Annals of Discrete Mathematics 17 (1983) 171–176

THE EXTENDED REED–SOLOMON CODES CONSIDERED AS IDEALS OF A MODULAR ALGEBRA

Pascale CHARPIN

Département de Mathématiques, U.E.R. Sciences, 123 rue Albert Thomas, 87060 Limoges, Cedex, France

The extended Reed–Solomon codes are ideals of a modular algebra A. Some properties of A are described which permit the lower bound for each principal ideal dimension of A to be defined. The results are used to characterise among Reed–Solomon codes those which are A principal ideals.

1. Definitions and previous properties

p is a prime, m and r are integers different from zero, and K and G are, respectively, the Galois fields $GF(p^r)$ and $GF(p^m)$.

A is the modular algebra KG. It is the polynomial space:

$$A = \left\{ x = \sum_{g \in G} x_g X^g \,\middle|\, \forall g \in G, x_g \in K \right\},$$

with the usual operations of polynomial multiplication and addition.

The radical of a ring is the intersection of all its principal ideals. As A has characteristic p, an element of A is either invertible, or nilpotent, since

$$x \in A, \qquad x^p = \left(\sum_{g \in G} x_g X^g \right)^p = \sum x_g^p X^{pg} = \left(\sum_{g \in G} x_g^p \right) X^0.$$

An ideal of A, different from A, has only nilpotent elements. Hence A has only one maximal ideal which is also its radical:

$$P = \{ x \in A \mid x^p = 0 \}.$$

P^j, $j \geq 1$, is the j-power of the radical of A. P^j is the subspace of A generated by the set:

$$\left\{ \prod_{k=1}^{j} x_k \,\middle|\, x_k \in P \right\}.$$

Let $M = m(p-1)$. I_j, $0 \leq j \leq M$, is the subset of $\mathbb{N}^m$:

$$I_j = \left\{ (i_1, \ldots, i_m) \in [0, p-1]^m \,\middle|\, \sum_{k=1}^{m} i_k \geq j \right\}.$$

Theorem 1. *Let $\{e_1, \ldots, e_m\}$ be a basis of the F_p-vector space G and let for each j, $0 \leq j \leq M$, the subset of A:*

$$B^j = \left\{ \prod_{k=1}^{m} (X^{e_k} - 1)^{i_k} \,\middle|\, (i_1, \ldots, i_m) \in I_j \right\}.$$

Then B^0 is a basis of the K-vector space A and B^j, $1 \leq j \leq M$, is a basis of P^j.

Proof. Let j, $0 \leq j \leq M$, and let x be a linear combination of vectors of B^j:

$$x = \sum_{k \in R \subset I_j} \lambda_k v^k, \quad \lambda_k \in K^*, \, v^k \in B^j.$$

Let $i \in R$, $i = (i_1, \ldots, i_m)$, so that

$$\forall k, \, k \in R, \, k = (k_1, \ldots, k_m), \quad \sum_{l=1}^{m} i_l \leq \sum_{l=1}^{m} k_l.$$

Then

$$x \prod_{k=1}^{m} (X^{e_k} - 1)^{p-1-i_k} = \lambda_i \prod_{k=1}^{m} (X^{e_k} - 1)^{p-1} \neq 0.$$

This means that x is different from zero if R is not empty. The vectors of B^j are linearly independent.

B^0 has p^m elements, since

$$|B^0| = |[0, p-1]^m| = p^m.$$

Then B^0 is a basis of A. The space generated by B^1 is a hyperplane of A which is in P. Then B^1 is a basis of P. So is becomes, from the definition of P^j, $j > 1$, that each element of P^j can be written as a linear combination of elements of B^j. So B^j is a basis of P^j.

Remark. The index of nilpotency of P is $M+1$ since $P^{M+1} = \{0\}$.

