DESCRIPTION OF MINIMUM WEIGHT CODEWORDS OF CYCLIC CODES BY ALGEBRAIC SYSTEMS

DANIEL AUGOT

Abstract. We consider cyclic codes of length n over $\mathbb{F}_q$, n being prime to q. For such a cyclic code C, we describe a system of algebraic equations, denoted by $\mathcal{S}_C(w)$, where w is a positive integer. The system is constructed from Newton's identities, which are satisfied by the elementary symmetric functions and the (generalized) power sum symmetric functions of the locators of codewords of weight w.

The main result is that, in a certain sense, the *algebraic* solutions of $\mathcal{S}_C(w)$ are in one-to-one correspondence with all the codewords of C having weight lower than w. In the particular case where w is the minimum distance of C, all minimum weight codewords are described by $\mathcal{S}_C(w)$.

Because the system $\mathcal{S}_C(w)$ is very large, with many indeterminates, no great insight can be directly obtained, and specific tools are required in order to manipulate the algebraic systems. For this purpose, the theory of *Gröbner bases* can be used. A Gröbner basis of $\mathcal{S}_C(w)$ gives information about the minimum weight codewords.

1. Introduction

The aim of this paper is to study minimum weight codewords of cyclic codes, from a practical point a view. The problem is the following: given a cyclic code C of length n over $\mathbb{F}_q$, (n prime to q), how can one "find" the minimum codewords of C. The term "find" has to explained: minimum weight codewords will appear as solutions to algebraic systems, and "finding" minimum weight codewords is "finding" solutions to such an algebraic system. "Finding" will turn to the process of computing a Gröbner basis, for the lexicographical order.

In this first section we recall the usual definitions used in the theory of cyclic codes, mainly the Mattson-Solomon (or the Fourier) transform. The definitions and notations will be kept as close as possible to [12]. Next, in the second section, we introduce the Newton identities and define an algebraic system, denoted $\mathcal{S}_C(w)$, constructed from these. The existence of solutions to this system is a *necessary* condition to the existence of codewords of weight w in C. The main result is presented in theorem 2.3, it correlates codewords and solutions to $\mathcal{S}_C(w)$.

Key words and phrases. Cyclic Codes, Fourier Transform, Algebraic Systems, Gröbner bases.

In the paper [2], we only used the systems $\mathcal{S}_C(w)$ as a necessary condition. Establishing that there is no solution to this system is proving the non-existence of codewords of weight less or equal than w in C. Now we are able to use the converse: solutions to $\mathcal{S}_C(w)$ correspond to codewords of weight less or equal than w. Whereas the equations were manipulated "by hand" in [1, 2] for finding contradiction in the system, theorem 2.3 enables to use a more complete algorithmic tool. We propose to use Gröbner bases for computing solutions to algebraic systems. Gröbner bases are convenient for the manipulation of algebraic systems, and allow big systems of equations to be dealt with automatically. Basic definitions and results are recalled in the third section. Finally, some examples are presented, to show the method at work.

1.1. Background. We denote by $\mathbb{F}_q$ the finite field with q elements, q being a power of a prime number p. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$. Let n be an integer prime to q. A *cyclic code* C of length n is an ideal in the algebra $\mathbb{F}_q[X]/(X^n-1)$, a word $(c_0, c_1, \dots, c_{n-1})$ being identified with the polynomial $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$. The *weight* of a word c is the number of non-zero coordinates of c.

Let α be a primitive n-th root of unity in the field $\mathbb{F}_{q'}$ of $\mathbb{F}_q$, $\mathbb{F}_{q'}$ being the splitting field of $X^n - 1$ over $\mathbb{F}_q$, i.e. $q' = q^m$ where m is the least positive integer such that $n \mid q^m - 1$. The *defining set* of C, denoted $I(C)$, is

$$I(C) = \{i \in [0, n-1] \mid \forall c \in C,\ c(\alpha^i) = 0\}.$$

The *cyclotomic classes* of q modulo n are the sets

$$cl(i) = \{i, qi, q^2 i, \dots\}, \quad i \in [0, n-1].$$

If α^i belongs to $I(C)$, so does α^{qi}, and thus $I(C)$ is an union of cyclotomic classes. A cyclic code is completely defined by its defining set. Changing the primitive root α amounts to permuting the coordinates of codewords, thus obtaining an equivalent code. For a given primitive root α, one can define the locators of a word:

Definition 1.1. Let $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ and let w be the weight of c. The *locators* of c, denoted by $X_1, X_2, \dots, X_w$, are

$$\{X_1, X_2, \dots. X_w\} = \{\alpha^j, \text{ for } j \text{ such that } c_j \neq 0\}.$$

The *locator polynomial* of c is the polynomial $\sigma(Z) \in \mathbb{F}_{q'}[Z]$, as below:

$$\sigma(Z) = \prod_{i=1}^{w}(1 - X_i Z).$$

We recall that the minimum distance of C (the lowest weight of non zero codewords in C) can be bounded from below by some useful bounds, e.g. the BCH bound, the Hartmann-Tseng bound or the Roos bound [11]. These bounds can be computed directly from the defining set of the code C.

