Contemporary Mathematics
Volume **00**, 0000

Tools for coset weight enumerators of some codes

PASCALE CHARPIN

Abstract. Every extended primitive code C can be viewed in a group algebra $K[G,+]$, where K and G are finite fields of same characteristic. Our purpose is to show that the use of the multiplication of these algebra can provide, in some situations, some tools which apply to the determination of weight distributions of cosets of codes. Actually we will explain two formulae which provide relations between the set of elements orthogonal to a codeword x and the values of products xy, $y \in C^{\perp}$. We give some applications.

Keywords: cosets, cyclic codes, group algebra, equations on finite fields

1. Introduction

The p-ary Reed-Muller codes (RM-codes) can be seen as *polynomials* codes or as extended cyclic codes [**14**]. Moreover Berman [**4**] proved that they are the powers of the radical of the group algebra $\mathcal{A} = K[\{G,+\}]$, $K = GF(p)$ and $G = GF(p^m)$ ($m > 1$, p a prime). The Reed-Muller codes have remarkable properties and all results on them involve results on some codes of length p^m over K, the so-called extended primitive codes. For instance Kasami deduced weight distributions of two and triple error-correcting binary BCH codes from the weight distributions of binary Reed-Muller codes of order 1 and 2 [**15**].

Set $N = p^m$. In this paper we treat only linear codes of length N over K. Such a code C is viewed as a K-subspace of $\mathcal{A}$ and we are mainly interested by the weight distributions of cosets of C. Let D be the code generated by C and a coset $x + C$ of C. We will assume that the weight distribution of $C^{\perp}$ is known. As $C \subset D$, $D^{\perp} \subset C^{\perp}$ so that the weight distribution of $x + C$ can be deduced from the weight distribution of $C^{\perp}$ and of $D^{\perp}$. Hence the problem consists of the determination, for any nonzero weight λ of $C^{\perp}$, of the number of elements y of $C^{\perp}$ of weight λ which are orthogonal to x. We will study the

1991*Mathematics Subject Classification*, Primary 94B, 12E20 zeros of the products xy, for a fixed x. Through Formulae **(I)** and **(II)**, we will establish some relations between the possible values of xy and the set of codewords orthogonal to x.

The formulae are most interesting for codes C which contain the RM-code of order j and are contained in the RM-code of order $j+1$, for some j. In this case the code C is an ideal of $\mathcal{A}$. Moreover we often will suppose that C is an extended cyclic code; then we can use together the properties of RM-codes and the permutations which conserve the code C.

The principal results are obtained in the binary case, when $C^\perp$ is a subcode of the Reed-Muller code of order 2. For instance we were able to verify the conjecture of Camion, Courteau and Montpetit [**6**]: for m even there are eight distinct weight distributions for the cosets of any 2-error-correcting extended BCH codes of length 2^m [**10**]. We give here general tools we applied to the special case of 2-error-correcting extended BCH codes; we explain the possible applications and give some new results. Some examples with numerical results are given in [**12**].

2. Terminology and basic properties

2.1. Extended cyclic codes in a group algebra. We denote by $\mathcal{A}$ the group algebra $K[G,+]$, which is the set of formal polynomials

$$x = \sum_{g\in G} x_g X^g,\ x_g \in K,$$

with

$$0 = \sum_{g\in G} 0X^g\ ,\ 1 = \sum_{g\in G} X^g\ ,\ aX^g + bX^g = (a+b)X^g\ .$$

and

$$\sum_{g\in G} x_g X^g \sum_{g\in G} y_g X^g = \sum_{h\in G}\left(\sum_{g\in G} x_g y_{h-g}\right) X^h\ . \tag{1}$$

A *code of* $\mathcal{A}$ is a K-subspace of $\mathcal{A}$. Let C be such a code; we will denote by $C^\perp$ the *dual* of C:

$$C^\perp = \{\ y \in \mathcal{A} \mid\ < x, y >= 0\ ,\ \text{for all } x \in C\ \}$$

where $< x, y >= \sum_{g\in G} x_g y_g$.

The algebra $\mathcal{A}$ has only one maximal ideal, its so-called *radical*

$$\mathcal{P} = \{\ x \in \mathcal{A} \mid \sum_{g\in G} x_g = 0\ \} = \{\ x \in \mathcal{A} \mid x^p = 0\ \}\ . \tag{2}$$

For every j, we denote by $\mathcal{P}^j$ the jth power of $\mathcal{P}$; it is the ideal of $\mathcal{A}$ generated by the products $\prod_{i=1}^{j} x_i,\ x_i \in \mathcal{P}$. One obtains the decreasing sequence of ideals of $\mathcal{A}$:

$$\{0\} = \mathcal{P}^{m(p-1)+1} \subset \mathcal{P}^{m(p-1)} \subset \ldots \subset \mathcal{P}^2 \subset \mathcal{P} \ ,$$

where $\mathcal{P}^{m(p-1)} = \{ \ a1 \mid a \in K \ \}$. The position of an element or a subset of $\mathcal{A}$ in this sequence will appear as a useful parameter we define now:

Definition 1. *Let $x \in \mathcal{A}$; let U be a subset of $\mathcal{A}$. Let $j \in [0, m(p-1)]$.*

- *We will say that the depth of x equals j if and only if x is in $\mathcal{P}^j$ and not in $\mathcal{P}^{j+1}$.*
- *We will say that the depth of U equals j if and only if U is included in $\mathcal{P}^j$ and not included in $\mathcal{P}^{j+1}$.*

By convention, $\mathcal{P}^0 = \mathcal{A}$.

