On Codes, Matroids and Secure Multi-party Computation from Linear Secret Sharing Schemes

Ronald Cramer[1], Vanesa Daza[2,*], Ignacio Gracia[2,*], Jorge Jiménez Urroz[2,*], Gregor Leander[3], Jaume Martí-Farré[2,*], and Carles Padró[2,*]

[1] CWI, Amsterdam & Mathematical Institute, Leiden University
cramer@cwi.nl
[2] Dept. of Applied Maths. IV, Technical University of Catalonia, Barcelona
{vdaza, ignacio, jjimenez, jaumem, matcpl}@ma4.upc.edu
[3] CITS Research Group, Ruhr-University Bochum
leander@cits.ruhr-uni-bochum.de

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

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

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

The second one is to characterize the access structures of ideal multiplicative LSSSs. Specifically, we wonder 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 re-stated in terms of representability of identically self-dual matroids by self-dual codes. We introduce a new concept, the flat-partition, that provides a useful classification of identically self-dual matroids. Uniform identically self-dual matroids, which are known to be representable by self-dual codes, form one of the classes. We prove that this property also holds for the family of matroids that, in a natural way, is the next class in the above classification: the identically self-dual bipartite matroids.

[*] These authors' research is partially supported by the Spanish Ministry of Education and Science under project TIC 2003-00866.

V. Shoup (Ed.): Crypto 2005, LNCS 3621, pp. 327–343, 2005.

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

1 Introduction

Two open problems on multiplicative linear secret sharing schemes are studied in this paper. Our results deal with the connections between linear codes, representable matroids and linear secret sharing schemes. Some facts about these connections are recalled in Section 1.2. The reader is referred to [22] for a general reference on Matroid Theory and to [5,19,28,29] for more information about the relation between secret sharing schemes and matroids.

1.1 Multiplicative Linear Secret Sharing Schemes and General Secure Multi-party Computation

In a $\mathbb{K}$-*linear secret sharing scheme* ($\mathbb{K}$-LSSS) on the set of players $P = \{1, \ldots, n\}$, the share of every player $i \in P$ is a vector in E_i, a vector space of finite dimension over the finite field $\mathbb{K}$, and 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, any 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 of players $P = \{1, \ldots, n\}$. For any vector $\mathbf{x} \in E$, the values $(\pi_i(\mathbf{x}))_{1 \le i \le n}$ are shares of the secret value $k = \pi_{n+1}(\mathbf{x}) \in \mathbb{K}$. The access structure, $\Gamma_{n+1}(\Pi)$ of this scheme, that is, the family of qualified subsets, consists of all subsets $A \subset P_{n+1}$ such that $\bigcap_{i \in A} \ker \pi_i \subset \ker \pi_{n+1}$.

Linear secret sharing schemes 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 are not going to consider such LSSSs in this paper.

The *complexity* of a 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 any finite field $\mathbb{K}$ and for any access structure Γ, there exists a $\mathbb{K}$-LSSS for Γ [14]. We notate $\lambda_{\mathbb{K}}(\Gamma)$ for the minimum complexity of the $\mathbb{K}$-LSSSs with access structure Γ. 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*.

Linear secret sharing schemes were first considered, only in the ideal case, in [4]. General Linear secret sharing schemes were introduced by Simmons [27], Jackson and Martin [15] and Karchmer and Wigderson [16] under other names such as geometric secret sharing schemes or monotone span programs.

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

We illustrate the multiplicative property of LSSSs by analyzing the Shamir's (d, n)-threshold scheme [26]. In this scheme, the secret $k \in \mathbb{K}$ and the shares $k_i \in \mathbb{K}$, where $i = 1, \ldots, n$, are the values of a random polynomial with degree at most $d-1$ in some given points. The secret is recovered by Lagrange interpolation. If $n \geq 2d-1$, the product kk' of the two secret values is a linear combination of any $2d-1$ values $c_i = k_i k'_i$. This linear combination is obtained by interpolating the product of the two random polynomials that were used to distribute the shares. This multiplicative property of the Shamir's scheme is used in [3,8,9,11] to construct multi-party computation protocols that are secure against a threshold-based adversary.

In order to obtain efficient multi-party computation protocols for a general adversary structure, a generalization of the multiplicative property of the Shamir's scheme to any linear secret sharing scheme is proposed in [10].