1.2. Fourier transform. The Fourier transform of a word $c \in \mathbb{F}_q^n$ is also called the Mattson-Solomon polynomial of c. There is a one-to-one correspondence between words in $\mathbb{F}_q^n$ and their Mattson-Solomon polynomials. For describing minimum weight codewords, we shall describe the coefficients of their Mattson-Solomon polynomial. Algebraic properties of codewords are best seen in the coefficients of their Mattson-Solomon polynomial, instead in codewords themselves.

Definition 1.2. [12, 239] Let $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$, and let α be a primitive n-th root of unity in $\mathbb{F}_{q'}$. The *Mattson-Solomon polynomial* of c, denoted A, is:

$$A = \sum_{i=1}^{n} A_i Z^{n-i} \in \mathbb{F}_{q'}[Z] \text{ where } \forall i \in [1, n], \quad A_i = c(\alpha^i). \tag{1.1.1}$$

Theorem 1.1. [12, p 240] *Let $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ and $A(Z)$ the Mattson-Solomon polynomial of a. Then*

$$\forall i \in [0, n-1], \quad nc_i = A(\alpha^i).$$

As a consequence, the correspondence $c(X) \mapsto A(Z)$ is one-to-one. We shall alternatively use $(A_0, \ldots, A_{n-1})$ or $(A_1, \ldots, A_n)$, which is convenient since $A_0 = A_n$. We also consider A_{i+n} which is equal to A_i.

Proposition 1.1. [10, 218] *A polynomial $A(Z) \in \overline{\mathbb{F}}_q[Z]$ is the Mattson-Solomon polynomial of a word $c \in \mathbb{F}_q^n$ if and only if:*

$$\forall i \in [1, n], \quad A_{iq \bmod n} = A_i^q.$$

2. Codewords and Newton's identities

2.1. The (generalized) Newton identities.

Definition 2.1. Let $c \in \mathbb{F}_q^n$ be of weight w, and let $X_1, \ldots, X_w$ be the locators of c. The *elementary symmetric functions* of c, denoted $\sigma_0, \sigma_1, \ldots, \sigma_w$, are the elementary symmetric functions of the X_i's, that is,

$$\forall i \in [1, w], \quad \sigma_i = (-1)^i \sum_{1 \le j_1 < j_2 < \cdots < j_i \le w} X_{j_1} X_{j_2} \cdots X_{j_i}.$$

The elementary symmetric functions of a codeword c and the coefficients of the Mattson-Solomon polynomial of c are related by the (generalized) Newton identities.

Theorem 2.1. [12] *Let $c \in \mathbb{F}_q^n$ be a word of weight w, $A_1, \ldots, A_n$ the coefficients of the Mattson-Solomon polynomial of c and $\sigma_0, \sigma_1, \ldots, \sigma_w$ the elementary symmetric functions of c. Then the following identities hold:*

$$\forall i \ge 0, \quad A_{i+w} + \sigma_1 A_{i+w-1} + \cdots + \sigma_w A_i = 0. \tag{2.2.1}$$

Each of these equations is homogeneous in the X_i's, the X_i's being the locators. We number these equations $eq_w, \ldots, eq_i, \ldots$, eq_i being the equation homogeneous of degree i. The system 2.2.1 can be written using matrices:

$$C_{n,w}\begin{pmatrix} 1 \\ \sigma_1 \\ \vdots \\ \sigma_w \end{pmatrix} = 0, \tag{2.2.2}$$

where

$$C_{n,w} = \begin{pmatrix} A_{w+1} & A_w & \ldots & A_1 \\ \vdots & & & \\ A_{n+w} & A_{n+w-1} & \ldots & A_n \end{pmatrix},$$

since the equation eq_{n+i} is equal to the equation eq_i. An alternative form of the system 2.2.2 is the equation:

$$\tilde{A}(Z)\sigma(Z) = 0 \mod (Z^n - 1), \text{ where } \tilde{A}(Z) = \sum_{i=0}^{n} A_i Z^i. \tag{2.2.3}$$

The matrix $C_{n,w}$ is related to the weight of c, as indicates the following theorem[1].

Theorem 2.2. *Let $c \in \mathbb{F}_q^n$, and $A_0, \ldots, A_n$ be the coefficients of the Mattson-Solomon polynomial of c. Then the weight of c equals the rank of the circulant matrix*

$$C_c = \begin{pmatrix} A_0 & A_{n-1} & \cdots & A_1 \\ A_1 & A_0 & \cdots & A_2 \\ \vdots & & & \\ A_{n-1} & A_{n-2} & \cdots & A_0 \end{pmatrix}.$$

In fact $C_{n,w}$ is the sub-matrix of C_c which consists of the last $w+1$ columns of C_c.

