Representing small identically self-dual matroids by self-dual codes *

Carles Padró† Ignacio Gracia†

October 19, 2005

Abstract

The matroid associated to a linear code is the representable matroid that is defined by the columns of any generator matrix. The matroid associated to a self-dual code is identically self-dual, but it is not known whether every identically self-dual representable matroid can be represented by a self-dual code.

This open problem was proposed in [8], where it was proved to be equivalent to an open problem on the complexity of multiplicative linear secret sharing schemes.

Some contributions to its solution are given in this paper. A new family of identically self-dual matroids that can be represented by self-dual codes is presented. Besides, we prove that every identically self-dual matroid on at most eight points is representable by a self-dual code.

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

1 Introduction

1.1 Self-dual codes and identically self-dual matroids

Let $\mathcal{C}$ be a $[n,k]$ linear code over a finite field $\mathbb{K}$, where n and k are, respectively, the *length* and the *dimension* of $\mathcal{C}$. A *generator matrix* of $\mathcal{C}$ is any $k \times n$ matrix M with entries in $\mathbb{K}$ whose rows span the codewords in $\mathcal{C}$. That is, the vectors in the form $\mathbf{x} = \mathbf{u}M \in \mathbb{K}^n$, where $\mathbf{u} \in \mathbb{K}^k$, are precisely the codewords in $\mathcal{C}$. The columns of the matrix M define a $\mathbb{K}$-representable matroid $\mathcal{M}(M)$ on the set of points $Q = \{1, \ldots, n\}$. Some basic definitions and results on Matroid Theory are given in Section 2 and the reader is addressed to [13] for a reference book on this topic. All generator matrices of the code $\mathcal{C}$ define the same matroid and, hence, $\mathcal{M}(M)$ is said to be the *matroid associated to the code* $\mathcal{C}$ and is denoted by $\mathcal{M}(\mathcal{C})$. In addition, we say that the code

*This work was partially supported by the Spanish *Ministerio de Ciencia y Tecnología* under project TIC 2003-00866. This work was done while the first author was in a sabbatical stay in CWI, Amsterdam. This stay was funded by the *Secretaría de Estado de Educación y Universidades* of the Spanish Ministry of Education.

†Dept. of Applied Mathematics IV, Technical University of Catalonia, Barcelona. e-mail: {matcpl, ignacio}@ma4.upc.edu

$\mathcal{C}$ is a $\mathbb{K}$-representation of the matroid $\mathcal{M}$. While a unique matroid is associated to a linear code $\mathcal{C}$, different codes can represent the same matroid.

Greene's Theorem [10], which relates the weight enumerator of a code to the Tutte polynomial of its associated matroid, is the most well known result about that connection between codes and matroids. Several works have appeared afterwards on that subject [1, 5, 6, 9].

Let N be a *parity-check matrix* of the code $\mathcal{C}$, that is, any $(n-k)\times n$ matrix N with maximum rank such that $MN^\top = 0$, where $N^\top$ denotes the transpose of N. Then, N is the generator matrix of a $[n, n-k]$ linear code that is called the *dual code of* $\mathcal{C}$ and is denoted by $\mathcal{C}^\perp$. If $\mathcal{C}^\perp = \mathcal{C}$, we say that $\mathcal{C}$ is a *self-dual code*. Of course, $n = 2k$ in every self-dual code.

It is well known that the matroid associated to the dual code $\mathcal{C}^\perp$ is the *dual matroid* of the matroid associated to $\mathcal{C}$. Then, the matroid associated to a self-dual code is identically self-dual. Nevertheless, it is not known whether every identically self-dual representable matroid can be represented by a self-dual code. Specifically, the following open problem was stated in [8].

Open Problem 1. 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 $\mathbb{K}$.

Matroids that are represented by a self-dual code over the field $\mathbb{K}$ will be said to be *self-dually* $\mathbb{K}$*-representable*. Since every $\mathbb{Z}_2$-representable matroid admits an unique code representing it over $\mathbb{Z}_2$, all identically self-dual $\mathbb{Z}_2$-representable matroids are self-dually $\mathbb{Z}_2$-representable. The uniform matroids $U_{k,2k}$ form another family of identically self-dual matroids for which the answer to Open Problem 1 is affirmative. Moreover, if $\mathcal{M}_1$ and $\mathcal{M}_2$ are self-dually $\mathbb{K}$-representable matroids, the *sum* $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$ of these matroids is self-dually $\mathbb{L}$-representable, where $\mathbb{L}$ is an algebraic extension of $\mathbb{K}$ with $[\mathbb{L} : \mathbb{K}] \leq 2$. As a consequence of this fact and other properties of the sum of matroids, solving Open Problem 1 can be restricted to *indecomposable* matroids, that is, those that can not be expressed as the sum of two smaller matroids [8]. Finally, the identically self-dual bipartite matroids were proved to be self-dually representable in [8].

1.2 Ideal multiplicative linear secret sharing schemes

The interest of that open problem is increased by its relation to the multiplicative property of linear secret sharing schemes. That property was introduced by Cramer, Damgård and Maurer [7] in order to construct efficient secure multi-party computation protocols for a general (that is, not necessarily threshold-based) adversary. The readers are referred to [17, 7, 8] for more information about secret sharing, the multiplicative property and secure multi-party computation.