Let $\mathcal{R}$ be the quotient algebra $K[Z]/(Z^n - 1)$, where $n = p^m - 1$. A cyclic code C^* of length n over K is a principal ideal of $\mathcal{R}$. It is generated by a polynomial of $K[Z]$ whose roots are called the *zero's* of C^*. We consider the extension C of the code C^* in the algebra $\mathcal{A}$. Let α be a primitive root of unity in G. The extension is the usual one : each codeword $c^* \in \mathcal{R}$, $c^* = \sum_{i=0}^{n-1} c_i^* Z^i$, is as follows extended to $c \in \mathcal{A}$.

$$c = c_0 X^0 + \sum_{i=0}^{n-1} c_{\alpha_i} X^{\alpha_i} \ , \ c_0 = -(\sum_{i=0}^{n-1} c_i^*) \ , \ c_{\alpha^i} = c_i^* \ .$$

Now consider the set I of those k such that α^k is a zero of the cyclic code C^*. Then the codeword c is an element of C if and only if it satisfies:

$$\sum_{g \in G} c_g = 0 \ \text{ and } \ \sum_{i=0}^{n-1} c_{\alpha^i} (\alpha^k)^i = 0 \ , \ \text{for all } k \in I \ .$$

Therefore we can identify precisely an extended cyclic code in $\mathcal{A}$.

Definition 2. *Let $S = [0, n]$. An extended cyclic code C in $\mathcal{A}$ is uniquely defined by a subset T of S such that $0 \in T$ and T is a union of cyclotomic cosets of p modulo n. Let us define for all $s \in S$:*

$$\phi_s \ : \ x \in \mathcal{A} \ \longmapsto \ \sum_{g \in G} x_g g^s \in G \ .$$

In particular, $\phi_0(x) = \sum_{g \in G} x_g$. Then we have that

$$C = \{ \ x \in \mathcal{A} \mid \phi_s(x) = 0 \ , \ \textit{for all } s \in T \ \}$$

We say that T is the defining set of the code C.

The p-ary Reed-Muller codes are extended cyclic codes in $\mathcal{A}$ [**14**]. Their defining-sets are related with the *p-weights* of the elements of the interval $S =$

$[0, n]$: for any $s \in S$, let $\sum_{i=0}^{m-1} s_i p^i$, $s_i \in [0, p-1]$, be the p-ary expansion of s; then the p-weight of s is

$$\omega_p(s) = \sum_{i=0}^{m-1} s_i \ .$$

Definition 3. *The p-ary Reed-Muller code of order r, denoted by $R_p(r, m)$, is the extended cyclic code in $\mathcal{A}$, whose defining-set is*

$$I_p(j, m) = \{ \ s \in S \mid \omega_p(s) < j \ \} \ , \ j = m(p-1) - r \ .$$

Berman proved in [**4**] that *the p-ary Reed-Muller codes are the powers of the radical of $\mathcal{A}$.* More precisely:

$$\mathcal{P}^j = R_p(m(p-1) - j, m) \ , \ \text{for all } j \in [1, m(p-1)] \tag{3}$$

Therefore, we can deduce from a wellknown property of the generalized Reed-Muller codes that $(\mathcal{P}^j)^\perp = \mathcal{P}^{m(p-1)-j+1}$. In the following we will identify the p-ary RM-codes with the codes $\mathcal{P}^j$. Note that

$$dim \ \mathcal{P}^j = card \ \{ \ s \in S \mid \omega_p(s) \geq j \ \} \tag{4}$$

Cosets of extended cyclic codes and equations over finite fields: Let C be an extended cyclic code with defining set T. Let $x \in \mathcal{A}$ and consider the coset $C_x = x + C$. We have

$$\phi_s(z) = \phi_s(x) \ , \ \text{for all } z \in C_x \text{ and for all } s \in T \ .$$

So every coset C_x is uniquely determined by the sequence of elements of G:

$$\mathcal{S}(x) = (\ \phi_s(x) \mid s \in T \ ) \ , \tag{5}$$

the so-called *syndrome* of x (or of the coset containing x).

Let $x \in \mathcal{A}$ with syndrome $(\ \beta_s \mid s \in T \ )$. To find the number of codewords of weight λ in C_x consists in solving the following problem: *find the number of codewords $z = \sum_{g \in G} z_g X^g$ of weight λ satisfying*

$$\sum_{g \in G} z_g g^s \ = \ \beta_s \ , \ \forall \ s \in T \ .$$

When $p = 2$ we obtain a system of *diagonal equations* over the finite field of order 2^m; the problem consists in *finding the number of solutions*

$$(X_1, \ldots, \ X_\lambda) \ , \ X_i \in GF(2^m), \ X_i \neq X_j \ \forall \ i, j$$

satisfying

$$\sum_{i=0}^{\lambda} X_i^s \ = \ \beta_s \ , \ \forall \ s \in T \ . \tag{6}$$

2.2. Cosets of codes of $\mathcal{A}$. Let C be an $[N,k]$-code of $\mathcal{A}$. We first recall the MAC-WILLIAMS transform, which determines uniquely the weight polynomial of the dual of C from the weight polynomial of the code C itself.

