

# Error-Set Codes and Related Objects<sup>\*</sup>

An Braeken<sup>1</sup>, Ventzislav Nikov<sup>2</sup>, and Svetla Nikova<sup>1</sup>

<sup>1</sup> Department Electrical Engineering, ESAT/COSIC,  
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,  
B-3001 Heverlee-Leuven, Belgium

`an.braeken,svetla.nikova@kuleuven.ac.be`

<sup>2</sup> Department of Mathematics and Computing Science,  
Eindhoven University of Technology  
P.O. Box 513, 5600 MB, Eindhoven, the Netherlands  
`v.nikov@tue.nl`

**Abstract.** By considering a new metric, Nikov and Nikova defined the class of error-set correcting codes. These codes differ from the error-correcting codes in the sense that the minimum distance of the code is replaced by a collection of monotone decreasing sets  $\Delta$  which define the supports of the vectors that do not belong to the code. In this paper we consider a subclass of these codes - so called, ideal codes - investigating their properties such as the relation with its dual and a formula for the weight enumerator. Next we show that the  $\Delta$ -set of these codes corresponds to the independent sets of a matroid. Consequently, this completes the equivalence of ideal linear secret sharing schemes and matroids on one hand and linear secret sharing schemes and error-set correcting codes on the other hand.

## 1 Introduction

Nikov and Nikova introduced a class of generalized codes, called error-set codes in [9]. These codes were originally defined by the property that the codewords should belong to a monotone increasing set. In this paper, we show that the ideal error-set codes can be represented as  $[N, k, \Delta]$ -code, where  $N$  is the length,  $k$  the corresponding dimension and where the monotone decreasing set  $\Delta$  defines the forbidden supports of the codewords (forbidden distances). Error-set codes have been constructed by means of Monotone Span Programs (MSP) and have been used in order to establish the minimum conditions for security of linear secret sharing schemes (LSSS) and verifiable secret sharing (VSS) schemes.

This paper shows that the set of forbidden distances  $\Delta$  of the ideal error-set codes corresponds to the independent sets of a matroid. From

---

<sup>\*</sup> The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT and by Concerted Research Action GOA Ambiorix 2005/11 of the Flemish Government. An Braeken is research assistant of the FWO

this relation, we derive other properties and insights of the error-set codes. For instance, we show how the corresponding dual error-set code is constructed from a given error-set code. The equivalence between ideal LSSS and matroids was known since 1991 [1]. In 2003 [9], the equivalence between LSSS and the error-set codes has been proven. Consequently, the relation between ideal error-set codes and matroids follows.

The paper is organized as follows. In Sect. 2 we start with the definitions of matroids and the relation between linear codes and matroids. In Sect. 3, we study the properties of ideal error-set codes. In Sect. 4, we recall the relations between ideal LSSS and matroids, LSSS and codes, and show how the relation between matroids and ideal codes completes the equivalence relations. We end with some conclusions in Sect. 5.

## 2 Background

We first explain the definitions and properties of matroids together with a relation between matroids and error-correcting codes.

### 2.1 Matroids

Matroids have been introduced by Whitney [13]. We first recall some basic facts, but refer to [12] for a more comprehensive introduction into the subject. A *matroid*  $\mathcal{M} = (\mathcal{S}, \mathcal{I})$  is a finite set  $\mathcal{S}$  and a collection  $\mathcal{I}$  of subsets of  $\mathcal{S}$  (called the *independent sets*) such that (I1) – (I3) are satisfied:

- (I1)  $\emptyset \in \mathcal{I}$ .
- (I2) If  $X \in \mathcal{I}$  and  $Y \subseteq X$ , then  $Y \in \mathcal{I}$ .
- (I3) If  $U, V \in \mathcal{I}$  with  $|U| = |V| + 1$ , there exists  $x \in U \setminus V$  such that  $V \cup x \in \mathcal{I}$ .

A subset of  $\mathcal{S}$  not belonging to  $\mathcal{I}$  is called *dependent*. The maximal independent subsets of  $\mathcal{S}$  are called the *bases*, while the minimal dependent subsets are called *circuits*. The collection of bases is denoted by  $\mathcal{B}$ , while the collection of circuits is denoted by  $\mathcal{C}$ . A matroid is uniquely defined by  $\mathcal{B}$  or  $\mathcal{C}$ .