A $\mathbb{K}$-linear secret sharing scheme Σ with access structure Γ on the set of players P is said to be *multiplicative* if every player $i \in P$ can compute a value c_i from its shares s_i, s'_i corresponding to two shared secret values $s, s' \in \mathbb{K}$ in such a way that the product ss' is a linear combination of the values $(c_i)_{i\in P}$. Such schemes can be constructed if

and only the set of players is not the union of two unqualified subsets [11, 7]. In this case, we say that the *access structure* of the scheme is $\mathcal{Q}_2$. One of the key results in [7] is a method to construct, from any $\mathbb{K}$-linear secret sharing scheme with $\mathcal{Q}_2$ access structure, a multiplicative $\mathbb{K}$-linear secret sharing scheme with the same access structure and whose complexity is only twice the complexity of the original scheme. One of the main open problems about this topic is to determine for which $\mathcal{Q}_2$ access structures there exists a multiplicative scheme with the *same complexity* as the best linear scheme. This problem has been studied in [8] for minimally $\mathcal{Q}_2$ access structures that can be realized by an *ideal* linear secret sharing scheme, that is, a scheme in which all shares have the same length as the secret. Namely, the next open problem is proposed in that paper, where it is proved to be equivalent to Open Problem 1.

Open Problem 2. To determine whether there exists, for every minimally $\mathcal{Q}_2$ access structure Γ that can be realized by an ideal $\mathbb{K}$-linear secret sharing scheme, an ideal multiplicative $\mathbb{L}$-linear secret sharing scheme, being the finite field $\mathbb{L}$ an algebraic extension of $\mathbb{K}$.

The equivalence between these two problems is due to the close relation between ideal linear secret sharing schemes, linear codes and matroids. Actually, an ideal linear secret sharing schemes can be identified to a linear code. The access structure of the scheme is then determined by the matroid associated to the code. The connection between ideal secret sharing schemes and matroids, which applies to non-linear schemes as well, was discovered by Brickell and Davenport [4] and has been studied afterwards in may other works, being [17, 16, 12, 2] some of them. 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.

In addition, the notion of *duality* that applies to codes and matroids is extended to access structures. Self-dual access structures coincide with the minimally $\mathcal{Q}_2$ ones. Moreover, every self-dual code defines an ideal multiplicative linear secret sharing scheme with self-dual access structure.

1.3 Our results

The aim of this paper is to provide new results towards the solution of Open Problem 1.

A new family of indecomposable self-dually representable matroids is presented in Section 5. By using some of the matroids in that family and other techniques we get our main result. Namely, the answer to Open Problem 1 is affirmative for matroids on at most eight points.

Theorem 3. *Let $\mathcal{M}$ be an identically self-dual connected matroid on at most eight points (or, equivalently, with rank at most four). Then $\mathcal{M}$ is representable. Moreover, if $\mathcal{M}$ is $\mathbb{K}$-representable, then $\mathcal{M}$ can be represented by a self-dual linear code over some finite field $\mathbb{L}$, an algebraic extension of $\mathbb{K}$.*

This is proved by enumerating all non-isomorphic identically self-dual matroids with rank at most four and checking that the result holds for every one of them.

By taking into account the equivalence between Open Problems 1 and 2, the following result is a direct consequence of Theorem 3.

Corollary 4. *Let Γ be a self-dual access structure on a set P with at most seven players. Let us suppose that Γ can be realized by an ideal secret sharing scheme over a finite field $\mathbb{K}$. Then, for some algebraic extension $\mathbb{L}$ of $\mathbb{K}$, there exists an ideal multiplicative $\mathbb{L}$-linear secret sharing scheme with access structure Γ.*

1.4 Organization of the paper

Some basic definitions and facts about Matroid Theory are recalled in Section 2. Sections 3 and 4 contain some technicalities that are needed in the proofs in the following sections. A new family of self-dually representable matroids is introduced in Section 5. Finally, Section 6 contains the proof of Theorem 3, our main result.

2 Basics on Matroid Theory

Let E be a $\mathbb{K}$-vector space and $Q = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subset E$ a finite set of vectors. The subsets of Q can be linearly independent or dependent, every subset spans a subspace of E with a certain dimension and some of them are basis of the subspace spanned by Q. A matroid is an abstraction of these concepts. Several axioms that fit in the situation above are given to define the matroids on a set of points $Q = \{1, \ldots, n\}$. See [13] for a general reference on Matroid Theory.

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

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

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

The set Q is the *set of points* 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 the *rank* of $\mathcal{M}$. The most simple examples of matroids are the uniform ones. The *uniform matroid* $U_{k,n}$ is the matroid on a set Q of n points whose bases are all sets with exactly k points.

A subset $X \subset Q$ is said to be *independent* if there exists a basis $B \in \mathcal{B}$ with $X \subset B$, while we say that $X \subset Q$ is a *spanning subset* if $B \subset X$ for some basis $B \in \mathcal{B}$. The *dependent* subsets are those that are not independent. A point $p \in Q$ is called a *loop* if $\{p\}$ is a dependent subset and a *coloop* is a point $p \in Q$ such that $p \in B$ for every basis $B \in \mathcal{B}$. A *circuit* is a minimally dependent subset and the maximally independent subsets coincide with the bases. The *rank* of $X \subset Q$ is the maximum cardinality of the subsets of X that are independent. Observe that the rank of Q coincides with the rank of the matroid $\mathcal{M}$ that was defined before. A matroid is said to be *connected* if, for every two points $i, j \in Q$, there exists a circuit C with $i, j \in C$.

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

If $\mathcal{M}$ is a matroid on the set Q, with family of bases $\mathcal{B}$, then $\mathcal{B}^* = \{Q - B : B \in \mathcal{B}\}$ 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. Observe that $|Q| = 2\operatorname{rank}(\mathcal{M})$ if the matroid is self-dual.

