# Algebraic Characterization of Minimum Weight Codewords of Cyclic Codes

Daniel Augot

**Abstract**

We consider primitive cyclic codes of length $n$ over $GF(q)$, where $n = q^m - 1$, and for any such code with defining set $I(C)$, we define a system of algebraic equations, $\mathcal{S}_{I(C)}(w)$, constructed with the Newton identities for the weigth $w$.

We prove that *algebraic solutions* of this system are in correspondance with all codewords of $C$ of weight lower than $w$. In the particular case when there are no codewords of weight lower than $w$, the number of solutions of $\mathcal{S}_{I(C)}(w)$ is exactly the number of codewords of $C$ of weight $w$.

To deal effectively with the system $\mathcal{S}_{I(C)}(w)$, we compute a *groebner basis* of this system, which gives pertinent information on minimum weight codewords. A few examples are given.

# 1 Words of $GF(q)^n$ and their Fourier transform

## 1.1 Notation

We denote $GF(q)$ the finite field of size $q$, $q$ being a power of a prime number $p$. We consider primitive cyclic codes of length $n = q^m - 1$. A primitive $n$th root $\alpha$ of the unity is given in $GF(q^m)$. We denote $X_1, \ldots, X_w$ the locators of a word $c = (c_0, \ldots, c_n)$ of weight $w$, and the polynomial

$$\sigma(Z) = 1 + \sigma_1 Z + \cdots + \sigma_w Z^w = \prod_{i=1\ldots w} (1 - X_i Z)$$

is the locator polynomial of $c$, where $\sigma_1, \ldots, \sigma_w$ are the elementary symmetric functions of the locators of $c$. Let $c_{i_1}, \ldots, c_{i_w}$ be the non-zero coordinates of $c$, in correspondance with $X_1, \ldots, X_w$ (that is, $X_j = \alpha^{i_j}$), we denote $A_i$, $i \geq 0$, the generalized power sum functions of $X_1, \ldots, X_w$ weighted by $c_{i_1}, \ldots, c_{i_w}$ [6]. A cyclic code $C$ is defined by its defining-set $I(C)$:

$$I(C) = \{i \in [0, n-1],\ \alpha^i \text{ is a zero of the generating polynomial of } C\}.$$

## 1.2 Fourier transform of words of length $n$

We use the terminology of *Mattson-Solomon* polynomial for the Fourier transform of a word $c$ [6, page 239]. The coefficients of the Mattson-Solomon polynomial of $c$ are equals to the generalized power sum symmetric functions, and thus are also denoted $A_i$.

We shall use the Blahut theorem, as given in [7].

**Theorem 1** *Let $c$ be a word of length $n$, and $A_i$, $i = 1, ..., n$ be the Mattson-Solomon coefficients of $c$. The weight of $c$ equals the rank of the matrix*

$$CIRC(c) = \begin{bmatrix} A_{n-1} & \cdots & A_1 & A_0 \\ A_0 & A_{n-1} & \cdots & A_1 \\ \vdots & & & \\ A_{n-2} & A_{n-3} & \cdots & A_{n-1} \end{bmatrix}. \tag{1}$$

Remember that a word $c$ is in $C$ if and only if $A_i = 0$, $i \in I(C)$.

## 2 A necessary condition

We recall the generalized Newton's identities.

**Proposition 1 ([6])** *Let $X_1, \ldots, X_w$ be $w$ ideterminates, and let $\sigma_1, \ldots, \sigma_w$ be the elementary symmetric functions of $X_1, \ldots, X_w$, and $A_i$, $i \geq 0$, be the generalized power-sum functions of $X_1, \ldots, X_w$. The following identities hold*

$$A_{w+i} + A_{w+i-1}\sigma_1 + \cdots + A_i\sigma_w = 0, \qquad i \geq 1.$$

*These identities are the* generalized Newton's identities.

Let $X_1, \ldots, X_w$ be the locators of a codeword of weight $w$, and let $\sigma_1, \ldots, \sigma_w$ be the elementary symmetric functions of the locators of $c$, and $A_0, \ldots, A_{n-1}$ be the generalized power sum functions of $X_1, \ldots, X_w$ relatively to $c_{i_1}, \ldots, c_{i_w}$. If $c$ is in the code with defining set $I(C) = \{i_1, \ldots, i_l\}$ then $(\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1})$ is a solution of

$$\begin{cases} A_{w+1} + A_w\sigma_1 + \cdots + A_1\sigma_w = 0 \\ A_{w+2} + A_{w+1}\sigma_2 + \cdots + A_2\sigma_w = 0 \\ \vdots \\ A_{w+n} + A_{w+n-1}\sigma_1 + \cdots + A_n\sigma_w = 0 \\ A_{qi \bmod n} = A_i^q, \qquad i = 0, \ldots n-1 \\ A_{i+n} = A_i, \qquad i = 0, \ldots w \\ A_{i_1} = A_{i_2} = \cdots = A_{i_l} \end{cases} \tag{2}$$