THEOREM 1. [**16**, p.146] *Let C be a linear $[N,k]$-code. Define its weight polynomial:*

$$W_C(X,Y)=\sum_{i=0}^{N}A_iX^{N-i}Y^i \ , \ A_i=card\ \{\ c\in C\mid \omega(c)=i\ \}\ ,$$

where $\omega(c)$ is the weight of c. Then the weight polynomial of the dual code $C^{\perp}$ is

$$W_{C^{\perp}}(X,Y)=\frac{1}{p^k}W_C(X+(p-1)Y,X-Y)\ . \tag{7}$$

Denote by D_x the $[N,k+1]$-code generated by C and a coset $C_x=x+C$ of C:

$$D_x=\bigcup_{a\in K}(ax+C)\ .$$

As $C\subset D_x$, $D_x^{\perp}\subset C^{\perp}$; then every weight of $C^{\perp}$ can be a weight of $D_x^{\perp}$. Moreover the weight distributions of $x+C$ can be deduced from the weight distribution of $C^{\perp}$ and of $D_x^{\perp}$. Indeed suppose that the weight distribution of $C^{\perp}$ is known and that we can compute the weight polynomial of $D_x^{\perp}$. The dimension of D_x equals $k+1$ so that the dimension of $D_x^{\perp}$ equals $N-(k+1)$. Applying (7) we obtain the weight polynomial of D_x:

$$W_{D_x}(X,Y)=\frac{1}{p^{\ N-(k+1)}}W_{D_x^{\perp}}(X+(p-1)Y,X-Y)\ .$$

But, by definition, $W_{D_x}(X,Y)=(p-1)Q_x(X,Y)+W_C(X,Y)$, where $Q_x(X,Y)$ is the weight polynomial of the coset $x+C$. Then the expression of $Q_x(X,Y)$ is as follows:

$$\begin{aligned}Q_x(X,Y)\ &=\ \frac{1}{(p-1)p^{\ N-k}}\ \big(\ p\ W_{D_x^{\perp}}(X+(p-1)Y,X-Y)\\ &\quad -\ W_{C^{\perp}}(X+(p-1)Y,X-Y)\big)\ .\end{aligned}\tag{8}$$

In the following we always will assume that the polynomial $W_{C^{\perp}}(X,Y)$ is known and we want to have results on the polynomial $Q_x(X,Y)$, for every x. Then the problem consists in the determination of the polynomials $W_{D_x^{\perp}}(X,Y)$.

Let λ be a non zero weight of $C^{\perp}$ and $A_{\lambda}(x)$ be the number of codewords of weight λ in $D_x^{\perp}$. So $A_{\lambda}(x)$ is the number of elements of $C^{\perp}$ of weight λ which are orthogonal to x:

$$A_{\lambda}(x)=card\ \{\ y\in C^{\perp}\mid \omega(y)=\lambda \text{ and } <y,x>=0\ \}\ . \tag{9}$$

Indeed $y\in D_x^{\perp}$ if and only if $<y,z>=0$ for all z in D_x. But $z=ax+c$, $a\in K$ and $c\in C$; as $y\in C^{\perp}$, $<y,c>=0$. Hence $y\in D_x^{\perp}$ is equivalent to $<y,x>=0$,

3. Weight polynomials of cosets

3.1. Translations on codewords. Let h be any non zero element of G. We denote by τ_h the permutation on G which acts as follows on the elements of $\mathcal{A}$:

$$\tau_h\left(\sum_{g\in G} x_g X^g\right) = \sum_{g\in G} x_g X^{g+h} = \sum_{g\in G} x_{g-h} X^g \ .$$

We will say that τ_h is an *h-translation* on the codewords. An ideal of $\mathcal{A}$ is a code invariant under every τ_h.

Let x and y in $\mathcal{A}$. It follows easily from the definition of the multiplication in $\mathcal{A}$ that

$$xy = \sum_{h\in G}\left(\sum_{g\in G} x_g y_{h-g}\right) X^h = \sum_{h\in G} < x, X^h y > X^h = \sum_{h\in G} < x, \tau_h(y) > X^h \ .$$

Therefore we obtain a relation which links up the weight of xy with the set of codewords orthogonal to x:

$$\textbf{(I)} \qquad \omega(xy) = card\ \{\ g \in G \mid\ < x,\ \tau_h(y) > \neq 0\ \}\ .$$

Suppose that the code C is an ideal of $\mathcal{A}$. Then the dual of C is also an ideal. Let $y \in C^\perp$; so the set of the $\tau_h(y)$ is a subset of codewords of $C^\perp$ of same weight. So Formula **(I)** means that the weight of xy equals the number of elements of that subset which are orthogonal to x. In the applications we study later, we always consider the following ideals C of $\mathcal{A}$:

Proposition 1. *Let y in $\mathcal{A}$ such that $depth(y) = j$ with $j \in [0, m(p-1)-1]$. Then*

$$\tau_h(y + \mathcal{P}^{j+1}) = y + \mathcal{P}^{j+1}\ ,\ \forall\ h \in G\ .$$

Therefore let C be a code of $\mathcal{A}$ of depth j satisfying

$$\mathcal{P}^{j+1} \subset C \subset \mathcal{P}^j\ \left(\ i.e.\ \mathcal{P}^{m(p-1)-j+1} \subset C^\perp \subset \mathcal{P}^{m(p-1)-j}\right)\ .$$

Then C is an ideal of $\mathcal{A}$, so that $C^\perp$ is also an ideal.