Let $\mathbb{K}$ be a finite field and M be a $k \times n$ matrix with $\operatorname{rank}(M) = k$ with entries in $\mathbb{K}$. A matroid $\mathcal{M}$ on the set $Q = \{1, \ldots, n\}$ is defined from the matrix M by considering that a subset $B = \{i_1, \ldots, i_k\} \subset Q$ is a basis if and only if the corresponding columns of M form a basis of $\mathbb{K}^k$. In this situation, we say that the matrix M is a $\mathbb{K}$-*representation* of the matroid $\mathcal{M}$. The matroids that can be defined in this way are called *representable*. As it was said before, all generator matrices of a linear code $\mathcal{C}$ define the same matroid $\mathcal{M} = \mathcal{M}(\mathcal{C})$. In this case, we say that $\mathcal{C}$ is a $\mathbb{K}$-*representation* of $\mathcal{M}$, or that $\mathcal{C}$ *represents* $\mathcal{M}$ over $\mathbb{K}$.

3 Almost self-dual codes

We say that a $[2k, k]$ linear code $\mathcal{C}$ with generator matrix M is *almost self-dual* if there exists a non-singular diagonal matrix $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_{2k})$ such that MD is a parity check matrix. Since the matrices M and MD represent the same matroid, the matroid associated to an almost self-dual code is identically self-dual. By the next proposition, in order to prove that a matroid is self-dually representable, it is enough to prove that it can be represented by an almost self-dual code.

Proposition 6. *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 $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_{2k})$ 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 $D_1 = \operatorname{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_{2k}})$. Then, $M_1 = MD_1$ 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. □

Let $\mathcal{C}$ be a $[n, k]$ linear code with generator matrix M and let us put $E = \mathbb{K}^k$. In the dual space E^*, that is, the vector space formed by all linear forms $\pi\colon E \to \mathbb{K}$, let us consider the linear forms $\pi_1, \ldots, \pi_n$ such that $\mathbf{u}M = (\pi_1(\mathbf{u}), \ldots, \pi_n(\mathbf{u}))$ for every $\mathbf{u} \in E$. Observe that every one of these linear forms corresponds to a column of M. Then, we will write $M = (\pi_1, \ldots, \pi_n)$.

If $\pi \in E^*$, then $\pi \otimes \pi$ denotes the symmetric bilinear form $\pi \otimes \pi\colon E \times E \to \mathbb{K}$ defined by $(\pi \otimes \pi)(\mathbf{u}, \mathbf{v}) = \pi(\mathbf{u})\pi(\mathbf{v})$. We notate $\mathcal{S}(E)$ for the symmetric bilinear forms on E. The dimension of $\mathcal{S}(E)$ is $k(k+1)/2$, where $k = \dim E$. The following lemma is proved in [8].

Lemma 7. *Let $M = (\pi_1, \dots \pi_{2k})$ be a generator matrix of a $[2k, k]$ linear code $\mathcal{C}$ and let us take $Q = \{1, \dots, 2k\}$. Let us suppose that the matroid associated to $\mathcal{C}$ is identically self-dual and connected. Then, in the space $\mathcal{S}(E)$, the vectors $\{\pi_j \otimes \pi_j : j \in Q - \{i\}\}$ are linearly independent for every $i \in Q$. In addition, the code $\mathcal{C}$ is almost self-dual if and only if the vectors $\{\pi_j \otimes \pi_j : j \in Q\}$ are linearly dependent.*

We present in the following a method to prove that a code $\mathcal{C}$ whose associated matroid is identically self-dual and connected is almost self-dual.

Let $M = (\pi_1, \dots, \pi_{2k})$ be a generator matrix of $\mathcal{C}$. From Lemma 7, it is enough to check that the subspace $\langle \pi_1 \otimes \pi_1, \dots, \pi_{2k} \otimes \pi_{2k} \rangle \subset \mathcal{S}(E)$ has dimension $2k - 1$. Every symmetric bilinear form $\Lambda \in \mathcal{S}(E)$ can be represented by the symmetric $k \times k$ matrix $M(\Lambda) = (\lambda_{ij})$ such that $\Lambda(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{x}_1 M(\Lambda) \mathbf{x}_2^\top$ for every $\mathbf{x}_1, \mathbf{x}_2 \in E$. One can prove that $\dim\langle \pi_1 \otimes \pi_1, \dots, \pi_{2k} \otimes \pi_{2k} \rangle = 2k-1$ by showing $\dim \mathcal{S}(E) - (2k-1) = (k-1)(k-2)/2$ linearly independent linear equations in the form $\sum_{1 \le i \le j \le k} c_{ij} \lambda_{ij} = 0$ that are fulfilled by the coefficients $(\lambda_{ij})_{1 \le i \le j \le k}$ of every one of the bilinear forms $\pi_i \otimes \pi_i$.

Observe that, if $\pi = (v_1, \dots, v_d) \in E^*$, the coefficients of the bilinear form $\pi \otimes \pi$ are $\lambda_{ij} = v_i v_j$. Then, the code $\mathcal{C}$ is almost self-dual if the components of every one of the vectors $\{\pi_1, \dots, \pi_{2k}\}$ satisfy $(k-1)(k-2)/2$ linearly independent quadratic equations in the form $\sum_{1 \le i \le j \le k} c_{ij}\ v_i v_j = 0$.

In order to illustrate this method we apply it to prove the well known result that the uniform matroid $U_{k,2k}$ can be $\mathbb{K}$-represented by an almost self-dual code for every finite field with $|\mathbb{K}| \ge 2k$. Let us take $2k$ pairwise different elements $x_1, \dots, x_{2k} \in \mathbb{K}$ and, for every $i = 1, \dots, 2k$, the linear form $\pi_i = (1, x_i, x_i^2, \dots, x_i^{k-1}) \in E^*$. From the properties of the Vandermonde matrix, it is clear that the code $\mathcal{C}$ defined by those linear forms is a $\mathbb{K}$-representation of $U_{k,2k}$. Moreover, all vectors π_i verify the $(k-1)(k-2)/2$ linearly independent quadratic equations $v_i v_j = v_{i-1} v_{j+1}$, where $2 \le i \le j \le k-1$, and, hence, the code $\mathcal{C}$ is almost self-dual.

