Math.Comput.Sci. (2018) 12:339–347
https://doi.org/10.1007/s11786-018-0349-1

Mathematics in Computer Science

On the Weak Order Ideal Associated to Linear Codes

Mijail Borges-Quintana ·
Miguel Ángel Borges-Trenard ·
Edgar Martínez-Moro

Received: 30 May 2017 / Revised: 16 April 2018 / Accepted: 19 April 2018 / Published online: 19 June 2018

Abstract In this work we study a weak order ideal associated with the coset leaders of a non-binary linear code. This set allows the incrementally computation of the coset leaders and the definitions of the set of leader codewords. This set of codewords has some nice properties related to the monotonicity of the weight compatible order on the generalized support of a vector in $\mathbb{F}_q^n$ which allows to describe a test set, a trial set and the set of zero neighbours of a linear code in terms of the leader codewords.

Keywords Linear codes · Order ideals · Test set · Trial set · Zero neighbours · Correctable errors

Mathematics Subject Classification Primary 94B05; Secondary 13P10

1 Introduction

As it is pointed in [5] it is common folklore in the theory of binary linear codes that there is an ordering on the coset leaders chosen as the lexicographically smallest minimum weight vectors that provides a monotone structure. This is expressed as follows: if $\mathbf{x}$ is a coset leader and $\mathbf{y} \subseteq \mathbf{x}$ (i.e. $y_i \leq x_i$ for all i) then $\mathbf{y}$ is also a coset leader. This nice property has been proved of great value, see for example [10], and it has been used for analyzing the error-correction capability of binary linear codes [5]. In this last paper the authors introduce the concept of a *trial set* of codewords and they provide a gradient-like decoding algorithm based on this set.

Mijail Borges-Quintana has been partially supported by a post-doctorate scholarship at the University of Valladolid (09-2014 to 02-2015) by Erasmus Mundus Program, Mundus Lindo Project.
Edgar Martínez-Moro has been partially supported by the Spanish MINECO under Grants MTM2015-65764-C3-1-P and MTM2015-69138-REDT.

M. Borges-Quintana (✉) · M. Á. Borges-Trenard
Department of Mathematics, Faculty of Ciencias Naturales y Exactas, University of Oriente, Santiago de Cuba, Cuba
e-mail: mijail@uo.edu.cu

M. Á. Borges-Trenard
e-mail: mborges@uo.edu.cu

E. Martínez-Moro
Institute of Mathematics IMUVa, University of Valladolid, Valladolid, Castilla, Spain
e-mail: edgar.martinez@uva.es

Finding the weight distribution of coset leaders for a code $\mathcal{C}$ is a classic problem in coding theory. This problem is still unsolved for many families of linear codes even for first-order Reed–Muller codes (see [7]). The set of coset leaders is also related with the minimum distance decoding and bounded distance decoding problems as well with the set of minimal support codewords [1,8,9]. Despite their interest no generalization of these ideas is known by the authors of this communication to non-binary case. In this paper we provide such a (non straightforward) generalization.

The outline of the paper is as follows, Sect. 2 introduces the idea of a generalized support of a vector. In Sect. 3 is defined the weak order ideal associated with the coset leaders $\mathcal{O}(\mathcal{C})$ and it is shown that can be computed incrementally. Theorem 3.6 establishes that all the coset leaders of the code belong to $\mathcal{O}(\mathcal{C})$. Section 3.2 is devoted to the study of the set of leader codewords of a code as a zero neighbour set and their properties. In Sect. 4 we analyze the correctable and uncorrectable errors and we obtain a trial set for a linear code from the set of leader codewords. Finally, in Sect. 5 we show an example.

The limitation from a practical point view of the results and properties studied in this paper are clear because of the size and the complexity of computing the set of coset leaders. Anyway our main interest is the study and characterizations of some objects related to the codes like zero neighbours, trial set, and the set of correctable and uncorrectable errors.

2 Preliminaries

From now on we shall denote by $\mathbb{F}_q$ the finite field with with $q = p^m$ elements, p a prime. A *linear code* $\mathcal{C}$ over $\mathbb{F}_q$ of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_q^n$. We will call the vectors $\mathbf{v}$ in $\mathbb{F}_q^n$ words and those $\mathbf{v} \in \mathcal{C}$, codewords. For every word $\mathbf{v} \in \mathbb{F}_q^n$ its *support* is defined as $\mathrm{supp}(\mathbf{v}) = \{i \mid v_i \neq 0\}$ and its *Hamming weight*, denoted by $\mathrm{w_H}(\mathbf{v})$ as the cardinality of $\mathrm{supp}(\mathbf{v})$ and the *Hamming distance* $\mathrm{d_H}(\mathbf{x}, \mathbf{y})$ between two words $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_q^n$ is $\mathrm{d_H}(\mathbf{x}, \mathbf{y}) = \mathrm{w_H}(\mathbf{x} - \mathbf{y})$. The *minimum distance* $\mathrm{d}(\mathcal{C})$ of a linear code $\mathcal{C}$ is defined as the minimum weight among all nonzero codewords.

The words of minimal Hamming weight in the cosets of $\mathbb{F}_q^n/\mathcal{C}$ is the *set of coset leaders* of the code $\mathcal{C}$ in $\mathbb{F}_q^n$ and we will denote it by $\mathrm{CL}(\mathcal{C})$. $\mathrm{CL}(\mathbf{y})$ will denote the subset of coset leaders corresponding to the coset $\mathbf{y} + \mathcal{C}$. Given a coset $\mathbf{y} + \mathcal{C}$ we define the *weight of the coset* $\mathrm{w_H}(\mathbf{y} + \mathcal{C})$ as the smallest Hamming weight among all vectors in the coset, or equivalently the weight of one of its leaders. It is well known that given $t = \lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ where $\lfloor \cdot \rfloor$ denotes the greatest integer function then every coset of weight at most t has a unique coset leader.

