x,y]/I$. For a basis B of the matroid $\mathcal{M}$, consider the square submatrix M_B formed by the columns corresponding to the elements in B. Obviously, B is a basis of $\mathcal{M}(\Pi)$ if and only if $\det(M_B) \neq 0$.

Consider

$$\delta_B(\beta_1,\dots,\beta_{n_2}) = \left(\prod_{j=1}^{n_2} \beta_j^{r_2-1}\right) \det(M_B)$$

which is clearly a polynomial on the variables $\beta_1,\dots,\beta_{n_2}$. □

The proof of Theorem 2 is concluded by proving that, in some finite field $\mathbb{K}$ containing the n_1th roots of unity, there exist n_2 different elements $\beta_1,\dots,\beta_{n_2} \in \mathbb{K} - \{0\}$ such that $S_{n_2,i}(\beta_1,\dots,\beta_{n_2}) = 0$ for every $i = 1,\dots,t-1$ and $\delta_B(\beta_1,\dots,\beta_{n_2}) \neq 0$ for every basis B of the matroid $\mathcal{M}$.

Consider now the (infinite) field $\mathbb{F} = \overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$, and the algebraic variety M in the space $\mathbb{F}^{n_2}$ defined by

$$M = \{(y_1,\dots,y_{n_2}) \in \mathbb{F}^{n_2} : S_{n_2,i}(y_1,\dots,y_{n_2}) = 0 \\ \text{for every } i = 1,\dots,t-1\}.$$

As a consequence of [29, Lemma 9.4], the variety M is irreducible if the characteristic of $\mathbb{F}$ is large enough. This fact is proved in [29] for a field with characteristic zero, but the proof can be easily adapted to our case if the characteristic of our field is large enough. For every basis B of the matroid $\mathcal{M}$, consider in $\mathbb{F}^{n_2}$ the algebraic variety

$$V_B = \{(y_1,\dots,y_{n_2}) \in \mathbb{F}^{n_2} : \delta_B(y_1,\dots,y_{n_2}) = 0\}.$$

Lemma 7.8: There exists a point $(\beta_1,\dots,\beta_{n_2}) \in M$ such that $\beta_j \neq 0$ for every $j = 1,\dots,n_2$ and $(\beta_1,\dots,\beta_{n_2}) \notin V_B$ for every basis B of the matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, k)$.

Proof: For every $j = 1,\dots,n_2$, consider the algebraic variety $V_j \subset \mathbb{F}^{n_2}$ defined by the equation $y_j = 0$. We want to prove that there exists a point in M that is not in any of the varieties V_B nor V_j. By applying an elementary result in algebraic geometry (see [19], 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_2th root of unity. It is clear that the point $(\gamma_1, \gamma_2, \dots, \gamma_{n_2}) = (1, \theta, \dots, \theta^{n_2-1})$ is in M and it is not in any of the varieties V_j. Observe that $(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \dots, \gamma_{\sigma n_2}) \in M$ for every permutation σ on the set $\{1,\dots,n_2\}$. We claim that, for every basis B of $\mathcal{M}$, there exists a permutation σ such that $(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \dots, \gamma_{\sigma n_2}) \notin V_B$. Let B be a basis of $\mathcal{M}$ and take ℓ with $0 \le \ell \le t$ such that $|B \cap X_1| = s_1 + \ell$ and $|B \cap X_2| = r_2 - \ell$. By changing the order of the values α_i, we can assume that $B \cap X_1 = \{1,\dots,s_1+\ell\}$. Consider the sequence $\Pi = (\pi_1,\dots,\pi_{2k})$ of linear forms that is obtained from the values $(\alpha_1,\dots,\alpha_{n_1})$, which are the n_1th roots of unity reordered in some specific way, and $(\beta_1,\dots,\beta_{n_2}) = (\gamma_1, \gamma_2, \dots, \gamma_{n_2})$. From Lemma 7.6, $\{\pi_1,\dots,\pi_{s_1}, \pi_{n_1+1},\dots,\pi_{n_1+r_2}\}$ is a basis of E^* and $\{\pi_1,\dots,\pi_{s_1},\dots,\pi_{s_1+\ell}\}$ is a linearly independent set of vectors. By repeatedly applying Steinitz's Exchange Theorem, we obtain a basis of E^* of the form $\{\pi_1,\dots,\pi_{s_1},\dots,\pi_{s_1+\ell}, \pi_{j_1},\dots \pi_{j_{r_2-\ell}}\}$, where $\{j_1,\dots,j_{r_2-\ell}\} \subset X_2$. Therefore, there exists a basis B' of the matroid $\mathcal{M}(\Pi)$ with $B' \cap X_1 = B \cap X_1$. Observe that the polynomial $\delta_{B'}$ can be obtained from the polynomial δ_B by a suitable permutation of the variables. Since $\delta_{B'}(\gamma_1, \ldots, \gamma_{n_2}) \neq 0$, there exists a permutation σ with $\delta_B(\gamma_{\sigma 1}, \gamma_{\sigma 2}, \ldots, \gamma_{\sigma n_2}) \neq 0$. □