The following theorem, known as the augmentation theorem, gives as a consequence that all bases in  $\mathcal{M}$  have the same cardinality.

**Theorem 1.** [12] (*Augmentation Theorem*) *Suppose that  $X, Y \in \mathcal{I}$  and that  $|X| < |Y|$ . Then there exists  $Z \subseteq Y \setminus X$  such that  $|X \cup Z| = |Y|$  and  $X \cup Z \in \mathcal{I}$ .*

If every set of cardinality  $k$  is a base in  $\mathcal{S}$  with  $1 \leq k \leq n$  where  $n$  is the number of elements of  $\mathcal{S}$ , the matroid is said to be *uniform*, denoted by  $\mathcal{M}_{k,n}$ .

A matroid can also be uniquely defined by its *rank function*

$$\rho : 2^{\mathcal{S}} \rightarrow \mathbb{Z} : \rho(A) = \max\{|X| : X \subseteq A, X \in \mathcal{I}\}, \quad \forall A \subseteq \mathcal{S}.$$

The *rank of the matroid*, denoted by  $r(\mathcal{M})$  is the rank of the bases. Consequently, if  $C$  is a circuit then  $\rho(C) = |C| - 1$  and every proper subset of a circuit is independent. If for  $x \in \mathcal{S}$ ,  $A \subseteq \mathcal{S}$ ,  $\rho(A \cup x) = \rho(A)$  it is said that  $x$  *depends* on  $A$  and it is denoted by  $x \sim A$ . With any matroid, one can associate its dual.

**Definition 1.** [12] If  $\mathcal{B} = \{B_i : i \in I\}$  is the set of bases of a matroid  $\mathcal{M}$ . Then the dual matroid  $\mathcal{M}^*$  of a matroid  $\mathcal{M}$  is defined by the set of bases  $\mathcal{B}^* = \{\mathcal{S} \setminus B_i : i \in I\}$ . The corresponding rank function is defined by  $\rho^*(\mathcal{S} \setminus A) = |\mathcal{S}| - \rho(\mathcal{S}) - |A| + \rho(A)$ ,  $\forall A \subseteq \mathcal{S}$ .

The function  $\rho^*$  is called *corank* function of  $\mathcal{M}$ . A *cobase* of  $\mathcal{M}$  is a base of  $\mathcal{M}^*$ , a *cocircuit* of  $\mathcal{M}$  is a circuit of  $\mathcal{M}^*$  and so on.

It is said that a matroid  $\mathcal{M}$  is *connected* or *non-separable* if for every pair of distinct elements  $x$  and  $y$  of  $\mathcal{S}$  there is a circuit of  $\mathcal{M}$  containing  $x$  and  $y$ . Moreover, a matroid  $\mathcal{M}$  is connected if and only if its dual  $\mathcal{M}^*$  is connected. It appears that if a matroid  $\mathcal{M}$  is connected then we do not need to know the full set of circuits of  $\mathcal{M}$  in order to be able to specify the matroid completely.

**Theorem 2.** [12] Let  $\mathcal{M}$  be a connected matroid on  $\mathcal{S}$  and let  $x$  be a fixed element of  $\mathcal{S}$ . The collection of circuits of  $\mathcal{M}$  which contains  $x$  uniquely determines  $\mathcal{M}$ .

The Tutte polynomial of  $\mathcal{M}$  is defined as

$$T(\mathcal{M}, x, y) = \sum_{A \subseteq \mathcal{S}} (x - 1)^{\rho(\mathcal{S}) - \rho(A)} (y - 1)^{|A| - \rho(A)}.$$

The evaluation of this polynomial provides a lot of information about the matroid, e.g., the numbers of bases, the number of independent sets, the number of sets which contain a base, the number of all subsets in  $\mathcal{S}$ . Moreover, by definition we have that  $T(\mathcal{M}, x, y) = T(\mathcal{M}^*, y, x)$ .

A matroid is said to be representable over a field  $\mathbb{F}_q$  if there exists a vector space  $V$  over  $\mathbb{F}_q$  together with a map  $\phi : \mathcal{S} \rightarrow V$  which represents the rank. However, the representability problem for matroids is still not completely solved. See, for instance, [12, Chapter 9] for some results on this problem.