Proof: Let $h \in G$. Note that $X^h - 1$ is an element of $\mathcal{P}$. Then

$$X^h y = (X^h - 1)y + y \text{ where } (X^h - 1)y \in \mathcal{P}^{j+1}\ .$$

Thus the coset $y + \mathcal{P}^{j+1}$ is invariant under any h-translation. The code C can be considered as a union of such cosets. Hence it is an ideal of $\mathcal{A}$.
□

Remark: Assume that $p = 2$. It follows immediatly from the proposition above that any coset of depth j of the RM-code $\mathcal{P}^{j+1}$ is an *orphan* (see the terminology in [**5**]). Indeed the minimum weight codewords of these cosets cover all coordinate positions.

3.2. Application of Formula (I). In the application we present now, Formula (**I**) is most interesting, because xy has few possible weights, since the depth of y is $m-2$; moreover the $\tau_h(y)$ form the set of codewords of a given weight in the coset $y+\mathcal{P}^{m-1}$ (see Proposition 2). From now on, in this Section, $p=2$, K and G will be respectively the finite field of order 2 and 2^m. We will consider linear codes C of depth 2 such that:

$$\mathcal{P}^3 \subset C \subset \mathcal{P}^2 \text{ (i.e. } \mathcal{P}^{m-1} \subset C^{\perp} \subset \mathcal{P}^{m-2}) \ .$$

From Proposition 1, the code C is an ideal of the algebra $\mathcal{A}$. The code $C^{\perp}$ is an union of cosets of the Reed-Muller code of order 1, which are contained in the Reed-Muller code of order 2. These cosets are precisely described in [**16**, Chapter 15]; the reader can also refer to [**8**]. We only recall the results we need.

Such a coset $y+\mathcal{P}^{m-1}$ is uniquely defined by the symplectic form associated to y. Since y is in $\mathcal{P}^{m-2}$, then y can be identified to a quadratic boolean function f_y :

$$y=\sum_{g\in G} f_y(g)X^g \ - \ i.e. \ y_g=f_y(g).$$

The *associated symplectic form* of f_y is

$$\Psi_y \ : \ (u,v)\in G^2 \ \longmapsto \ \Psi_y(u,v)=f_y(0)+f_y(u)+f_y(v)+f_y(u+v) \ \in K \ .$$

The *kernel* of Ψ_y is as follows defined:

$$\mathcal{E}_y=\{ \ u\in G \mid \forall v\in G \ : \ \Psi_y(u,v)=0 \ \} \ .$$

The set $\mathcal{E}_y$ is a K-subspace of G of dimension $\kappa=m-2h$, where $2h$ is the *rank* of Ψ_y. Let $E_y=y+\mathcal{P}^{m-1}$; then $\Psi_y=\Psi_b$ for all $b\in E_y$. Moreover the weight distribution of E_y only depends on h; that is (cf. [**16**, p. 441]):

weights	$2^{m-1}-2^{m-h-1}$	2^{m-1}	$2^{m-1}+2^{m-h-1}$
number	2^{2h}	$2^{m+1}-2^{2h+1}$	2^{2h}

where $h\in[0,\lfloor m/2\rfloor \ ]$. Note that such a coset has exactly three weights unless m is even and $h=m/2$.

Definition 4. *Let $y\in\mathcal{P}^{m-2}$. Let $2h$ be the rank of the symplectic form associated to y. We will say that the coset $E_y=y+\mathcal{P}^{m-1}$ is of type (h).*

The proofs of Proposition 2, Lemma 1 and Proposition 3 can be found in [**10**] and [**12**]. In the following we will always consider $y\in\mathcal{P}^{m-2}\backslash\mathcal{P}^{m-1}$, $E_y=y+\mathcal{P}^{m-1}$. If $C_x=x+C$ is any coset of C, then we will denote by D_x the code $C_x\cup C$ (see Section 2.2). We suppose that the weight polynomial of $C^{\perp}$ is known and we want to determine the weight polynomial of $D_x^{\perp}$. In accordance with Formula (8), the weight distribution of the coset $x+C$ is:

$$(10) \quad Q_x(X,Y)=\frac{1}{2^{2^m-k}}\left(2W_{D_x^{\perp}}(X+Y,X-Y)-W_{C^{\perp}}(X+Y,X-Y)\right)$$

where k is the dimension of C.

