

# GBLA & Codes: Gröbner basis associated with linear codes

M. Borges-Quintana, M.A. Borges-Trenard  
 Universidad de Oriente (Cuba)  
 mijail@mbq.uo.edu.cu, mborges@mabt.uo.edu.cu

E. Martínez-Moro  
 Universidad de Valladolid (Spain)  
 edgar@maf.uva.es

## Abstract

The connection between Gröbner bases and linear algebra comes from the very beginning, i.e. from Buchberger's PhD thesis. In [6, 7] these techniques were generalized to different settings (change of orderings, ideal defined by functionals). In [4, 5] the algorithm for monoid and group algebras was specialized for the case of algebras associated to linear codes. This poster is a concise presentation of some results in [1, 2, 3].

## The structures associated with a code

consider the elements of  $\mathbb{F}_q$  represented as

$$a_0 + a_1\alpha + \dots + a_{m-1}\alpha^{m-1}$$

where  $\alpha$  is a root of an irreducible polynomial of degree  $m$  over  $\mathbb{F}_p$  and  $a_i \in \mathbb{F}_p$  for all  $i$ . Let us consider the free commutative monoid  $[X]$  generated by the  $nm$  variables  $X := \{x_{11}, \dots, x_{1m}, \dots, x_{n1}, \dots, x_{nm}\}$ . We have the following morphism of monoids from  $[X]$  onto  $\mathbb{F}_q^n$ :

$$\psi : [X] \rightarrow \mathbb{F}_q^n$$

$$x_{ij} \mapsto (0, \dots, 0, \underbrace{\alpha^{j-1}}_i, 0, \dots, 0),$$

and, by morphism extension,

$$\prod_{i=1}^n \prod_{j=1}^m x_{ij}^{\beta_{ij}} \mapsto \left( \left( \sum_{j=1}^m \beta_{1j} \alpha^{j-1} \right)_{\text{mod } p}, \dots, \left( \sum_{j=1}^m \beta_{nj} \alpha^{j-1} \right)_{\text{mod } p} \right) \quad (1)$$

Let  $w \in [X]$ . We will denote by  $\text{Supp}(w)$  the set of variables that divide  $w$  and by  $\text{Ind}(w)$  the set of indices associated to  $w$ , i.e.

$$\text{Ind}(w) := \{i \in \{1, \dots, n\} \mid \exists j \in \{1, \dots, m\} \text{ such that } x_{ij} \in \text{Supp}(w)\}.$$

**Definition 1 (The error vector ordering).** We say that  $u$  is less than  $w$  w.r.t. the error-vector ordering, and denote it by  $u <_e w$ , if one of the following conditions holds:

- $|\text{Ind}(u)| < |\text{Ind}(w)|$ .
- $|\text{Ind}(u)| = |\text{Ind}(w)|$  and  $u < w$ , where  $<$  denotes an arbitrary but fixed admissible ordering on  $[X]$ .

It is easy to prove that  $<_e$  is a total ordering on  $[X]$ . However, it is not admissible. It is the multiplicative property of admissible orders that sometimes fails here.

A linear code  $\mathcal{C}$  defines an equivalence relation  $R_{\mathcal{C}}$  in  $\mathbb{F}_q^n$  by

$$(x, y) \in R_{\mathcal{C}} \Leftrightarrow x - y \in \mathcal{C}.$$

If we define  $\xi_{\mathcal{C}}(u) := \psi(u)H$  ( $H$  is the parity check matrix), where  $u \in [X]$ , the above congruence can be translated to  $[X]$  by the morphisms  $\psi$  as

$$u \equiv_{\mathcal{C}} w \Leftrightarrow (\psi(u), \psi(w)) \in R_{\mathcal{C}} \Leftrightarrow \xi_{\mathcal{C}}(u) = \xi_{\mathcal{C}}(w).$$

The morphism  $\xi_{\mathcal{C}}$  represents the transition of the syndromes from  $\mathbb{F}_q^n$  to  $[X]$ , so that,  $\xi_{\mathcal{C}}(w)$  is the syndrome of  $w$ , which is equal to the syndrome of  $\psi(w)$ .

**Definition 2 (Canonical forms).** We define a set of canonical forms  $N \subset [X]$  by the following properties:

- $1 \in N \subseteq [X]$ .
- $|N| = q^{n-k}$ .
- If  $u, v \in N$  and  $u \neq v$ , then  $\xi_{\mathcal{C}}(u) \neq \xi_{\mathcal{C}}(v)$ .
- For all  $w \in N \setminus \{1\}$  there exists  $x \in X$  such that  $w = w'x$  and  $w' \in N$ .

**Definition 3 ("Multiplicative structure function", matphi).** Let  $\text{matphi}$  be a function  $\phi$  from  $N \times X$  onto  $N$ , such that for all  $x \in X$  and for all  $w \in [X]$  we have that  $\xi_{\mathcal{C}}(\phi(w, x)) = \xi_{\mathcal{C}}(wx)$ .