Let $f(X)$ be an irreducible polynomial over $\mathbb{F}_p$ of degree m and β be a root of $f(X)$, then any element $a \in \mathbb{F}_q$ can be represented as $a_1 + a_2\beta + \cdots + a_m\beta^{m-1}$ with $a_i \in \mathbb{F}_p$ for $i \in \{1, \ldots, m\}$. For a word $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in \mathbb{F}_q^n$, such that the i-th component of $\mathbf{v}$ is $\mathbf{v}_i = v_{i_1} + v_{i_2}\beta + \cdots + v_{i_m}\beta^{m-1}$, then we introduce the following definition

Definition 2.1 We define the *generalized support* of a vector $\mathbf{v}$ as the support of the nm-tuple given by the concatenations of the p-adic expansion of each component $\mathbf{v}_i$ of $\mathbf{v}$, i.e.

$$\mathrm{supp}_{\mathrm{gen}}(\mathbf{v}) = \left(\mathrm{supp}\left((v_{i_1}, \ldots, v_{i_m})\right) : i = 1 \ldots n\right),$$

and $\mathrm{supp}_{\mathrm{gen}}(\mathbf{v})[i] = \mathrm{supp}((v_{i_1}, \ldots, v_{i_m}))$. We will say that $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{v})$ if the corresponding v_{i_j} is not zero.

From now on the set

$$\left\{\mathbf{e}_{ij} = \beta^{j-1}\mathbf{e}_i : i = 1, \ldots, n;\ j = 1, \ldots m\right\}$$

will be denoted as $\mathrm{Can}(\mathbb{F}_q, f)$ and it represents the canonical basis of $(\mathbb{F}_q^n, +)$, the additive monoid $\mathbb{F}_q^n$ with respect to the "+" operation, where f is the irreducible polynomial used to define $\mathbb{F}_q$.

We state the following connection between $\mathbb{F}_q^n$ and $\mathbb{N}^{nm}$:

$$\Delta : \mathbb{F}_q^n \to \mathbb{N}^{nm}$$
$$\mathbf{v} \mapsto \left(\psi\left(v_{i_j}\right) : i = 1, \ldots, n,\ j = 1, \ldots, m\right), \text{ where}$$
$$\psi : \mathbb{F}_p \to \mathbb{N}$$
$$k \cdot 1_{\mathbb{F}_p} \mapsto k \bmod p.$$

On the other hand,

$$\nabla : \mathbb{N}^{nm} \to \mathbb{F}_q^n$$
$$\mathbf{a} \mapsto \left(\left(a_{m(i-1)+1} + a_{m(i-1)+2}\beta + \cdots + a_{m(i-1)+m}\beta^{m-1}\right) : i = 1, \ldots, n\right).$$

Definition 2.2 Given $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_q^n, +)$, $\mathbf{x} = \sum_{i,j} x_{i_j}\mathbf{e}_{ij}$, $\mathbf{y} = \sum_{i,j} y_{i_j}\mathbf{e}_{ij}$, we say $\mathbf{x} \subset \mathbf{y}$ if $\psi(x_{i_j}) \leq \psi(y_{i_j})$ for all $i \in [1, n]$, and $j \in [1, m]$.

By using Δ it is possible to relate orders on $\mathbb{F}_q^n$ with orders on $\mathbb{N}^{nm}$, and vice versa. An *admissible order* on $(\mathbb{N}^{nm}, +)$ is a total order $<$ on $\mathbb{N}^{nm}$ satisfying the following two conditions

1. $\mathbf{0} < \mathbf{x}$, for all $\mathbf{x} \in \mathbb{N}^{nm}$, $\mathbf{x} \neq \mathbf{0}$.
2. If $\mathbf{x} < \mathbf{y}$, then $\mathbf{x} + \mathbf{z} < \mathbf{y} + \mathbf{z}$, for all $\mathbf{z} \in \mathbb{N}^{nm}$.

In particular, Any admissible order on $(\mathbb{N}^{nm}, +)$, like the lexicographical, degree lexicographical, degree reverse lexicographical orders, induces an order on $(\mathbb{F}_q^n, +)$.

We will say that a representation of a word $\mathbf{v}$ as an nm-tuple over $\mathbb{N}$ is in *standard form* if $\Delta(\nabla(\mathbf{v})) = \mathbf{v}$. We will denote the standard form of $\mathbf{v}$ as $\mathrm{SF}(\mathbf{v}, f)$ (note that $\nabla(\mathbf{v}) = \nabla(\mathrm{SF}(\mathbf{v}, f))$). Therefore, $\mathbf{v}$ is in standard form if $\mathbf{v} = \mathrm{SF}(\mathbf{v}, f)$ (we will also say $\mathbf{v} \in \mathrm{SF}(\mathbb{F}_q^n, f)$).

Remark 2.3 From now on we will use $\mathrm{Can}(\mathbb{F}_q)$ and $\mathrm{SF}(\mathbb{F}_q^n)$ instead of $\mathrm{Can}(\mathbb{F}_q, f)$ and $\mathrm{SF}(\mathbb{F}_q^n, f)$ respectively, since it is clear that different elections of f or β provide equivalent generalized supports.

Definition 2.4 A subset $\mathcal{O}$ of $\mathbb{N}^k$ is an order ideal if for all $\mathbf{w} \in \mathcal{O}$ and $\mathbf{v} \in \mathbb{N}^k$ s.t. $\mathbf{v}_i \leq \mathbf{w}_i$, $i = 1, \ldots, k$, then $\mathbf{v} \in \mathcal{O}$.

In the same fashion we say that a subset $\mathcal{S}$ of $\mathbb{F}_q^n$ is an order ideal if $\Delta(\mathcal{S})$ is an order ideal in $\mathbb{N}^{nm}$. It is easy to check that an equivalent definition for the order ideal would be that for all $\mathbf{w} \in \mathcal{S}$, and for all $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$, and $\mathbf{v} \in \mathbb{F}_q^n$ s.t. $\mathbf{w} = \mathbf{v} + \mathbf{e}_{ij}$ we have $\mathbf{v} \in \mathcal{S}$. If instead of for all $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$ the condition is satisfied at least for one $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$ we say that $\mathcal{S}$ is a *weak order ideal*.

Definition 2.5 A subset $\mathcal{S}$ of $\mathbb{F}_q^n$ is a weak order ideal if for all $\mathbf{w} \in \mathcal{S}\backslash\mathbf{0}$ there exists $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$ s.t. for $\mathbf{v} \in \mathbb{F}_q^n$ s.t. $\mathbf{w} = \mathbf{v} + \mathbf{e}_{ij}$ then $\mathbf{v} \in \mathcal{S}$.

