Trial set and Gröbner bases for binary codes

M. Borges-Quintana[1 a], M. A. Borges-Trenard[2], Edgar Martínez Moro[3]

[1 2] *Department of Mathematics, Faculty of Mathematics and Computer Science, University of Oriente, Santiago de Cuba, Cuba, mijail@csd.uo.edu.cu, mborges@csd.uo.edu.cu*
[3] *Institute of Mathematics IMUVa, University of Valladolid. Valladolid, Castilla, Spain, edgar@maf.uva.es*

We show the connections between trial sets and Gröbner bases for binary codes, which gives more characterizations of trial sets in the context of Gröbner bases and algorithmic ways for compute them. In this sense, minimal trial set are characterized as trial sets associated with minimal Gröbner bases.

The concept of trial set was introduced in [6]. This set of codewords can be used to derive and algorithm for doing complete decoding in a similar way that a gradient decoding algorithm uses a test set (see [1]). A trial set allows to characterize the so called *correctable errors* and to investigate the monotone structure of correctable and uncorrectable errors, also important bounds on the error-correction capability of binary codes beyond half of minimum distance using trial sets are presented in [6]. One problem posted in the conclusion of [6] was the importance of charactherize minimal trial sets for families of binary codes.

The ideal associated with any linear code (code ideal for simplicity) was introduced in [2] together with applications of Gröbner bases theory in this context, such that the reduction process by Gröbner bases of code ideals w.r.t. to specific orders corresponds to the decoding process of the code.

In Section 1 we give the main concepts and results related with binary codes, trial sets, the code ideals and Gröbner bases which are needed for an understanding of this work. The connection between trial sets for binary codes and Gröbner bases for the corresponding code ideal is presented in Section 2. The main results in this contribution are Proposition 2, Theorems 4 and 5, and the subsection 2.1 about minimal trial sets and minimal Gröbner bases.

1 Preliminaries

Binary codes
By $\mathbb{Z}$, $\mathbb{K}$, $\mathbb{K}[\mathbf{X}]$ and $\mathbb{F}_2$ we denote the ring of integers, an arbitrary field, the polynomial ring in n variables over the field $\mathbb{K}$ and the finite field with 2 elements.

[a]Supported by a Post-doctorate scholarship at the University of Valladolid (09-2014 to 02-2015) by Erasmus Mundus Program, Mundus Lindo Project.

A *binary linear code* $\mathscr{C}$ over $\mathbb{F}_2$ of length n and dimension k, or an $[n,k]$ binary code for short, is a k-dimensional subspace of $\mathbb{F}_2^n$. We will call the vectors $\mathbf{v}$ in $\mathbb{F}_2^n$ words and in the particular case where $\mathbf{v} \in \mathscr{C}$, codewords. For every word $\mathbf{v} \in \mathbb{F}_2^n$ 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 $\mathrm{supp}(\mathbf{v})$.

The *Hamming distance*, between two vectors $\mathbf{x},\ \mathbf{y} \in \mathbb{F}_2^n$ is $d_H(\mathbf{x},\mathbf{y}) = \mathrm{w}_H(\mathbf{x}-\mathbf{y})$. The *minimum distance* $d(\mathscr{C})$ of a linear code $\mathscr{C}$ is defined as the minimum weight among all nonzero codewords.

For the rest of this section we follow [6]. We will consider $\prec$ a so called α-ordering on $\mathbb{F}_2^n$ (a weight compatible total ordering on $\mathbb{F}_2^n$) which is monotone:

$$\left.\begin{array}{l}\text{for any } \mathbf{y}_1, \mathbf{y}_2 \; s.t. \; 2 \leq \mathrm{w}_H(\mathbf{y}_1) = \mathrm{w}_H(\mathbf{y}_1) < n \text{ and } \mathrm{supp}(\mathbf{y}_1) \cap \mathrm{supp}(\mathbf{y}_1) \neq \emptyset \\ \text{and for any } i \in \mathrm{supp}(\mathbf{y}_1) \cap \mathrm{supp}(\mathbf{y}_1) \text{ and vectors } \mathbf{x}_1 \text{ and } \mathbf{x}_2 \text{ defined by} \\ \mathrm{supp}(\mathbf{x}_1) = \mathrm{supp}(\mathbf{y}_1) \setminus \{i\} \text{ and } \mathrm{supp}(\mathbf{x}_2) = \mathrm{supp}(\mathbf{y}_2) \setminus \{i\} \text{ then } \mathbf{y}_1 \prec \mathbf{y}_2 \text{ if} \\ \mathbf{x}_1 \prec \mathbf{x}_2.\end{array}\right\} \quad (1)$$

The set of correctable errors of a binary code $\mathscr{C}$ ($E^0(\mathscr{C})$) are the minimal elements w.r.t. $\prec$ in each coset of $\mathbb{F}_2^n/\mathscr{C}$, and the elements of $E^1(\mathscr{C}) = \mathbb{F}_2^n \setminus E^0(\mathscr{C})$ are called uncorrectable errors. A *trial set* $T \subset \mathscr{C} \setminus \mathbf{0}$ of the code $\mathscr{C}$ is a set which has the property $\mathbf{y} \in E^0(\mathscr{C})$ if and only if $\mathbf{y} \leq \mathbf{y}+\mathbf{c},$ for all $\mathbf{c} \in T$.