## Computation of N and $\phi$

The following algorithm for building  $N$  and  $\phi$  can be found in [5]. There are three functions needed to understand the algorithm:

- InsertNexts** $[t, List]$  inserts all the products  $xt$  in  $List$ , where  $x \in X$ , keeping the increasing order of  $List$  w.r.t. the order  $<_e$ .
- NextTerm** $[List]$  returns the first element from  $List$  and deletes it from that set.
- Member** $[obj, G]$  returns the position  $j$  of  $obj$  in  $G$ , if  $obj \in G$ , and false otherwise.

**Input:** A linear code  $\mathcal{C} \subset \mathbb{F}_q^n$  given by  $p, n, m$ , such that  $q = p^m$ , and a parity check matrix  $H$ .

**Output:** A set of canonical forms for  $\mathcal{C}$ , and  $\phi$  the corresponding function  $\text{matphi}$ .

```
List := {1}, N :=  $\emptyset$ , r := 0
while List  $\neq \emptyset$  do
  w := NextTerm[List]
  v' :=  $\xi_{\mathcal{C}}(w)$ 
  j := Member[v', {v1, ..., vr}]
  if j  $\neq$  false then
    foreach k such that w = uxk with u  $\in N$  do
      |  $\phi(u, x_k) := w_j$ 
    end
  else
    r := r + 1, vr := v', wr := w, N := N  $\cup$  {wr}
    List := InsertNexts[wr, List]
    foreach k such that w = uxk with u  $\in N$  do
      |  $\phi(u, x_k) := w$ 
    end
  end
end
end
```

**Example:** Consider the code  $\mathcal{C}$  in  $\mathbb{F}_2^6$  with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

The number of variables is 6,  $<$  is set to be the lex. ordering induced by  $x_1 < x_2 < \dots < x_6$ .

We can compute  $N = \{1, x_1, \dots, x_6, x_2x_3\}$  and  $\phi$  as

In each triple the first entry correspond to the elements  $\psi(w)$  where  $w \in N$  ( $w = N[i]$ ), the second one is 1 if  $\psi(w) \in B(\mathcal{C}, t)$  or 0 otherwise, and the third component points to the values  $\phi(w, x_j)$ , for  $j = 1, \dots, nm$ , that is  $\phi(w, x_j) = N[\phi[i][3][j]]$ .

$$\phi = \begin{bmatrix} [[0, 0, 0, 0, 0, 0], 1, [2, 3, 4, 5, 6, 7]], [[1, 0, 0, 0, 0, 0], 1, [1, 6, 5, 4, 3, 8]] \\ [[0, 1, 0, 0, 0, 0], 1, [6, 1, 8, 7, 2, 5]], [[0, 0, 1, 0, 0, 0], 1, [5, 8, 1, 2, 7, 6]] \\ [[0, 0, 0, 1, 0, 0], 1, [4, 7, 2, 1, 8, 3]], [[0, 0, 0, 0, 1, 0], 1, [3, 2, 7, 8, 1, 4]] \\ [[0, 0, 0, 0, 0, 1], 1, [8, 5, 6, 3, 4, 1]], [[0, 1, 1, 0, 0, 0], 0, [7, 4, 3, 6, 5, 2]] \end{bmatrix}$$

## Gradient-like decoding

**Theorem 1.** Let  $\mathcal{C}$  be a linear code. Let  $w \in [X]$  an arbitrary word and  $v \in N$  its corresponding canonical form. If  $\text{weight}(\psi(v)) \leq t$  (the error correcting capacity) then  $\psi(v)$  is the error vector corresponding to  $\psi(w)$ . Otherwise, if  $\text{weight}(\psi(v)) > t$ ,  $\psi(w)$  contains more than  $t$  errors.

**Example:** Consider the  $(10, 4, 1)$ -code over  $\mathbb{F}_2$  with parity check matrix (Number of code-words: 16, number of canonical forms: 64)

$$H := \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The vector  $(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \in \mathbb{F}_2^{10}$  (corresponding to the word  $x_1x_2x_3x_7x_8x_9$ ) is reduced to  $(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$  (corresponding to the word  $x_1x_3x_{10}$ ). But the weight of the resulting vector is 3, and the error-correcting capability of that code is 1. So this is not a correctable error pattern.

Let us take now the vector  $v = (1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$ , the corresponding word is  $w = x_1x_2x_3x_4x_9x_{10}$ . Let us reduce now  $w$ .

$$w = x_1x_2x_3x_4x_9x_{10} \xrightarrow{G_{26}} x_1x_9^2x_{10}^2 \xrightarrow{G_9} x_1^2x_{10}^2 \xrightarrow{G_{10}} x_1.$$

$\text{weight}(\psi(x_1)) = \text{weight}((1, 0, 0, 0, 0, 0, 0, 0, 0, 0)) = 1$ , then

$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$  is the error vector corresponding to  $v$ , and the codeword is  $(0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$ .