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

Observe that the Shamir's (d, n)-secret sharing scheme is multiplicative if and only if $n \geq 2d-1$, and it is strongly multiplicative if and only if $n \geq 3d-2$. 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 [10,13], an access structure Γ can be realized by a multiplicative LSSS if and only if it is $\mathcal{Q}_2$, and Γ admits an strongly multiplicative LSSS if and only if it is $\mathcal{Q}_3$.

Cramer, Damgård and Maurer [10] presented a method to construct, from any $\mathbb{K}$-MLSSS Σ with $\mathcal{Q}_2$ access structure Γ, an error-free multi-party computation protocol secure against a passive adversary which is able to corrupt any set of players $B \notin \Gamma$ and computing any arithmetic circuit C over $\mathbb{K}$. The complexity of this protocol is polynomial in the size of C, $\log |\mathbb{K}|$ and $\lambda(\Sigma)$. They prove a similar result for an active adversary. In this case, the resulting protocol is perfect with zero error probability if the LSSS is strongly multiplicative, with a $\mathcal{Q}_3$ access structure Γ.

One of the key results in [10] is a method to construct, from any $\mathbb{K}$-LSSS Σ with $\mathcal{Q}_2$ access structure Γ, a multiplicative $\mathbb{K}$-LSSS Σ' with the same access structure and complexity $\lambda(\Sigma') = 2\lambda(\Sigma)$. That is, if $\mu_{\mathbb{K}}(\Gamma)$ denotes the minimum complexity of all $\mathbb{K}$-MLSSSs with access structure Γ, the above result means that $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$ for any finite field $\mathbb{K}$ and for any $\mathcal{Q}_2$ access structure Γ.

Therefore, in the passive adversary case, the construction of efficient multi-party computation protocols can be reduced to the search of efficient linear secret sharing schemes. Specifically, a multi-party computation protocol computing any 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 any LSSS whose access structure Γ' is $\mathcal{Q}_2$ and $\Gamma' \subset \Gamma$.

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

Nevertheless, the active adversary case is also solved in [10] if an exponentially small error probability is allowed. A construction is given in [10] for the active adversary case that efficiently provides, from any 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.

1.2 Codes, Matroids and Secret Sharing Schemes

Let us take $Q = \{1, \ldots, n, n+1\}$ and $P_i = Q - \{i\}$ for any $i \in Q$. 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 $\Pi = (\pi_1, \ldots, \pi_n, \pi_{n+1})$ be a sequence of surjective linear mappings $\pi_i \colon E \to \mathbb{K}$, that is, non-zero vectors in the dual space E^*. We are going to suppose always that those vectors span E^*. Observe that Π can be seen as a linear mapping $\Pi \colon E \to \mathbb{K}^{n+1}$ and, once a basis of E is fixed, it can be represented by the $d \times (n+1)$ matrix $M = M(\Pi)$ such that $\Pi(\mathbf{x}) = \mathbf{x}M$ for all $\mathbf{x} \in E$. Observe that $\operatorname{rank}(M) = d$ and that the i-th column of M corresponds to the linear form π_i.

The matrix M is a generator matrix of a $[n+1, d]$-linear code $\mathcal{C} = \mathcal{C}(\Pi)$. The columns of M define a $\mathbb{K}$-representable matroid $\mathcal{M} = \mathcal{M}(\Pi)$ on the set of points Q. 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. Important properties about the weight distribution of a linear code can be studied from its associated matroid. Several results on this relation between matroids and codes are given in [1,6,7,12] and other works.

Besides, the code $\mathcal{C}$ defines an ideal linear secret sharing scheme $\Sigma_i(\Pi)$ for every $i \in Q$. Every codeword of $\mathcal{C}$ is in the form $(\pi_1(\mathbf{x}), \ldots, \pi_i(\mathbf{x}), \ldots, \pi_{n+1}(\mathbf{x}))$ and can be seen as a distribution of shares for the secret value $\pi_i(\mathbf{x}) \in \mathbb{K}$ 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 $A \subset P_i$ such that $\pi_i \in \langle \pi_j : j \in A \rangle$. Therefore, $A \subset P_i$ 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 non-linear schemes as well, was discovered by Brickell and Davenport [5] and has been studied afterwards by several authors [2,19,20,21,28,29,30]. 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.

Actually, non-ideal linear secret sharing schemes 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 corrupted.