Theorem 2. *Let $j \in [1, M]$; s and t are, respectively, the quotient and the remainder of the division of j by $p-1$.*

Then P^j is the ideal of A generated by the subset of A.

$$\mathcal{G}^J = \{(X^{g_1} - 1)^{p-1} \cdots (X^{g_s} - 1)^{p-1} (X^{g_{s+1}} - 1)^t \mid g_1, \ldots, g_{s+1} \text{ are linearly independent in } G\}.$$

Proof. The ideal generated by $\mathcal{G}^j$ is in P^j and not in P^{j+1} since each element of $\mathcal{G}^j$ is the product of $j = s(p-1) + t$ factors $(X^{g_i} - 1)$.

Let σ be an automorphism of the Fp-vector space G and let the A automorphism be defined so that

$$x \in A, \qquad x = \sum_{g \in G} x_g X^g, \qquad \phi_\sigma(x) = \sum_{g \in G} x_g X^{\sigma(g)}.$$

It is clear that $\phi_\sigma(\mathcal{G}^j) = \mathcal{G}^j$.

Poli shows in [1] that if an ideal of A is invariant under the group $\{\phi_\sigma \mid \sigma \in \mathrm{GL}(F_p, m)\}$, it is one of the powers of the radical of A. Hence, the ideal generated by $\mathcal{G}^j$ is P^j.

Corollary 1. *Let j, $j \in [1, M]$; $j = s(p-1)+t$, $t \in [0, p-1[$. If $x \in P^j \setminus P^{j+1}$, there is a y, $y \in \mathcal{G}^{M-j}$ such that:*

$$yx = \lambda (X^{e_1}-1)^{p-1} \cdots (X^{e_m}-1)^{p-1}, \quad \lambda \in K^*.$$

Proof. Let $x \in P^j \setminus P^{j+1}$. There is a z, $z \in P^{M-j}$, such that $zx \neq 0$. Since $\mathcal{G}^{M-j}$ generate P^{M-j}, then $\exists y$, $y \in \mathcal{G}^{M-j}$, $yx \neq 0$. Since $yx \in P^M$, we have that $yx = \lambda (X^{e_1}-1)^{p-1} \cdots (X^{e_m}-1)^{p-1}$ with $\lambda \in K^*$.

The powers of the radical P of A are the Reed and Muller codes when $p^r = 2$ and the generalized Reed and Muller codes when $p^r > 2$ [2] and [3]. Theorem 2 is the generalization of a well-known property of Reed and Muller codes [4, p. 385].

2. The dimensions of the principal ideals in A

If x is an element of A, the principal ideal of A generated by x is denoted (x); $\dim(x)$ denotes the dimension of the K-vector space (x).

Property 1. *Let x, $x \in P^j \setminus P^{j+1}$, $1 \leq j \leq M$. Then each y, $y \in (P^j \setminus P^{j+1}) \cap (x)$ is such that $(y) = (x)$.*

Proof. Let y, $y \in (x)$ and $y \in P^j \setminus P^{j+1}$. Then $y = ax$ with $a \in A \setminus P$: so a is invertible; that proves the property $(x) = (y)$.

Theorem 3. *Let j, $1 \leq j \leq M$ and $j' = M - j$; s' and t' are, respectively, the quotient and the remainder of the division of j' by $p-1$. Then,*

$$\forall x, x \in P^j \setminus P^{j+1}, \quad \dim(x) \geq p^{s'}(t'+1). \tag{1}$$

If x is an element of $\mathcal{G}^j$ (Theorem 2), then $\dim(x) = p^{s'}(t'+1)$. (2)

Proof. Let $x \in P^j \setminus P^{j+1}$. From Corollary 1: $\exists y$, $y \in \mathcal{G}^{M-j}$, $yx \neq 0$. So

$$y = (X^{g_1}-1)^{p-1} \cdots (X^{g_{s'}}-1)(X^{g_{s'+1}}-1)^{t'}$$

where $(g_1, \ldots, g_{s'+1})$ are linearly independent in G.