2.2. The system $\mathcal{S}_C(w)$ and its solutions. In view of the proposition 1.1, and of the Newton identities, we define the following system of algebraic equations.

[1]This theorem is known as "Blahut's Theorem" in coding theory, since Blahut has shown the use of this theorem in coding theory, in [4], as pointed out by the referee.

Definition 2.2. Let C be a cyclic code over $\mathbb{F}_q$ of length n and let $I(C)$ be the defining set of C. We define the system $\mathcal{S}_C(w)$ as follows.

$$\mathcal{S}_C(w) = \begin{cases} A_{w+1} + A_w\sigma_1 + \cdots + A_1\sigma_w = 0, \\ A_{w+2} + A_{w+1}\sigma_1 + \cdots + A_2\sigma_w = 0, \\ \vdots \\ A_{n+w} + A_{n+w-1}\sigma_1 + \cdots + A_n\sigma_w = 0, \\ \forall i \in [0, n-1], \quad A_{qi \bmod n} = A_i^q, \\ \forall i \in [0, n-1], \quad A_{i+n} = A_i, \\ \forall i \in I(C), \quad A_i = 0. \end{cases} \tag{2.2.4}$$

In this system both A_i's and σ_i's are indeterminates. Thus the system defines an ideal in the ring $\mathbb{F}_q[A_0, \ldots, A_{n-1}, \sigma_1, \ldots, \sigma_w]$.

It is clear that existence of solutions to the system $\mathcal{S}_C(w)$ is a *necessary* condition to the existence of codewords of weight w. This was used in [2], where it was also established that the systems $\mathcal{S}_{BCH(59)}(59)$ and $\mathcal{S}_{BCH(61)}(61)$, in length 255 have no solutions. This completed a table of minimum distance of BCH codes presented in [12, page 267]. Dealing with the converse, we answer the question: what is the meaning of the algebraic solutions to $\mathcal{S}_C(w)$, or more precisely, do the σ_i's that are algebraic solutions to $\mathcal{S}_C(w)$ define locator polynomials of codewords? It turns out that the important indeterminates are the A_i's, rather than the σ_i's.

We shall describe the n-tuples $(A_0, \ldots, A_{n-1}) \in \overline{\mathbb{F}}_q$ which are solutions to $\mathcal{S}_C(w)$.

Definition 2.3. We say that $(A_0, \ldots, A_{n-1}) \in \overline{\mathbb{F}}_q$ is a *solution* to $\mathcal{S}_C(w)$ if there exists $(\sigma_1, \ldots, \sigma_w) \in \overline{\mathbb{F}}_q$ such that $(A_0, \ldots, A_{n-1}, \sigma_1, \ldots, \sigma_w)$ is a solution to $\mathcal{S}_C(w)$.

Theorem 2.3. *Let C be a cyclic code of length n. The n-tuples $(A_0, \ldots, A_{n-1}) \in \overline{\mathbb{F}}_q$ that are solutions to $\mathcal{S}_C(w)$ are the Fourier transform of the codewords of C of weight less than or equal to w.*

Proof. Let $(A_0, \ldots, A_{n-1}) \in \overline{\mathbb{F}}_q$ be such a solution. The equations

$$(\forall i \in [0, n-1],\ A_{qi \bmod n} = A_i^q)$$

imply that $(A_0, \ldots, A_{n-1})$ is the Fourier transform of some word c of $\mathbb{F}_q^n$, using proposition 1.1. The equations

$$(\forall i \in I(C),\ A_i = 0)$$

imply that c belongs to the code C.

One has to see that the weight w_0 of c is less or equal to w. Since there exists a w-tuple $(\sigma_1, \ldots, \sigma_w) \in \overline{\mathbb{F}}_q^w$ such that

$$C_{n,w} \begin{pmatrix} 1 \\ \sigma_1 \\ \vdots \\ \sigma_w \end{pmatrix} = 0,$$

then, completing with 0's:

$$C_c \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \sigma_1 \\ \vdots \\ \sigma_w \end{pmatrix} = 0.$$

Since C_c is a circulant matrix, we get

$$C_c \begin{pmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & & \sigma_1 \\ 0 & 1 & & \vdots \\ 1 & \sigma_1 & & \sigma_w \\ \sigma_1 & \sigma_2 & & 0 \\ \vdots & \vdots & & \vdots \\ \sigma_w & 0 & \cdots & 0 \end{pmatrix} = 0.$$

This proves that all columns of the matrix C_c are in the vector space generated by the w last columns of C_c. Thus the rank of C_c is smaller than or equal to w, and by theorem 2.2, the weight of c is smaller than or equal to w. $\square$

We now describe the w-tuples $(\sigma_1, \dots, \sigma_w)$ that are solutions to $\mathcal{S}_C(w)$.