4 Sum of matroids and flat-partitions

We present next the definition of the *sum* of two matroids, an operation that is usually called 2-*sum* in the literature. 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 $q_2 \in Q_2$ such that q_i is neither a loop nor a coloop of $\mathcal{M}_i$. 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 $Q = (Q_1 \cup Q_2) - \{q_1, q_2\}$ whose family of bases is $\mathcal{B} = \mathcal{B}_1' \cup \mathcal{B}_2'$, where

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

It is not difficult to check that $\mathcal{B}$ verifies the axioms in Definition 5 and that $\mathcal{M}$ is a connected matroid with $\operatorname{rank} \mathcal{M} = \operatorname{rank} \mathcal{M}_1 + \operatorname{rank} \mathcal{M}_2 - 1$. Observe that, if $\mathcal{M}_2$ is the uniform matroid $U_{1,2}$, then $\mathcal{M}_1 \oplus_{(q_1,q_2)} U_{1,2} \cong \mathcal{M}_1$ for every possible pair of points (q_1, q_2). This is said to be a *trivial* sum. A matroid is said to be *indecomposable* if it is

not isomorphic to any non-trivial sum of matroids. 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 [8]. The next proposition was also proved in [8].

Proposition 8. *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 $[\mathbb{L} : \mathbb{K}] \leq 2$.*

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 $\mathcal{M}$. If $\mathcal{M}$ is connected and $\emptyset \neq X \subset Q$, then $\text{rank}(X) + \text{rank}(Q - X) > \text{rank}(\mathcal{M})$ [13, Proposition 4.2.1]. The following lemma is a direct consequence of this fact.

Lemma 9. *Let $\mathcal{M}$ be a connected matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Then, $\text{rank}(X_1) + \text{rank}(X_2) > \text{rank}(\mathcal{M})$ and $\text{rank}(X_i) > 1$ for $i = 1, 2$.*

The next proposition, which is a consequence of [13, Theorem 8.3.1], provides a characterization of indecomposable identically self-dual matroids in terms of their flat-partitions.

Proposition 10. *Let $\mathcal{M}$ be a connected identically self-dual matroid. Then $\mathcal{M}$ is indecomposable if and only if $\text{rank}(X_1) + \text{rank}(X_2) > \text{rank}(\mathcal{M}) + 1$ for every flat-partition (X_1, X_2) of $\mathcal{M}$. Moreover, if there exists a flat-partition of $\mathcal{M}$ with $\text{rank}(X_1) + \text{rank}(X_2) = \text{rank}(\mathcal{M}) + 1$, then, there exist two connected identically self-dual matroids $\mathcal{M}_1$, $\mathcal{M}_2$ with $\text{rank}(\mathcal{M}_i) = \text{rank}(X_i)$ and $\mathcal{M} = \mathcal{M}_1 \oplus_{(q_1,q_2)} \mathcal{M}_2$.*

The next two technical lemmas deal with properties of flat-partitions in identically self-dual matroids that will be needed in the following sections. The first one is a direct consequence of the fact that $\text{rank}^*(X) = |X| - \text{rank}(\mathcal{M}) + \text{rank}(Q - X)$ for every matroid $\mathcal{M}$ and for every subset $X \subset Q$, where $\text{rank}^*(X)$ is the rank of X in the dual matroid [13, Proposition 2.1.9].

Lemma 11. *Let $\mathcal{M}$ be a connected identically self-dual matroid and let (X_1, X_2) be a flat-partition of $\mathcal{M}$. Let us take $k = \text{rank}(\mathcal{M})$ and $r_i = \text{rank}(X_i)$. Then, $|X_1| = k + r_1 - r_2$.*

Lemma 12. *Let $\mathcal{M}$ be an identically self-dual matroid and let $C \subset Q$ be a circuit of $\mathcal{M}$ with $\text{rank}(C) < \text{rank}(\mathcal{M})$. Let us consider the flat $X_1 = \langle C \rangle$ and $X_2 = Q - X_1$. 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 $B' = Q - B$ and we take $B_2 = B' \cap X_2$.

We claim that, in this situation, $X_2 \subset \langle B_2 \rangle$. Let us suppose that, on the contrary, there exists $y \in X_2 - \langle B_2 \rangle$. Observe that $y \in C_2$ and that $B_2 \cup \{y\}$ is an independent

set. Therefore, $Q-(B_2\cup\{y\})=X_1\cup(C_2-\{y\})$ is a spanning set. Since $\langle B_1\rangle=X_1$, we have that $B''=B_1\cup(C_2-\{y\})$ is equally a spanning set, a contradiction with $B''\subsetneq B$.

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

5 A family of self-dually representable paving matroids

For a matroid $\mathcal{M}$, we notate $\delta(\mathcal{M})$ for the minimum rank of the circuits of $\mathcal{M}$. Observe that $\delta(\mathcal{M})\leq \mathrm{rank}(\mathcal{M})$ and that the uniform matroids are the only ones with $\delta(\mathcal{M})=\mathrm{rank}(\mathcal{M})$. Matroids with $\delta(\mathcal{M})\geq \mathrm{rank}(\mathcal{M})-1$ are called *paving matroids*. We study in this section the identically self-dual matroids with $\delta(\mathcal{M})=\mathrm{rank}(\mathcal{M})-1$.

