Newton's identities for minimum codewords of a family of alternant codes

Daniel Augot, Daniel.Augot@inria.fr
INRIA, France

Abstract — **We are able to define minimum weight codewords of some alternant codes in terms of solutions to algebraic equations. Particular attention is given to the case of the classical Goppa codes. Gröbner bases are used to solve the system of algebraic equations.**

I. Words of length n

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

We introduce the definition of a spectrally defined code:

Définition 1 *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 $P(A_0, \ldots, A_{n-1}) = \ldots = P_l(A_0, \ldots, A_{n-1}) = 0$, 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 [1], is the following theorem:

Théorème 1 *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 $\le w$.

II. "Spectral Definition" of some 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 $GRS_k(\underline{\alpha}, \underline{v})$. 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 consider a partial class of alternant codes, the alternant codes $\Gamma(L, G)$ where $L = \{1, \alpha, \ldots, \alpha^{n-1}\}$, the set of all n-th roots of unity. We denote these codes $\Gamma(\alpha, \underline{v})$. We get that the code spectral equations of $\mathcal{A}_k(\alpha, \underline{v})$ are

$$\begin{cases} \sum_{i+j=t \bmod n} A_i H_j = 0, & t = 0 \ldots n-k-1 \\ A_{iq \bmod n} = A_i^q, & i = 0 \ldots n-1 \end{cases}$$

where H is the Fourier Transform of h defining the dual of the $GRS_k(\underline{v})$.

III. A short Goppa code

Since classical Goppa codes with support $L = \{\alpha^i, \ i = 0 \ldots n-1\}$ are alternant codes, we are also able to construct spectral equations for these codes. As an example we study the Goppa code of length 32, with defining polynomial $g(x) = x^3 + x + 1$. We index codewords c in the following way: $c = (c_\infty, c_0, \ldots, c_{30})$, where the defining set of the Goppa code is $L = \{0, 1, \alpha, \ldots, \alpha^{30}\}$. Since our result works for a support of length n prime to 2, we first consider the sub-code C_{31} of C which is the shortened code with respect to the coordinate c_∞. This code is also a Goppa code with support $L_{31} = \{1, \alpha, \ldots, \alpha^{30}\}$ and defining polynomial $g(X)$. Thus writing the system $S_{C_{31}}(7)$, we get equations for codewords such that $c_\infty = 0$. Computing a Gröbner basis of the system, we get 105 solutions. Next, we want to study minimum weight codewords such that $c_\infty \neq 0$. The parity check matrix for C is

$$G = \begin{bmatrix} 1 & g(\alpha^0)^{-1} & \ldots & g(\alpha^{30})^{-1} \\ 0 & \alpha^0 g(\alpha^0)^{-1} & \ldots & \alpha^{30} g(\alpha^{30})^{-1} \\ 0 & (\alpha^0)^2 g(\alpha^0)^{-1} & \ldots & (\alpha^{30})^2 g(\alpha^{30})^{-1} \end{bmatrix}.$$

We search for words $c_0, \ldots, c_{30}$ of weight 6, of length 31 such that $G' c^t = (1, 0, \ldots, 0)^t$. where G' is the parity check matrix for C_{31}. Thus the spectral equations for these codewords are:

$$\begin{cases} \sum_{i+j=0 \bmod 31} A_i H_j = 1 \\ \sum_{i+j=t \bmod 31} A_i H_j = 0, \ t = 1, 2 \\ A_{2i \bmod 31} = A_i^2, \ i = 0 \ldots 30 \end{cases}$$

These equations, plus the Newton's identities for the weight 6, gives equations for codewords of C of weight 7 whose support is not included in $[0, 30]$. The Gröbner basis gives 23 solutions, thus 128 codewords of weight 7 for the whole code C, as in the table of [2, p344].

References

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

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