Proc. Indian Acad. Sci. (Math. Sci.), Vol. 111, No. 4, November 2001, pp. 371–379.

Cyclic codes of length 2^m

MANJU PRUTHI

Department of Mathematics, M.D. University P.G. Regional Centre, Rewari 123 401, India
E-mail: m_pruti22@yahoo.com

MS received 15 March 2000; revised 26 March 2001

Abstract. In this paper explicit expressions of $m+1$ idempotents in the ring $R = F_q[X]/\langle X^{2^m} - 1\rangle$ are given. Cyclic codes of length 2^m over the finite field F_q, of odd characteristic, are defined in terms of their generator polynomials. The exact minimum distance and the dimension of the codes are obtained.

Keywords. Cyclotomic cosets; generator polynomial; idempotent generator; $[n, k, d]$ cyclic codes.

1. Introduction

Throughout in this paper we consider F_q to be a field of odd characteristic and the ring $R = F_q[X]/\langle X^{2^m} - 1\rangle$. The ring R can be viewed as semi-simple group ring $F_q C_{2^m}$ where C_{2^m} is a cyclic group of order 2^m generated by x. It is assumed that reader is familiar with the properties of cyclic codes based on the theory of idempotents [3]. In §2 of this paper complete set of equivalence classes (modulo 2^m) is given and also the construction of explicit expressions of idempotents is given. In §3, we completely describe the cyclic codes of length 2^m in terms of their generator polynomials. In §4 we obtain q-cyclotomic cosets (modulo 2^m) when order of q modulo $2^m = 2^{m-2}$. An example has been given to illustrate the results.

2. Construction of idempotents

For any positive integer m, consider the set $S = \{1, 2, 3, \ldots, 2^m - 1\}$. Divide the set S into disjoint classes S_i (modulo 2^m) as follows:

For $1 \leq i \leq m$, consider the set

$$S_i = \{2^{i-1}, 2^{i-1}3, \ldots, 2^{i-1}(2n_i - 1)\}, 1 \leq n_i \leq 2^{m-i}$$

Clearly the elements of S_i are incongruent to each other modulo 2^m. Note that the elements of S_i are the product of 2^{i-1} with odd numbers. So these are divisible by 2^{i-1} but no higher power of 2. In the set S, the number of elements divisible by 2^{i-1} but no higher power of 2 are

$$(2^{m-i+1} - 1) - (2^{m-i} - 1) = 2^{m-i+1} - 2^{m-i} = 2^{m-i}(2 - 1) = 2^{m-i}.$$

Hence the number of elements in the set S_i is

$$\#S_i = 2^{m-i}.$$

Clearly for $i \neq j$, $S_i \cap S_j = \Phi$ and so

$$\#\left(\bigcup_{i=1}^{m} S_i\right) = \sum_{i=1}^{m}(\# S_i) = \sum_{i=1}^{m}(2^{m-i}) = 2^m - 1.$$

Hence the sets $S_i (1 \leq i \leq m)$ form the partitioning of the set S (modulo 2^m).

For $1 \leq i \leq m$, define the element $S_i(x)$ as

$$S_i(X) = \sum_{s \in S_i} x^s = \sum_{n_i=1}^{2^{m-i}} x^{2^{i-1}(2n_i-1)}.$$

Let α be a primitive 2^mth root of unity in an extension of the field F_q. To prove the main theorem we require the following facts:

Fact 2.1 For $1 \leq i \leq m$,

$$S_i(\alpha^j) = \left| \begin{array}{ccc} 0 & \text{if} & 2^{m-i} \not| j \\ -2^{m-i} & \text{if} & j = 2^{m-i} \\ 2^{m-i} & \text{if} & 2^{m-i+1} | j \end{array} \right. .$$

Proof. By definition, for $1 \leq i \leq m$,

$$\begin{aligned} S_i(X) &= \sum_{n_i=1}^{2^{m-i}} x^{2^{i-1}(2n_i-1)} \\ &= \sum_{n_i=1}^{2^{m-i}} x^{2^{i-1}(2n_i-1)} + \sum_{n_i=1}^{2^{m-i}} x^{2^{i-1}(2n_i-2)} - \sum_{n_i=1}^{2^{m-i}} x^{2^{i-1}(2n_i-2)} \\ &= \sum_{k=0}^{2^{m-i+1}-1} (x^{2^{i-1}})^k - \sum_{n_i=1}^{2^{m-i}} x^{2^i(n_i-1)}. \end{aligned}$$