## Permutation equivalent codes

**Definition 4.** Let  $\phi : N \times X \rightarrow N$  and  $\phi^* : N^* \times X \rightarrow N^*$  be two  $\text{matphi}$  functions. Then  $\phi \sim \phi^*$  if and only if the following two conditions hold:

- There exists a  $\sigma \in S_n$  such that  $N^* = \sigma(N)$ , and
- For all  $v \in N$  and  $i = 1, \dots, mn$  we have  $\phi^*(\sigma(v), \sigma(x_i)) = \sigma(\phi(v, x_i))$ .

Note that condition 2 states that the image by the permutation should preserve the multiplicative structures of  $\text{matphi}$ . If two codes satisfy 2 for a permutation  $\sigma$ , then the  $\text{matphi}$ 's will be equivalent, and it would be enough to change to  $\sigma(N)$  the set of canonical forms of  $\mathcal{C}^*$ .

**Theorem 2.** Let  $\phi$  be a  $\text{matphi}$  function for the code  $\mathcal{C}$ , and  $\phi^*$  a  $\text{matphi}$  for a code  $\mathcal{C}^*$ . Then  $\mathcal{C}$  is permutation equivalent to  $\mathcal{C}^* \Leftrightarrow \phi \sim \phi^*$ .

## Binary case

In the binary case the ordering defined is admissible, thus we have the following definition

**Definition 5.** Let  $\mathcal{C}$  be a code and  $R_{\mathcal{C}}$  the class-equivalence relation. The ideal  $I(\mathcal{C})$  associated with  $\mathcal{C}$  is

$$I(\mathcal{C}) = \langle \{w - v \mid (\psi(w), \psi(v)) \in R_{\mathcal{C}}\} \subseteq K[X] \rangle. \quad (2)$$

Let  $w_1, \dots, w_k$  be the row vectors of a generator matrix for a code, or more general, any set of row vectors that span the code  $\mathcal{C}$ . Let  $I$  be the ideal defined by

$$I = \langle \{w_1 - 1, \dots, w_k - 1\} \cup \{x_i^2 - 1 \mid i = 1, \dots, n\} \rangle \quad (3)$$

Since the set  $\{w_1, \dots, w_k\}$  generates  $\mathcal{C}$  it is clear that  $I = I(\mathcal{C})$ . Note that the ideal is a toric ideal, thus the structure of the Gröbner basis is close related to the combinatorics of the code (see [3]). The following algorithm computes reduced Gröbner basis for  $I(\mathcal{C})$ :

**Input:**  $F = \{w_1 - 1, w_2 - 1, \dots, w_r - 1\}$  and  $<$  a total degree compatible ordering.

**Output:** The reduced Gröbner basis  $G$  of the ideal  $\langle F \cup \{x_i^2 - 1 \mid i = 1, \dots, n\} \rangle$  w.r.t.  $<$ .

List :=  $[(1, 1), (1, w_i)_{i=1, \dots, r}, (1, x_i^2)_{i=1, \dots, n}]$  // the elements ordered following  $<$  in the second component

$G := \{ \}, N := [ ]$

while List  $\neq \emptyset$  do

$w := \text{NextTerm}(\text{List})$

  if  $w \notin T(G)$  then

$v' := w[2], j := \text{Member}(v', \{v_1, \dots, v_r\})$

    if  $j \neq \text{false}$  then

$G := G \cup \{w[1] - w_j\}$

      else  $r := r + 1, v_r := v', w_r := w[1], N := N \cup \{w_r\}$ ,

      List := InsertNexts( $w_r$ , List);

    end

  end

end

## References

- M. Borges-Quintana, M. Borges-Trenard and E. Martínez-Moro. On a Gröbner bases structure associated to linear codes. To appear in Journal of Discrete Mathematical Sciences & Cryptography. <http://arxiv.org/abs/math.AC/0506045>
- M. Borges-Quintana, M. Borges-Trenard, and E. Martnez-Moro. A general framework for applying FGLM techniques to linear codes. *AAECC 16, Lecture Notes in Computer Science*, 3857:76–86, 2006.
- M. Borges-Quintana, M. Borges-Trenard, P. Fitzpatrick and E. Martínez-Moro. On a Gröbner bases and combinatorics for binary codes. Submitted to Appl. Algebra Engrg. Comm. Comput. <http://arxiv.org/abs/math.CO/0509164>
- M. Borges-Quintana, M. A. Borges-Trenard, and F. Winkler. An application of the FGLM techniques to linear codes. In *Fourth Italian-Latin American Conference on Applied and Industrial Mathematics*, Inst. Cybern. Math. Phys., Havana, p. 280–286, 2001.
- M. Borges-Quintana, F. Winkler, and M. Borges-Trenard. FGLM Techniques Applied to Linear Codes – An Algorithm for Decoding Linear Codes. Techn. Rep. RISC-Linz, RISC - 00-14, J. Kepler Univ., Linz, Austria, 2000. <ftp://ftp.risc.uni-linz.ac.at/pub/techreports/2000/00-14.ps.gz>.
- J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, vol. 16(4), p. 329–344, 1993.
- M. G. Marinari, H. M. Möller, T. Mora. Gröbner Bases of Ideals Defined by Functionals with an Application to Ideals of Projective Points. *Applicable Algebra in Engineering, Communication and Computing*, vol. 4, p. 103–145, 1993.