Proposition 2. *Let λ be a weight of E_y such that $\lambda \neq 2^{m-1}$ and suppose that $\omega(y) = \lambda$. We denote by κ the dimension of the kernel of the symplectic form Ψ_y. Then we have:*

$$\{ \ X^g y \mid g \in G \ \} = \{ \ a \in E_y \mid \omega(a) = \lambda \ \} \ ,$$

and the cardinal of the set above is $2^{m-\kappa}$. So each codeword b of E_y, of weight different from 2^{m-1} is invariant under 2^κ translations

Lemma 1. *Let $x \in \mathcal{A} \backslash \mathcal{P}^2$, $y \in C^\perp$, $E_y = y + \mathcal{P}^{m-1}$; D_x is the code $C_x \cup C$, where C_x is the coset $x + C$. Then $D_x^\perp$ contains half of elements of E_y:*

$$card \ \{ \ a \in E_y \mid \ < x, a >= 0 \ \} = \frac{card \ E_y}{2} = 2^m \ .$$

Proposition 3. *Let $x \in \mathcal{A} \backslash \mathcal{P}^2$. Let λ be a weight of E_y and suppose that $\omega(y) = \lambda$. We denote by N_λ the number of codewords of E_y of weight λ. Set*

$$\hat{N}_\lambda = card \ \{ \ a \in E_y \mid \omega(a) = \lambda \ and \ < x, a >= 0 \ \} \ .$$

Then

$$\begin{aligned} x \in \mathcal{P} \backslash \mathcal{P}^2 &\implies \hat{N}_\lambda = \hat{N}_{2^m - \lambda} \\ x \in \mathcal{A} \backslash \mathcal{P} &\implies \hat{N}_\lambda = N_\lambda - \hat{N}_{2^m - \lambda} \ . \end{aligned}$$

Moreover, if $\lambda \neq 2^{m-1}$ we have:

$$\hat{N}_\lambda = 2^{-\kappa} \ (2^m - \omega(xy)) \ . \tag{11}$$

By hypothesis the code $C^\perp$ is an ideal of $\mathcal{A}$, since it is invariant under any translation. Thus the cosets of C of minimum weight 1 have the same weight distribution. By applying Formula (11), we can compute this weight distribution.

Corollary 1. *Suppose that the dual of the code C consists of the code $\mathcal{P}^{m-1}$ itself and L sets of cosets of same type; that is : L_i cosets of type (h_i), $i \in [1, L]$. Let $x = X^g$, $g \in G$ and $D_x = (x + C) \cup C$. Set*

$$A_l = card \ \{ \ c \in D_x^\perp \mid \omega(c) = l \ \} \ and \ \lambda_i = 2^{m-1} - 2^{m-h_i-1} \ , \ i \in [1, L] \ .$$

So the weights of $D_x^\perp$ are elements of the set $\{ \ 0, \ 2^{m-1}, \ \lambda_i, \ 2^m - \lambda_i \ (i \in [1, r]) \ \}$. Then the coefficients of the weight polynomial of $D_x^\perp$ are, for each i in $[1, L]$:

$$A_{\lambda_i} = L_i(2^{2h_i - 1} + 2^{h_i - 1}) \ , \ A_{2^m - \lambda_i} = L_i(2^{2h_i - 1} - 2^{h_i - 1}) \ ,$$

$A_0 = 1$ and $A_{2^m - 1} = \beta/2$ where β is the number of codewords of weight 2^{m-1} in $C^\perp$. The weight distribution of the coset $x + C$ can be calculated from the Formula (10).

Proof: We will apply the Proposition 3 to each type of cosets. Let $E_y = y + \mathcal{P}^{m-1}$ be a coset of type (h_i); recall that the dimension of the kernel of the symplectic form associated to y is $\kappa = m - 2h_i$. Assume that $\omega(y) = \lambda_i$. Since $\omega(x) = 1$, $\omega(xy) = \omega(y)$. Thus, according to (11), we have:

$$\begin{array}{rcl} \hat{N}_{\lambda_i} & = & 2^{2h_i - m}(2^m - \lambda_i) = 2^{2h_i - m}(2^m - 2^{m-1} + 2^{m-h_i-1}) \\ & = & 2^{2h_i} - 2^{2h_i-1} + 2^{h_i-1} = 2^{2h_i-1} + 2^{h_i-1} \ , \end{array}$$

and $A_{\lambda_i} = L_i \hat{N}_{\lambda_i}$. Since $\hat{N}_{2^m-\lambda_i} = N_{\lambda_i} - \hat{N}_{\lambda_i}$, then

$$\hat{N}_{2^m-\lambda_i} = 2^{2h_i} - 2^{2h_i-1} - 2^{h_i-1} = 2^{2h_i-1} - 2^{h_i-1} \ .$$

The null vector belongs to $D_x^\perp$ while the all-one vector does not. Since $2^{m-1} = 2^m - 2^{m-1}$, we obtain for any coset of any type $2\hat{N}_{2^{m-1}} = N_{2^{m-1}}$. That means that $D_x^\perp$ contains half of codewords of $C^\perp$ of weight 2^{m-1}.
□

3.3. Shifts of codewords. From now on we will treat only extended cyclic codes as they are defined in Section 2.1. Such codes are invariant under the *shifts*. Recall that we consider codes of length $N = p^m$ over the finite field K of order p. A shift of a given codeword x is as follows:

$$\sigma_j \ : \ \sum_{g \in G} x_g X^g \ \longmapsto \ \sum_{g \in G} x_g X^{\alpha^j g} \ , \ j \in [0, p^m - 2].$$

Proposition 4. *Set* $S = [0, n]$, *where* $n = p^m - 1$. *Any* $s \in S$ *is identified with its* p*-ary expansion* $(s_0, \dots, s_{m-1})$*. Then we define a partial order on* S*:*

$$\textit{for all } s,\ t \textit{ in } S \ : \ s \prec t \iff \forall\ i \in [0, m-1] \ : \ s_i \leq t_i$$