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 a $(n-d+1) \times (n+1)$ matrix with $\mathrm{rank}(N) = n-d+1$ and $MN^\top = 0$, where $N^\top$ denotes the transpose of N. The matrix N is a generator matrix of a $[n+1, n-d+1]$-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, $2d = n+1$ 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, then the dual code $\mathcal{C}^\perp$ defines a LSSS for the *dual access structure* $\Gamma^* = \{A \subset P : P - A \notin \Gamma\}$. 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 $\mathcal{B}(\mathcal{M}^*) = \{B \subset Q : Q - B \in \mathcal{B}(\mathcal{M})\}$, 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 $\Gamma^* \subset \Gamma$. 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 [10]. Besides, the ideal LSSS defined by a self-dual code is multiplicative and, hence, its access structure is such that $\mu_{\mathbb{K}}(\Gamma) = \lambda_{\mathbb{K}}(\Gamma)$.

2 Our Results

2.1 On Strongly Multiplicative Linear Secret Sharing Schemes

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, which is proved in Section 4, 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* $\mathbf{s} = (s_1, \ldots, s_n)$ *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* $\mathbf{e}$ *denote the all zero vector, except where it states the errors that a set of players* $A \notin \Gamma$ *have introduced in their respective shares. Define* $\mathbf{c} = \mathbf{s} + \mathbf{e}$*. Then the secret* s *can be recovered from* $\mathbf{c}$ *in time* $\mathrm{poly}(n, \log |\mathbb{K}|)$*.*

2.2 On Ideal Multiplicative Linear Secret Sharing Schemes

The characterization of the access structures of ideal 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 [10] 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 (d, n)-threshold structures with $n \geq 2d - 1$ 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 those 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 will be given in the full version of the paper.

Self-dual access structures coincide with the *minimally* $\mathcal{Q}_2$ access structures, that is, with the $\mathcal{Q}_2$ access structures Γ such that any substructure $\Gamma' \subsetneq \Gamma$ is not $\mathcal{Q}_2$. The results in this paper lead us to believe that any self-dual vector space access structure can be realized by an ideal multiplicative linear secret sharing scheme and, hence, to state the following open problem. One of the goals of this paper is to move forward in the search of its solution.

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

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

First, due to the minimality of the $\mathcal{Q}_2$ property, self-dual access structures are an extremal case in the theory of MLSSSs. Moreover, self-duality seems to be in the core of the multiplicative property. For instance, the construction in [10] 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, as we pointed out before, it can be stated in terms of an interesting open problem about the relation between Matroid Theory and Code Theory. Namely, by studying how the connection between codes, matroids and LSSSs applies to multiplicative LSSSs, we prove in Section 5.1 that Problem 1 is equivalent to the following one.

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

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 $\mathbb{K}$. Any self-dually representable matroid is identically self-dual and representable. The open problem we consider here is to decide whether the reciprocal of this fact is true.

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

There exist several methods to combine some given matroids into a new one. The *sum*, which is defined in Section 5.3, is one of them. We show in Section 5.3 that the the 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 non-trivial sum of two other matroids.

In order to take the first steps in solving Problem 2, we introduce the concept of *flat-partition* of a matroid, which is defined in Section 5.3. On one hand, we use the flat-partitions to characterize in Proposition 4 the indecomposable identically self-dual matroids. On the other hand, the number of flat-partitions provide a useful classification of identically self-dual matroids. The identically self-dual matroids that do not admit any flat-partition are exactly the uniform matroids $U_{d,2d}$, which, as we said before, are self-dually representable.

We prove in Theorem 2 that the identically self-dual matroids with exactly one flat-partition are self-dually representable as well. These matroids are precisely the identically self-dual bipartite matroids. In a *bipartite matroid*, the set of points is divided in two parts and all points in each part are symmetrical. The access structures defined by these matroids are among the *bipartite access structures*, which were introduced in [23]. As a consequence of the results in [23], bipartite matroids are representable. Bipartite matroids have been independently studied in [20,21], 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 [30] and the weighted threshold access structures [2,26].

