Discrete Mathematics 56 (1985) 117–124
North-Holland

A DESCRIPTION OF SOME EXTENDED CYCLIC CODES WITH APPLICATION TO REED–SOLOMON CODES

P. CHARPIN

Institute de Programmation et LITP, 75230 Paris Cedex 05, France

Received December 1984

Let A be the modular algebra in which a large class of extended cyclic codes is examined. We characterize the set of A-codes which are the results of the peculiar sums of principal A-codes. The set described contains extended cyclic codes that we specify. Some of them are Reed–Solomon codes.

Soit A l'algèbre modulaire dans laquelle est étudiée une classe importante de codes cycliques étendus. Nous caractérisons un ensemble de codes de A obtenus par des sommes particulières de codes principaux de A. L'ensemble décrit contient des codes cycliques étendus que nous déterminons. Parmi ceux-ci certains sont des codes de Reed–Solomon.

1. Introduction

Let p be a prime; m and r are two positive numbers; K and G are respectively the Galois fields $\mathrm{GF}(p^r)$ and $\mathrm{Gf}(p^m)$. We denote by A the modular algebra $K[G]$; A is the polynomial algebra

$$A = \left\{ x = \sum_{g \in G} x_g X^g \mid x_g \in K \right\}. \tag{1}$$

We denote by R the quotient algebra $K[X]/(X^n - 1)$ with $n = p^m - 1$. By convention an A-*code* is an ideal in A and an R-*code* is a cyclic code of length n over K.

An R-code, the extension of which is invariant under the affine permutation group on G, is characterized by Kasami in [9]. Such a code is an A-code. For example the extended BCH codes, the generalized Reed–Muller codes, the extended Reed–Solomon codes are A-codes. So we study the algebraic properties of A-codes, in the same way we study a large class of cyclic codes.

We have described in [7] the R-codes, and particularly the Reed–Solomon codes, the extension of which is a principal ideal of A. We give here a more general presentation: the A-codes in question are particular sums of principal A-codes; they are defined in Section 2. In Section 3 all R-codes, the extensions of which are A-codes, are explicitly characterized. So, in Section 4, we can point out for an extended Reed–Solomon code, the relation between its minimum distance and its representation in the modular algebra.

The proofs of Sections 2, 3 and 4 require a theory which is developed in [4]. Here we only give the useful definitions and properties.

When we say *distance* we always mean the *Hamming distance.*

2. Definition of an A-code set

Let P be the set of all nilpotent elements of A, called *the radical of the algebra* [2];

$$P=\left\{x\in A \;\middle|\; \sum_{g\in G} x_g=0\right\}. \tag{2}$$

The jth power of the radical P is denoted P^j; the ideals P^j are described in [4, 11, 12].

Particularly we have shown in [8] that they are the generalized Reed–Muller codes. Each element and therefore each ideal of A has a position in the decreasing sequence $\{P^j \mid j\leq m(p-1)\}$ which is called its depth by Poli [12].

Definition 1. $j\in[1, m(p-1)]$; $x\in A$; I is an *A-code.*
(1) *x has the depth j* if and only if $x\in P^j$ and $x\notin P^{j+1}$;
(2) *I has the depth j* if and only if $I\subset P^j$ and $I\not\subset P^{j+1}$.

Notations. The principal ideals of A generated by an element x: is denoted by (x). Let $\{I_1,\ldots,I_k\}$ be k ideals of A; their sum is

$$\overset{k}{\underset{i=1}{+}} I_i=\left\{\sum_{i=1}^{k} a_i \mid a_i\in I_i\right\}. \tag{3}$$

Theorem 1. *Let I be an A-code with depth j. The two following propositions are equivalent:*

(i) *There are $\{x_1,\ldots,x_k\}$, k elements of A such that:*

$$\sum_{i=1}^{k} \lambda_i x_i\in P^j\setminus P^{j+1} \quad \textit{with } (\lambda_i)_i\in K^k-\{0\}$$

and

$$I=\overset{k}{\underset{i=1}{+}} (x_i),$$

(ii) $PI=P^{j+1}\cap I$ *and* $\dim PI=\dim I-k$.

Remark. In (i), the first condition involves that the I-expression is minimal.