## 2.2 Matroids and Codes

An  $[n, k, d]$  linear code  $\mathbf{C}$  over a finite field  $\mathbb{F}_q$  defines a subspace of dimension  $k$  in  $\mathbb{F}_q^n$ . All codewords have minimum weight  $d$ . The dual code  $\mathbf{C}^\perp$  consists of elements  $\{y : y \cdot x = 0 \text{ for all } x \in \mathbf{C}\}$ . Consequently,  $\mathbf{C}^\perp$  has parameters  $[n, n - k, d^\perp]$ , where  $d^\perp$  is the minimum distance of the code  $\mathbf{C}^\perp$ .

A linear code can be defined by two matrices: the generator matrix and the parity check matrix. The generator matrix  $G$  of an  $[n, k, d]$ -code is a  $k \times n$ -matrix, whose rows form a basis for  $\mathbf{C}$ . The generator matrix  $H$  of  $\mathbf{C}^\perp$  is called the parity check matrix of the code, which is an  $(n - k) \times n$ -matrix. Hence,  $x \in \mathbf{C}$  if and only if  $xH^T = 0$ , (since  $GH^T = 0$ ).

The weight enumerator  $W_{\mathcal{C}}(x, y)$  of the code  $\mathcal{C}$  is the homogeneous polynomial

$$W_{\mathcal{C}}(x, y) = \sum_{c \in \mathcal{C}} x^{n-wt(c)} y^{wt(c)} = \sum_{i=0}^n A_i x^{n-i} y^i,$$

where  $A_i$  represents the number of words of weight  $i$  in  $\mathbf{C}$ .

The connection between the weight enumerator  $W_{\mathcal{C}^\perp}(x, y)$  of the dual code  $\mathcal{C}^\perp$  and the weight enumerator of  $\mathcal{C}$  is as follows:

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathbf{C}|} W_{\mathcal{C}}(x + (q - 1)y, x - y).$$

We refer to [8] for more details on linear codes.

The relation between matroids and linear codes over a given field has been studied in [5]. In short, if  $G$  is the generator matrix of a linear code  $\mathbf{C}$  in  $\mathbb{F}_q^n$ , then the matroid  $\mathcal{M}(\mathbf{C})$  associated with the code  $\mathbf{C}$  is the matroid defined over the set of column indices  $\{1, \dots, n\}$  whose independent sets are the linearly independent columns of  $G$ .

**Theorem 3.** [2,3] *If the matroid  $\mathcal{M}$  corresponds to the code  $\mathbf{C}$ , then the dual matroid  $\mathcal{M}^*$  corresponds to the dual code  $\mathbf{C}^\perp$ .*

**Theorem 4.** [2,3] *Let  $\mathbf{C}$  be a code over a field with  $q$  elements, and  $\mathcal{M}$  is the corresponding matroid. Then*

$$W_{\mathbf{C}}(x, y) = y^{n-\dim(\mathbf{C})} (x - y)^{\dim(\mathbf{C})} T(\mathcal{M}, \frac{x + (q - 1)y}{x - y}, \frac{x}{y}).$$

The analogues of *deletion* and *contraction* of a matroid are the operations of *puncturing* and *shortening* a code.

### 2.3 Secret Sharing Schemes

Define the set of participants in a secret sharing scheme (SSS) by  $\mathcal{P} = \{1, \dots, n\} = \{P_1, \dots, P_n\}$  and denote the power set of  $\mathcal{P}$  by  $P(\mathcal{P})$ . The set  $\Gamma \subseteq P(\mathcal{P})$  is called monotone increasing if for each set  $A$  in  $\Gamma$ , each set containing  $A$  is also in  $\Gamma$ . Similarly, the set  $\Delta \subseteq P(\mathcal{P})$  is called monotone decreasing, if for each set  $B$  in  $\Delta$  each subset of  $B$  is also in  $\Delta$ . A monotone increasing set  $\Gamma$  can be described efficiently by the set  $\Gamma^-$  consisting of the minimal elements (sets) in  $\Gamma$ , i.e., the elements in  $\Gamma$  for which no proper subset is also in  $\Gamma$ . Similarly, the set  $\Delta^+$  consists of the maximal elements (sets) in  $\Delta$ , i.e., the elements in  $\Delta$  for which no proper superset is also in  $\Delta$ .