Theorem 2. *Let $\mathcal{M}$ be an identically self-dual bipartite matroid. Then, $\mathcal{M}$ can be represented by a self-dual linear code over some finite field $\mathbb{K}$. Equivalently, every self-dual bipartite vector space access structure can be realized by an ideal MLSSS over some finite field $\mathbb{K}$.*

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

3 Multiplicative Linear Secret Sharing Schemes

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

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

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

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

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

Let $\Sigma = \Sigma_{n+1}(\Pi)$ be an ideal LSSS. Every bilinear form $\phi \colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ can be defined by $\phi(x, y) = \lambda x y$ for some $\lambda \in \mathbb{K}$. Therefore, Σ is multiplicative if and only if there exist values $\lambda_i \in \mathbb{K}$ such that $\pi_{n+1} \otimes \pi_{n+1} = \sum_{i=1}^{n} \lambda_i(\pi_i \otimes \pi_i)$. Equally, Σ is strongly multiplicative if and only if, for every $A \notin \Gamma_{n+1}(\Pi)$, there exist values $\lambda_{i,A} \in \mathbb{K}$ such that $\pi_{n+1} \otimes \pi_{n+1} = \sum_{i \in P_{n+1}-A} \lambda_{i,A}(\pi_i \otimes \pi_i)$. The values λ_i or $\lambda_{i,A}$ form the *recombination vector* introduced in [10].

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

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

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

4 Reconstruction of a Secret in the Presence of Errors

In any LSSS with a $\mathcal{Q}_3$ access structure Γ, unique reconstruction of the secret from the full set of n shares is possible, even if the shares corresponding to an unqualified set $A \notin \Gamma$ are corrupted. Nevertheless, it is not known how to do that efficiently. In this section we prove Theorem 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 $t < \frac{n}{3}$, unique reconstruction of the secret from the full set of n shares is possible, even if at most t shares are corrupted. This can be done efficiently, for instance by the Berlekamp-Welch decoding algorithm for Reed-Solomon codes.

Let p be a polynomial of degree at most t, and define $p(0) = s$. Let $\mathbf{s}$ be the vector with $s_i = p(i)$, $i = 1, \ldots, n$, and let $\mathbf{e}$ be a vector of Hamming-weight at most t. Write $\mathbf{c} = \mathbf{s} + \mathbf{e}$. Given $\mathbf{c}$ only, compute non-zero polynomials F and E

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

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

Pellikaan [24] has previously generalized the Berlekamp-Welch algorithm and has shown that his generalized decoding algorithm applies to a much wider class of error correcting codes. Technically, our generalization bears some similarity to that of [24].

Strong multiplication was first considered in [10] and was used to construct efficient multi-party computation protocols with zero error in the active adversary model. More precisely it is used in the *Commitment Multiplication Protocol* to ensure that commitments for a, b and c are consistent in the sense that $ab = c$ with zero probability to cheat.

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

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

If $\mathbf{u}, \mathbf{v} \in \mathbb{K}^k$, then $\mathbf{u} * \mathbf{v}$ denotes the vector $(u_1 v_1, \ldots, u_k v_k)$. Observe that

$$(\mathbf{x} \otimes \mathbf{y})\widehat{M} = ((\pi_i \otimes \pi_i)(\mathbf{x} \otimes \mathbf{y}))_{1 \leq i \leq n+1} = (\pi_i(\mathbf{x})\pi_i(\mathbf{y}))_{1 \leq i \leq n+1} = (\mathbf{x}M) * (\mathbf{y}M)$$

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

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

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

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

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

This is argued as follows. Note that $(\widehat{\mathbf{y}}, \mathbf{y})$ is a solution if and only if $(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y})\widehat{N} = \mathbf{e} * (\mathbf{y}N)$. Since $A \notin \Gamma$, there exists a vector $\mathbf{z} \in E$ such that $\pi_{n+1}(\mathbf{z}) = 1$ while $\pi_i(\mathbf{z}) = 0$ for every $i \in A$. Observe that $(\mathbf{x} \otimes \mathbf{z}, \mathbf{z})$ is a solution for every vector $\mathbf{z} \in E$ in that situation. Indeed, $\mathbf{e} * (\mathbf{z}N) = 0$, because $\mathbf{z}N$ is zero where $\mathbf{e}$ is non-zero. Let $(\widehat{\mathbf{y}}, \mathbf{y})$ be an arbitrary solution and consider $(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y})\widehat{M} = (t_1, \ldots, t_n, t_{n+1})$. Then, $(t_1, \ldots, t_n)$ are shares of the secret t_{n+1} according to the LSSS Σ^{μ}. Since $(t_1, \ldots, t_n) = \mathbf{e} * (\mathbf{y}N)$, we get that $t_i = 0$ for every $i \in P_{n+1} - A$ and, hence, $t_{n+1} = 0$ because $P_{n+1} - A \in \Gamma^* \subset \Gamma^{\mu}$. Finally, $(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\mathbf{y}} - \mathbf{x} \otimes \mathbf{y}) = t_{n+1} = 0$ and $(\pi_{n+1} \otimes \pi_{n+1})(\widehat{\mathbf{y}}) = (\pi_{n+1} \otimes \pi_{n+1})(\mathbf{x} \otimes \mathbf{y}) = \pi_{n+1}(\mathbf{x})\pi_{n+1}(\mathbf{y}) = s_{n+1}$. □