Let $\mathcal{M}$ be an identically self-dual matroid with $\mathrm{rank}(\mathcal{M})=k$ and $\delta(\mathcal{M})=k-1$ and let $Q=\{1,\ldots,2k\}$ be its set of points. The matroid $\mathcal{M}$ is completely determined by the set $\mathbf{C}^k$ of all circuits of $\mathcal{M}$ with exactly k points, that is, the subsets of k elements of Q that are not a basis of $\mathcal{M}$. Observe that, for every $i\in Q$, the set $\mathbf{C}^k(i)=\{C\in\mathbf{C}^k\,:\,i\in C\}$ contains exactly one half of the circuits in $\mathbf{C}^k$, being the other half their complements, that is, $\mathbf{C}^k=\mathbf{C}^k(i)\cup\{Q-C\,:\,C\in\mathbf{C}^k(i)\}$. From Lemmas 11 and 12, $\langle C\rangle=C$ and $(C,Q-C)$ is a flat-partition of $\mathcal{M}$ for every $C\in\mathbf{C}^k$.

Lemma 13. *Let us consider two circuits $C_1,C_2\in\mathbf{C}^k$ such that $C_1\neq C_2,Q-C_2$. Then, $2\leq|C_1\cap C_2|\leq k-2$.*

Proof: If $|C_1\cap C_2|\geq k-1$, then $C_1\subset\langle C_2\rangle=C_2$ and, hence, $C_1=C_2$. Therefore, there are at most $k-2$ points in the intersection of any two different circuits in $\mathbf{C}^k$. Finally, if $|C_1\cap C_2|\leq 1$, then $|C_1\cap(Q-C_2)|\geq k-1$, a contradiction with $C_1\neq Q-C_2$. □

Let $\mathbb{K}$ be a finite field with $|\mathbb{K}|\geq 2k$ and let $\alpha_1,\alpha_2,\ldots,\alpha_{2k}\in\mathbb{K}$ be pairwise different elements such that $\alpha_1+\cdots+\alpha_{2k}=0$. Let us take $Q=\{1,\ldots,2k\}$. It is not difficult to check that $\mathcal{B}(\alpha_1,\alpha_2,\ldots,\alpha_{2k})=\{\{i_1,\ldots,i_k\}\subset Q\,:\,\alpha_{i_1}+\cdots+\alpha_{i_k}\neq 0\}$ is the family of bases of a matroid on the set of points Q, which will be denoted by $\mathcal{S}(\alpha_1,\alpha_2,\ldots,\alpha_{2k})$. All matroids in this form are identically self-dual paving matroids. Moreover, we prove in the next proposition that they are self-dually representable.

Proposition 14. *Let $\mathbb{K}$ be a finite field with $|\mathbb{K}|\geq 2k$ and let $\alpha_1,\alpha_2,\ldots,\alpha_{2k}\in\mathbb{K}$ be pairwise different elements such that $\alpha_1+\cdots+\alpha_{2k}=0$ Then, the matroid $\mathcal{M}=\mathcal{S}(\alpha_1,\alpha_2,\ldots,\alpha_{2k})$ can be represented over $\mathbb{K}$ by an almost self-dual code and, hence, it is self-dually $\mathbb{L}$-representable, where $\mathbb{L}$ is some algebraic extension of $\mathbb{K}$.*

Proof: If $\delta(\mathcal{M})=k$, then $\mathcal{M}$ is the uniform matroid $U_{k,2k}$. Since $|\mathbb{K}|\geq 2k$, there exists an almost self-dual code representing $\mathcal{M}$ over $\mathbb{K}$.

If $\delta(\mathcal{M})=k-1$, we can suppose without loss of generality that $\alpha_1+\cdots+\alpha_k=0$. Let us consider the linear forms $\pi_i=(1,\alpha_i,\alpha_i^2,\ldots,\alpha_i^{k-2},\alpha_i^k)\in(\mathbb{K}^k)^*$, where $i=1,\ldots,2k$, and the matrix $M=(\pi_1,\ldots,\pi_{2k})$. We are going to prove that M is a $\mathbb{K}$-representation of the matroid $\mathcal{M}$ and a generator matrix of an almost self-dual code.

The first affirmation is proved by showing that k different vectors $\pi_{i_1},\ldots,\pi_{i_k}$ are linearly dependent if and only if $\alpha_{i_1}+\cdots+\alpha_{i_k}=0$. These vectors are linearly dependent if and only if there exist values $(c_1,\ldots,c_k)\neq(0,\ldots,0)$ such that $c_1+c_2\alpha_{i_j}+c_3\alpha_{i_j}^2+$

$\cdots + c_{k-1}\alpha_{i_j}^{k-2} + c_k\alpha_{i_j}^k = 0$ for every $j = 1, \ldots, k$. This is equivalent to the fact that the polynomial $(x-\alpha_{i_1})\cdots(x-\alpha_{i_k})$ has the form $c'_1 + c'_2x + \cdots c'_{k-1}x^{k-2} + x^k$, which is equivalent to $\alpha_{i_1} + \cdots + \alpha_{i_k} = 0$.

In order to prove that the code $\mathcal{C}$ with generator matrix M is almost self-dual, we are going to check that the vectors $\pi_1, \ldots, \pi_{2k}$ verify $(k-1)(k-2)/2$ linearly independent quadratic equations $\sum_{1\leq i\leq j\leq k} c_{ij}\ v_iv_j = 0$. Observe that the $(k-2)(k-3)/2$ equations $v_iv_j = v_{i-1}v_{j+1}$, where $2 \leq i \leq j \leq k-2$, are fulfilled by those vectors. The same occurs with the $k-3$ equations $v_iv_k = v_{i+2}v_{k-1}$, where $1 \leq i \leq k-3$. Only one more equation is needed, which is $(a_0v_1 + \ldots + a_{k-2}v_{k-1} + v_k)(b_0v_1 + \ldots + b_{k-2}v_{k-1} + v_k) = 0$, where $(x-\alpha_1)\cdots(x-\alpha_k) = a_0 + a_1x + a_2x^2 \cdots + a_{k-2}x^{k-2} + x^k$ and $(x-\alpha_{k+1})\cdots(x-\alpha_{2k}) = b_0 + b_1x + b_2x^2 \cdots + b_{k-2}x^{k-2} + x^k$. □

6 Identically self-dual matroids with rank at most four

This section is devoted to prove Theorem 3. We determine all the identically self-dual connected matroids with rang at most four and we prove that every one of them is self-dually representable.