Definition 2.6 The *Voronoi region* of a codeword $\mathbf{c} \in \mathcal{C}$ is the set

$$\mathrm{D}(\mathbf{c}) = \left\{\mathbf{y} \in \mathbb{F}_q^n \mid \mathrm{d_H}(\mathbf{y}, \mathbf{c}) \leq \mathrm{d_H}\left(\mathbf{y}, \mathbf{c}'\right),\ \forall \mathbf{c}' \in \mathcal{C}\backslash\{\mathbf{c}\}\right\}.$$

The set of all the Voronoi regions for a given linear code $\mathcal{C}$ covers the space $\mathbb{F}_q^n$ and $\mathrm{D}(\mathbf{0}) = \mathrm{CL}(\mathcal{C})$. However, some words in $\mathbb{F}_q^n$ may be contained in several regions. For any subset $A \subset \mathbb{F}_q^n$ we define

$$\mathcal{X}(A) = \left\{\mathbf{y} \in \mathbb{F}_q^n \mid \min\left\{\mathrm{d_H}\left(\mathbf{y}, \mathbf{a}\right) : \mathbf{a} \in A\right\} = 1\right\}$$

as the set of words at Hamming distance 1 from A. The *boundary* of A is defined as $\delta(A) = \mathcal{X}(A) \cup \mathcal{X}(\mathbb{F}_q^n\backslash A)$.

Definition 2.7 A nonzero codeword $\mathbf{z} \in \mathcal{C}$ is called a *zero neighbour* if its Voronoi region shares a common boundary with the set of coset leaders, i.e. $\delta(\mathrm{D}(\mathbf{z})) \cap \delta(\mathrm{D}(\mathbf{0})) \neq \emptyset$. The set of all zero neighbours of $\mathcal{C}$ is denoted by $\mathcal{Z}(\mathcal{C}) = \{\mathbf{z} \in \mathcal{C}\backslash\{\mathbf{0}\} \ :\ \delta(\mathrm{D}(\mathbf{z})) \cap \delta(\mathrm{D}(\mathbf{0})) \neq \emptyset\}$.

Definition 2.8 A *test-set* $\mathcal{T}$ for a given linear code $\mathcal{C}$ is a set of codewords such that every word $\mathbf{y}$

1. either $\mathbf{y}$ lies in $\mathrm{D}(\mathbf{0})$
2. or there exists $\mathbf{v} \in \mathcal{T}$ such that $\mathrm{w_H}(\mathbf{y} - \mathbf{v}) < \mathrm{w_H}(\mathbf{y})$.

The set of zero neighbours is a test set, also from the set of zero neighbours can be obtained any minimal test set according to the cardinality of the set [1].

3 The Weak Order Ideal of the Coset Leaders

The first idea that allows us to compute incrementally the set of all coset leaders for a linear code was introduced in [2]. In that paper we used the additive structure of $\mathbb{F}_q^n$ with the set of canonical generators $\mathrm{Can}(\mathbb{F}_q)$. Unfortunately in [2] most of the chosen coset representatives may not be coset leaders if the weight of the coset is greater than t.

Theorem 3.1 ([6], Theorem 1.12.6.v) *Assume that* $\mathbf{x}$ *is a coset leader of* $\mathcal{C}$. *If* $\mathbf{x}' \in \mathbb{F}_q^n$ *and* $\mathbf{x}'_i = \mathbf{x}_i$ *for all* $i \in \mathrm{supp}(\mathbf{x}')$, *then* $\mathbf{x}'$ *is also a coset leader of* $\mathcal{C}$.

In order to incrementally generate all coset leaders starting from $\mathbf{0}$ adding elements in $\mathrm{Can}(\mathbb{F}_q)$, we must consider words with weight one more than the previous chosen coset leader. Next result is a byproduct of Theorem 3.1, we may characterize which vectors we need to generate with weight one more than its coset leader in order to ensure all coset leaders are generated.

Theorem 3.2 *Let* $\mathbf{x} \in \mathrm{SF}(\mathbb{F}_q^n)$ *be an element in* $\mathrm{CL}(\mathcal{C})$, *let* $i \in \mathrm{supp}(\mathbf{x})$. *If* $\mathbf{x}' \in \mathbb{F}_q^n$ *and* $\mathbf{x}'_j = \mathbf{x}_j$ *for all* $j \in \mathrm{supp}(\mathbf{x})\backslash\{i\}$, *then* $\mathrm{w_H}(\mathbf{x}') \leq \mathrm{w_H}(\mathbf{x}' + \mathcal{C}) + 1$.

Proof By Theorem 3.1, $\mathbf{x} - \mathbf{x}_i \in \mathrm{CL}(\mathcal{C})$. The proof of the Theorem is analogous to the proof of Theorem 1.12.6.v in [6]. Note that if we suppose that $\mathrm{w_H}(\mathbf{x}') \geq \mathrm{w_H}(\mathbf{x}' + \mathcal{C}) + 2$ it would imply that $\mathbf{x}$ is not a coset leader, which is a contradiction. □

Let $\mathbf{w} \in \mathrm{SF}(\mathbb{F}_q^n)$ be an element in $\mathrm{CL}(\mathcal{C})$, and $i_j \in \mathrm{supp_{gen}}(\mathbf{w})$. Let $\mathbf{y} \in \mathrm{SF}(\mathbb{F}_q^n)$ s.t. $\mathbf{w} = \mathbf{y} + \mathbf{e}_{ij}$ then, as a consequence of the previous theorem we have that

$$\mathrm{w_H}(\mathbf{y}) \leq \mathrm{w_H}(\mathbf{y} + \mathcal{C}) + 1. \tag{3.1}$$

In the situation above we will say that the coset leader $\mathbf{w}$ is an *ancestor* of the word $\mathbf{y}$, and that $\mathbf{y}$ is a *descendant* of $\mathbf{w}$. In the binary case this definitions behave as the ones in [6, §11.7] but in the case $q \neq 2$ there is a subtle difference, a coset leader could be an ancestor of another coset leader or an ancestor of a word at Hamming distance 1 to a coset leader (this last case is not possible in the binary case).

3.1 The set $\mathcal{O}(\mathcal{C})$

Given $\prec_1$ an admissible order on $(\mathbb{N}^{nm}, +)$ we define the *weight compatible order* $\prec$ on $(\mathbb{F}_q^n, +)$ associated to $\prec_1$ as the ordering given by

1. $\mathbf{x} \prec \mathbf{y}$ if $\mathrm{w_H}(\mathbf{x}) < \mathrm{w_H}(\mathbf{y})$ or
2. if $\mathrm{w_H}(\mathbf{x}) = \mathrm{w_H}(\mathbf{y})$ then $\Delta(\mathbf{x}) \prec_1 \Delta(\mathbf{y})$.