The tuple  $(\Gamma, \Delta)$  defines an *access structure* on  $\mathcal{P}$  when  $\Gamma \cap \Delta = \emptyset$ . When  $\Delta = P(\mathcal{P}) \setminus \Gamma$  (i.e.  $\Delta = \Gamma^c$ ) then the access structure  $(\Gamma, \Delta)$  is said to be *complete* and is denoted just by  $\Gamma$ . If  $\Delta$  consists of all elements of weight less than  $k$ , we call the access structure threshold and denote it by  $\Gamma_{k,n}$ .

The dual sets  $\Delta^*$  and  $\Gamma^*$  to  $\Gamma$  and  $\Delta$ , respectively, are defined by  $\Gamma^* = \{A : \mathcal{P} \setminus A \in \Delta\}$  and  $\Delta^* = \{A : \mathcal{P} \setminus A \in \Gamma\}$ . The tuple  $(\Gamma^*, \Delta^*)$  (or  $\Gamma^*$  when it is complete) is called the *dual access structure*. It is easy to see that  $\Delta^*$  is monotone decreasing and  $\Gamma^*$  is monotone increasing. For two monotone decreasing sets  $\Delta_1$  and  $\Delta_2$  define  $\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2; A_1 \in \Delta_1, A_2 \in \Delta_2\}$ . Note that  $\Delta_1 \uplus \Delta_2$  is again a monotone decreasing set.

A secret sharing scheme allows the dealer  $P_0$  to share a secret among  $n$  participants in such a way that some sets of participants (those in  $\Gamma$ ), called allowed coalitions, can recover the secret, while any other set of participants (non-allowed coalitions) cannot get any information about the secret. The scheme is called *ideal* if the size of any share coincides with the size of the secret. If the share of any participant is computed by a fixed linear function of the key and some other random elements, the SSS is said to be linear (shortly denoted as LSSS).

An access structure is called *ideal* if there is an ideal SSS realizing it. For an access structure  $(\Gamma, \Delta)$ ,  $core(\Gamma)$  is defined to be the set of players which are in some minimal qualified set, that is,  $core(\Gamma) = \cup_{A \in \Gamma^-} A$ . An access structure  $(\Gamma, \Delta)$  is called *connected* if  $core(\Gamma) = \mathcal{P}$ .

### 3 Error-Set Codes

The linear  $[n, k, d]$ -code over  $\mathbb{F}_q$  can be generalized to the linear  $[N, k, \Delta]$ -code  $\mathbf{C}$  over  $\mathbb{F}_q$ . The  $[N, k, \Delta]$ -code is called an error-set code [9] because

of the property that all vectors for which the support belongs to  $\Delta$  are no codewords. It also implies that if  $x$  is a codeword then  $\text{sup}(x) \notin \Delta$ . The set  $\Delta$  is called the set of forbidden distances and denoted by  $\Delta(\mathbf{C})$ . In its most general definition for the error-set code, the set  $\Delta$  is defined over the set (of sub-vectors formed by a partition)  $\{1, \dots, n+1\}$ . When instead  $\Delta$  is defined over the set (of coordinates)  $\{1, \dots, N\}$  the code is called ideal and thus  $N = n+1$ . It is clear that for  $\Delta = \{A : |A| \leq d-1\}$ , the  $[n+1, k, \Delta]$ -code coincides with the usual definition of  $[n+1, k, d]$ -code. We will consider further only the ideal error-set codes. Let us first derive some new properties of these codes.

**Theorem 5.** *The parity check matrix of an  $[n+1, k, \Delta(\mathbf{C})]$ -code is a matroid defined on the set of column indices  $\mathcal{S} = \{1, \dots, n+1\}$  with independent set  $\mathcal{I} = \Delta(\mathbf{C})$ .*

*Proof.* A vector  $x$  does not belong to the code if and only if  $Hx^T \neq 0$ . This also means that the columns corresponding to the indices defined by  $\text{sup}(x)$  are linearly independent. Recall that by Theorem 1 the columns corresponding to the indices defined by the supports of the vectors from  $\Delta(\mathbf{C})$  define the independent sets of a matroid on  $\mathcal{S}$ .  $\square$

**Theorem 6.** *The dual of an  $[n+1, k, \Delta(\mathbf{C})]$ -code is an  $[n+1, n+1-k, \Delta(\mathbf{C}^\perp)]$ -code with  $\Delta(\mathbf{C}^\perp) = \Delta(\mathbf{C})^*$ .*

