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

Daniel Augot

Newton's identities for minimum codewords of a family of alternant codes (extended abstract for submission)

Daniel Augot*

Abstract

We consider systems of algebraic equations which, in some way, define the minimum weight codewords of alternant codes. Results are presented which are natural generalization of the case of cyclic code [1]. Particular attention is devoted to *classical Goppa* codes, and a short example from [5] is presented. We use the tool of Gröbner bases for counting and describing solutions of algebraic systems [2].

1 Fourier Transform of words on length n

1.1 Basic Properties

Let $GF(q)$ be a finite field, let n be an integer prime to q. We fix α a primitive n-th root of unity, which belongs to $GF(q')$, an extension of $GF(q)$. 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 $A = (A_0, A_1, \ldots, A_{n-1})$, $A_i = a(\alpha^i)$, $i = 0 \ldots n-1$. We denote by $\odot$ the component-wise product in $GF(q')^n$. Some properties of the Fourier transform are summarized:

Theorem 1 *Let $a = (a_0, a_1, \ldots, a_{n-1}) \in GF(q')^n$ and let $A = \phi(a)$ be the Fourier transform of a. Then $a_i = \frac{1}{n}A(\alpha^{-i})$, $i = 0 \ldots n-1$. The word a belongs to $GF(q)^n$ if and only if $A_{iq \mod n} = A_i^q$, $i = 0 \ldots n$ ("conjugacy constraints"[3]).*

*Institut National de Recherche en Informatique et Automatique (INRIA) Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex FRANCE

If a, b are two words of $GF(q')^n$, then $\phi(ab) = \phi(a) \odot \phi(b)$, $\phi(a \odot b) = \frac{1}{n}\phi(a)\phi(b)$.

1.2 Newton's Identities

Definition 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 $\sigma_i = (-1)^i \sum_{1 \leq j_1 < \ldots < j_i \leq w} X_{j_1} \cdots X_{j_i}$, $i = 1 \ldots w$.*

The elementary symmetric functions of c and the Fourier transform of c are related by the (generalized) Newton's identities.

Theorem 2 *[5] Let $c \in GF(q')^n$ be a word of weight w, $A = (A_1, \ldots, A_n)$ be the Fourier transform of c and $\sigma_1, \ldots, \sigma_w$ the elementary symmetric functions of c. Then $\forall i \geq 0, \quad A_{i+w} + \sigma_1 A_{i+w-1} + \ldots + \sigma_w A_i = 0$.*

A converse property is easy to prove:

Theorem 3 *Let $c \in GF(q')^n$ and suppose that there exists $\gamma_1, \ldots, \gamma_w$ such that $\forall i \geq 0, \quad A_{i+w} + \gamma_1 A_{i+w-1} + \ldots + \gamma_w A_i = 0$. Then the weight of c is lower or equal to w.*

1.3 Spectral Definition of a Code

We consider codes C of length n over $GF(q')$. The *Reed-Solomon* code, denoted RS_k is the code of length $n = q' - 1$ over $GF(q')$, whose codewords are $(F(\alpha^0), \ldots, F(\alpha^{n-1}))$, for all polynomials $F \in GF(q')[X]$, $\deg F < k$. A *parity check matrix* for RS_k is

$$\begin{bmatrix} 1 & \ldots & 1 \\ \alpha^0 & \ldots & \alpha^{n-1} \\ \vdots & & \vdots \\ (\alpha^0)^{n-k-1} & \ldots & (\alpha^{n-1})^{n-k-1} \end{bmatrix},$$

since the dual of RS_k is RS_{n-k} [5].

Definition 2 *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.

Note that the code may not be linear. If the polynomials $P_1, \ldots, P_l$ are linear, the code is linear. As an example, the code spectral equations of RS_k are $A_0 = A_1 = \cdots = A_{n-k-1} = 0$.

Our main theorem is the following.

Theorem 4 *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 $\leq w$.

Proof: The equations $P_1(A_0, \ldots, A_{n-1}) = \cdots = P_l(A_0, \ldots, A_{n-1}) = 0$ implies that A is the Fourier transform of some codeword. Theorem 3 concludes the proof. □

In the particular case where w is the minimum weight of C, we get all the Fourier transforms of minimum weight codewords.

2 Spectral Equations for some Alternant Codes

Definition 3 *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, denoted $GRS_k(\underline{\alpha}, \underline{v})$, 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 $\Gamma(\alpha, \underline{v})$.

From the spectral code equations of RS_k, we derive spectral code equations for GRS_k and $\mathcal{A}_k(\alpha, \underline{v})$. Let c be a codeword of $GRS_k(\alpha, \underline{v})$, let $A = (A_0, \ldots, A_{n-1}) = \phi(c)$, $H = (H_0, \ldots, H_{n-1}) = \phi(h)$, $A' = (A'_0, \ldots, A'_{n-1}) = \phi(h \odot c)$. Since $h \odot c$ belongs to the RS_k code, we have $A'_0 = A'_1 = \ldots = A'_{n-k-1} = 0$. Thus, using theorem 1, the Fourier transform of the codewords of $GRS_k(\alpha, \underline{v})$ satisfy $\sum_{i+j=t \mod n} A_i H_j = 0$, $t = 0 \ldots n-k-1$. In the case of the alternant code $\mathcal{A}(\alpha, \underline{v})$, the Fourier transforms of the codewords satisfy the "conjugacy constraints".

Property 1 *The code spectral equations as defined in 2 of* $GRS_k(\alpha, \underline{v})$ *are* $\sum_{i+j=t \mod n} A_i H_j = 0,\ t = 0 \dots n-k-1$. *The code spectral equations of* $\mathcal{A}_k(\alpha, \underline{v})$ *are*

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

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

We consider a particular class of the classical Goppa codes: the codes $\Gamma(L, G)$, where $L = \{\alpha^i,\ i = 0 \dots n-1\}$. It is known ([5, p. 339-340]) that $\Gamma(L, G)$ is an alternant code which is the subfield sub-code of the dual of $GRS_r(\alpha, h)$ with $h = (G(\alpha^0)^{-1}, \dots, G(\alpha^{n-1})^{-1})$. We compute $H = \phi(h)$, the Fourier transform of h. The polynomial H is in fact the inverse modulo $Z^n - 1$ of $\tilde{G}(Z) = g_0 + \sum_{i=1}^{n-1} g_{n-i} Z^i$, where $G = \sum_{i=0}^{n-1} g_i Z^i$. Then the code spectral equations can be constructed.

The next section shows with an example how to deal with Goppa codes with support $L = \{0\} \cup \{\alpha^i,\ i = 0 \dots n-1\}$.

3 An example of a Goppa Code

We study the Goppa code of length 32, and with defining polynomial $g(x) = x^3 + x + 1$. We index codewords c in the following way: $c = (c_\infty, c_0, \dots, c_{30})$, where the defining set of the Goppa code is $L = \{0, 1, \alpha, \dots, \alpha^{30}\}$.

First we 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 $L_{31} = \{1, \alpha, \dots, \alpha^{30}\}$ 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 $c_\infty \neq 0$. The parity check matrix for C is

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

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

equations for these codewords are:

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

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 [5, p344].

We point out that these Gröbner basis computations take a few minutes on a Sparc workstation.

4 Conclusion

Results from [1] are generalized, and applied to alternant codes whose support is the set of n-th roots of unity. A transform approach as in [4] could be used to generalize these results to Goppa codes with arbitrary support.

References

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

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

[3] Richard E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

[4] Mansour Loeloeian and Jean Conan. A transform approach to Goppa codes. *IEEE Transaction on Information Theory*, 33(1):105–115, January 1987.

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