Note that with a trial set we obtain an algorithm which returns the corresponding correctable error for a received word $\mathbf{y}$. Since we choose a monotone α-ordering on $\mathbb{F}_2^n$, the set of correctable and uncorrectable errors form a monotone structure, namely, that if $\mathbf{x} \subset \mathbf{y}$, then $\mathbf{x} \in E^1(\mathscr{C})$ implies $\mathbf{y} \in E^1(\mathscr{C})$ and $\mathbf{y} \in E^0(\mathscr{C})$ implies $\mathbf{x} \in E^0(\mathscr{C})$.

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

For $\mathbf{c} \in \mathscr{C} \setminus \mathbf{0}$, a *larger half* is defined as a minimal word $\mathbf{u}$ in the ordering $\preceq$ such that $\mathbf{u}+\mathbf{c} \prec \mathbf{u}$. The set of larger halves for a codeword $\mathbf{c}$ is denoted by $\mathrm{L}(\mathbf{c})$, and for $U \subseteq \mathscr{C} \setminus \mathbf{0}$ the set of larger halves for elements of U is denoted by $\mathrm{L}(U)$. Note that $\mathrm{L}(\mathscr{C}) \subseteq E^1(\mathscr{C})$.

For any $\mathbf{y} \in \mathbb{F}_2^n$, let $H(\mathbf{y}) = \{c \in \mathscr{C} : \mathbf{y}+\mathbf{c} \prec \mathbf{y}\}$, and we have $\mathbf{y} \in E^0(\mathscr{C})$ if and only if $H(\mathbf{y}) = \emptyset$, and $\mathbf{y} \in E^1(\mathscr{C})$ if and only if $H(\mathbf{y}) \neq \emptyset$. Theorem 1 of [6] provides a characterization of the set $M^1(\mathscr{C})$ in terms of $H(\cdot)$ and larger halves of the set of minimal codewords $M(\mathscr{C})$.

Proposition 1 (Corollary 3, [6]) *Let $\mathscr{C}$ be a binary code and $T \subseteq \mathscr{C} \setminus \mathbf{0}$. The following statements are equivalent:*

1. *T is a trial set for $\mathscr{C}$.*

2. *If $\mathbf{y} \in M^1(\mathscr{C})$, then $T \cap H(\mathbf{y}) \neq \emptyset$.*

3. *$M^1(\mathscr{C}) \subseteq \mathrm{L}(T)$.*

Gröbner bases and binary codes

We define the following characteristic crossing function: $\Delta : \mathbb{F}_2^s \longrightarrow \mathbb{Z}^s$ which replace the class of $0,1$ by the same symbols regarded as integers. This map will be used with matrices and vectors acting coordinate-wise. Also, for the reciprocal case, we defined $\nabla : \mathbb{Z}^s \longrightarrow \mathbb{F}_2^s$. Let $\mathbf{X}$ denotes n variables $x_1, \ldots, x_n$ and let $\mathbf{a} = (a_1, \ldots, a_n)$ be an n-tuple of elements of the field $\mathbb{F}_2$. We will adopt the following notation:

$$\mathbf{X}^{\mathbf{a}} := x_1^{\Delta a_1} \cdots x_n^{\Delta a_n} \in [\mathbf{X}]. \tag{2}$$

The code ideal can be given by the two equivalent formulas in (3) and (4) below, the equivalency between (3) and (4) was proved in [4]. Let W be a generator matrix of an $[n,k]$ binary code $\mathscr{C}$ (the row space of the matrix generates $\mathscr{C}$) and $\mathbf{w}_i$ denotes its rows for $i = 1, \ldots k$.

$$I(\mathscr{C}) = \left\langle \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathscr{C} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]. \tag{3}$$

$$I(\mathscr{C}) = \left\langle \{\mathbf{X}^{\mathbf{w}_i} - 1 : i = 1, \ldots k\} \cup \{x_i^2 - 1 : i = 1, \ldots, n\} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]. \tag{4}$$

Note that $I(\mathscr{C})$ is a zero-dimensional ideal since the quotient ring $R = \mathbb{K}[\mathbf{X}]/I(\mathscr{C})$ is a finite dimensional vector space and its dimension is equal to the number of cosets in $\mathbb{F}_2^n/\mathscr{C}$.