*Proof.* By Theorem 3 the dual of a matroid with independent sets defined by  $\Delta(\mathbf{C})$  is the matroid with independent sets defined by  $\Delta(\mathbf{C})^*$ . This matroid defines the parity check matrix of the dual code. By Theorem 5, the dual code cannot have vectors with support belonging to  $\Delta(\mathbf{C}^\perp)$ .  $\square$

**Corollary 1.** *The generator matrix of an  $[n+1, k, \Delta(\mathbf{C})]$ -code is equivalent to a matroid defined on the set  $\mathcal{S} = \{1, \dots, n+1\}$  with an independent set  $\mathcal{I} = \Delta(\mathbf{C})^*$ .*

*Example 1.* Consider the  $[5, 3, \Delta(\mathcal{C})]$ -code with its corresponding dual the  $[5, 2, \Delta(\mathcal{C})^*]$ -code where  $(\Delta(\mathcal{C})^*)^+ = \{\{2, 3, 5\}, \{1, 3, 5\}, \{1, 2, 5\}, \{2, 4, 5\}, \{1, 4, 5\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$  and  $\Delta(\mathcal{C})^+ = \{\{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 3\}, \{2, 3\}, \{3, 5\}, \{2, 5\}, \{1, 5\}\}$ . The generator matrix  $G$  and parity check matrix  $H$  of the code are given by:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

The linearly independent sets of columns in  $H$  correspond to the elements of  $\Delta(\mathbf{C})$ , while the linearly independent sets of columns in  $G$  correspond to the elements of  $\Delta(\mathbf{C})^*$ .

Another way for determining codes and matroids for a given generator matrix  $G$  is given in the following two theorems.

**Theorem 7.** *Set  $A$  belongs to  $\Delta(\mathbf{C})^+$  if and only if the matrix  $G$  of an  $[n+1, k, \Delta(\mathbf{C})]$ -code obtained by removing the columns corresponding to  $A$  has rank  $k$ .*

**Theorem 8.** *Set  $A$  belongs to  $\Delta(\mathbf{C}^\perp)^+$  if and only if the columns of the generator matrix  $G$  of an  $[n+1, k, \Delta(\mathbf{C})]$ -code corresponding to  $A$  are linearly independent.*

**Theorem 9.** *Consider the  $[n+1, k, \Delta(\mathbf{C})]$ -code  $\mathcal{C}$  and the corresponding dual  $[n+1, n+1-k, \Delta(\mathbf{C}^\perp)]$ -code  $\mathcal{C}^\perp$ . The elements of  $\Delta(\mathbf{C})^+$  have size  $(n+1-k)$  and the elements of  $\Delta(\mathbf{C}^\perp)$  have size  $k$ .*

*Proof.* The size of the elements of  $\Delta(\mathbf{C})^+$  (resp.  $\Delta(\mathbf{C}^\perp)^+$ ) follows from the rank of matrix  $H$  (resp.  $G$ ).  $\square$

By Corollary 1 and by Theorem 4 we can derive the weight enumerator of an  $[n+1, k, \Delta(\mathbf{C})]$ -code.

**Theorem 10.** [5] *Let  $\mathcal{C}$  be an  $[n+1, k, \Delta(\mathbf{C})]$ -code and  $\mathcal{M}$  be the matroid with independent sets defined by  $\Delta(\mathbf{C})^*$ . Then*

$$W_{\mathcal{C}}(x, y) = y^{n+1-r(\mathcal{M})}(x-y)^{r(\mathcal{M})}T(M; \frac{x+(q-1)y}{x-y}, \frac{x}{y}). \quad (1)$$

## 4 Relations between Matroids, Codes and LSSS

The following equivalence relations between matroids and ideal LSSS on one hand and LSSS and error-set codes on the other hand are known. First we briefly recall these equivalences and using the results from the previous section we close the chain of relations by establishing directly the equivalence between ideal error-set codes and matroids.

### 4.1 LSSS and Matroids

Brickell and Davenport were the first to point out the relation between ideal LSSS and matroids over the set  $S = \{0, 1, \dots, n\} = \{P_0\} \cup \mathcal{P}$ .