Therefore,

$$S_i(\alpha^j) = \sum_{k=0}^{2^{m-i+1}-1} (\alpha^{2^{i-1}j})^k - \sum_{n_i=1}^{2^{m-i}} \alpha^{2^i j(n_i-1)}. \tag{1}$$

Case 1. If $2^{m-i} \not| j$, then $2^{m-1} \not| 2^{i-1}j$ so $2^{i-1}j \not\equiv 0 \pmod{2^m}$ hence $\alpha^{2^{i-1}j} \not\equiv 1$. Similarly $\alpha^{2^i j} \neq 1$. Therefore (1) gives that

$$S_i(\alpha^j) = \frac{(\alpha^{2^{i-1}j})^{2^{m-i+1}} - 1}{\alpha^{2^{i-1}j} - 1} - \frac{(\alpha^{2^i j})^{2^{m-i}} - 1}{\alpha^{2^i j} - 1} = 0 - 0 = 0$$

(denominator being non-zero). This proves the Case 1.

Case 2. If $j = 2^{m-i}$, then $2^{i-1}j = 2^{m-1}$ and $2^i j = 2^m$. Since α is a primitive 2^mth root of unity in an extension of F_q, so $\alpha^{2^i j} = \alpha^{2^m} = 1$ and $\alpha^{2^{i-1}j} = \alpha^{2^{m-1}} = -1$. Again (1) gives that

$$S_i(\alpha^j) = \sum_{k=0}^{2^{m-i+1}-1} (-1)^k - \sum_{n_i=0}^{2^{m-i}} (+1)^{n_i-1}$$
$$= 0 - 2^{m-i} = -2^{m-i}.$$

This proves the Case 2.

Case 3. If $2^{m-i+1}/j$ then $2^m/2^{i-1}j$ implies that $\alpha^{2^{i-1}j} = 1$ and also $\alpha^{2^i j} = 1$. Again from (1) we have

$$S_i(\alpha^j) = \sum_{k=0}^{2^{m-i+1}-1} (1)^k - \sum_{n_i=0}^{2^{m-i}} (1)^{n_i-1}$$
$$= 2^{m-i+1} - 2^{m-i} = 2^{m-i}(2-1) = 2^{m-i}.$$

This proves the Fact 2.1.

Fact 2.2. For $0 \le i \le m-1$,

$$1 + \sum_{r=i+1}^{m} S_r(\alpha^j) = \left| \begin{array}{ll} 0 & \text{if} \quad 2^{m-i} \not| \, j \\ 2^{m-i} & \text{if} \quad 2^{m-i} \mid j \end{array} \right. .$$

Proof. By definition

$$1 + \sum_{r=i+1}^{m} S_r(\alpha^j) = \sum_{k=0}^{2^{m-i}-1} (\alpha^{2^i j})^k.$$

If $2^{m-i} \not| \, j$ then $2^m \not| \, 2^i j$ implies that $\alpha^{2^i j} \neq 1$. Hence the required sum takes the value zero. Secondly if $2^{m-i}/j$, then $2^m/2^i j$ implies that $\alpha^{2^i j} = 1$ in the extension field and hence the required sum takes the value

$$\sum_{k=0}^{2^{m-i}-1} (1)^k = 2^{m-i}.$$

This proves the Fact 2.2.

Our construction of idempotents is based on the following two facts developed in §2 and 3 of chapter 8 of [3].

Fact 2.3. An expression $e(x)$ in R is an idempotent iff $e(\alpha^j) = 0$ or 1.

Fact 2.4. An idempotent $e_i(x)$ is primitive iff

$$e_i(\alpha^j) = \left| \begin{array}{ll} 1 & \text{if } j \in Y_r \text{ for some } r, 0 \le r \le m \\ 0 & \text{otherwise,} \end{array} \right.$$

where Y_r is some q-cyclotomic coset (modulo 2^m) with $Y_0 = \{0\}$.