Let $x \in \mathcal{A}$ *and* $y \in \mathcal{A}$*. Then*

$$\forall\ s \in S \ : \ \phi_s(xy) = \sum_{i \prec s} \binom{s}{i} \phi_i(x)\phi_{s-i}(y) \ . \tag{12}$$

Proof:

$$\begin{array}{rcl} \phi_s(xy) & = & \displaystyle\sum_{g \in G} x_g \sum_{h \in G} y_h (g+h)^s = \sum_{g \in G} x_g \sum_{h \in G} y_h \sum_{i=0}^{s} \binom{s}{i} g^i h^{s-i} \\ & = & \displaystyle\sum_{i=0}^{s} \binom{s}{i} \sum_{g \in G} x_g g^i \sum_{h \in G} y_h h^{s-i} = \sum_{i \prec s} \binom{s}{i} \phi_i(x)\phi_{s-i}(y) \ , \end{array}$$

since, by Lucas's Theorem, $\binom{s}{i} \not\equiv 0 \pmod{p}$ is equivalent to $i \prec s$.
□

Theorem 2. *Let* $x \in \mathcal{P}^r$ *and* $y \in \mathcal{P}^{m(p-1)-r}$ *. Then the product* xy *is zero if and only if* $\phi_n(xy) = 0$. *Moreover if* $xy = 0$ *then* $x(y+\mathcal{P}^{m(p-1)-r+1}) = \{0\}$. *Define the polynomial of* $G[Z]$*:*

$$R(Z) = \sum_{\omega_p(i)=r} \phi_i(x)\phi_{n-i}(y)Z^{n-i} \ .$$

Then we have for all $j \in [0, n-1]$ *:*

$$\textbf{\textit{(II)}} \qquad \phi_n(x\sigma_j(y)) = (-1)^r R(\alpha^j) \ .$$

The number of shifts of y *(i.e. the* $\sigma_j(y)$*) which are orthogonal to* x *equals the number of zeros of the polynomial* $R(Z)$*.*

Proof: The product xy is in $\mathcal{P}^r\mathcal{P}^{m(p-1)-r} = \mathcal{P}^{m(p-1)}$. A codeword z of $\mathcal{P}^{m(p-1)}$ is defined by $\phi_s(z) = 0$ unless $s = n$. If $\phi_n(z) = 0$, z is the null vector; otherwise $z = a1$, $a \in K$ and 1 is the all-one vector (see Section 2.1). If $xy = 0$ then $xb = 0$ for every codeword b of the coset $y + \mathcal{P}^{m(p-1)-r+1}$, since $x\mathcal{P}^{m(p-1)-r+1}$ is in $\mathcal{P}^{m(p-1)+1}$ which is the null space.

From the definition of the functions ϕ_s and of σ_j, we have:

$$\phi_s(\sigma_j(y)) = \sum_{g\in G} y_g(\alpha^j g)^s = \alpha^{js}\phi_s(y).$$

Thus (noting that every i in S satisfies $i \prec n$):

$$\phi_n(x\sigma_j(y)) = \sum_{i=0}^{n} \binom{n}{i} \phi_i(x)\phi_{n-i}(\sigma_j(y)) = \sum_{i=0}^{n} \binom{n}{i} \phi_i(x)\phi_{n-i}(y)\alpha^{-ji}$$

Since $x \in \mathcal{P}^r$, $\phi_i(x) = 0$ for all i such that $\omega_p(i) < r$ (see Definition 3). When $\omega_p(i) > r$, $\omega_p(n-i) < m(p-1) - r$; in this case $\phi_{n-i}(y) = 0$, since $y \in \mathcal{P}^{m(p-1)-r}$. Then the sum above is a sum on the i such that $\omega_p(i) = r$.

Now we consider such an i and its p-ary expansion $(i_0, \ \ldots \ , \ i_{m-1})$ and we want to compute the coefficient $\binom{n}{i}$ modulo p:

$$\binom{n}{i} = \prod_{t=0}^{m-1} \binom{p-1}{i_t} = \prod_{t=0}^{m-1} (-1)^{i_t} = (-1)^{\omega_p(i)} = (-1)^r \ ,$$

since $\binom{p-1}{i_t} = (p-1)\ldots(p-i_t)/(i_t!) = (-1)^{i_t}$ (modulo p). Therefore

$$\phi_n(x\sigma_j(y)) = \sum_{\omega_p(i)=r} (-1)^r\phi_i(x)\phi_{n-i}(y)\alpha^{-ji} = (-1)^r R(\alpha^j) \ .$$

□

Remarks: 1) The set of the i whose p-weight equals r is invariant under the multiplication by p (modulo n); moreover $\phi_{sp}(z) = \sum_{g\in G} z_g g^{ps} = (\phi_s(z))^p$, for any z. *The polynomial* $R(Z)$ *is in fact a trace-function from* G *to* K*.*

2) Suppose that a code C is such that its dual is a union of L cosets $y + \mathcal{P}^{m(p-1)-r+1}$, $y \in \mathcal{P}^{m(p-1)-r}$, where all cosets have the same weight enumerator. Then there is only one weight distribution for the cosets $x + C$, $x \in \mathcal{P}^r$ and this result holds for non extended cyclic codes C. It becomes from the fact that $L/2$ cosets composing $C^\perp$ are orthogonal to x, for any x. We will treat later a special application of this fact (see Corollary 3).