Definition 2.4. For each solution $(A_0, \dots, A_{n-1})$ to $\mathcal{S}_C(w)$, let $\mathcal{F}_{(A_0,\dots,A_{n-1})}$ be the space of the w-tuples $(\sigma_1, \dots, \sigma_w)$, associated to $(A_0, \dots, A_{n-1})$, such that $(\sigma_1, \dots, \sigma_w, A_0, \dots, A_{n-1})$ is a solution to $\mathcal{S}_C(w)$.

Theorem 2.4. *Let $(A_0, \dots, A_{n-1})$ be a solution to $\mathcal{S}_C(w)$, and c be the codeword of weight $w_0 \leq w$, given by the inverse Fourier transform of $(A_0, \dots, A_{n-1})$. Let $\sigma_c(Z)$ be the locator polynomial of c. Then the set $\mathcal{F}_{(A_0,\dots,A_{n-1})}$ associated to $(A_0, \dots, A_{n-1})$, is:*

$$\mathcal{F}' := \{(\sigma_1, \dots, \sigma_w) \in \overline{\mathbb{F}}_q^w \mid \quad \sigma_c(Z) \textit{ divides } \left(1 + \sum_{i=1}^{w} \sigma_i Z^i\right)\}.$$

Proof. It is clear that $\mathcal{F}_{(A_0,\dots,A_{n-1})}$ is an affine space of dimension $w - w_0$, because the coefficients of $\sigma_c(Z)$ belong to $\mathcal{F}_{(A_0,\dots,A_{n-1})}$, and the rank of $C_{n,w}$ is w_0. The dimension of the affine space $\mathcal{F}'$ is $w - w_0$ and the coefficients of $\sigma_c(Z)$ belongs to $\mathcal{F}'$. Now let $(\sigma_1, \dots, \sigma_w) \in \mathcal{F}'$ and let $\sigma(Z)$ be the polynomial $1 + \sum_{i=1}^{w} \sigma_i Z^i$. Then $\sigma(Z) = p(Z)\sigma_c(Z)$ for some polynomial $p(Z)$ and

$$A(Z)\sigma(Z) = A(Z)\sigma_c(Z)p(Z) = 0 \mod Z^n - 1,$$

since $\sigma_c(Z)$ satisfies the alternative form 2.2.3 of the Newton identities. Thus $\sigma(Z)$ also satisfies 2.2.3, and thus $(\sigma_1, \dots, \sigma_w)$ belongs to $\mathcal{F}_{(A_0,\dots,A_{n-1})}$ $\square$

Corollary 2.1. *Let C be a cyclic code of length n, of minimum distance d. The number of solutions to $\mathcal{S}_C(d)$ is finite. Each solution $(A_0, \ldots, A_{n-1})$ is the Fourier transform of a minimum weight codeword. Each solution $(\sigma_1, \ldots, \sigma_w)$ is the set of coefficients of the locator polynomial of a minimum weight codeword.*

The theorems 2.3 and 2.4 completely describe the solutions of the system $\mathcal{S}_C(d)$, in terms of codewords of C. The important consequence is the following. Given a cyclic code C of length n, such that there exists no codewords of weight less than w (from the BCH bound for instance), if there are solutions to $\mathcal{S}_C(w)$, then the minimum distance of C is w. In that case the number of these solutions is equal to the number of minimum weight codewords of C. Furthermore, all the polynomials $1 + \sum_{i=1}^{w} \sigma_i Z^i$ in which $(\sigma_1, \ldots, \sigma_w)$ is a solution to $\mathcal{S}_C(w)$ are locators polynomials of minimum weight codewords.

To be able to use this correspondence between solutions of algebraic systems and words of cyclic codes, one must be able to deal efficiently with algebraic systems. The next section introduces *Gröbner bases*, which are a commonly used tool for studying these systems.

3. Gröbner bases

The theory of Gröbner bases is well developed and quite useful. One can say that, as soon as practical problems with algebraic systems are encountered, then Gröbner bases come into play. We introduce here only the concepts and results needed for our purpose, without proofs. No new material will be found here about Gröbner bases. Rather complete books on the subject are [3] and [6], while in [8] a more practical point of view is adopted.

3.1. Definition. Let k be an algebraically closed field. The number of zeros of a univariate polynomial P, counted with multiplicities, equals the degree of P, and the number of common solutions to the polynomials $P_1, \ldots, P_i$ equals the degree of the gcd of the P_i's. When multivariate polynomials are considered, $k[\overline{Y}] = k[Y_1, \ldots, Y_n]$ is not a principal ideal domain. The notion of Gröbner bases can be seen as a generalization of gcd's of univariate polynomials. All the notions related to Gröbner bases depends on some ordering on $\mathbb{N}^n$. We shall make use of the *lexicographical* order on $\mathbb{N}^n$.