**Definition 1** *Let $C$ be a cyclic code with defining set $I(C)$, let $\bar{GF}(Q)$ denote the algebraic closure of $GF(q)$ and let $\mathcal{S}_{I(C)}(w)$ be the system 2. An* algebraic solution *of $\mathcal{S}_{I(C)}(w)$ is $(\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1}) \in \bar{GF}(Q)^{n+w}$ which satisfies $\mathcal{S}_{I(C)}(w)$.*

Thus:

**Proposition 2** *Let $C$ be a cyclic code with defining $I(C)$. If the system $\mathcal{S}_{I(C)}(w)$ has no algebraic solution, then there is no codewords of weight $w$ in $C$.*

The use of the Newton's identities as a necessary condition has been considered in [1], to prove that the BCH code of length 255 and designed distance 59 (resp. 61) has minimum distance 61 (resp. 63).

The aim of this paper is to show that the system can be seen as a suffisant system, as will be shown by theorem 2.

## 3 The converse

**Definition 2** *We say that a n-uple* $(A_0, \ldots, A_{n-1})$ *is an* algebraic solution *of* $\mathcal{S}_{I(C)}(w)$ *if there exists a w-uple* $(\sigma_1, \ldots, \sigma_w) \in G\bar{F}(q)$ *such that* $(\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1})$ *is an algebraic solution of* $\mathcal{S}_{I(C)}(w)$.

**Theorem 2** *Let* $(A_0, \ldots, A_{n-1})$ *be an algebraic solution of* $\mathcal{S}_{I(C)}(w)$. *Then* $(A_0, \ldots, A_{n-1})$ *are the Mattson-Solomon coefficients of a codeword of* $C$ *of weight* $\leq w$. *If there is no codewords of weight strictly less than* $w$, *than the number of solutions of* $\mathcal{S}_{I(C)}(w)$ *equals the number of codewords of* $C$ *of weight* $w$.

*Proof* It is easy to show that $(A_0, \ldots, A_{n-1})$ are the Fourier transform of some codeword $c$ of $C$. It remains to prove that the weight $w_0$ of $C$ is lower than $w$. Using the fact that there exists $(\sigma_1, \ldots, \sigma_w)$ such that $(\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1})$ satisfies $\mathcal{S}_{I(C)}(w)$, one can show that the rank of the matrix

$$CIRC(c) = \begin{bmatrix} A_{n-1} & \cdots & A_1 & A_0 \\ A_0 & A_{n-1} & \cdots & A_1 \\ \vdots & & & \\ A_{n-2} & A_{n-3} & \cdots & A_{n-1} \end{bmatrix}$$

is lower than $w$. Thus the weight of $c$ is lower than $w$, by theorem 1. □

## 4 An example

To deal with the algebraic system $\mathcal{S}_{I(C)}(w)$, we compute a *groebner basis* of the ideal generated by the polynomials of the system $\mathcal{S}_{I(C)}(w)$. We shall not introduce all the material for dealing with groebner bases, and refer to [4, 5, 2]. For our concern, a groebner basis of an ideal is a privilegied system of generators, which gives some insight on the ideal: it is possible to determinate if the system has solutions (solutions exists if and only if the groebner basis is not (1)), and to find the number of solutions.

Here is an 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 BCH bound shows that the minimum distance of $C$ is greater than 6. Writing the system $\mathcal{S}_{I(C)}(6)$, and computing a groebner basis of $\mathcal{S}_{I(C)}(6)$, we get:

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

and thus:

1. There are solutions, so there are codewords of weight 6. There are 21 such codewords, since the number of solutions is 21.
2. All these solutions lie in the subcode with defining set $I(C) \cup \{31\}$.
3. Letting $A_3$ equals to 1, we get a minimum weight idempotent, which only admit 21 conjugates by shifting, which are all the minimum weight codewords. The locator polynomial of the idempotent is $Z^6 + Z^3 + 1$.

# 5 Conclusion

We have tranformed a problem from coding theory into a purely algebraic one. We do not claim to easily solve the coding theory problem by this way, but there exists algorithms for computing groebner bases, which are very powerful objects. The very high complexity of these algorithms limits the application of this algebraic approach.

# References


[1] D. Augot, P. Charpin, and N. Sendrier. Studying the locator polynomial of minimum weight codewords of bch codes. *IEEE Transaction on Information Theory*, 38(3):960–973, 1992.

[2] T. Becker and V. Weispfenning. *Groebner Bases, a Computationnal Approach to Commutative Algebra*. Graduate Texts in Mathematics. Springer-Verlag, 1993.

[3] Jean-Charles Faugère. *Résolution de systèmes d'équations algébriques avec GB*. PhD thesis, Université Paris VI, LITP, 1993. En préparation.

[4] K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, 1992.

[5] Daniel Lazard. Systems of algebraic equations (algorithms and complexity). In *Proceedings of Cortona Conference*. University of Carolina Press, 1993.

[6] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error Correcting Codes*. North-Holland, 1986.

[7] T. Schaub. *A Linear Complexity Approach to Cyclic Codes*. PhD thesis, Swiss Federal Institute of Technology, Zuerich, 1988.