**Definition 2.** [1] Let  $M$  be an ideal SSS, The  $\Delta$ -set of such a scheme is

$$D(M) = \{A \subseteq \mathcal{P} : \exists y \in A \text{ such that } y \sim A \setminus y\}.$$

**Theorem 11.** [1,6,4] Let  $\Gamma$  be an ideal connected access structure on  $\mathcal{P}$  with  $\Gamma^- = \{C_i, i \in I\}$ . Then the sets  $\{P_0\} \cup C_i, i \in I$  are all circuits through  $P_0$  of a unique matroid (by Theorem 2) defined on  $\mathcal{S} = \{P_0\} \cup \mathcal{P}$ . This matroid is called to be induced by  $\Gamma$ , and denoted by  $\mathcal{M}(\Gamma)$ . The sets  $D(M)$  are the dependent sets of the connected matroid.

**Theorem 12.** [11] Let  $\Gamma$  be an ideal access structure for the ideal SSS  $M$ . The sets  $X \in \Gamma^-$  and sets  $(X \setminus \{P_i\}) \cup \{P_0\}$  for  $P_i \in X, X \in \Gamma^-$  form the bases of a representable matroid  $\mathcal{M}(\Gamma)$  if and only if  $\Gamma$  and  $M$  satisfy the requirement  $X \in \Gamma^- \Leftrightarrow$  rows of  $M_X$  are independent.

The opposite relation is also true.

**Theorem 13.** [1] Let  $\mathcal{M} = (\mathcal{S}, \mathcal{I})$  be a connected representable matroid and let  $P_0 \in \mathcal{S}$ . Then there exists a connected ideal SSS  $M$  on  $\mathcal{P} = \mathcal{S} \setminus \{P_0\}$  with a dealer  $P_0$  and a target vector  $\varepsilon$  and such that  $D(M) = \mathcal{I}$ .

A relation between the dual access structures and matroids also holds.

**Theorem 14.** [6,4] Let  $\Gamma$  be a connected ideal access structure that induces a matroid  $\mathcal{M}(\Gamma)$ . Then  $\Gamma^*$  induces a matroid  $\mathcal{M}(\Gamma^*)$  and

$$\mathcal{M}(\Gamma)^* = \mathcal{M}(\Gamma^*).$$

**Theorem 15.** [6,4] Let  $\Gamma$  be an ideal access structure that induces a matroid  $\mathcal{M}(\Gamma)$ . Then  $\Gamma$  is connected if and only if  $\mathcal{M}(\Gamma)$  is connected.

## 4.2 LSSS and Codes

The connection between LSSS and error-set codes is made using the concept of MSP.

**Definition 3.** [7] A Monotone Span Program (MSP)  $\mathcal{M}$  is defined by the quadruple  $(\mathbb{F}, M, \varepsilon, \psi)$ , where  $\mathbb{F}$  is a finite field,  $M$  is a matrix (with  $m$  rows and  $d \leq m$  columns) over  $\mathbb{F}$ ,  $\psi : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$  is a surjective functions and  $\varepsilon = (1, 0, \dots, 0)$  is a fixed non-zero vector, called target vector. The function  $\psi$  labels each row with a number  $i$  that corresponds to player  $P_{\psi(i)}$ . The size of  $\mathcal{M}$  is the number of rows and is denoted as  $\text{size}(\mathcal{M})$ .

Let  $M$  be an  $m \times d$  matrix and let  $M_A$  be the matrix consisting of the rows owned by  $A$ . An MSP is said to compute the access structure  $\Gamma$  when  $\varepsilon \in M_A^T$  if and only if  $A \in \Gamma$ . Or equivalently

$$\begin{aligned} A \in \Gamma &\Leftrightarrow \exists \lambda \in \mathbb{F}^{|A|} \text{ such that } M_A^T \lambda = \varepsilon \\ B \notin \Gamma &\Leftrightarrow \exists k \in \mathbb{F}^d \text{ such that } M_B k = 0 \text{ and } k_1 = 1. \end{aligned}$$

The MSP which computes  $\Gamma^*$  is called the dual MSP  $\mathcal{M}^*$  with corresponding matrix  $M^*$ . A relation between dual access structures and dual codes has been established as follows.

**Theorem 16.** [10] *Let  $\mathcal{M}$  be an MSP program computing  $\Gamma$ , and  $\mathcal{M}^\perp$  be an MSP computing the dual access structure  $\Gamma^\perp$ . Let code  $\mathcal{C}^\perp$  have the parity check matrix  $H^\perp = (\varepsilon \mid (M^\perp)^T)$  and let code  $\mathcal{C}$  have the parity check matrix  $H = (\varepsilon \mid M^T)$ . Then for any MSP  $\mathcal{M}$  there exists an MSP  $\mathcal{M}^\perp$ , such that  $\mathcal{C}$  and  $\mathcal{C}^\perp$  are dual.*

For expressing the relations between LSSS and error-set codes, we need to work with a particular type of MSP.