Obviously, the uniform matroid $U_{1,2}$ is the only identically self-dual matroid with rank one. Let $\mathcal{M}$ be an identically self-dual connected matroid with $2 \leq \text{rank}(\mathcal{M}) \leq 4$. By Lemmas 9 and 12, the connectedness of $\mathcal{M}$ implies that $\delta(\mathcal{M}) \geq 2$. Then, it is clear that $\mathcal{M} = U_{2,4}$ if $\text{rank}(\mathcal{M}) = 2$. If $\text{rank}(\mathcal{M}) = \delta(\mathcal{M}) = k = 3, 4$, then $\mathcal{M} = U_{k,2k}$. If $\text{rank}(\mathcal{M}) = 3$ and $\delta(\mathcal{M}) = 2$, by Lemma 12 there exists a flat-partition (X_1, X_2) of $\mathcal{M}$ with $\text{rank}(X_1) = \text{rank}(X_2) = 2$. From Proposition 10, $\mathcal{M} = U_{2,4} \oplus U_{2,4}$. If $\text{rank}(\mathcal{M}) = 4$ and $\delta(\mathcal{M}) = 2$, we apply again Lemmas 9 and 12 and Proposition 10 and we get that $\mathcal{M} = U_{2,4} \oplus \mathcal{M}_1$, where $\mathcal{M}_1$ is an identically self-dual connected matroid with $\text{rank}(\mathcal{M}_1) = 3$. Therefore, $\mathcal{M} = U_{2,4} \oplus U_{3,6}$ or $\mathcal{M} = U_{2,4} \oplus U_{2,4} \oplus U_{2,4}$.

Summarizing, if $\mathcal{M}$ is an identically self-dual connected matroid with rank at most three or it has rank four and $\delta(\mathcal{M}) = 2, 4$, then $\mathcal{M}$ is an uniform matroid or a sum of uniform matroids. Therefore, for every prime p, the matroid $\mathcal{M}$ is self-dually $\mathbb{K}$-representable for some finite field $\mathbb{K}$ with characteristic p.

Let us suppose now that $\mathcal{M}$ is an identically self-dual connected matroid on the set of points $Q = \{1, 2, \ldots, 8\}$ with $\text{rank}(\mathcal{M}) = 4$ and $\delta(\mathcal{M}) = 3$. Let us consider the set $\mathbf{C}^4$ of the circuits of $\mathcal{M}$ with exactly four points and $\mathbf{C}^4(8) = \{C \in \mathbf{C}^4 : 8 \in C\} = \{C_1, \ldots, C_m\}$, which contains half of the circuits in $\mathbf{C}^4$.

Let us consider $\mathbf{D} = \{D_1, \ldots, D_m\}$, where $D_i = C_i - \{8\} \subset \{1, \ldots, 7\}$. From Lemma 13, $|D_i \cap D_j| = 1$ if $i \neq j$. The matroid $\mathcal{M}$ is completely determined by $\mathbf{D}$, which is a family of subsets of 3 elements taken from $\{1, \ldots, 7\}$ verifying that any two of them intersect in exactly one point. Moreover, there exists an identically self-dual paving matroid with rank 4 for every such family $\mathbf{D}$.

The projective plane over the finite field $\mathbb{Z}_2$, which is called the *Fano Plane*, consists of 7 points and 7 lines and every line has exactly 3 points. Of course, any two lines intersect in a single point. Observe that $\mathbf{D}$ must be a subset of $\{R_1, \ldots, R_7\}$, the set of the lines of some Fano Plane defined on the set of points $Q - \{8\} = \{1, \ldots, 7\}$.

If we identify every point in $\{1, \ldots, 7\}$ with the point in $\mathbb{Z}_2^3 - \{(0,0,0)\}$ corre-

sponding to its binary representation, we obtain a Fano Plane whose lines are: $R_1 = \{2,4,6\}$, $R_2 = \{1,4,5\}$, $R_3 = \{3,4,7\}$, $R_4 = \{1,2,3\}$, $R_5 = \{2,5,7\}$, $R_6 = \{1,6,7\}$, $R_7 = \{3,5,6\}$. Therefore, up to isomorphism, the only identically self-dual matroids with rank equal to 4 and $\delta(\mathcal{M}) = 3$ are the matroids $\mathcal{M}_i$, where $i = 1, \ldots, 9$, determined by: $\mathbf{D}_1 = \{R_1\}$, $\mathbf{D}_2 = \{R_1, R_2\}$, $\mathbf{D}_3 = \{R_1, R_2, R_3\}$ (three lines intersecting in one point), $\mathbf{D}_4 = \{R_1, R_2, R_4\}$ (three lines without any common point), $\mathbf{D}_5 = \{R_1, R_2, R_4, R_7\}$ (the other three lines intersect in one point), $\mathbf{D}_6 = \{R_1, R_2, R_3, R_4\}$ (the other three lines do not have any common point), $\mathbf{D}_7 = \{R_1, R_2, R_3, R_4, R_5\}$, $\mathbf{D}_8 = \{R_1, R_2, R_3, R_4, R_5, R_6\}$, $\mathbf{D}_9 = \{R_1, R_2, R_3, R_4, R_5, R_6, R_7\}$.