3.4. Application of Formula (II). In this section we will consider extended cyclic codes C of depth r, for some r, such that:

$$\mathcal{P}^{r+1} \subset C \subset \mathcal{P}^r \text{ (i.e. } \mathcal{P}^{m(p-1)-r+1} \subset C^\perp \subset \mathcal{P}^{m(p-1)-r}) .$$

Let $T^\perp$ be the defining set of the dual code $C^\perp$. In accordance with Definition 3 and with the definition of C, $T^\perp$ has the following form:

$$T^\perp = I_p(m(p-1) - r + 1, m) \setminus \{s_1, \dots , s_l\} , \tag{13}$$

where the s_i are some elements of S of p-weight $m(p-1) - r$. Note that the defining set of C is $T = I_p(r, m) \cup \{n - s_1, \dots , n - s_l\}$. Set $U = \{s_1, \dots , s_l\}$ and let E be the cyclic code (in the algebra $\mathcal{R}$) whose nonzeros are the α^t, $t \in U$. The code E can be viewed in the algebra $\mathcal{A}$, by adding an all-zero column to the generator matrix. Clearly *depth*(E) equals *depth*$(C^\perp)$ equals $m(p-1)-r$.Then, since the dimension of E equals the number of elements of U, which is the dimension of the quotient space $C^\perp/\mathcal{P}^{m(p-1)-r+1}$, we have clearly

$$C^\perp = \bigcup_{y \in E} (y + \mathcal{P}^{m(p-1)-r+1}) . \tag{14}$$

The definitions of $C^\perp$, U and E hold in all this section. Recall that D_x is the linear code generated by C and the coset of C containing x; we want to determine the weight distribution of the dual of D_x.

Proposition 5. *Let a coset of C: $C_x = x + C$, $x \in \mathcal{P}^r \setminus C$. Let y in E. Then, for every $j \in [0, n-1]$:*

$$\phi_n(x\ \sigma_j(y)) = 0 \textit{ if and only if } \sum_{t=1}^{l} \phi_{n-s_t}(x)\phi_{s_t}(y)\alpha^{s_t j} = 0 .$$

That means that the number of shifts of y orthogonal to x is related with the weight of the codeword y' of E defined by

$$\phi_{s_t}(y') = \phi_{n-s_t}(x)\phi_{s_t}(y) , \ t \in [1, l] . \tag{15}$$

Let $n(y)$ be the number of elements of the set $\{\sigma_j(y) \mid j \in [0, n-1] \}$. Then we have

$$L(y) = card \ \{ \ \sigma_j(y) \mid \ < x, \sigma_j(y) >= 0 \ \} = \frac{n(y)}{n}(n - \omega(y')) \ ;$$

the code $D_x^\perp$ contains $L(y)$ cosets $\sigma_j(y) + \mathcal{P}^{m(p-1)-r+1}$.

Proof: In accordance with Theorem 2, $\phi_n(x\ \sigma_j(y)) = 0$ if and only if $R(\alpha^j) = 0$. Moreover, by hypothesis, $\phi_{n-i}(y) = 0$ for every i such that $\omega_p(i) = r$ unless $n-i \in U$. Since $U = \{s_1, \ldots, s_l\}$ we have :

$$R(\alpha^j) = \sum_{n-i\in U} \phi_i(x)\phi_{n-i}(y)\alpha^{-ij} = \sum_{r=1}^{l} \phi_{n-s_r}(x)\phi_{s_r}(y)\alpha^{s_r j} = 0\ .$$

Let $z \in \mathcal{A}$. Recall that the Mattson-Solomon polynomial of z is

$$MS_z(Z) = \sum_{i=0}^{n-1} \phi_i(z) Z^{n-i}\ .$$

It is well-known that $MS_z(\alpha^j) = z_{\alpha_j}$ [**16**, p.239]. Then

$$\omega(z) = n - (card\ \{j \in [0, n-1] \mid MS_z(\alpha^j) = 0\}) + \epsilon\ .$$

where ϵ equals 0 if $z_0 = 0$ and 1 otherwise.

Let y' be the codeword of E whose coefficients ϕ_{s_t} are given by Formula (15) (the other coefficients $\phi_i(y')$ are zero, by definition of the cyclic code E). For every j in $[0, n-1]$, we have obviously

$$MS_{y'}(\alpha^j) = \sum_{t=1}^{l} \phi_{s_t}(y')(\alpha^j)^{n-s_t} = \sum_{t=1}^{l} \phi_{n-s_t}(x)\phi_{s_t}(y)(\alpha)^{-js_t} = R(\alpha^j)\ .$$

Hence $R(\alpha^j) = 0$ if and only if $y'_{\alpha^j} = 0$. Let $n(y)$ be the number of distinct shifts of y and let $n = n(y)n_1$. Then

$$card\,\{\ \sigma_j(y) \mid\ < x, \sigma_j(y) >= 0\ \} = \frac{1}{n_1} card\,\{\ j \mid\ < x, \sigma_j(y) >= 0\ \} = \frac{1}{n_1}(n - \omega(y')\ .$$

Note that $y'_0 = 0$, by definition.
□

Now we want to show how it is possible to achieve the computation of the weight distribution of the code $D_x^{\perp}$ – then of the coset $x + C$ of depth r. We will examine this problem when U contains only one cyclotomic class of p modulo n. From Proposition 5, we have immediate corollaries.