**Definition 4.** [10] *An MSP  $\mathcal{M} = (\mathbb{F}, M, \varepsilon, \psi)$  is called a  $\Delta$ -non-redundant monotone span program (denoted by  $\Delta$ -rMSP), if  $\ker(M_A^T) = \{0\}$  holds for any  $A \in \Delta$ .*

**Theorem 17.** [9] *Consider the  $\Delta$ -rMSP  $\mathcal{M}$ . Let  $\mathbf{C}$  be an error-set correcting code with a generator matrix  $G$  of the form  $G = (\varepsilon \mid M^T)$ . Then  $\mathbf{C}$  defines an LSSS with the set of forbidden distances  $\Delta(\mathbf{C})$  equal to  $\Delta^\perp \uplus \{\emptyset, \{P_0\}\}$ .*

### 4.3 Codes and Matroids

For the threshold case, all relations are well known: every threshold access structure  $\Gamma_{k,n}$  realized by an SSS over  $\mathbb{F}_q$  has an associate uniform matroid  $\mathcal{M}_{k,n+1}$  and corresponds to an MDS  $[n+1, k, n-k+2]$ -code. Thus  $\mathcal{M}_{k,n+1} = \mathcal{M}(\Gamma_{k,n}) = \mathcal{M}([n+1, k, n-k+2])$  hold. It seems that similar relations hold for general access structures.

Let us analyze the equivalence between Theorem 12 and Theorem 17 for the ideal case. The definition of  $\Delta$ -rMSP corresponds to the property that  $X \in \Gamma^-$  if and only if the rows of  $M_X$  are linearly independent. Furthermore, Theorem 5 where the relation between matroids and error-set codes is expressed, shows the equivalence between the assumptions of both theorems.

For a relation between the connected LSSS and the error-set codes, it is clear by Theorem 5 that the only extra requirement in Theorem 17 will be that the set  $\Delta(\mathbf{C})$  satisfies the properties of a connected matroid. Moreover, the equivalence between Theorem 14 and Theorem 16 follows from Theorem 17.

## 5 Conclusion

We continued the study of combinatorial objects defined in a setting where the set of positions in which two vectors differ is used as a metric and the support of a vector as a norm. More precisely, we have shown the relation between the  $[N, k, \Delta]$ -error-set codes and the matroids.

## References

1. E. Brickell and D. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, (4):123–134, 1991.
2. P. Cameron. Polynomial aspects of codes, matroids and permutation groups, 2002. Lecture Notes.
3. P. Cameron. Codes, matroids and trelises, 2004. Preprint.
4. M.van Dijk, W.-A. Jackson, and K. Martin. A note on duality in linear secret sharing scheme. *Bulletin of the Institute of Combinatorics and its Application*, 19:93–101, 1997.
5. C. Greene. Weight enumerator and the geometry of linear codes. *Studies in Applied Mathematics*, 55:119–128, 1976.
6. W.-A. Jackson and K. Martin. Geometric secret sharing schemes and their duals. *Designs Codes and Cryptography*, 4:83–95, 1994.
7. M. Karchmer and A. Wigderson. On span programs. *Proceedings of 8-th Annual Structure in Complexity Theory Conference*, pages 102–111, 1993.
8. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier Science Publisher, 1991. ISBN 0-444-85193-3.
9. V. Nikov and S. Nikova. On a relation between verifiable secret sharing schemes and a class of error-correcting codes. Cryptology ePrint Archive, Report 2003/210, 2003. <http://eprint.iacr.org/2003/210>.
10. V. Nikov, S. Nikova, and B. Preneel. On the size of monotone span programs. In *2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 252–265. C. Blundo, and S. Cimato, editors, Springer, 2004.
11. T. Uehara, T. Nishizeki, T. Okamoto, and K. Nakamura. A secret sharing system with matroid access structure. *Tran. IECE Japan*, 69.
12. D. Welsh. *Matroid Theory*. Academic Press, London, 1976.
13. H. Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57:509–533, 1935.