The proof of Theorem 3 is concluded by proving that, for every $i = 1, \ldots, 9$, the matroid $\mathcal{M}_i$ is representable and that, for every finite field $\mathbb{K}$ such that $\mathcal{M}_i$ is $\mathbb{K}$-representable, there exists an almost self-dual code that is a $\mathbb{L}$-representation of $\mathcal{M}_i$ for some algebraic extension $\mathbb{L}$ of $\mathbb{K}$. This is done in Propositions 15, 16, 17 and 18. For every $i = 1, \ldots, 7$, we notate $C_i = R_i \cup \{8\} \subset Q$.

Proposition 15. *For $i = 1, 3$ and for every prime p, and for $i = 2$ and for every prime $p \neq 2$, there exists a finite field $\mathbb{K}$ with characteristic p and 8 pairwise different elements $\alpha_1, \ldots, \alpha_8 \in \mathbb{K}$ such that $\mathcal{M}_i = \mathcal{S}(\alpha_1, \ldots, \alpha_8)$ and, hence, $\mathcal{M}_i$ can be represented by an almost self-dual code over the field $\mathbb{K}$.*

Proof: Let $\mathbb{K}$ be any finite field with characteristic p and let us consider the vector space $E = \mathbb{K}^8$ and the subspace $V = \{(\alpha_1, \ldots, \alpha_8) \in E : \sum_{j=1}^{8} \alpha_j = 0\}$. For every $A \subset Q$ with $|A| = 4$, let us take the subspace $V(A) = \{(\alpha_1, \ldots, \alpha_8) \in E : \sum_{j \in A} \alpha_j = 0\}$ and, for every pair of different points $j, k \in Q$, the subspace $V_{j,k} = \{(\alpha_1, \ldots, \alpha_8) \in E : \alpha_j = \alpha_k\}$. Finally, we consider the subspaces $W_1 = V \cap V(C_1)$, $W_2 = V \cap V(C_1) \cap V(C_2)$ and $W_3 = V \cap V(C_1) \cap V(C_2) \cap V(C_3)$.

It is not difficult to check that $W_3 \subset W_2 \subset W_1 \not\subset V_{j,k}$ for all $j, k \in Q$. In addition, $W_1 \not\subset V(A)$ for all $A \subset Q$ with $|A| = 4$ and $A \neq C_1, Q - C_1$. Equally, $W_3 \not\subset V(A)$ for all $A \subset Q$ with $|A| = 4$ and $A \neq C_i, Q - C_i$ for every $i = 1, 2, 3$. Moreover, if $p \neq 2$, $W_2 \not\subset V(A)$ for all $A \subset Q$ with $|A| = 4$ and $A \neq C_i, Q - C_i$ for every $i = 1, 2$.

Therefore, for every prime p, there exists a large enough finite field $\mathbb{K}$ with characteristic p such that there exists a vector $\mathbf{x} = (\alpha_1, \ldots, \alpha_8) \in W_1$ with $\mathbf{x} \notin V_{j,k}, V(A)$ for all $j, k \in Q$ and for all $A \subset Q$ with $|A| = 4$ and $A \neq C_1, Q - C_1$. Then, $\mathcal{M}_1 = \mathcal{S}(\alpha_1, \ldots, \alpha_8)$. A similar argument applies for the matroid $\mathcal{M}_3$ and, if $p \neq 2$, for the matroid $\mathcal{M}_2$. $\square$

It is not difficult in general to find a set of values α_i whose existence is given by Proposition 15. For instance, if $\mathbb{K}$ is a finite field with characteristic $p \geq 17$, by using a very simple computer program one can check that $\mathcal{M}_1 = \mathcal{S}(5, -3, -1, 1, 6, 0, -10, 2)$, $\mathcal{M}_2 = \mathcal{S}(-4, 0, 5, 3, -3, -7, 2, 4)$ and $\mathcal{M}_3 = \mathcal{S}(2, 1, -3, 5, -2, -1, 3, -5)$.

Proposition 16. *The matroid $\mathcal{M}_2$ can be represented by an almost self-dual code over some finite field $\mathbb{K}$ with characteristic 2.*

Proof: In the corresponding algebraic extension $\mathbb{K}$ of $\mathbb{Z}_2$, let us take $\omega \in \mathbb{K}$ with

$\omega^{13} = 1$ and $\omega \neq 1$. Then, the matrix

$$M = M(\pi_1, \ldots, \pi_8) = \begin{pmatrix} \omega & 0 & \omega^3 & 0 & \omega^{-1} & 0 & \omega^{-3} & 0 \\ 0 & \omega^2 & 1 & 0 & 0 & \omega^{-2} & 1 & 0 \\ 0 & 1 & 0 & \omega^5 & 0 & 1 & 0 & \omega^{-5} \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

is the generator matrix of an almost self-dual code $\mathcal{C}$ that represents the matroid $\mathcal{M}_2$ over $\mathbb{K}$. This can be proved by using a simple computer program to check that $\det(\pi_{i_1}, \pi_{i_2}, \pi_{i_3}, \pi_{i_4}) = 0$ if and only if $\{i_1, i_2, i_3, i_4\} = C_1, Q - C_1, C_2, Q - C_2$ and that $\dim\langle \pi_1 \otimes \pi_1, \ldots, \pi_8 \otimes \pi_8 \rangle = 7$. □

Proposition 17. *For every finite field $\mathbb{K}$ and for every $i = 4, \ldots, 9$, if a code $\mathcal{C}$ is a $\mathbb{K}$-representation of the matroid $\mathcal{M}_i$, then $\mathcal{C}$ is almost self-dual.*