Proof. (1) We suppose that I verifies (i). Clearly $PI\subset P^{j+1}\cap I$. Let $y\in P^{j+1}\cap I$; by (i) we have $y=\sum_{i=1}^{k} a_i x_i$ with $a_i\in P$; so $y\in PI$. We have proved that $P^{j+1}\cap I= PI$.

Let $h = \dim PI$, $\{y_1, \ldots, y_h\}$ a basis of PI and $y \in I$. We recall that $A = K \oplus P$. We have

$$y = \sum_{i=1}^{k} a_i x_i, \quad a_i \in A;$$

$$y = \sum_{i=1}^{k} \lambda_i x_i + \sum_{i=1}^{k} b_i x_i, \quad \lambda_i \in K,\ b_i \in P,\ \lambda_i + b_i = a_i;$$

$$y = \sum_{i=1}^{k} \lambda_i x_i + \sum_{i=1}^{h} \mu_i y_i, \quad \lambda_i \in K,\ \mu_i \in K.$$

So the set $\{x_1, \ldots, x_k, y_1, \ldots, y_h\}$ is a generator system of the K-vector space I; it is a maximal generator system because we cannot have

$$\sum_{i=1}^{k} \lambda_i x_i = -\sum_{i=1}^{h} \mu_i y_i \quad \text{with } \mu_i y_i \in PI \text{ and } \lambda_i x_i \in P^j \setminus P^{j+1}.$$

So $\dim I = \dim PI + k$; (ii) is proved.

(2) We suppose that I verifies (ii). Let $\{y_1, \ldots, y_h\}$ be a basis of PI; it is completed in order to obtain a basis of $I: \{x_1, \ldots, x_k, y_1, \ldots, y_h\}$. Let x be a K-linear combination of the vectors x_i. From (ii) x has the depth j. Each y_i, $1 \leqslant i \leqslant h$, is an elements of PI. From the definition of the ideal product, we have

$$y_i = \sum_{s=1}^{k} x_s^i x_s + \sum_{s=1}^{h} y_s^i y_s, \quad y_s^i \in P,\ x_s^i \in P$$

and we deduce the system

$$\begin{bmatrix} 1-y_1^1 & -y_2^1 & \cdots & -y_h^1 \\ -y_1^2 & \ddots & & \vdots \\ \vdots & & \ddots & -y_h^{h-1} \\ -y_1^h & \cdots & -y_{h-1}^h & 1-y_h^h \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_h \end{bmatrix} = \begin{bmatrix} \sum_{s=1}^{k} x_s^1 x_s \\ \vdots \\ \sum_{s=1}^{k} x_s^h x_s \end{bmatrix}$$

Let M be the representative matrix of the system. Its determinant is a unit of the algebra because the only terms of M that are units of A are the principal diagonal terms. So each y_i is a P-linear combination of x_i, therefore every element of PI too. (i) is proved. $\square$

From Theorem 1 we get a necessary and sufficient condition for the A-code to be principal. It is the particular case $k = 1$; in this case we note that

$$\dim I = \dim PI + 1 \Rightarrow PI = P^{j+1} \cap I.$$

Corollary 1. *An A-code is principal if and only if* $\dim PI = \dim I - 1$.

We give a notation for the A-codes characterized by Theorem 1:

$$\mathscr{C} = \{I \subset A \mid I \text{ is an } A\text{-}code,\quad I \text{ verifies (i) or (ii)}\}. \tag{4}$$

3. Extended cyclic codes and $\mathscr{C}$ elements

Let $n = p^m - 1$. Let α be a primitive element of G and let C be an R-*code* with generator polynomial,

$$g(X) = \prod_{t \in T} (X - \alpha^t), \quad T \subset]0, n[, \; g \in K[X]. \tag{5}$$

We denote by C' the extended code C, C' is defined usually as in van Lint [13].

$$a \in C, \quad a = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1},$$

$$a' \in C', \quad a' = \left(-\sum_{i=0}^{n-1} a_i\right) X^0 + a_0 X^{\alpha^0} + \cdots + a_{n-1} X^{\alpha^{n-1}}.$$