For every element $\mathbf{X}^a$ in the monoid $[\mathbf{X}]$, with $a \in \mathbb{N}^n$, we have a corresponding vector $\nabla(a) \in \mathbb{F}_2^n$, and viceversa, any vector $\mathbf{w} \in \mathbb{F}_2^n$ has a unique standard representation[b] $\mathbf{X}^{\mathbf{w}}$ as an element of $[\mathbf{X}]$ (see (2)).

Let $<$ be a term order, let us $\mathrm{T}(f)$ denotes the maximal term of a polynomial f with respect to the order $<$. The set of maximal terms of the set $F \subseteq K[X]$ is denoted $\mathrm{T}\{F\}$ and $\mathrm{T}(F)$ denotes the semigroup ideal generated by $\mathrm{T}\{F\}$. Finally, $\langle F \rangle$ is the polynomial ideal in $\mathbb{K}[\mathbf{X}]$ generated by F. In particular, for the code ideal $I(\mathscr{C})$, $\mathrm{T}(I(\mathscr{C}))$ is the set of maximal terms and $N(I(\mathscr{C})) = [\mathbf{X}] \setminus \mathrm{T}(I(\mathscr{C}))$ the set of canonical forms. We emphasize that there is a one to one correspondence between the set of canonical forms and the cosets in $\mathbb{F}_2^n/\mathscr{C}$. One characterization of Gröbner bases is that G is a *Gröbner basis* of the ideal $\langle \mathrm{G} \rangle$ if and only if $\mathrm{T}(\langle \mathrm{G} \rangle) = \mathrm{T}(\mathrm{G})$.

[b] The exponents of the variables are 0 or 1.

2 Gröbner bases and trial set for binary codes

It is not difficult to see also the conection between total degree orders $<$ on $[\mathbf{X}]$ and α-orderings monotone $\prec$ on $\mathbb{F}_2^n$. In essence, any total degree compatible ordering induces an α-ordering monotone $\prec$ on $\mathbb{F}_2^n$ such that $\mathbf{v} \prec \mathbf{w}$ if $\mathbf{X}^{\mathbf{v}} < \mathbf{X}^{\mathbf{w}}$ for any $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2^n$. On the other hand, given an α-ordering monotone on $\mathbb{F}_2^n$ we could define a total ordering on $[\mathbf{X}]$ which is not admisible, a class of these orders on $[\mathbf{X}]$ were called in [2] error-vector orderings.

In this work we will focus in the first situation, the α-ordering monotone which is defined in [6] it is derived from the Graduated Lexicographical order. In general, let $<$ be a total degree term order on $[\mathbf{X}]$, and let $\prec$ be the corresponding α-ordering monotone on $\mathbb{F}_2^n$.

Proposition 2 [Correctable and uncorrectable errors and canonical forms and maximal terms] *Let $X^{\mathbf{w}} \in [\mathbf{X}]$, $\mathbf{w} \in \mathbb{N}^n$ then*

1. *If $X^{\mathbf{w}}$ is not the standard representation of the word $\nabla(\mathbf{w})$ in $\mathbb{F}_2^n$, then it is a maximal term i.e. $X^{\mathbf{w}} \in \mathrm{T}(I(\mathscr{C}))$.*
2. *If $\nabla(\mathbf{w}) \in E^1(\mathscr{C})$, then $X^{\mathbf{w}} \in \mathrm{T}(I(\mathscr{C}))$.*
3. *If $X^{\mathbf{w}}$ is the standard representation of the word $\nabla(\mathbf{w})$ and $\nabla(\mathbf{w}) \in E^0(\mathscr{C})$, then $X^{\mathbf{w}}$ is a canonical form i.e. $X^{\mathbf{w}} \in N(I(\mathscr{C}))$.*
4. *If $X^{\mathbf{w}}$ is the standard representation of the word $\nabla(\mathbf{w})$ and $\nabla(\mathbf{w}) \in M^1(\mathscr{C})$, then $X^{\mathbf{w}}$ is an irredundant maximal term, i.e. $X^{\mathbf{w}} \notin \mathrm{T}(I(\mathscr{C})) \setminus \{X^{\mathbf{w}}\}$ and is a maximal term of any Gröbner basis. The set of irredundant maximal terms are the maximal terms of any minimal Gröbner basis, for example, of the reduced Gröbner basis.*

For simplicity, we will assume that the coefficients of the maximal terms in a Gröbner basis are positive.