A positive application of Theorem 1 is as follows. Using a strongly multiplicative LSSS, the Commitment Multiplication Protocol (CMP) from [10] is directly a Verifiable Secret Sharing scheme (VSS). This saves a multiplicative factor n in the volume of communication needed, since the general reduction from VSS to CMP is not needed in this case.

5 Ideal Multiplicative Linear Secret Sharing Schemes, Self-dual Linear Codes and Identically Self-dual Matroids

5.1 Equivalence Between the Two Problems

A matroid $\mathcal{M}$ is said to be *connected* if, for every two different points $i, j \in Q$, there exists a circuit C with $i, j \in C$. In a *connected access structure*, every participant is at least in a minimal qualified subset. If $\mathcal{M}(\Pi)$ is a connected matroid, all access structures $\Gamma_i(\Pi)$ are connected. Moreover, as a consequence of [22, Proposition 4.1.2], if one of the access structures $\Gamma_i(\Pi)$ is connected, then $\mathcal{M}(\Pi)$ is connected and, hence, all the other access structures $\Gamma_j(\Pi)$ are connected.

We say that a linear code $\mathcal{C}$ with generator matrix M is *almost self-dual* if there exists a non-singular diagonal matrix $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n, \lambda_{n+1})$ such that MD is a parity check matrix.

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

are linearly independent for any $i \in Q$. Besides, the code $\mathcal{C}(\Pi)$ is almost self-dual if and only if the vectors $\{\pi_j \otimes \pi_j : j \in Q\}$ are linearly dependent.

Proof. Let us suppose that the vectors $\{\pi_j \otimes \pi_j : 1 \le j \le 2d-1\}$ are linearly dependent. Then, we can suppose that $\pi_1 \otimes \pi_1 = \sum_{i=2}^{2d-1} \lambda_i(\pi_i \otimes \pi_i)$. The access structure $\Gamma_1(\Pi)$ is self-dual and connected. Then, there exists a minimal qualified subset $A \subset P_1$ such that $2d \in A$. We can suppose that $A = \{r+1, \dots, 2d-1, 2d\}$. Since $\Gamma_1(\Pi)$ is self-dual, $P_1 - A = \{2, \dots, r\}$ is not qualified. Then, there exists a vector $\mathbf{x} \in E$ such that $\pi_1(\mathbf{x}) = 1$ and $\pi_i(\mathbf{x}) = 0$ for every $i = 2, \dots, r$. Therefore, $\pi_1 = \sum_{i=r+1}^{2d-1}(\lambda_i \pi_i(\mathbf{x}))\pi_i$, a contradiction with the fact that $A = \{r+1, \dots, 2d-1, 2d\}$ is a *minimal* qualified subset of the access structure $\Gamma_1(\Pi)$.

Observe that $\sum_{i=1}^{2d} \lambda_i(\pi_i \otimes \pi_i) = 0$ if and only if the diagonal matrix $D = \mathrm{diag}(\lambda_1, \dots, \lambda_{2d-1}, \lambda_{2d})$ is such that $MDM^\top = 0$. □

By taking into account that a non-connected matroid can be divided into connected components [22, Proposition 4.1.2], the equivalence between Problems 1 and 2 is an immediate consequence of the following two propositions. We skip the proof of the first one.

Proposition 1. *Let $\mathcal{M}$ be an identically self-dual representable connected matroid on the set of points $Q = \{1, \dots, 2d\}$ and let $\Gamma_{2d}(\mathcal{M})$ be the access structure induced by $\mathcal{M}$ on the set P_{2d}. Then $\Gamma_{2d}(\mathcal{M})$ can be realized by an ideal multiplicative $\mathbb{K}$-LSSS if and only if $\mathcal{M}$ can be represented by an almost self-dual code $\mathcal{C}$ over the field $\mathbb{K}$.*

Proposition 2. *Let $\mathcal{M}$ be an identically self-dual matroid that is represented, over the finite field $\mathbb{K}$, by an almost self-dual code. Then, there exists a finite field $\mathbb{L}$, which is an algebraic extension of $\mathbb{K}$, such that $\mathcal{M}$ is represented by a self-dual code over $\mathbb{L}$.*

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

5.2 Known Families of Self-dually Representable Matroids

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

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

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

5.3 Flat-Partitions and Sum of Matroids

We recall next the definition and some properties of the sum of two matroids. More information on that topic can be found in [22, Chapter 7].

Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be connected matroids on the sets Q_1 and Q_2, respectively. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be their families of bases. Let us suppose that $Q_1 \cap Q_2 = \emptyset$ and let us take two points $q_1 \in Q_1$ and $q_2 \in Q_2$. The *sum of* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *at the points* q_1 *and* q_2, which will be denoted by $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$, is the matroid on the set of points $Q = (Q_1 \cup Q_2) \setminus \{q_1, q_2\}$ whose family of bases is $\mathcal{B} = \mathcal{B}_1' \cup \mathcal{B}_2'$, where $\mathcal{B}_1' = \{B_1 \cup C_2 \subset Q : B_1 \in \mathcal{B}_1, C_2 \cup \{q_2\} \in \mathcal{B}_2\}$ and $\mathcal{B}_2' = \{C_1 \cup B_2 \subset Q : C_1 \cup \{q_1\} \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}$.

It is not difficult to check that $\mathcal{B}$ is the family of bases of a matroid and that $\mathcal{M}$ is a connected matroid with $\dim \mathcal{M} = \dim \mathcal{M}_1 + \dim \mathcal{M}_2 - 1$. The proof of the following proposition will be given in the full version of the paper.

Proposition 3. *The matroid* $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ *is identically self-dual if and only if both* $\mathcal{M}_1$ *and* $\mathcal{M}_2$ *are identically self-dual.*

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

Let $\mathcal{M}$ be a matroid on a set of points Q and let (X_1, X_2) be a partition of Q. We say that (X_1, X_2) is a *flat-partition* of $\mathcal{M}$ if X_1 and X_2 are flats of $\mathcal{M}$. The next proposition, which is a consequence of the results in [22, Chapter 7], provides a characterization of indecomposable identically self-dual matroids in terms of their flat-partitions

Proposition 4. *Let* $\mathcal{M}$ *be a connected identically self-dual matroid. Then* $\mathcal{M}$ *is indecomposable if and only if there is no flat-partition* (X_1, X_2) *of* $\mathcal{M}$ *with* $\operatorname{rank}(X_1) + \operatorname{rank}(X_2) = \dim(\mathcal{M}) + 1$.

As a consequence of Proposition 3 and the next two propositions, whose proofs will be given in the full version of the paper, the search for an answer to Problem 2 can be restricted to indecomposable matroids.

Proposition 5. *Let $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ be a non-trivial sum of two identically self-dual matroids. Then $\mathcal{M}$ is $\mathbb{K}$-representable if and only if both $\mathcal{M}_1$ and $\mathcal{M}_2$ are $\mathbb{K}$-representable.*

Proposition 6. *Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two matroids that are represented over a finite field $\mathbb{K}$ by almost self-dual codes. Then, the sum $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ can be represented over $\mathbb{K}$ by an almost self-dual code. Besides, if $\mathcal{M}_1$ and $\mathcal{M}_2$ are self-dually $\mathbb{K}$-representable, the sum $\mathcal{M}$ is self-dually $\mathbb{L}$-representable, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ with $(\mathbb{K} : \mathbb{L}) \leq 2$.*

5.4 Identically Self-dual Bipartite Matroids

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

Lemma 3. *Let $\mathcal{M}$ be an identically self-dual matroid and let $C \subset Q$ be a circuit of $\mathcal{M}$ with $\operatorname{rank}(C) < \dim(\mathcal{M})$. Let us consider the flat $X_1 = \langle C \rangle$ and $X_2 = Q \setminus X_1$. Then, (X_1, X_2) is a flat-partition of $\mathcal{M}$.*

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

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

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

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

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 8 shows that these matroids coincide with the identically self-dual bipartite matroids.

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

We skip the proof of the next proposition, which determines which bipartite matroids are identically self-dual.