Let $\alpha_1, \ldots, \alpha_{n_1} \in \mathbb{F}$ be the n_1th roots of unity, and let $\beta_1, \ldots, \beta_{n_2} \in \mathbb{F}$ be the values whose existence is assured by Lemma 7.8. Since $\mathbb{F}$ is the algebraic closure of $\mathbb{Z}_p$ for some prime p, there exists a finite extension $\mathbb{K}$ of $\mathbb{Z}_p$ containing all the elements α_i and β_j. At this point, the proof of Theorem 2 is concluded by considering the sequence $\Pi = (\pi_1, \ldots, \pi_{2k})$ of linear forms that is obtained from $\alpha_1, \ldots, \alpha_{n_1}$ and $\beta_1, \ldots, \beta_{n_2}$. Clearly, $\mathcal{M}(\Pi) = \mathcal{M}(X_1, X_2, r_1, r_2, k)$ by Lemmas 7.5 and 7.7, and the code $\mathcal{C}(\Pi)$ is almost self-dual by Lemmas 5.1, 7.3, and 7.4.

References

[1] A. Barg, "On some polynomials related to weight enumerators of linear codes," *SIAM J. Discr. Math.*, vol. 15, no. 2, pp. 155–164, 2002.

[2] A. Beimel and N. Livne, "On matroids and non-ideal secret sharing," in *Proc. 3rd Theory of Cryptography Conf., TCC 2006 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2006, vol. 3876, pp. 482–501.

[3] A. Beimel, T. Tassa, and E. Weinreb, "Characterizing ideal weighted threshold secret sharing," in *Proc. 2nd Theory of Cryptography Conference, TCC 2005 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2005, vol. 3378, pp. 600–619.

[4] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proc. ACM Symp. Theory of Computing (STOC 1988)*, Chicago, IL, May 1988, pp. 1–10.

[5] E. F. Brickell, "Some ideal secret sharing schemes," *J. Combin. Math. Combin. Comput.*, vol. 9, pp. 105–113, 1989.

[6] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptol.*, vol. 4, pp. 123–134, 1991.

[7] T. Britz, "MacWilliams identities and matroid polynomials," *Electron. J. Combin.*, vol. 9, no. 1, 2002.

[8] P. J. Cameron, "Cycle index, weight enumerator, and Tutte polynomial," *Electron. J. Combin.*, vol. 9, no. 1, 2002.

[9] R. Canetti, U. Feige, O. Goldreich, and M. Naor, "Adaptively secure multi-party computation," in *Proc. ACM Symp. Theory of Computing (STOC 1996)*, Philadelphia, PA, May 1996, pp. 639–648.