I.e. the words are ordered according their weights and the order $\prec_1$ break ties. These class of orders is a subset of the class of monotone α-orderings in [5]. In fact we will need a little more than monotonicity, for the purpose of this work we will also need that for every pair $\mathbf{v}, \mathbf{w} \in \mathrm{SF}(\mathbb{F}_q^n)$

$$\text{if } \mathbf{v} \subset \mathbf{w}, \text{ then } \mathbf{v} \prec \mathbf{w}. \tag{3.2}$$

Note that (3.2) is satisfied for a weight compatible order. In addition, for any weight compatible order $\prec$ every strictly decreasing sequence terminates (due to the finiteness of the set $\mathbb{F}_q^n$). In the binary case the behavior of the coset leaders can be translated to the fact that the set of coset leader is an order ideal of $\mathbb{F}_2^n$; whereas, for non binary linear codes this is no longer true even if we try to use the characterization of order ideals given in [4], where order ideals do not need to be associated with admissible orders.

Definition 3.3 We define *the weak order ideal of the coset leaders* of $\mathcal{C}$ as the set $\mathcal{O}(\mathcal{C})$ of elements in $\mathbb{F}_q^n$ verifying one of the following items:

1. $\mathbf{0} \in \mathcal{O}(\mathcal{C})$.
2. If $\mathbf{v} \in \mathcal{O}(\mathcal{C})$ and $\mathrm{w}_H(\mathbf{v}) = \mathrm{w}_H(\mathbf{v}+\mathcal{C})$ then
$$\left\{\mathbf{v}+\mathbf{e}_{ij} \mid \Delta(\mathbf{v}) + \Delta\left(\mathbf{e}_{ij}\right) \in \mathrm{SF}\left(\mathbb{F}_q^n\right)\right\} \subset \mathcal{O}(\mathcal{C}).$$
3. If $\mathbf{v} \in \mathcal{O}(\mathcal{C})$ and $\mathrm{w}_H(\mathbf{v}) = \mathrm{w}_H(\mathbf{v}+\mathcal{C}) + 1$ then
$$\left\{\mathbf{v}+\mathbf{e}_{ij} \mid i \in \mathrm{supp}(\mathbf{v}),\ \Delta(\mathbf{v}) + \Delta\left(\mathbf{e}_{ij}\right) \in \mathrm{SF}\left(\mathbb{F}_q^n\right),\ \mathbf{v}-\mathbf{v}_i \in \mathrm{CL}(\mathcal{C})\right\} \subset \mathcal{O}(\mathcal{C}).$$

Remark 3.4 It is clear by the items 2 and 3 of the definition above that $\mathcal{O}(\mathcal{C})$ is a weak order ideal.

Theorem 3.5 *Let* $\mathbf{w} \in \mathbb{F}_q^n$. *If there exists* $i \in 1, \ldots, n$ *s.t.* $\mathbf{w} - \mathbf{w}_i \in \mathrm{CL}(\mathcal{C})$ *then* $\mathbf{w} \in \mathcal{O}(\mathcal{C})$.

Proof We will proceed by induction on $\mathbb{F}_q^n$ with respect to the order $\prec$. The statement is true for $\mathbf{0} \in \mathbb{F}_q^n$. Now for the inductive step, we assume that the desired property is true for any word $\mathbf{u} \in \mathbb{F}_q^n$ such that there exists $i \in 1, \ldots, n$ s.t. $\mathbf{u} - \mathbf{u}_i \in \mathrm{CL}(\mathcal{C})$ and also $\mathbf{u}$ is smaller than an arbitrary but fixed $\mathbf{w} \neq \mathbf{0}$ with respect to $\prec$ and $\mathbf{w} - \mathbf{w}_j \in \mathrm{CL}(\mathcal{C})$, for some $j \in 1, \ldots, n$. If $\mathbf{u} - \mathbf{u}_i \in \mathrm{CL}(\mathcal{C})$, for some $i \in 1, \ldots, n$, and $\mathbf{u} \prec \mathbf{w}$ then $\mathbf{u} \in \mathcal{O}(\mathcal{C})$. We will show that the previous conditions imply that $\mathbf{w}$ is also in $\mathcal{O}(\mathcal{C})$.

Let $\mathbf{w} = \mathbf{v} + \mathbf{e}_{ij}$, with $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$ then $\mathbf{v} \prec \mathbf{w}$ by (3.2). As $\mathbf{w} - \mathbf{w}_i \in \mathrm{CL}(\mathcal{C})$, the same is true for $\mathbf{v}$, i.e, $\mathbf{v} - \mathbf{v}_i \in \mathrm{CL}(\mathcal{C})$ then by the induction hypothesis we have that $\mathbf{v} \in \mathcal{O}(\mathcal{C})$. By Theorem 3.2, $\mathrm{w_H}(\mathbf{v}) \leq \mathrm{w_H}(\mathbf{v}+\mathcal{C})+1$; therefore, by items 2 and 3 in Definition 3.3 it is guaranteed that $\mathbf{w} \in \mathcal{O}(\mathcal{C})$. □

Theorem 3.6 *Let* $\mathbf{w} \in \mathbb{F}_q^n$ *and* $\mathbf{w} \in \mathrm{CL}(\mathcal{C})$ *then* $\mathbf{w} \in \mathcal{O}(\mathcal{C})$.

Proof Let $i_j \in \mathrm{supp}_{\mathrm{gen}}(\mathbf{w})$, since $\mathbf{w} \in \mathrm{CL}(\mathcal{C})$, by Theorem 3.2, $\mathbf{w} - \mathbf{w}_i \in \mathrm{CL}(\mathcal{C})$; then, by Theorem 3.5, $\mathbf{w} \in \mathcal{O}(\mathcal{C})$. □

The previous theorem has been shown that $\mathcal{O}(\mathcal{C})$ contains the set of coset leaders of the linear code $\mathcal{C}$.