Definition 3.1. The *lexicographical* order on $\mathbb{N}^n$, denoted $\underset{\text{lex}}{\leq}$, is defined as follows

$$(a_1, a_2, \ldots, a_n) \underset{\text{lex}}{\leq} (b_1, b_2, \ldots, b_n) \iff \exists\ s \in [1, n],\ (\forall i < s,\ a_i = b_i) \text{ and } (a_s < b_s).$$

Definition 3.2. Let $f = \sum f_a \overline{Y}^a$. The *leading monomial* of f is $\overline{Y}^a$, where a is maximal (for $\underset{\text{lex}}{\leq}$) such that $f_a \neq 0$. The *leading term* of f, denoted $\exp(f)$, is the exponent of the leading monomial of f. The *initial* of f, denoted $in(f)$ is $c_{\exp(f)} \overline{Y}^{\exp(f)}$.

Theorem 3.1. *Let I be an ideal of $k[\overline{Y}]$. The set*

$$\{\exp(f), f \in I\}$$

is denoted $E(I)$. There exists a finite set $S \subset \mathbb{N}^n$ such that

$$E(I) = \bigcup_{\alpha \in S} (\alpha + \mathbb{N}^n). \tag{3.3.1}$$

A set $B \subset I$ of polynomials is a Gröbner basis *of I if the set of leading terms of the polynomials of B satisfy* 3.3.1*. A* minimal *Gröbner basis is a Gröbner basis of minimal cardinality.*

Thus the set $E(I)$ of an ideal I is the set of the leading terms of all polynomials in I. Previous theorem states that there exists a finite number of polynomials in I such that their leading terms are a basis for $E(I)$.

3.2. Main properties of Gröbner bases. When a Gröbner basis B of the ideal I is known, many problems can be addressed using Hironaka's division. In the following theorem, we only use the "remainder" of the division, which I call the reduction map.

Proposition 3.1. *Let I be an ideal of $k[\overline{Y}]$, and let $(f_1, \ldots, f_s)$ be a Gröbner basis of I. There exists a* reduction map *$\mathcal{R}\{f_1, \ldots, f_s\} : k[\overline{Y}] \to k[\overline{Y}]$, such that :*

$$\forall f \in k[\overline{Y}], \exp(f\mathcal{R}I) \in \mathbb{N}^n \setminus E(I).$$

This map is independent of the choice of the Gröbner basis.

Theorem 3.2. *Let $B = \{f_1, \ldots f_s\}$ be a Gröbner basis of I, we note $f\mathcal{R}I$ for $f\mathcal{R}\{f_1 \ldots f_s\}$. Then $f \in I$ if and only if $f\mathcal{R}I = 0$.*

Hironaka's division enables also to show that a Gröbner basis of I is a set of generating polynomials of I (see [6, 3])

Definition 3.3. Let I be an ideal of $k[\overline{Y}]$. A Gröbner basis $(f_1, \ldots, f_s)$ of I is said to be *reduced* if and only if:

(1) $inf_i = Y^{\exp f_i}$, $i \in [1, s]$,
(2) $f_i\mathcal{R}\{f_1, \ldots, \hat{f_i}, \ldots, f_s\} = f_i$,

where $(f_1, \ldots, \hat{f_i}, \ldots, f_s)$ denotes $(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_s)$.

A reduced Gröbner basis can be seen as a Gröbner basis in which each polynomial is monic and is reduced modulo the ideal generated by the other ones.

Proposition 3.2. *Two reduced Gröbner basis of the ideal I are equal, modulo a permutation of indices.*

So we can talk about *the* Gröbner basis of the ideal I, meaning a reduced Gröbner basis of I. Knowing the Gröbner basis of I is knowing the set $E(I)$ of exponents of I. Let I be an ideal generated by $g_1, \ldots, g_l$ (not necessarily a Gröbner basis). Then the equations $g_1 = \cdots = g_l = 0$ define an algebraic system of equations.

Proposition 3.3. *Let I be an ideal of $k[\overline{Y}]$ generated by $(f_1, \ldots, f_s)$. If*

$$\mathrm{Card}(\mathbb{N}^n \setminus E(I)) < \infty,$$

then the set S of solutions to the system $(f_1, \ldots, f_s)$ is finite, and the cardinality s of S is such that

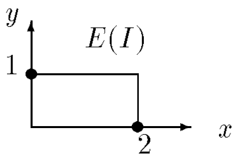
$$s \leq \mathrm{Card}(\mathbb{N}^n \setminus E(I)).$$

The number of solutions to the system $(f_1, \ldots, f_s)$, counted with multiplicities, is exactly $\mathrm{Card}(\mathbb{N}^n \setminus E(I))$.

Example 3.1. Let $k = \mathbb{F}_3$, and consider the ideal generated by the polynomials $x^2 + y^2 - 1$, $x - y + 1$. The Gröbner basis, for the lexicographical ordering $y > x$, is

$$y - x - 1, x^2 + x. \tag{3.3.2}$$

The set $E(I)$ can be shown as:



Since there is a finite number of points, which is two, under $E(I)$, the system of equations 3.3.2 has two solutions.