[10] D. Chaum and C. C. Damgård, "Multi-party unconditionally secure protocols," in *Proc. ACM Symp. Theory of Computing (STOC 1988)*, Chicago, IL, May 1988, pp. 11–19.

[11] R. Cramer, I. Damgård, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," in *Advances in Cryptology, EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 316–334.

[12] I. M. Duursma, "Combinatorics of the two-variable zeta function," in *Finite Fields and Applications (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 2948, pp. 109–136.

[13] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in *Proc. ACM Symp. Theory of Computing (STOC 1987)*, New York, 1987, pp. 218–229.

[14] C. Greene, "Weight enumeration and the geometry of linear codes," *Studies in Appl. Math.*, vol. 55, no. 2, pp. 119–128, 1976.

[15] M. Hirt and U. Maurer, "Complete characterization of adversaries tolerable in secure multi-party computation," in *Proc. PODC 1997*, Santa Barbara, CA, Aug. 1997, pp. 25–34.

[16] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing any access structure," in *Proc. IEEE Globecom'87*, Tokyo, Japan, Nov. 1987, pp. 99–102.

[17] W.-A. Jackson and K. M. Martin, "Geometric secret sharing schemes and their duals," *Des., Codes, Cryptogr.*, vol. 4, no. 1, pp. 83–95, 1994.

[18] M. Karchmer and A. Wigderson, "On span programs," in *Proc. Structure in Complexity Theory Conf. 1993*, San Diego, CA, May 1993, pp. 102–111.

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

[20] J. Martí-Farré and C. Padró, "Secret sharing schemes on access structures with intersection number equal to one," *Discr. Appl. Math.*, vol. 154, no. 3, pp. 552–563, 2006.

[21] J. Martí-Farré and C. Padró, "On secret sharing schemes, matroids and polymatroids," in *Proc. 4th Theory of Cryptography Conf., TCC 2007 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, to be published.

[22] F. Matúš, "Matroid representations by partitions," *Discr. Math.*, vol. 203, no. 1–3, pp. 169–194, 1999.

[23] S.-L. Ng, "A representation of a family of secret sharing matroids," *Des., Codes, Cryptogr.*, vol. 30, no. 1, pp. 5–19, 2003.

[24] S.-L. Ng and M. Walker, "On the composition of matroids and ideal secret sharing schemes," *Des., Codes, Cryptogr.*, vol. 24, no. 1, pp. 49–67, 2001.

[25] J. G. Oxley, *Matroid Theory*. New York: Clarendon/Oxford Univ. Press, 1992.

[26] C. Padró and I. Gracia, "Representing small identically self-dual matroids by self-dual codes," *SIAM J. Discr. Math.*, vol. 20, no. 4, pp. 1046–1055, 2006.

[27] C. Padró and G. Sáez, "Secret sharing schemes with bipartite access structure," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2596–2604, Nov. 2000.

[28] R. Pellikaan, "On decoding by error location and dependent sets of error positions," *Discr. Math.*, vol. 106/107, pp. 369–381, 1992.

[29] Z. Reichstein and 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.*, vol. 52, no. 5, pp. 1018–1056, 2000.

[30] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[31] G. J. Simmons, "An introduction to shared secret and/or shared control schemes and their application," in *Contemporary Cryptology. The Science of Information Integrity*. New York: IEEE Press, 1991, pp. 441–497.

[32] J. Simonis and A. Ashikhmin, "Almost affine codes," *Des., Codes, Cryptogr.*, vol. 14, no. 2, pp. 179–197, 1998.

[33] D. R. Stinson, "An explication of secret sharing schemes," *Des., Codes, Cryptogr.*, vol. 2, no. 4, pp. 357–390, 1992.

[34] T. Tassa, "Hierarchical threshold secret sharing," in *Proc. 1st Theory of Cryptography Conf., TCC 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 2951, pp. 473–490.

[35] D. J. A. Welsh, *Matroid Theory*. London, U.K.: Academic, 1976.