3.2 Zero Neighbours and Leader Codewords

Definition 3.7 The set of *leader codewords* of a linear code $\mathcal{C}$ is defined as

$$\mathrm{L}(\mathcal{C}) = \left\{ \begin{array}{c} \mathbf{v}_1 + \mathbf{e}_{ij} - \mathbf{v}_2 \in \mathcal{C}\backslash\{\mathbf{0}\} \mid \Delta(\mathbf{v}_1) + \Delta\left(\mathbf{e}_{ij}\right) \in \mathrm{SF}\left(\mathbb{F}_q^n\right), \\ \mathbf{v}_2 \in \mathrm{CL}(\mathcal{C}) \text{ and } \mathbf{v}_1 - \mathbf{v}_{1i} \in \mathrm{CL}(\mathcal{C}) \end{array} \right\}.$$

Note that the definition is a bit more complex that the one for binary codes in [3], due to the fact that in the general case not all coset leaders need to be ancestors of coset leaders. The name of leader codewords comes from the fact that one could compute all coset leaders of a corresponding word knowing the set $\mathrm{L}(\mathcal{C})$ adapting [3, Algorithm 3].

Remark 3.8 The algorithm for computing $\mathrm{L}(\mathcal{C})$ is based on the construction of $\mathcal{O}(\mathcal{C})$. Theorem 3.5 guarantees that $\mathbf{w} \in \mathcal{O}(\mathcal{C})$ provided that $\mathbf{w} - \mathbf{w}_i \in \mathrm{CL}(\mathcal{C})$ for some i, then the associated set of leader codewords may be computed as $\{\mathbf{w} - \mathbf{v} : \mathbf{w} \in \mathcal{O}(\mathcal{C}),\ \mathbf{w} - \mathbf{w}_i \in \mathrm{CL}(\mathcal{C}),\ \mathbf{v} \in \mathrm{CL}(\mathbf{w}) \text{ and } \mathbf{v} \neq \mathbf{w}\}$.

Next theorem shows that any leader codeword is a zero neighbour (item *3*). However, one of the differences with the binary case is that it is not always true that a leader codeword $\mathbf{w}$ satisfies that $\mathcal{X}(\mathrm{D}(\mathbf{0})) \cap \mathrm{D}(\mathbf{w}) \neq \emptyset$, although we have that $\mathbf{w}$ is a leader codeword provided this condition (item *4*). Furthermore, (item *4*) guarantees that the set of leader codewords contains all the minimal test set according to its cardinality (see [1]). As a consequence of all these properties in Theorem 3.9 we could say that the the set of leader codewords is a "good enough" subset of the set of zero neighbours.

Theorem 3.9 (Properties of $\mathrm{L}(\mathcal{C})$) *Let $\mathcal{C}$ be a linear code then*

1. $\mathrm{L}(\mathcal{C})$ *is a test set for* $\mathcal{C}$.
2. *Let* $\mathbf{w}$ *be an element in* $\mathrm{L}(\mathcal{C})$ *then* $\mathrm{w_H}(\mathbf{w}) \leq 2\rho(\mathcal{C}) + 1$ *where* $\rho(\mathcal{C})$ *is the covering radius of the code* $\mathcal{C}$.
3. *If* $\mathbf{w} \in \mathrm{L}(\mathcal{C})$ *then* $\mathcal{X}(\mathrm{D}(\mathbf{0})) \cap (\mathrm{D}(\mathbf{w}) \cup \mathcal{X}(D(\mathbf{w}))) \neq \emptyset$.
4. *If* $\mathcal{X}(\mathrm{D}(\mathbf{0})) \cap \mathrm{D}(\mathbf{w}) \neq \emptyset$ *then* $\mathbf{w} \in \mathrm{L}(\mathcal{C})$.

Proof (1) Let $\mathbf{y} \notin \mathrm{CL}(\mathcal{C})$ and $\mathrm{supp}(\mathbf{y}) = \{i_k : k = 1, \ldots, l\}$, $l \leq n$. Let s be such that $1 \leq s < l$, $\mathbf{v}_1 = \sum_{k=1}^{s} \mathbf{y}_{i_k}\mathbf{e}_{i_k} \in \mathrm{CL}(\mathcal{C})$, $\mathbf{v}_1 + \mathbf{y}_{i_{S+1}}\mathbf{e}_{i_{S+1}} \notin \mathrm{CL}(\mathcal{C})$ and $\mathbf{v}_2 = \mathrm{CL}(\mathbf{v}_1 + \mathbf{y}_{i_{S+1}}\mathbf{e}_{i_{S+1}})$.

Let $\mathbf{y}_{i_{S+1}}\mathbf{e}_{i_{S+1}} = \sum_{t=1}^{z} \mathbf{e}_{i_{S+1}j_t}$ and $\mathbf{v_1}' = \mathbf{v}_1 + \mathbf{y}_{i_{S+1}}\mathbf{e}_{i_{S+1}} - \mathbf{e}_{i_{S+1}j_Z}$. Then $\mathbf{v_1}' - \mathbf{v}'_{1_{i_{S+1}}} = \mathbf{v}_1 \in \mathrm{CL}(\mathcal{C})$ implies that $\mathbf{w} = \mathbf{v_1}' + \mathbf{e}_{i_{S+1}j_Z} - \mathbf{v}_2 \in \mathrm{L}(\mathcal{C})$. In addition,

$\mathrm{w_H}(\mathbf{y}-\mathbf{w}) = \mathrm{w_H}(\mathbf{v}_2+(\mathbf{y}-\mathbf{v_1}'-\mathbf{e}_{i_{S+1}j_Z})) \leq \mathrm{w_H}(\mathbf{v}_2)+\mathrm{w_H}(\mathbf{y}-\mathbf{v_1}'-\mathbf{e}_{i_{S+1}j_Z})$ and $\mathrm{w_H}(\mathbf{v}_2)+\mathrm{w_H}(\mathbf{y}-\mathbf{v_1}'-\mathbf{e}_{i_{S+1}j_Z}) < \mathrm{w_H}(\mathbf{v_1}' + \mathbf{e}_{i_{S+1}j_Z}) + \mathrm{w_H}(\mathbf{y} - \mathbf{v_1}' - \mathbf{e}_{i_{S+1}j_Z})$.