Thus, given a system of equations $p_1, \ldots, p_k$, a Gröbner basis of the ideal I generated by the polynomials $p1, \ldots, p_k$ gives us the knowledge of $E(I)$, and then we are able to know if the system has solutions, and to know the number of solutions if it is finite.

As a final note, Gröbner bases can be computed. Buchberger's algorithm is the basic scheme for computing Gröbner bases. It is well known [3, 8] and, for instance, one can use the implementation provided by most Computer Algebra systems. However, for our purpose, the reader is warned that we had to use a more powerful tool, called `Gb`, designed by Jean-Charles Faugère [7].

4. Examples

Here we give some examples of Gröbner bases for the system $\mathcal{S}_C(w)$ for the minimum distance of some codes. Note that the number of variables for the system $\mathcal{S}_C(w)$, for a code of length n is $n + w$. Before feeding the Buchberger's algorithm with our system, we do the following manipulations:

- Choose one representative i_0 for the cyclotomic class $cl(i_0)$. Then the A_i's, for i belonging to $cl(i_0)$, are replaced by the convenient power of A_{i_0}.
- Let the A_i equal 0 for $i \in I(C)$ (that is, they do not appear in the system).
- Replace A_{i+n} by A_i.

As an example, consider the cyclic code C of length 7 over $\mathbb{F}_2$, with defining set $\{1\}$. The cyclotomic classes of 2 modulo 7 are $\{\{0\},\{1,2,4\},\{3,6,5\}\}$.

The system $\mathcal{S}_C(3)$ is transformed as follows:

$$\left\{\begin{array}{c} A_4+A_3\sigma_1+A_2\sigma_2+A_1\sigma_3=0\\ A_5+A_4\sigma_1+A_3\sigma_2+A_2\sigma_3=0\\ A_6+A_5\sigma_1+A_4\sigma_2+A_3\sigma_3=0\\ A_7+A_6\sigma_1+A_5\sigma_2+A_4\sigma_3=0\\ A_8+A_7\sigma_1+A_6\sigma_2+A_5\sigma_3=0\\ A_9+A_8\sigma_1+A_7\sigma_2+A_6\sigma_3=0\\ A_{10}+A_9\sigma_1+A_8\sigma_2+A_7\sigma_3=0\\ A_0^2=A_0 \end{array}\right. \to \mathcal{S}_C(3) : \left\{\begin{array}{rcl} A_3\sigma_1 &=& 0\\ A_3^4+A_3\sigma_2 &=& 0\\ A_3^2+A_3^4\sigma_1+A_3\sigma_3 &=& 0\\ A_0+A_3^2\sigma_1+A_3^4\sigma_2 &=& 0\\ A_0\sigma_1+A_3^2\sigma_2+A_3^4\sigma_3 &=& 0\\ A_0\sigma_2+A_3^2\sigma_3 &=& 0\\ A_3+A_0\sigma_3 &=& 0\\ A_0^2 &=& A_0 \end{array}\right. .$$

4.1. First example. We consider the binary cyclic code C of length 63 with defining set

$$I(C)=cl(1)\cup cl(5)\cup cl(7)\cup cl(9)\cup cl(11)\cup cl(13)\cup cl(23)\cup cl(27).$$

The sequence $\{7,8,9,10,11\}$ belongs to $I(C)$, thus the minimum distance of C is greater than or equal to 6. The minimal Gröbner basis for $\mathcal{S}_C(6)$ is:

(4.4.1)
$$\left[\sigma_6+{A_3}^2,\ \sigma_5,\ \sigma_4,\ \sigma_3+A_3,\ \sigma_2,\ \sigma_1,\ A_{31},\ A_{21}+{A_3}^7,\ A_{15}+{A_3}^5,\ {A_3}^{21}+1,\ A_0\right]$$

Since the Gröbner basis does not reduce to $\{1\}$, the system has solutions. Thus there are codewords of weight 6 in C, and the minimal distance of C is 6. There are 21 solutions, so there are 21 minimum weight codewords. All these codewords belongs to the subcode with defining set $I(C)\cup\{0,31\}$ (Note that the fact $A_0=0$, which is obvious because the weight is even, has been retrieved by the computation of the Gröbner basis).