We note by I the subset of $\mathbb{N}^{s'+1}: I = [0, p-1]^{s'} \times [0, t']$ and $\forall i,\ i \in I,\ i = (i_1, \dots, i_{s'+1}),\ u^i = (X^{g_1} - 1)^{i_1} \cdots (X^{g_{s'+1}} - 1)^{i_{s'+1}}$,

$$\mathcal{U} = \{u^i x \mid i \in I\}.$$

The cardinal of $\mathcal{U}$ is $p^{s'}(t'+1)$. Let z be a K-linear combination of elements of $\mathcal{U}$:

$$z = \sum_{k \in R \subset I} \lambda_k u^k x, \quad \lambda_k \in K^*,$$

and let $i,\ i \in R,\ i = (i_1, \dots, i_{s'+1})$ so that for each $k,\ k \in R,\ k = (k_1, \dots, k_{s'+1})$,

$$(k_1, \dots, k_{s'}) = (i_1, \dots, i_{s'}) \Rightarrow i_{s'+1} < k_{s'+1},$$

$$(k_1, \dots, k_{s'}) \neq (i_1, \dots, i_{s'}) \Rightarrow \sum_{l=1}^{s'} i_l \leq \sum_{l=1}^{s'} k_l.$$

Then

$$(X^{g_1} - 1)^{p-1-i_1} \cdots (X^{g_{s'}} - 1)^{p-1-i_{s'}} (X^{g_{s'+1}} - 1)^{t'-i_{s'+1}} z = yx \neq 0.$$

So $z \neq 0$, if R is not empty.

$\mathcal{U}$ is a system of $p^{s'}(t'+1)$ linearly independent vectors of the K-vector space (x). (1) is proved.

We now suppose that $x = (X^{g_{s'+1}} - 1)^{p-1-t'}(X^{g_{s'+2}} - 1)^{p-1} \cdots (X^{g_m} - 1)^{p-1}$, where $(g_1, \dots, g_m)$ is a basis of G.

B^0 is expressed from $(g_1, \dots, g_m)$ (Theorem 1). So, if v is in B^0, either $vx \in \mathcal{U}$ or $vx = 0$. Then $\mathcal{U}$ is a basis of (x). (2) is proved.

3. The extended Reed–Solomon codes considered as ideals of A

Notations. $n = p^m - 1,\ S = [0, n]$.

$\forall k,\ k \in S$, the weight of k is $\omega(k)$:

$$\omega(k) = \sum_{i=0}^{m-1} k_i, \qquad k_i \in [0, p-1], \quad \sum_{i=0}^{m-1} k_i p^i = k.$$

$\forall j,\ 1 \leq j \leq M,\ S_j = \{k \in S \mid \omega(k) < j\}$.

$\forall x,\ x \in A,\ x = \sum_{g \in G} x_g X^g$, and $\forall k,\ k \in S,\ x(k) = \sum_{g \in G} x_g g^k$.

$x(k)$ is calculated in an overfield of K and G.

Property 2. $\forall j,\ 1 \leq j \leq M,\ P^j = \{x \in A \mid \forall k,\ k \in S_j,\ x(k) = 0\}$.

Proof. For the proof, cf. [3].

Henceforth $K = G$. The Reed–Solomon code, here denoted by C_d, of length n, with minimum distance d over G, is the cyclic code with generator

$$g_d(X) = \prod_{k=1}^{d-1} (X - \alpha^k),$$

where α is a primitive element of G.

The extended Reed–Solomon code, here denoted by $\hat{C}_d$, is invariant under the affine permutation group on GF(p^m). (Theorem of Kasami [5].)

It is therefore an ideal of A, expressed as

$$\hat{C}_d = \{x \in A \mid x(k) = 0 \text{ for } k = 0, 1, \ldots, d-1\}. \tag{3}$$

The dimension of $\hat{C}_d$ is $\dim \hat{C}_d = n - d + 1$ [5].