Corollary 2. *Let* $U = \{\ s,\ ps, \ldots\ \}$, $x \in \mathcal{P}^r \setminus C$ *; let* y *be any element in* E. *Set* $\beta = \phi_{n-s}(x)\phi_s(y)$. *Let* $t = (n, s)$ *and* $n = tn_1$. *Then , for every* $j \in [0, n-1]$*:*

$$\phi_n(x\ \sigma_j(y)) = 0 \ \ \textit{if and only if}\ \ Tr(\beta\alpha^{js}) = 0\ .$$

Let y' *be the element of* E *such that* $\phi_s(y') = \beta$. *Then the number* $L(y)$ *of cosets* $\sigma_j(y) + \mathcal{P}^{m(p-1)-r+1}$ *contained in* $D_x^{\perp}$ *equals* $(n - \omega(y'))/t$.

Note that in this case the code E is an irreductible cyclic code viewed as a cyclic code of length n, even when n and s are not relatively prime (by t repetitions of each symbol). When $t = 1$, E is equivalent to the simplex code whose all codewords have a same weight λ. In this case the corollary above means that the weight polynomial of $D_x^\perp$ does not depend on β, i.e. on x. In fact $L(y) = n - \lambda$ and every element in E is a shift of y.

Corollary 3. *If all codewords of the code E have same weight, every coset of C of depth r (the same depth than C) have the same weight enumerator.*

We suppose now that E has more than one weight. The code $C^\perp$ consists of L separate sets:

$$\bigcup_{j\in[0,n-1]} (\sigma_j(y_l) + \mathcal{P}^{m(p-1)-r+1}) \ , \ y_l \in E \ , \ l \in [1, L] \ .$$

Each set is a union of cosets of same weight polynomial, since the RM-codes are invariant under the shift. Assume that for each l, this weight polynomial, the weight of y_l and $\phi_s(y_l)$ are known. Then, by applying Corollary 2, we can compute the values $L(y_l)$ for every l and obtain the weight polynomial of $D_x^\perp$.

The most simple case appears when the code E is such that only two weights occur. For instance, using the tools we present here, we treat in [**10**] the cosets of depth 2 of the extended 2-error-correcting BCH codes.

References

1. E.F. Assmus & V. Pless *On the covering radius of extremal self-dual codes*, IEEE Trans. on Info. Theory, vol. IT-29, n. 3, May 1983.
2. L.A. Bassalygo, G.V. Zaitsev & V.A. Zinoviev, *Uniformly packed codes*, translated from Problemy Peredachi Informatsii, vol. 10, N. 1, pp. 9-14, January-March, 1974.
3. L.D. Baumert & R.J. McEliece, *Weights of irreductible cyclic codes*, Information and Control 20, pp. 158-175 (1972).
4. S.D. Berman, *On the theory of group codes*, KIBERNETICA, Vol. 1, n. 1, pp. 31-39, 1967.
5. R.A. Brualdi & V.S. Pless, *Orphans of the first order Reed-Muller codes*, IEEE Trans. Inform. Theory, Vol. 36, N. 2, March 1990.
6. P. Camion, B. Courteau & A. Montpetit, *Weight distribution of* 2*-error correcting binary BCH codes of length* 15*,* 63 *and* 255, IEEE Trans. on Inform. Theory, vol. 38, No. 4, pp. 1353-1357, 1992.
7. P. Camion, B. Courteau & P. Delsarte, *On r-partition designs in Hamming spaces*, Applicable Algebra in Eng. Comm. and Computing 2, 147-162 (1992).
8. C. Carlet *Codes de Reed et Muller, codes de Kerdock et de Preparata*, Thèse de l'Université PARIS VI, Janvier 89.
9. P. Charpin, *Codes idéaux de certaines algèbres modulaires*, Thèse de Doctorat d'Etat, Université Paris 7, 1987.
10. P. Charpin, *Weight distributions of cosets of* 2*-error-correcting binary BCH codes, extended or not*, IEEE Trans. on Info. Theory., to appear.
11. P. Charpin, *Distributions de poids des translatés des codes BCH binaires* 2*-correcteurs*, Comptes Rendus de l'Académie des Sciences de Paris, t. 317, Série I, p. 975-980, 1993.
12. P. Charpin, *Tools for coset weight enumerators of some codes*, INRIA-report, to appear.
13. P. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Information and Control, vol. 23, N. 5, pp.407-438, 1973.

14. T. Kasami, S. Lin & W.W. Peterson, *New generalisations of the Reed-Muller codes*, IEEE Trans. on Info. Theory, vol. IT-14, pp. 189-199 (1968) .
15. T. Kasami, *Weight distributions of Bose-Chaudhuri-Hocquenghem codes*, in: Proceedings of the conference on combinatorial mathematics and its applications (R.C. Bose and T.A. Dowling, eds., The Univ. of North Carolina Press, Chapel Hill, N.C., 1968, pp. 335-357.
16. F.J. Macwilliams & N.J.A. Sloane, *The theory of Error Correcting Codes*, North-Holland 1986.
17. H.C.A. Van Tilborg, *Uniformly packed codes*, Ph.D. thesis, Tech. Univ. Eindhoven, 1976.

INRIA, projet CODES,

Current address: Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, FRANCE.

E-mail adress: charpin@nuri.inria.fr.