All the coefficients of the Mattson-Solomon polynomial of minimum weight codewords can be expressed in terms of A_3, which satisfies $A_3^{21}=1$. The locator polynomials are of the form

$$\sigma_c(Z)=A_3^2Z^6+A_3Z^3+1.$$

Since $A_3^{21}=1$, one can write $A_{21}=\gamma^3$, for some $\gamma\in\mathbb{F}_{64}^\star$. Thus $\sigma_c(Z)=Y^2+Y+1$, where $Y=(\gamma Z)^3$. The polynomial Y^2+Y+1 has two roots, namely α^{21} and α^{42}, and the locators of the minimum weight codewords are

$$\{\alpha^7/\gamma,\alpha^{28}/\gamma,\alpha^{56}/\gamma,\alpha^{14}/\gamma,\alpha^{49}/\gamma,\alpha^{35}/\gamma\}.\quad \gamma\in\mathbb{F}_{64}^\star.$$

Letting A_3 equal 1 (that is, $\gamma=1$), we get a codeword such that $A_i\in\mathbb{F}_2$, $i\in[0,62]$. This codeword is an idempotent, which admits 21 conjugates by cyclic shift, which are all the minimum weight codewords.

4.2. A dual of a BCH code. We consider the dual of the BCH code of length 63 and designed distance 7. By the BCH bound it can be seen that minimum distance is bounded from below by 16. Computing a Gröbner basis for $\mathcal{S}_C(16)$, one gets:

$$[\sigma_{16} + {A_{15}}^{20}\ A_{31} + {A_{15}}^{19}\ {A_{23}}^2,\ \sigma_{15} + A_{15},\ \sigma_{14} + {A_{15}}^{12}\ A_{23},\ \sigma_{12},\ \sigma_{10},$$
$$\sigma_8 + {A_{15}}^{20}\ A_{23},\ \sigma_6,\ \sigma_4,\ \sigma_2,\ {A_{31}}^3 + {A_{15}}^{20}\ {A_{23}}^2\ {A_{31}}^2 + {A_{15}}^2,\ {A_{23}}^3 + {A_{15}}^{13},$$
$${A_{15}}^{21} + 1]$$

There are $189 = 3\times3\times21$ solutions, and thus 189 minimum weight codewords. These codewords do not belong to any proper cyclic subcode, a fact which can be seen by checking that each of the equations $A_{15} = 0$, or $A_{23} = 0$, or $A_{31} = 0$ is impossible for a minimum weight codeword. There are no minimum weight idempotents: a idempotent should satisfy $A_{15} = 1$, which implies $A_{23} = 1$ and $A_{31}^3 + A_{31}^2 + 1 = 0$, which is impossible in $\mathbb{F}_2$.

4.3. A Quadratic residue code. Let C be the quadratic residue code of length 31 (it is the cyclic code with defining set $\{1, 5, 7\}$). The minimum distance is 7, and the Gröbner basis for $\mathcal{S}_C(7)$ is

$$[\sigma_7 + {A_{11}}^4{A_3}^{29} + {A_{11}}^2{A_3}^{26}, \sigma_6 + {A_3}^2, \sigma_5 + A_{11}{A_3}^{29}, \sigma_4 + {A_{11}}^4\ {A_3}^{28} + {A_{11}}^2{A_3}^{25},$$
$$\sigma_3 + A_3, \sigma_2 + A_{11}{A_3}^{28}, \sigma_1, A_{15} + {A_{11}}^3{A_3}^{25} + {A_3}^5,$$
$${A_{11}}^5 + {A_{11}}^4{A_3}^{14} + {A_{11}}^2{A_3}^{11} + A_{11}{A_3}^{25} + {A_3}^8, {A_3}^{31} + 1]$$

There are 155 solutions and thus 155 minimum weight codewords. They do not belong to any cyclic subcode, and can not be idempotent.

The subcode of C with even weight, i.e. the cyclic code C_e with defining set $\{1, 5, 7, 0\}$ has minimum distance 8. A Gröbner basis for $\mathcal{S}_{C_e}(8)$ is