Theorem 4. *The extended Reed–Solomon code $\hat{C}_d$ is a principal ideal of A iff d is in the set*:

$$D = \left\{ d_l = jp^k + \sum_{i=k+1}^{m-1} (p-1)p^i \;\middle|\; \begin{array}{l} j \in [1, p-1], k \in [0, m-1] \\ l = j + (p-1)|[k+1, m-1]| \end{array} \right\}.$$

(If $k = m-1$, then $d_l = jp^{m-1}$.) If $d = d_l$, $d_l \in D$, then $\hat{C}_d = (\hat{g}_d)$, where $\hat{g}_d$ is the word g_d extended.

Proof. (1) First we suppose that $d \in D$. Then

$$\exists l, \qquad l = j + (p-1)|[k+1, m-1]|, \quad d = d_l.$$

We have

$$\dim \hat{C}_d = n - d + 1 = p^m - d = p^k \left(p^{m-k} - \sum_{i=k+1}^{m-1} (p-i)p^{i-k} - j \right)$$

$$= p^k (p - j).$$

But d is such that for all i, $i \in S$ and $\omega(i) < l$, then $i < d$. Therefore it follows from (3) and from Property 2 that $\hat{C}_d \subset P^l$. $\hat{g}_d$ is such that $\hat{g}_d(l) \neq 0$ by the definition of the generator g_d. Then $\hat{g}_d \notin P^{l+1}$.

We have shown:

Property 3. *If $d = d_l$, $d_l \in D$, then $\hat{g}_d \in P^l \setminus P^{l+1}$ and then $\hat{C}_d \subset P^l$, $\hat{C}_d \not\subset P^{l+1}$.*

Then, appealing to Theorem 3, we have $\dim(\hat{g}_d) \geq p^s(t+1)$ where $s = m - |[k+1, m-1]| - 1 = k$ and $t = p - 1 - j$. We have

$$(\hat{g}_d) \subset \hat{C}_d \quad \text{and} \quad \dim(\hat{g}_d) \geq \dim \hat{C}_d.$$

Therefore $\hat{C}_d = (\hat{g}_d)$.

(2) We suppose now that $d \notin D$. Let l be the first index such that $d < d_l$. Since $\hat{C}_{d_l} \subset \hat{C}_d$, it follows from Property 3 that $\hat{C}_d \notin P^{l+1}$. If $l = 1$, $\hat{C}_d \subset P$ and $\hat{C}_d \not\subset P^2$. If $l > 1$, $\hat{C}_d \subset \hat{C}_{d_{l-1}}$. So, it follows from Property 3 that $\hat{C}_d \subset P^{l-1}$. But $\hat{C}_{d_{l-1}} = (\hat{g}_{d_{l-1}})$. If there is one x, $x \in \hat{C}_d \cap (P^{l-1} \setminus P^l)$, then, by Property 1, $\hat{C}_{d_{l-1}} = (x)$ with $(x) \subset \hat{C}_d$. So $\hat{C}_d = \hat{C}_{d_{l-1}}$. This equation is impossible because $d > d_{l-1}$. So $\hat{C}_d \subset P^l$.

In all the cases, the definition of the generator gives $\hat{g}_d \notin P^{l+1}$. We have proved Property 4.

Property 4. *Let d be such that $d \notin D$. If l is the first index such that $d < d_1$, then $\hat{C}_d \subset P^l$, $\hat{C}_d \not\subset P^{l+1}$ and $\hat{g}_d \in P^l \setminus P^{l+1}$.*

Then, if $\hat{C}_d$ is a principal ideal of A, it follows from Property 4 and Property 1 that $\hat{C}_d = (\hat{g}_d) = (\hat{g}_{d_l})$. This equation is impossible because $d < d_l$. Theorem 4 is thus proved.

References

[1] A. Poli, Codes stables sous le groupe des automorphismes isométriques de $A = F_p[X_1, \ldots, X_n]/(X_1^p - 1, \ldots, X_n^p - 1)$, C.R. Acad. Sci. Paris (1980).
[2] S.D. Berman, Kibernetika 3(1) (1967) 31–39.
[3] P. Charpin, Puissances du radical d'une algèbre modulaire et codes cycliques, Revue CETHEDEC (1981).
[4] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).
[5] J.H. Van Lint, Coding Theory (Springer, New York, 1971).