Note that $\mathrm{supp}(\mathbf{v_1}' + \mathbf{e}_{i_{S+1}j_Z}) \cap \mathrm{supp}(\mathbf{y} - \mathbf{v_1}' - \mathbf{e}_{i_{S+1}j_Z}) = \emptyset$; consequently,

$$\mathrm{w_H}(\mathbf{y}) = \mathrm{w_H}\left(\mathbf{v_1}' + \mathbf{e}_{i_{S+1}j_Z}\right) + \mathrm{w_H}\left(\mathbf{y} - \mathbf{v_1}' - \mathbf{e}_{i_{S+1}j_Z}\right) \text{ and } \mathrm{w_H}(\mathbf{y} - \mathbf{w}) < \mathrm{w_H}(\mathbf{y}).$$

Thus, $\mathrm{L}(\mathcal{C})$ is a test set.

(2) Let $\mathbf{c} \in \mathrm{L}(\mathcal{C})$ then there exists $\mathbf{v}_2 \in \mathrm{CL}(\mathcal{C})$, $\mathbf{v}_1 \in \mathrm{SF}(\mathbb{F}_q^n)$, $1 \leq i \leq n$ and $1 \leq j \leq m$ such that $\mathbf{v}_1 - \mathbf{v}_{1i} \in \mathrm{CL}(\mathcal{C})$ and $\mathbf{c} = \mathbf{v}_1 + \mathbf{e}_{ij} - \mathbf{v}_2$. Applying the definition of covering radius we have that $\mathrm{w}_H(\mathbf{v}_1 - \mathbf{v}_{1i}) \leq \rho$ and $\mathrm{w}_H(\mathbf{v}_2) \leq \rho$, thus $\mathrm{w}_H(\mathbf{c}) \leq 2\rho + 1$.

(3) Let $\mathbf{w} \in \mathrm{L}(\mathcal{C})$, then $\mathbf{w} = \mathbf{v}_1 + \mathbf{e}_{ij} - \mathbf{v}_2$, where $\mathbf{v}_1$, $\mathbf{v}_2$ are elements in $\mathbb{F}_q^n$ such that $\mathbf{v}_1 + \mathbf{e}_{ij} \in \mathrm{SF}(\mathbb{F}_q^n)$, $\mathbf{v}_2 \in \mathrm{CL}(\mathcal{C})$ and $\mathbf{v}_1 - \mathbf{v}_{1i} \in \mathrm{CL}(\mathcal{C})$.

- If $\mathbf{v}_1 + \mathbf{e}_{ij} \notin \mathrm{CL}(\mathcal{C})$, then $\mathbf{v}_1 + \mathbf{e}_{ij} \in \mathcal{X}(\mathrm{D}(\mathbf{0}))$ and $(\mathbf{v}_1 + \mathbf{e}_{ij}) - \mathbf{w} = \mathbf{v}_2 \in \mathrm{CL}(\mathcal{C})$ implies that $\mathbf{v}_1 + \mathbf{e}_{ij} \in \mathrm{D}(\mathbf{w})$.
- If $\mathbf{v}_1 + \mathbf{e}_{ij} \in \mathrm{CL}(\mathcal{C})$ we define $\mathbf{v}'_1 = \mathbf{v}'_1(0) = \mathbf{v}_1 + \mathbf{e}_{ij}$. It is clear that $\mathbf{v}'_1$, $\mathbf{v}_2 \in \mathrm{CL}(\mathbf{v}_2)$. Since $\mathbf{w} \neq \mathbf{0}$ let l be a number in the set $\{1, \ldots, n\}$ such that $\mathbf{v}'_{1l} - \mathbf{v}_{2l} \neq 0$. Let $\mathbf{v}_{2l} = \sum_{j=1}^{T} \mathbf{e}_{li_j}$, for $1 \leq h \leq T$, $\mathbf{v_1}'(h) = \mathbf{v}'_1 + \sum_{j=1}^{h} \mathbf{e}_{li_j}$ and $\mathbf{v}_2(h) = \mathbf{v}_2 - \sum_{j=1}^{h} \mathbf{e}_{li_j}$.
  If there exists an h $(1 \leq h < T)$ such that $\mathbf{v}'_1(h) \notin \mathrm{CL}(\mathcal{C})$ and $\mathbf{v}'_1(h-1) \in \mathrm{CL}(\mathcal{C})$ then these two conditions imply that $\mathbf{v}'_1(h) \in \mathcal{X}(\mathrm{D}(\mathbf{0}))$. On the other hand, $\mathbf{v}_2(h) = \mathbf{v}'_1(h) - \mathbf{w}$ is either a coset leader $(\mathbf{v}'_1(h) \in \mathrm{D}(\mathbf{w}))$ or $\mathrm{d_H}(\mathbf{v}_2(h), \mathbf{v}_2) = 1$ $(\mathbf{v}'_1(h) \in \mathcal{X}(\mathrm{D}(\mathbf{w})))$.
  If there is no such and h $(1 \leq h < T)$ satisfying the condition then $\mathrm{w_H}(\mathbf{v}'_1(T)) = \mathrm{w}_H(\mathbf{v}_2(T)) + 1$, which means that $\mathbf{v}'_1(T)$ is not a coset leader and $\mathbf{v}'_1(T-1)$ is a coset leader. Then using the same idea of the previous paragraph we have that $\mathbf{v}'_1(T) \in \mathcal{X}(\mathrm{D}(\mathbf{0}))$ and $\mathbf{v}'_1(T) \in \mathrm{D}(\mathbf{w}) \cup \mathcal{X}(\mathrm{D}(\mathbf{w}))$.

(4) If $\mathcal{X}(\mathrm{D}(\mathbf{0})) \cap \mathrm{D}(\mathbf{w}) \neq \emptyset$, let $\mathbf{u} \in \mathcal{X}(\mathrm{D}(\mathbf{0})) \cap \mathrm{D}(\mathbf{w})$. The first condition $\mathbf{u} \in \mathcal{X}(\mathrm{D}(\mathbf{0}))$ implies $\mathbf{u} = \mathbf{v}_1 + \mathbf{e}_{ij}$ for some $\mathbf{v}_1 \in \mathrm{SF}(\mathbb{F}_q^n)$, $i_j \in \mathrm{supp_{gen}}(\mathbf{u})$ and $\mathbf{v}_1 - \mathbf{v}_{1i} \in \mathrm{CL}(\mathcal{C})$. On the other hand, $\mathbf{v}_1 + \mathbf{e}_{ij} \in \mathrm{D}(\mathbf{w})$ implies that $\mathbf{v}_2 = (\mathbf{v}_1 + \mathbf{e}_{ij}) - \mathbf{w} \in \mathrm{CL}(\mathcal{C})$. Therefore, $\mathbf{w} = \mathbf{v}_1 + \mathbf{e}_{ij} - \mathbf{v}_2 \in \mathrm{L}(\mathcal{C})$. □