Proof: Let $\mathcal{M}$ be one of the matroids $\mathcal{M}_4, \ldots, \mathcal{M}_9$ and let $M = (\pi_1, \ldots, \pi_8)$ be such that the code $\mathcal{C}$ with generator matrix M is a $\mathbb{K}$-representation of $\mathcal{M}$. Since $\{R_1, R_2, R_4\} \subset \mathbf{D}_i$ for every $i = 4, \ldots, 9$, we have that $C_1 = \{2, 4, 6, 8\}$, $C_2 = \{1, 4, 5, 8\}$ and $C_4 = \{1, 2, 3, 8\}$ and their complements are circuits of $\mathcal{M}$. For every $i = 1, 2, 4$, let $a_1^i v_1 + a_2^i v_2 + a_3^i v_3 + a_4^i v_4 = 0$ and $b_1^i v_1 + b_2^i v_2 + b_3^i v_3 + b_4^i v_4 = 0$ be, respectively, the equations of the hyperplanes $V_i = \langle \pi_j \ : \ j \in C_i \rangle$ and $W_i = \langle \pi_j \ : \ j \in Q - C_i \rangle$. Therefore, there exist three quadratic equations in the form

$$(a_1^i v_1 + a_2^i v_2 + a_3^i v_3 + a_4^i v_4)(b_1^i v_1 + b_2^i v_2 + b_3^i v_3 + b_4^i v_4) = 0,$$

where $i = 1, 2, 4$, that are fulfilled by all the vectors π_j. We only have to prove that these quadratic equations are linearly independent. Let $Q_1, Q_2, Q_4 \subset \mathbb{K}^4$ be the quadrics defined by those equations. Observe that $Q_i = V_i \cup W_i$. By symmetry, it is enough to prove that $Q_1 \cap Q_2 \not\subset Q_4$. This is clear by taking into account that $Q_1 \cap Q_2 = \langle \pi_4, \pi_8 \rangle \cup \langle \pi_2, \pi_6 \rangle \cup \langle \pi_1, \pi_5 \rangle \cup \langle \pi_3, \pi_7 \rangle$ and $Q_4 = \langle \pi_1, \pi_2, \pi_3, \pi_8 \rangle \cup \langle \pi_4, \pi_5, \pi_6, \pi_7 \rangle$. □

In order to conclude the proof of Theorem 3, it is enough to prove that the matroids $\mathcal{M}_4, \ldots, \mathcal{M}_9$ are representable. This is done in the next proposition and, even though it is not necessary, we determine for completeness the characteristics of the fields over which those matroids admit a representation.

Proposition 18. *For every $i = 4, \ldots, 7$ and for every prime p the matroid $\mathcal{M}_i$ is $\mathbb{K}$-representable for some finite field $\mathbb{K}$ with characteristic p. The matroid $\mathcal{M}_8$ is $\mathbb{K}$-representable if and only if the characteristic of $\mathbb{K}$ is not equal to 2. Finally, the matroid $\mathcal{M}_9$ is $\mathbb{K}$-representable if and only if the characteristic of $\mathbb{K}$ is equal to 2.*

Proof: Let p be a prime and let us take a prime number q with $q \geq 5$ and $q \neq p$. Let $\mathbb{K}$ be a finite field of characteristic p such that it contains a primitive q-root of unity $\omega \in \mathbb{K}$. Then, the code with generator matrix

$$M_4 = \begin{pmatrix} \omega^3 & 0 & \omega^2 & 0 & \omega^4 & 0 & \omega & 0 \\ 0 & \omega & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & \omega^3 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

is a $\mathbb{K}$-representation of $\mathcal{M}_4$. The matrix

$$M_5 = \begin{pmatrix} ab & 0 & a & 0 & 1 & 0 & 1 & 0 \\ 0 & b & 1 & 0 & 0 & a^{-1} & 1 & 0 \\ 0 & 1 & 0 & a & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

provides a representation of the matroid $\mathcal{M}_5$ if $a, b \neq 0, 1$ and $b \neq a^{-1}$. A representation of the matroid $\mathcal{M}_6$ is given given by the matrix

$$M(a,b) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & a & b & a+b-1 & 0 \end{pmatrix}$$

if $a, b \neq 0, 1$ and $a \neq b$ and $a+b \neq 1$. The code with generator matrix $M(a, 1)$ represents $\mathcal{M}_7$ if $a \neq 0, 1, -1$. Therefore, $\mathcal{M}_5$, $\mathcal{M}_6$ and $\mathcal{M}_7$ are $\mathbb{K}$-representable for every finite field with $|\mathbb{K}| \geq 5$ and, hence, they can be represented over fields of every characteristic. Moreover, the matrix $M(1, 1)$ is a representation of $\mathcal{M}_8$ for every finite field with characteristic different from 2 and it provides a $\mathbb{K}$-representation of the matroid $\mathcal{M}_9$ if $\mathbb{K}$ has characteristic 2. Finally, it is well known that $\mathcal{M}_8$ can not be represented over any field with characteristic 2 while $\mathcal{M}_9$ only can be represented over fields with characteristic 2. See, for instance, the Appendix "Some interesting matroids" in [13], in which $\mathcal{M}_8$ and $\mathcal{M}_9$ appear, respectively, as R_8 and $AG(3, 2)$. □

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

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

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

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

[7] R. 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.

[8] R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, G. Leander, J. Martí-Farré, C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *Advances in Cryptology - CRYPTO 2005, Lecture Notes in Comput. Sci.* **3621** (2005) 327–343. The full version of this paper is available in *Cryptology ePrint Archive*, http://eprint.iacr.org/2004/245.

[9] I.M. Duursma. Combinatorics of the two-variable zeta function. *Finite fields and applications, Lecture Notes in Comput. Sci.* **2948** (2004) 109–136.

[10] C. Greene. Weight enumeration and the geometry of linear codes. *Studies in Appl. Math.* **55** (1976) 119–128.

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

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

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

[14] 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.

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

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

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