The code C' is therefore a linear code contained in P. Its definition in A is [4, 9],

$$C' = \{x \in A \mid t \in T \Rightarrow \phi_t(x) = 0\} \tag{6}$$

with

$$T' = T \cup \{0\} \quad \text{and} \quad \phi_t(x) = \sum_{g \in G} x_g g^t. \tag{7}$$

The ϕ_t, $t \in [0, n]$, are K-linear applications from A to an overfield of K and G. We say that T *is the definition set of* C and T' *is the definition set of* C'. Recall that

$$\dim C = \dim C' = n - T. \tag{8}$$

Let $s \in [0, n]$, the p-weight of the integer s, where s is written in the p-ary number system, is

$$\omega_p(s) = \sum_{i=0}^{m-1} s_i \quad \text{with } s = \sum_{i=0}^{m-1} s_i p^i, \; s_i \in [0, p-1]. \tag{9}$$

A relation of partial order, denoted $\prec$, is defined over $[0, n]$: $v \in [0, n]$, $s \in [0, n]$,

$$v \prec s \Leftrightarrow v_i \leqslant s_i, \quad i \in [0, m-1] \tag{10}$$

(where v and s are here exprimed in the p-ary number system).

When (10) is verified, we say that s is *an ascendant of* v or that v *is a descendant of* s.

The code C' is an A-code if and only if it verifies the Kasami theorem hypothesis. We write this condition with our notation:

$$C' \text{ is an } A\text{-code} \Leftrightarrow t \in T' \text{ and } s \prec t \Rightarrow s \in T'. \tag{11}$$

The condition (11) is obtained for the following formula which will be used further on:

$$\phi_s(xy) = \sum_{\substack{i \in [0, n] \\ i \prec s}} \binom{s}{i} \phi_{s-i}(x) \phi_i(y). \tag{12}$$

We suppose now that C is such that C' is an *A-code*. Let j be the depth of C, we recall that the defining set of P^j is

$$T_j = \{s \in [0, n] \mid \omega_p(s) < j\}. \tag{13}$$

Lemma 1. *The code PC' is an extended R-code and its definition set is*

$$\bar{T} = \{t \in [0, n] \mid s \prec t,\ s \neq t \Rightarrow s \in T'\}. \tag{14}$$

Proof. From (6) and (7) it is clear that an extended cyclic code is a linear code invariant under the A-automorphism:

$$\sigma : \sum_{g \in G} x_g X^g \to \sum_{g \in G} x_g X^{\alpha_g}.$$

The codes P and C' and therefore the product PC' are invariant under the automorphism σ. So, the code PC' is an extended R-*code*. Let T'' be the defining set of PC'. From the definition of the ideal product we have:

$$T'' = \{t \in [0, n] \mid \phi_t(xy) = 0,\ x \in P,\ y \in C'\}.$$

Let $x \in P$, $y \in C'$ and $t \in [0, n]$, $\bar{T}$ is defined by (14). If $t \in \bar{T}$, we have

$$s \prec t \text{ and } s \neq t \Rightarrow s \in T' \Rightarrow \phi_s(y) = 0.$$

So, according to the formula (12), $\phi_t(xy) = \phi_0(x)\phi_t(y)$. But $\phi_0(x) = 0$, therefore $t \in T''$. Let $x = X^g - 1$ where g is any element of G. From (12),

$$\phi_t((X^g - 1)y) = \sum_{\substack{s \prec t \\ s \in [0, t[}} \binom{t}{s} g^{t-s} \phi_s(y).$$

If $t \in T''$, we have $\forall g$, $\phi_t((X^g - 1)y) = 0$.

We can deduce that $\phi_s(y) = 0$ for each s such that $s \prec t$ and $s \neq t$. Then $t \in \bar{T}$; we have proved that $\bar{T} = T''$ $\square$

Lemma 2. *Let j be the depth of C'. The code $P^{j+1} \cap C'$ is an extended R-code the defining set of which is:*

$$\hat{T} = \{t \in [0, n] \mid t \in T' \text{ or } \omega_p(t) = j\}. \tag{15}$$

Proof. The *A-codes* P^{j+1} and C' are both extended R-*codes*, so the code $P^{j+1} \cap C'$ is an *A-code* and an extended R-*code*. We obtain its defining set by adding the defining set of P^{j+1} with the defining set of C'. $\square$