4 Correctable and Uncorrectable Errors

We define the relation $\subset_1$ in the additive monoid which describe exactly the relation $\subset$ in the vector space $\mathbb{F}_q^n$. Given $\mathbf{x}, \mathbf{y} \in (\mathbb{F}_q^n, +)$

$$\mathbf{x} \subset_1 \mathbf{y} \text{ if } \mathbf{x} \subset \mathbf{y} \text{ and } \operatorname{supp}(\mathbf{x}) \cap \operatorname{supp}(\mathbf{y} - \mathbf{x}) = \emptyset. \tag{4.1}$$

Note that this definition translates to $\mathbb{F}_q^n$ the binary case situation in [5]. In this case given a $\mathbf{y} \in (\mathbb{F}_q^n, +)$ there are more words $x \in (\mathbb{F}_q^n, +)$ such that $\mathbf{x} \subset \mathbf{y}$ than if we consider $\mathbf{x}, \mathbf{y}$ as elements in the vector space $\mathbb{F}_q^n$. Of course, any relation $\mathbf{x} \subset \mathbf{y}$ in $\mathbb{F}_q^n$ as a vector space it is also true in the additive monoid, but it is not necessarily true in the other way round.

The set $E^0(\mathcal{C})$ of *correctable errors* of a linear code $\mathcal{C}$ is the set of the minimal elements with respect to $\prec$ in each coset. The elements of the set $E^1(\mathcal{C}) = \mathbb{F}_q^n \backslash E^0(\mathcal{C})$ will be called *uncorrectable errors*.

Definition 4.1 A *trial set* $T \subset \mathcal{C}\backslash\{\mathbf{0}\}$ of the code $\mathcal{C}$ is a set which has the following property

$\mathbf{y} \in E^0(\mathcal{C})$ if and only if $\mathbf{y} \preceq \mathbf{y} + \mathbf{c}$, for all $\mathbf{c} \in T$.

Since $\prec$ is a monotone α-ordering on $\mathbb{F}_q^n$, the set of correctable and uncorrectable errors form a monotone structure. Namely, if $\mathbf{x} \subset_1 \mathbf{y}$ then $\mathbf{x} \in E^1(\mathcal{C})$ implies $\mathbf{y} \in E^1(\mathcal{C})$ and $\mathbf{y} \in E^0(\mathcal{C})$ implies $\mathbf{x} \in E^0(\mathcal{C})$. In the general case $q \neq 2$ there is a difference with respect to the binary case, there may be words $\mathbf{y}' \in \mathbb{F}_q^n$ s.t. $\operatorname{supp}_{\text{gen}}(\mathbf{y}') = \operatorname{supp}_{\text{gen}}(\mathbf{y})$, $\mathbf{y}' \subset \mathbf{y}$ and $\mathbf{y}'$ could be either a correctable error or an uncorrectable error, so, the monotone structure it is not sustained by $\subset$ in the additive monoid $(\mathbb{F}_q^n, +)$.

Let the set of minimal uncorrectable errors $M^1(\mathcal{C})$ be the set of $\mathbf{y} \in E^1(\mathcal{C})$ such that, if $\mathbf{x} \subseteq_1 \mathbf{y}$ and $\mathbf{x} \in E^1(\mathcal{C})$, then $\mathbf{x} = \mathbf{y}$. In a similar way, the set of maximal correctable errors is the set $M^0(\mathcal{C})$ of elements $\mathbf{x} \in E^0(\mathcal{C})$ such that, if $\mathbf{x} \subseteq_1 \mathbf{y}$ and $\mathbf{y} \in E^0(\mathcal{C})$, then $\mathbf{x} = \mathbf{y}$.

For $\mathbf{c} \in \mathcal{C}\backslash\{\mathbf{0}\}$, a *larger half* is defined as a minimal word $\mathbf{u} \subseteq_1 \mathbf{c}$ in the ordering $\preceq$ such that $\mathbf{u} - \mathbf{c} \prec \mathbf{u}$. The weight of such a word $\mathbf{u}$ is such that

$$\mathrm{w_H}(\mathbf{c}) \leq 2\mathrm{w_H}(\mathbf{u}) \leq \mathrm{w}_H(\mathbf{c}) + 2,$$

see [5] for more details. The set of larger halves of a codeword $\mathbf{c}$ is denoted by $\mathrm{L_H}(\mathbf{c})$, and for $U \subseteq \mathcal{C}\backslash\{\mathbf{0}\}$ the set of larger halves for elements of U is denoted by $\mathrm{L_H}(U)$. Note that $\mathrm{L_H}(\mathcal{C}) \subseteq E^1(\mathcal{C})$.

For any $\mathbf{y} \in \mathbb{F}_q^n$, let $H(\mathbf{y}) = \{c \in \mathcal{C} : \mathbf{y} - \mathbf{c} \prec \mathbf{y}\}$, and we have $\mathbf{y} \in E^0(\mathcal{C})$ if and only if $H(\mathbf{y}) = \emptyset$, and $\mathbf{y} \in E^1(\mathcal{C})$ if and only if $H(\mathbf{y}) \neq \emptyset$.

In [5, Theorem 1] there is a characterization of the set $M^1(\mathcal{C})$ in terms of $H(\cdot)$ and larger halves of the set of minimal codewords $M(\mathcal{C})$ for the binary case. It is easy to proof that this Theorem and [5, Corollary 3] are also true for any linear code.

Proposition 4.2 (Corollary 3 in [5]) *Let $\mathcal{C}$ be a linear code and $T \subseteq \mathcal{C}\backslash\{\mathbf{0}\}$. The following statements are equivalent:*

1. *T is a trial set for $\mathcal{C}$.*
2. *If $\mathbf{y} \in M^1(\mathcal{C})$, then $T \cap H(\mathbf{y}) \neq \emptyset$.*
3. *$M^1(\mathcal{C}) \subseteq \mathrm{L_H}(T)$.*

Now we will formulate the result which relates the trial sets for a given weight compatible order $\prec$ and the set of leader codewords.