Definition 3 (Gröbner codewords [3]) *Let* G *be a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$, the set of Gröbner codewords $\mathscr{C}_{\mathrm{G}}$ corresponding to* G *are the codewords associated with* G *by $\mathscr{C}_{\mathrm{G}} = \{\mathbf{c} \in \mathscr{C} : \mathbf{c} = \mathbf{w} + \mathbf{v},\ s.t.\ X^{\mathbf{w}} - X^{\mathbf{v}} \in \mathrm{G}, \mathbf{w}, \mathbf{v} \in \mathbb{F}_2^n, \mathbf{v} \prec \mathbf{w}\}$.*

Theorem 4 *Let* G *be a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$, then $\mathscr{C}_{\mathrm{G}}$ is a trial set.*

Proof. We will prove the stament 2 in Proposition 1. Let $\mathbf{w} \in M^1(\mathscr{C})$, then $X^{\mathbf{w}} \in \mathrm{T}(\mathrm{G})$ (see Proposition 2.4) and there exists $\mathbf{c} \in \mathscr{C}_{\mathrm{G}}$ s.t. $\mathbf{c} = \mathbf{w} + \mathbf{v}$ s.t. $\mathbf{v} \prec \mathbf{w}$. Thus $\mathbf{c} + \mathbf{w} = \mathbf{v} \prec \mathbf{w}$ and $\mathbf{c} \in H(\mathbf{w})$.

Theorem 5 *Let T be a trial set, the set $\mathrm{G}_T = \{\mathbf{X}^{\mathbf{w}} - \mathbf{X}^{\mathbf{v}} : \mathbf{w} \in \mathrm{L}(\mathbf{c})$ for some $\mathbf{c} \in T$ and $\mathbf{v} = \mathbf{c} - \mathbf{w}\} \cup \{x_i^2 - 1 : i = 1, \ldots, n\}$ is a Gröbner basis for $I(\mathscr{C})$ w.r.t. $<$.*

Proof. If $X^{\mathbf{u}}$ is a maximal term which is not the standard representation of $\nabla(\mathbf{u})$, then it can be reduced to the standard representation of $\nabla(\mathbf{u})$ by means of the set $\{x_i^2 - 1 : i = 1, \ldots, n\}$. Thus, let us assume that $X^{\mathbf{u}} \in \mathrm{T}(I(\mathscr{C}))$ and $\mathbf{u} \in E^1(\mathscr{C})$. It is clear that there exists $\mathbf{w} \subseteq \mathbf{u}$ s.t. $\mathbf{w} \in M^1(\mathscr{C})$, $\mathbf{w} \in M^1(\mathscr{C})$ implies there exists $\mathbf{c} \in T$ s.t. $\mathbf{w} \in \mathrm{L}(\mathbf{c})$ (by Proposition 1.3). Let $\mathbf{v} = \mathbf{c} - \mathbf{w}$, then we have $\mathbf{X}^{\mathbf{w}} - \mathbf{X}^{\mathbf{v}} \in \mathrm{G}_T$ and $\mathbf{X}^{\mathbf{w}} \mid \mathbf{X}^{\mathbf{u}}$ (remember $\mathbf{w} \subseteq \mathbf{u}$). Consequently, G_T is a Gröbner basis for $I(\mathscr{C})$.

2.1 Minimal trial sets and minimal Gröbner bases

A minimal trial set is a trial set such that any strictly subset is not a trial set. Having an smaller trial set, it is an smaller set that it is used for decoding in order to compute the corresponding correctable error to a received word, althought smaller trial sets do not necessaryly ensure more efficiency. In [6] is given a main advantage of having a minimal trial set, because the size of trial sets are used to derive some important bounds on the error correction beyond half the minimum distance.

By Proposition 1.3, the set of larger halves of a trial set T should contains at least the set $M^1(\mathscr{C})$, by Theorem 5 and Proposition 2.4 this means that the corresponding Gröbner basis G_T should coontains at least the irredundant maximal terms (it is the case for any Gröbner basis); therefore, there is a direct connection between minimal trial sets and minimal Gröbner bases. In particular, a distinguished minimal trial set would be the set of Gröbner codewords corresponding to the reduced Gröbner basis.

References

[1] A. Barg, *Complexity issues in coding theory*, in *Handbook of coding theory*, **I**, North-Holland, Amsterdam, pp. 649-754 (1998).

[2] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *On a Gröbner bases structure associated to linear codes*, J. Discret. Math. Sci. Cryptogr, **10(2)**, pp. 151-191 (2007).

[3] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *A Gröbner representation for linear codes*, in *Advances in coding theory and cryptography, Ser. Coding Theory Cryptol.*, **3**, World Sci. Publ., Hackensack, NJ, pp. 17-32, (2007).

[4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro, *Gröbner bases and combinatorics for binary codes*, Appl. Algebra Engrg. Comm. Comput., **19(5)**, pp. 393-411 (2008).

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge (2003).

[6] T. Helleseth, T. Kløve and I.L. Vladimir, *Error-correction capability of binary linear codes*, IEEE Transactions on Information Theory, **51(4)**, pp. 1408-1423 (2005).