Theorem 2. *Let C' be an A-code with the depth j. So, C' belongs to the set $\mathscr{C}$, defined by* (4), *if and only if there are k elements*

$$\{t_i \mid i \in [1, k],\ t_i \in [0, n],\ w_p(t_i) = j\}, \tag{16}$$

which characterize T':

$$T' = \{t \in [0, n] \mid \forall i,\ i \in [1, k],\ t_i \not< t\}. \tag{17}$$

Proof. (1) We suppose that C' belongs to $\mathscr{C}$. From Theorem 1 the codes PC' and $P^{j+1} \cap C'$ are equal, therefore their defining sets are also equal. From (14) and (15) we have

$$T'' = \{t \notin T' \mid s < t, s \neq t \Rightarrow s \in T'\} = \{t \notin T' \mid \omega_p(t) = j\}.$$

We want to show that (17) characterizes the defining set T' of C'.

Let $T'' = \{t_1, \ldots, t_k\}$ and $s \in T'$. The t_i elements do not belong to T'; then s cannot be an ascendant of t_i because C' as A-*code*, verifies (11). So: $T' \subset \{s \mid \forall_i,\ t_i \not< s\}$. Inversely let $s \in [0, n]$ such that, for each t_i, s is not an ascendant of t_i. Two cases may occur:

(i) $\omega_p(s) \leq j$. The code C' has the depth j and the code PC' has the depth $j+1$. To obtain the definition set of PC', we add to T' k elements which have a p-weight j. Then we conclude that $s \in T'$.

(ii) $\omega_p(s) > j$. Suppose that $\omega_p(s) = j+1$. Then each descendant of s is in T' because $\omega_p(t) \leq j$ and $t \notin T''$. From Lemma 1, s belongs to $\bar{T}$ and therefore s belongs to T'. By recurrence we can deduce: $w_p(s) > j \Rightarrow s \in T'$.

(2) We suppose now that T' is defined by (16) and (17). The code C is an A-*code*, which verifies (11). Let $\bar{T} = T' \cup T''$ be the defining set of the code PC'. For each i we have $t_i \in \bar{T} \setminus T'$ because,

$$t \neq t_i,\ t < t_i \Rightarrow t \in T'.$$

On the other hand, if $t \in T''$ with $t \neq t_i$ for each i, then $t \in T'$ or t is an ascendant of a t_i. So $T'' = \{t_1, \ldots, t_k\}$. We know from (15) the defining set of the code $P^{j+1} \cap C'$; this set is also equal to $T' \cup T''$ from (16) and (17). Then

$$P^{j+1} \cap C' = PC' \quad \text{and} \quad \dim PC' = \dim C' - |T''| = \dim C' - k.$$

From Theorem 1, $C' \in \mathscr{C}$. $\square$

4. Application to Reed–Solomon codes

We suppose from now on that $K = G$. The Reed–Solomon code, here denoted by RS, of length n and minimum distance d over K is the R-*code* with the following generator polynomial:

$$g(X) = \prod_{k=1}^{d-1} (X - \alpha^k) \tag{18}$$

We note RS′ the extension of the code RS:

$$\mathrm{RS}' = \{x \in A \mid t \in [0, d[\Rightarrow \phi_t(x) = 0\}. \tag{19}$$

The code RS′ is an A-*code* because obviously the interval $[0, d[$ verifies (11).

Theorem 3. *Let $M = m(p-1)$, $j \in [0, M]$ and,*

$$d_j = \max\{k \in [0, n] \mid \omega_p(k) = j\}. \tag{20}$$

So the A-code RS′ *has the depth j, $j > 0$, if and only if $d \in]d_{j-1}, d_j]$.*

The proof of Theorem 3 is given in [5]. We have also shown that an extended Reed–Solomon code is a principal ideal of A if and only if its minimal distance is equal to a d_j. The d_j representation in the p-ary number system is

$$d_j = tp^{m-s-1} + \sum_{i=m-s}^{m-1} (p-1)p^i, \tag{21}$$

where $j = s(p-1) + t$, $t \in [0, p-1[$. If $s = 0$, then $d_j = tp^{m-1}$.

Theorem 4. *Let j be the depth of the A-code* RS′.