Theorem 4.3 *Let $\mathcal{C}$ be a linear code and $\mathrm{L}(\mathcal{C})$ the set of leader codewords for $\mathcal{C}$, then $\mathrm{L}(\mathcal{C})$ is a trial set for any given $\prec$.*

Proof We will prove statement 2 of Proposition 4.2. Let $\mathbf{y} \in M^1(\mathcal{C})$, let i such that $\mathrm{supp}_{\mathrm{gen}}(\mathbf{y})[i] \neq \emptyset$ and $\mathbf{v}_1 = \mathbf{y} - \mathbf{y}_i$. Since $\mathbf{y} \in M^1(\mathcal{C})$ we have that $\mathbf{v}_1 \in E^0(\mathcal{C})$, thus it is a coset leader. On the other hand, let $\mathbf{v}_2 \in E^0(\mathcal{C})$ such that $\mathbf{v}_2 \in \mathrm{CL}(\mathbf{y})$ and $\mathbf{c} = \mathbf{y} - \mathbf{v}_2$. It is clear that $\mathbf{c}$ is a leader codeword and $\mathbf{y} - \mathbf{c} = \mathbf{v}_2 \prec \mathbf{y}$. Therefore $\mathbf{c} \in H(\mathbf{y})$. □

Remark 4.4 Algorithm 2 in [3] can be adapted to compute a set of leader codewords which is a trial set T for a given $\prec$ such that satisfies the following property

- For any $\mathbf{c} \in T$, there exists $\mathbf{y} \in M^1(\mathcal{C}) \cap \mathrm{L_H}(\mathbf{c})$ s.t. $\mathbf{y} - \mathbf{c} \in E^0(\mathcal{C})$.

In the algorithm, it is necessary to add to the function `InsertNext` the item 3 of the construction of $\mathcal{O}(\mathcal{C})$, whose elements are stored in `Listing`. On the other hand, in the steps of the construction of the leader codewords (Steps 11 - 13) it is enough to state the condition $\mathbf{t} - \mathbf{t}_i \in \mathrm{CL}(\mathcal{C})$ for some $i \in \mathrm{supp}(\mathbf{t})$, taking all $\mathbf{t}_k \in \mathrm{CL}(\mathbf{t})$ and adding the corresponding codewords $\mathbf{t} - \mathbf{t}_k$ to the set $\mathrm{L}(\mathcal{C})$.

5 An Example

Let $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$ be the finite field of four elements, where a is a root of the irreducible polynomial $f(x) = 1 + x + x^2$ over $\mathbb{F}_2$.

Let $\mathcal{C}$ be the linear code of length 8 ($n = 8$), dimension 5 ($k = 5$) defined by the parity check matrix

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & a & a & a^2 & a^2 \\ 0 & 1 & a & a^2 & a & a^2 & a & a^2 \end{pmatrix}.$$

Then we compute the set $\mathrm{L}(\mathcal{C})$ of leader codewords of $\mathcal{C}$ and it results that there are 354 leader codewords among 1024 codewords. We have that $\mathbf{c} = \{(1, 1, 1, 1, 0, 0, 0, 0), (a, a, 0, 0, 0, 0, a, a)\} \subset \mathrm{L}(\mathcal{C})$.

Let the vector $\mathbf{y} = (a, a, 1, 1, 0, 0, a, a)$, then the vectors of the set $w = \{\mathbf{e}_1 + \mathbf{e}_2,\ \mathbf{e}_3 + \mathbf{e}_4,\ \mathbf{e}_5 + \mathbf{e}_6, \mathbf{e}_7 + \mathbf{e}_8\}$ are the coset leaders of the coset of $\mathbf{y}$. Since $\mathrm{L}(\mathcal{C})$ is a test set, a gradient descent decoding algorithm may be done to compute a coset leader of $\mathbf{y} + \mathcal{C}$ (see Definition 2.8). Then, taking $\mathbf{c}_2$ from the set $\mathrm{L}(\mathcal{C})$ we obtain $\mathbf{w}_2 = \mathbf{y} - \mathbf{c}_2$, whose weight can not be reduced by using the test set $\mathrm{L}(\mathcal{C})$, this means that $\mathbf{w}_2$ is a coset leader. In addition, $\mathrm{L}(\mathcal{C})$ allows to compute all coset leaders corresponding to any vector. In this case, by taking $\mathbf{c}_1$ and computing $\mathbf{w}_2 - \mathbf{c}_1$ we get $\mathbf{w}_1$ which is also a coset leader corresponding to $\mathbf{y}$.

Also if we choose $\prec$ as the weight compatible order associated to the degree reverse lexicographical order, we have that $\mathbf{w}_1$ is the correctable error corresponding to $\mathbf{y} + \mathcal{C}$. Then as $\mathrm{L}(\mathcal{C})$ is also a trial set, by Definition 4.1 it is possible to obtain from any vector $\mathbf{y}$ the corresponding correctable error in a finitely many steps as we have been shown above.

References

1. Barg, A.: Complexity issues in coding theory. In: Pless, V., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of Coding Theory, vol. I, pp. 649–754. Elsevier, Amsterdam (1998)
2. Borges-Quintana, M., Borges-Trenard, M.A., Martínez-Moro, E.: On a Gröbner bases structure associated to linear codes. J. Discrete Math. Sci. Cryptogr. **10**(2), 151–191 (2007)
3. Borges-Quintana, M., Borges-Trenard, M.A., Márquez-Corbella, I., Martínez-Moro, E.: Computing coset leaders and leader codewords of binary codes. J. Algebr. Appl. https://doi.org/10.1142/S0219498815501285 (2015)
4. Braun, G., Pokutta, S.: A polyhedral characterization of border bases. SIAM J. Discrete Math. **30**(1), 239–265 (2016)
5. Helleseth, T., Kløve, T., Vladimir, I.L.: Error-correction capability of binary linear codes. IEEE Trans. Inf. Theory **51**(4), 1408–1423 (2005)
6. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)

7. Kurshan, R.P., Sloane, N.J.A.: Coset analysis of Reed Muller codes via translates of finite vector spaces. Inf. Control **20**(5), 410–414 (1972)
8. Márquez-Corbella, I., Martínez-Moro, E.: Algebraic structure of the minimal support codewords set of some linear codes. Adv. Math. Commun. **5**(2), 233–244 (2011)
9. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 246–249 (1993)
10. Zémor, G., Cohen, G.: The threshold probability of a code. IEEE Trans. Inf. Theory **41**(2), 469–477 (1995)