$$[\sigma_8 + {A_{11}}^{14}{A_3}^3 + {A_{11}}^{12} + {A_{11}}^{11}{A_3}^{14} + {A_{11}}^9{A_3}^{11} + {A_{11}}^6{A_3}^{22} + {A_{11}}^5{A_3}^5,$$
$$\sigma_7 + {A_{11}}^{14}{A_3}^{13} + {A_{11}}^{13}{A_3}^{27} + {A_{11}}^{11}{A_3}^{24} + {A_{11}}^8{A_3}^4 + {A_{11}}^7{A_3}^{18} + {A_{11}}^3{A_3}^{12} + {A_3}^{23},$$
$$\sigma_6 + {A_3}^2,$$
$$\sigma_5 + {A_{11}}^{14}{A_3}^2 + {A_{11}}^{12}{A_3}^{30} + {A_{11}}^{11}{A_3}^{13} + {A_{11}}^9{A_3}^{10} + {A_{11}}^6{A_3}^{21} + {A_{11}}^5{A_3}^4 + A_{11}{A_3}^{29},$$
$$\sigma_4 + {A_{11}}^{14}{A_3}^{12} + {A_{11}}^{13}{A_3}^{26} + {A_{11}}^{11}{A_3}^{23} + {A_{11}}^8{A_3}^3 + {A_{11}}^7{A_3}^{17} + {A_{11}}^3{A_3}^{11} + {A_3}^{22},$$
$$\sigma_3 + A_3,$$
$$\sigma_2 + {A_{11}}^{14}A_3 + {A_{11}}^{12}{A_3}^{29} + {A_{11}}^{11}{A_3}^{12} + {A_{11}}^9{A_3}^9 + {A_{11}}^6{A_3}^{20} + {A_{11}}^5{A_3}^3 + A_{11}{A_3}^{28},$$
$$\sigma_1,$$
$$A_{15} + {A_{11}}^{13}{A_3}^9 + {A_{11}}^{12}{A_3}^{23} + {A_{11}}^{10}{A_3}^{20} + {A_{11}}^9{A_3}^3 + {A_{11}}^8{A_3}^{17} + {A_{11}}^7$$
$$+ {A_{11}}^6{A_3}^{14} + {A_{11}}^5{A_3}^{28} + {A_{11}}^4{A_3}^{11} + A_{11}{A_3}^{22},$$
$${A_{11}}^{15} + {A_{11}}^{14}{A_3}^{14} + {A_{11}}^{12}\ {A_3}^{11} + {A_{11}}^{11}{A_3}^{25} + {A_{11}}^{10}{A_3}^8 + {A_{11}}^8{A_3}^5 + {A_{11}}^6{A_3}^2$$
$$+ {A_{11}}^4{A_3}^{30} + {A_{11}}^3{A_3}^{13} + {A_{11}}^2{A_3}^{27} + {A_3}^{24},$$
$${A_3}^{31} + 1]$$

There are $465 = 31 \times 15$ solutions. The minimal weight codewords do not belong to a cyclic subcode, and are not idempotent. This code has been studied in [5], where the complete distribution of the weight has been established. For the minimum weight codewords, the results are the same.

5. Concluding remarks

We have transformed a problem from coding theory (finding codewords in a cyclic code), into a purely algebraic one (finding solutions to an algebraic system). The most interesting case is when w is the minimum distance of C. We want to emphasize that the Gröbner basis contains a lot of information about minimum weight codewords. The main drawback of this method is the high complexity of the Buchberger's algorithm. It is stated to be $d^{O(m^2)}$ [9], where d is the maximum degree of the generators of the ideal, and m the number of variables, and $d^{O(m)}$ for a particular family of systems. Fortunately, it appears that the systems $\mathcal{S}_C(w)$ are solved at a cost much lower than this theoretical complexity. Yet the general Buchberger algorithm can be modified in many ways, by choosing different strategies, and a "good" strategy has to be found for the very particular systems $\mathcal{S}_C(w)$, for our method to be practical for longer codes.

Acknowledgments

The author wish to think Jean-Charles Faugère, at LITP, Université Paris VI, for the system *Gb*, a tool for computing Gröbner Bases [7], which could compute bases for the systems $\mathcal{S}_C(w)$.

References

1. D. Augot, P. Charpin, and N. Sendrier, *Weights of some binary cyclic codes throughout the newton's identities*, Eurocode' 90 (G. Cohen and P. Charpin, eds.), Springer-Verlag, 1990.
2. ______, *Studying the locator polynomial of minimum weight codewords of BCH codes*, IEEE Transaction on Information Theory **38** (1992), no. 3, 960–973.
3. T. Becker and V. Weispfenning, *Groebner bases, a computationnal approach to commutative algebra*, Springer-Verlag, 1993.
4. Richard E. Blahut, *Transform techniques for error control codes*, IBM J. Res. Dev. **23** (1979), 299–315.
5. P. Camion, B. Courteau, and A. Monpetit, *Coset weight enumerators of the extremal self-dual binary codes of length 32*, , Lecture Notes in Computer Science, Springer-Verlag, 1992, to appear.
6. David Cox, John Little, and Donal O'Shea, *Ideal, varieties, and algorithms*, Springer Verlag, 1992.
7. Jean-Charles Faugère, *Résolution de systèmes d'équations algébriques avec GB*, Ph.D. thesis, Université Paris VI, LITP, 1993, In preparation.
8. K. O. Geddes, S. R. Czapor, and G. Labahn, *Algorithms for computer algebra*, Kluwer Academic Publishers, 1992.
9. Daniel Lazard, *Systems of algebraic equations (algorithms and complexity)*, Proceedings of Cortona Conference, University of Carolina Press, 1993.
10. W. W. Peterson and E. J. Weldon Jr., *Error-correcting codes*, 2 ed., MIT Press, 1986.
11. J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes*, IEEE Transactions on Information Theory **IT-32** (1986), no. 1, 23–40.
12. F.J. Mac Williams and N.J.A. Sloane, *The theory of error correcting codes*, North-Holland, 1986.

Daniel Augot, Projet Codes, INRIA Rocquencourt, Domaine de Voluceau, BP105, 78153, Le Chesnay Cedex
E-mail address: Daniel.Augot@inria.fr