So, the code RS′ *is an element of $\mathscr{C}$ if and only if its minimal distance has the following type:*

$$d = d_{j-1} + h \quad \textit{with } \omega_p(h) = 1. \tag{22}$$

Proof. Let d be the minimum distance of the code RS; we have $d \in]d_{j-1}, d_j]$. According to Theorem 2 we shall show that

$$d \text{ verifies (22)} \Leftrightarrow [0, d[\text{ verifies (16) and (17).}$$

(1) We suppose that d verifies (22). From (21) we have $h = p^i$ with $i \in [0, m-s-1]$. Let

$$T'' = \{t_i \mid d \leq t_i, t_i = d_{j-1} + p^i, i \in [0, m-s-1]\}.$$

It is clear that $\omega_p(t_i) = j$; then T'' verifies (16). Let $t \notin [0, d[$, so $\omega_p(t) > j$ and $\omega_p(t) \geq j$ and $d \leq t \Leftrightarrow \exists t_i$, $t_i \in T''$ and $t_i < t$. This proves that $[0, d[$ verifies (17).

(2) We suppose that $[0, d[$ verifies (16) and (17). By hypothesis we have $d = d_{j-1} + h$ with $h \in]0, d_j - d_{j-1}]$. From (21), $\omega_p(d) \geq j$. Suppose that $\omega_p(d) > j$; there is a t which belongs to $[d, n[$ such that

$$d \leq s \text{ and } \omega_p(s) = j \Rightarrow s < t.$$

This is inconsistent with (16) and (17). So $\omega_p(d) = j$, therefore $\omega_p(h) = 1$. □

5. Conclusion

The extension of the Reed–Solomon code of length n and minimal distance d over K is an element of $\mathscr{C}$ if and only if d has the following type:

$$d = p^k + tp^{m-s-1} + \sum_{i=m-s}^{m-1} (p-1)p^i,$$

with $t \in [0, p-1[$, $s \in [0, m-1]$ and $k \in [0, m-s-1]$. If $s = 0$, then

$$[m-s, m-1] = \emptyset.$$

References

[1] S.D. Berman, On the theory of group codes, Kibernetica 1 (1967) 31–39.
[2] N. Bourbaki, Livre II, Algébre (Hermann, Paris, 1958).
[3] P. Camion, A proof of some properties of Reed–Muller codes by means of the normal basis theorem, in: R.C. Bose and T.A. Dowlings, eds., Combinatorial Mathematics and its Applicants (Univ. North. Carolina Press, Chapel Hill, N.C., 1969).
[4] P. Charpin, Codes idéaux de certaines algèbres modulaires—Thèse de 3ème cycle, Université de Paris VII (1982).
[5] P. Charpin, The extended of Reed–Solomon codes considered as ideals of a modular algebra, Ann. Discrete Math. 17 (1983) 171–176.
[6] P. Charpin, Les codes de Reed–Solomon en tant qu'idéaux d'une algèbre modulaire, C.R. Acad. Sci. Paris Sér. I (1982) 597–600.
[7] P. Charpin, Codes cycliques étendus et idéaux principaux d'une algèbre modulaire. C.R. Acad. Sci. Paris Sér. I (1982) 313–315.
[8] P. Charpin, Puissances du radical d'une algèbre modulaire et codes cycliques, Rev. CETHEDEC 81-2, (1981) 35–43.
[9] T. Kasami, S. Lin and W.W. Peterson, Some results of cyclic codes which are invariant under the affine group and their applications, Inform. and Control 11 (1967) 475–496.
[10] F.J. MacWilliams and N.J.A. Sloane, The theory of error correcting codes (North-Holland, Amsterdam, 1977).
[11] A. Poli, Codes dans certaines algèbres modulaires, Thèse de Doctorat d'Etat, Université Paul Sabatier, Toulouse (1978).
[12] A. Poli, Idéaux de $A = K[X_1, \ldots, X_n]/(X_1, \ldots, X_n)$ stables sous le groupe des automorphismes isométriques de A. C.R. Acad. Sci. Ser. A (1980) 1029–1042.
[13] J.H. van Lint, Coding Theory (Springer, Berlin, 1971).
[14] J. Wolfmann, A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field, Discrete Math. 31 (1980) 337–338.