Algebraic Solutions of Newton's identities for cyclic codes

Daniel Augot
INRIA

Abstract — **This paper consider the use of Newton's identities for establishing properties of cyclic codes. The main tool is to consider these identities as equations, and to look for the properties of the solutions.**

First these equations have been considered as necessary conditions for establishing non existence properties of cyclic codes, such as the non existence of codewords of a given weight.

The properties of these equations are studied, and the properties of the solution to the algebraic system are given. The main theorem is that codewords in a hamming sphere around a given word can be characterized by algebraic conditions. This theorem enables to describe the minimum codewords of a given cyclic codes, by algebraic conditions. The equations are solved using the Buchberger's algorithm for computing a Groebner basis.

Examples are also given with alternant codes, and with a non linear code.

I. Introduction

We consider words of length n over $GF(q)$, n being prime to q. A primitive root α is fixed. The word $c = (c_0, \ldots, c_{n-1})$ is identified with the polynomial $c_0 + c_1 X + \ldots + c_{n-1} X^{n-1}$ mod $X^n - 1$. The *Fourier Transform* of $c \in GF(q')^n$, denoted $\phi(c)$, is $A = (A_0, A_1, \ldots, A_{n-1})$, $A_i = a(\alpha^i)$, $i = 0 \ldots n-1$.

Let $c = (c_0, \ldots, c_{n-1}) \in GF(q')^n$. The *locators* of c are $\{X_1, \ldots, X_w\} = \{\alpha^{i_1}, \ldots, \alpha^{i_w}\}$, where $i_1, \ldots, i_w$ are the indices of non zero coordinates of c. The *elementary symmetric functions* of c, denoted by $\sigma_1, \ldots, \sigma_w$, are $\sigma_i = (-1)^i \sum_{1 \le j_1 < \ldots < j_i \le w} X_{j_1} \cdots X_{j_i}$, $i = 1 \ldots w$. The generalized Newton's identities hold: $\forall i \ge 0, \quad A_{i+w} + \sigma_1 A_{i+w-1} + \ldots + \sigma_w A_i = 0$.

These equations have been used for establishing contradictions. This way, the true minimum distance of BCH codes of length 244 and designed distance 59 and 61 have been found [2].

II. Main Theorem

Theorem[1] Let C be a cyclic code defined by the equations $A_1, \ldots, A_l = 0$. Let $S_C(w)$ be the following system of equations:

$$A_1 = \cdots = A_l = 0$$
$$A_{i+w} + \sigma_1 A_{i+w-1} + \ldots + \sigma_w A_i = 0, \quad i = 0..n-1$$

with indeterminates $\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1}$. Let $A = (A_0, \ldots, A_{n-1})$ be a solution to $S_C(w)$ (i.e. there exists $\sigma_1, \ldots, \sigma_w$ such that $(\sigma_1, \ldots, \sigma_w, A)$ is a solution), then A is the Fourier transform of a codeword of weight $\le w$.

III. Generalization to alternant codes and other

Cyclic codes are the easiest to deal with, because of the many indeterminates which are zero in the system $S_C(w)$. However the theorem easily generalize to other codes, as long as we are able to define these codes by algebraic conditions on the coefficients of the Fourier transform of codewords.

Definition Let C be a code in $GF(q')^n$ (or $GF(q)^n$). If there exists l polynomials in n variables $P_1, \ldots, P_l$, such that, for all $c \in GF(q')^n$ (or $GF(q)^n$), c belongs to C if and only if $P_1(A_0, \ldots, A_{n-1}) = \ldots = P_l(A_0, \ldots, A_{n-1}) = 0$, where $A = \phi(c)$, then the code has a *spectral definition*. The polynomials $P_1, \ldots, P_l$ are the *code spectral equations*.

Our result, which is a generalization of a case of a cyclic code [3], is the following theorem:

Theorem Let C be a code defined by the spectral equations $P_1, \ldots, P_l$. Let $S_C(w)$ be the following system of equations:

$$P_1(A_0, \ldots, A_{n-1}) = \cdots = P_l(A_0, \ldots, A_{n-1}) = 0$$
$$A_{i+w} + \sigma_1 A_{i+w-1} + \ldots + \sigma_w A_i = 0, \quad i = 0..n-1$$

with indeterminates $\sigma_1, \ldots, \sigma_w, A_0, \ldots, A_{n-1}$. Let $A = (A_0, \ldots, A_{n-1})$ be a solution to $S_C(w)$ (i.e. there exists $\sigma_1, \ldots, \sigma_w$ such that $(\sigma_1, \ldots, \sigma_w, A)$ is a solution), then A is the Fourier transform of a codeword of weight $\le w$.

Now we consider alternant codes. Let $\underline{\alpha} = (\alpha_0, \ldots, \alpha_{n-1}) \in GF(q')^n$ be distinct elements in $GF(q')$, and let $\underline{v} = (v_0, \ldots, v_{n-1})$ be nonzero elements in $GF(q')$. The generalized Reed Solomon code, $GRS_k(\underline{\alpha}, \underline{v})$, is the code whose codewords are $(v_0 F(\alpha_0), \ldots, v_{n-1} F(\alpha_{n-1}))$, for all $F \in GF(q')[X]$, $\deg F < k$.

The alternant code $\mathcal{A}_k(\underline{\alpha}, \underline{v})$ is the $GF(q)$-subfield sub-code of $GRS_k(\underline{\alpha}, \underline{v})$. We show how the alternant codes when v is the set of n-th root of unity, where are defined with spectral equations.

Next, we consider the Preparata code of length 15 can be defined (Blahut) by spectral equations. The code is binary, of length 15, and its codewords satisfy

$$\begin{aligned} A_1 &= 0, \\ A_3 A_5 &= 0, \\ (A_3^5 - 1)(A_5^3 - 1) &= 0. \end{aligned}$$

which are spectral equations. This example is worked out.

References

[1] D. Augot. Description of Minimum Weight Codewords of Cyclic Codes by Algebraic Systems. In *Finite Fields and their Applications* vol. 2, 1996.

[2] D. Augot and P. Charpin and N. Sendrier Studying the Locator Polynomial of Minimum Weight Codewords of BCH codes. IEEE Transaction on Information Theory, vol. 38, year 1992.

[3] D. Augot. Algebraic characterization of minimum weight codewords of cyclic codes. In *Proceedings IEEE, ISIT'94*, Trondheim, Norway, June 1994.

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