Proposition 7. *Let $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ be a bipartite matroid. Then, $\mathcal{M}$ is identically self-dual if and only if $|Q| = 2d$ and $|X_1| = d + r_1 - r_2$.*

Proposition 8. *Let $\mathcal{M}$ be a connected identically self-dual matroid. Then, $\mathcal{M}$ is bipartite if and only if it admits exactly one flat-partition.*

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

Let us suppose now that (X_1, X_2) is the only flat-partition of $\mathcal{M}$. We are going to prove that $\mathcal{M}$ is the bipartite matroid $\mathcal{M}(X_1, X_2, r_1, r_2, d)$, where $r_i = \operatorname{rank}(X_i)$ and $d = \dim(\mathcal{M})$. It is not difficult to check that $1 < r_i < d < r_1 + r_2$ and that $d - r_j \leq |B \cap X_i| \leq r_i$ if B is a basis of $\mathcal{M}$ and $\{i, j\} = \{1, 2\}$. We only have to prove that any set $B \subset Q$ such that $|B| = d$ and $d - r_j \leq |B \cap X_i| \leq r_i$ for $\{i, j\} = \{1, 2\}$ is a basis of $\mathcal{M}$. Let us suppose that, on the contrary, there exists such a subset B that is not a basis. Then, there exists a circuit $C \subset B$. Let us consider $Y_1 = \langle C \rangle$ and $Y_2 = Q \setminus Y_1$. From Lemma 3, (Y_1, Y_2) is a flat-partition of $\mathcal{M}$. The proof is concluded by showing that this flat-partition is different from (X_1, X_2). If $Y_1 = X_i$ for some $i = 1, 2$, we have $C \subset X_i$. Since $|C| \leq r_i$ and C is a circuit, $\operatorname{rank}(Y_1) < r_i$, a contradiction. □

The access structures defined by bipartite matroids were first considered in [23], where the authors proved that they are vector space access structures, that is, they admit an ideal LSSS. As a direct consequence of this fact, any bipartite matroid is representable.

Theorem 2 extends this result of [23] by showing that, additionally, the identically self-dual bipartite matroids are self-dually representable. This is done by a refinement of the approach of [23] based on techniques from Algebraic Geometry.

From Propositions 4, 7 and 8, if $r_1 + r_2 - d > 1$, the identically self-dual bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$ is indecomposable. Therefore, we found a new large family of identically self-dual matroids giving an affirmative answer to Problem 2 and, hence, a new large family of self-dual vector space access structures for which Problem 1 has a positive answer.

The proof of Theorem 2, which is quite long and involved, will be given in the full version of the paper. In the following, we present a brief sketch of it. Given an identically self-dual bipartite matroid $\mathcal{M} = \mathcal{M}(X_1, X_2, r_1, r_2, d)$, one has to prove the existence of a finite field $\mathbb{K}$ and a set of $\mathbb{K}$-linear forms $\{\pi_1, \ldots, \pi_{2d}\}$ satisfying two requirements: first, they must be a $\mathbb{K}$-representation of the matroid $\mathcal{M}$ and, second, the vectors $\{\pi_i \otimes \pi_i : 1 \leq i \leq 2d\}$ must be linearly dependent.

In order to prove the existence of those linear forms, we conveniently choose some fixed vectors $\{\pi_1, \ldots, \pi_{n_1}\}$ corresponding to the points in the flat X_1 and a family of vectors $\{\mathbf{w}(x) : x \in \mathbb{K}\} \subset (\mathbb{K}^d)^*$ depending on one parameter. Afterwards, we use some Algebraic Geometry to prove that there exist vectors $\pi_{n_1+i} = \mathbf{w}(\beta_i^{-1})$, where $i = 1, \ldots, n_2 = |X_2|$, such that the vectors $\{\pi_1, \ldots, \pi_{2d}\}$ have the required properties. Specifically, the second requirement above is satisfied if the point $(\beta_1, \ldots, \beta_{n_2})$ is a zero of a system of polynomial equations on n_2 variables. These equations define an algebraic variety M in $\overline{\mathbb{Z}}_p^{n_2}$, where $\overline{\mathbb{Z}}_p$ is the algebraic closure of the finite field $\mathbb{Z}_p$. If p is large enough, the variety M is irreducible [25]. The first requirement is verified if other polynomials on the same variables are not zero in the point $(\beta_1, \ldots, \beta_{n_2})$. Every one of these equations defines and algebraic variety V_j in $\overline{\mathbb{Z}}_p^{n_2}$. We prove that M is not a subset of any of the varieties V_j and, since M is irreducible, this implies $M \not\subset \bigcup V_j$ [17]. Therefore there exists a point $(\beta_1, \ldots, \beta_{n_2}) \in M - (\bigcup V_j) \subset \overline{\mathbb{Z}}_p^{n_2}$. Finally, we take a finite field $\mathbb{K}$, an algebraic extension of $\mathbb{Z}_p$ containing all values β_i, and over that field, the linear forms $\pi_{n_1+i} = \mathbf{w}(\beta_i^{-1})$.

References

1. A. Barg. On some polynomials related to weight enumerators of linear codes. *SIAM J. Discrete Math.* **15** (2002) 155–164.
2. A. Beimel, T. Tassa, E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Comput. Sci.* **3378** (2005) 600–619.
3. M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proc. ACM STOC'88* (1988) 1–10.
4. E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.
5. E.F. Brickell, D.M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology.* **4** (1991) 123–134.
6. T. Britz. MacWilliams identities and matroid polynomials. *Electron. J. Combin.* **9** (2002), Research Paper 19, 16 pp.
7. P.J. Cameron. Cycle index, weight enumerator, and Tutte polynomial. *Electron. J. Combin.* **9** (2002), Note 2, 10 pp.
8. R. Canetti, U. Feige, O. Goldreich, M. Naor. Adaptively secure multi-party computation. *Proc. ACM STOC'96* (1996) 639–648.
9. D. Chaum, C. Crépeau, I. Damgård. Multi-party unconditionally secure protocols. *Proc. ACM STOC'88* (1988) 11–19.
10. R. Cramer, I. Damgård, U. Maurer. General Secure Multi-Party Computation from any Linear Secret-Sharing Scheme. *Advances in Cryptology - EUROCRYPT 2000, Lecture Notes in Comput. Sci.* **1807** (2000) 316–334.
11. O. Goldreich, M. Micali, A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. *Proc.19th ACM Symposium on the Theory of Computing STOC'87* (1987) 218–229.
12. C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Appl. Math.* **55** (1976) 119–128.

13. M. Hirt, U. Maurer. Complete characterization of adversaries tolerable in secure multi-party computation. *Proc. 16th Symposium on Principles of Distributed Computing PODC '97* (1997) 25–34.
14. M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.* (1987) 99–102.
15. W.-A. Jackson, K.M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptogr.* **4** (1994) 83–95.
16. M. Karchmer, A. Wigderson. On span programs. *Proceedings of the Eighth Annual Structure in Complexity Theory Conference* (San Diego, CA, 1993), 102–111, 1993.
17. E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, Boston, 1985.
18. J. Martí-Farré, C. Padró. Secret sharing schemes on access structures with intersection number equal to one. In *Proceedings of the Third Conference on Security in Communication Networks '02, Lecture Notes in Comput. Sci.* **2576** (2003) 354–363. Amalfi, Italy, 2002.
19. F. Matúš. Matroid representations by partitions. *Discrete Mathematics* **203** (1999) 169–194.
20. S.-L. Ng. A Representation of a Family of Secret Sharing Matroids. *Des. Codes Cryptogr.* **30** (2003) 5-19.
21. S.-L. Ng, M. Walker. On the composition of matroids and ideal secret sharing schemes. *Des. Codes Cryptogr.* **24** (2001) 49-67.
22. J.G. Oxley. *Matroid theory.* Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.
23. C. Padró, G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory.* **46** (2000) 2596–2604. A previous version appeared in *Advances in Cryptology - EUROCRYPT'98, Lecture Notes in Comput. Sci.* **1403** (1998) 500-511.
24. R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.* **106/107** (1992) 369–381.
25. Z. Reichstein, B. Youssin. Essential dimensions of algebraic groups and a resolution theorem for G-varieties. With an appendix by János Kollár and Endre Szabó. *Canad. J. Math.* **52** (2000) 1018–1056.
26. A. Shamir. How to share a secret. *Commun. of the ACM.* **22** (1979) 612–613.
27. G.J. Simmons. An introduction to shared secret and/or shared control schemes and their application. *Contemporary Cryptology. The Science of Information Integrity.* IEEE Press (1991), 441-497.
28. J. Simonis, A. Ashikhmin. Almost affine codes. *Des. Codes Cryptogr.* **14** (1998) 179–197.
29. D.R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.* **2** (1992) 357–390.
30. T. Tassa. Hierarchical Threshold Secret Sharing. *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004. Lecture Notes in Comput. Sci.* **2951** (2004) 473–490.