Theorem 2.5. *The following polynomial expressions are* $(m+1)$ *idempotents in the ring* R,

$$e_o(x) = \frac{1}{2^m} \sum_{j=0}^{2^m-1} x^j = \frac{1}{2^m} \left\{ 1 + \sum_{k=1}^{m} S_k(x) \right\}$$

and for $1 \le i \le m$

$$e_i(x) = \frac{1}{2^{m-i+1}} \left\{ 1 + \sum_{k=i+1}^{m} S_k(x) - S_i(x) \right\}.$$

Proof. By Fact 2.2

$$e_0(\alpha^j) = \frac{1}{2^m} \left\{ 1 + \sum_{k=1}^{m} S_k(\alpha^j) \right\} = \left| \begin{array}{lll} 0 & \text{if} & 2^m \nmid j \\ 1 & \text{if} & 2^m \mid j \end{array} \right.$$
$$= \left| \begin{array}{lll} 0 & \text{if} & j \in S_k \\ 1 & \text{if} & 2^m \mid j \end{array} \right. .$$

By Fact 2.4, $e_0(x)$ is a primitive idempotent with single non-zero $\alpha^0 = 1$. For $1 \le i \le m$, Facts 2.1 and 2.2 show that

$$e_i(\alpha^j) = \left| \begin{array}{lll} 0 & \text{if} & 2^{m-i} \nmid j \\ 1 & \text{if} & 2^{m-i} = j \\ 0 & \text{if} & 2^{m-i+1} | j \end{array} \right| .$$

Thus for $1 \le i \le m$, $e_i(\alpha^j) = 0$ or 1 and $e_i(\alpha^j) = 1$ only if $j = 2^{m-i}$ or equivalently by definition only if $j \in S_{m-i+1}$. Hence by the Fact 2.3 the expressions $e_i(x)$ are idempotents.

3. Cyclic codes of length 2^m

Let for $0 \le i \le m$, E_i denotes the cyclic code of length 2^m with idempotent generator $e_i(x)$. By (Theorem 56, [4]), (Remark 6.3, [6]) the generator polynomial $g_i(x)$ of the cyclic code E_i is given by

$$g_i(x) = \text{g.c.d.}(e_i(x), x^{2^m} - 1). \tag{2}$$

Define

$$g_0(x) = \sum_{t=0}^{2^m-1} x^t = \frac{1 - x^{2^m}}{1 - x}$$

and for $1 \le i \le m$,

$$g_i(x) = (1 - x^{2^{i-1}})[1 + S_{i+1} + \cdots + S_m].$$

Then to show $g_i(x)$ $(0 \le i \le m)$ is the generating polynomial of the cyclic code E_i. In view of (2) it is sufficient to prove the following two facts:

Fact 3.1. $g_i(\alpha^j) = 0$ iff $e_i(\alpha^j) = 0$.

Fact 3.2. $g_i(x)/x^{2^m} - 1$.

To prove the Fact 3.1, consider for $1 \le i \le m$,

$$\begin{aligned}
e_i(x) &= \frac{1}{2^{m-i+1}}\{1 + S_{i+1} + \cdots + S_m - S_i\} \\
&= \frac{1}{2^{m-i+1}}\left\{\sum_{k=0}^{2^{m-i}-1}(x^{2^i})^k - \sum_{n_i=1}^{2^{m-i}}(x^{2^{i-1}})^{(2n_i-1)}\right\} \\
&= \frac{1}{2^{m-i+1}}\left\{\sum_{k=0}^{2^{m-i}-1}(x^{2^i})^k - x^{2^{i-1}}\sum_{n_i=1}^{2^{m-i}}(x^{2^{i-1}})^{(2n_i-2)}\right\} \\
&= \frac{1}{2^{m-i+1}}\left\{\sum_{k=0}^{2^{m-i}-1}(x^{2^i})^k - x^{2^{i-1}}\sum_{k=0}^{2^{m-i}-1}(x^{2^i})^k\right\} \\
&= \frac{1}{2^{m-i+1}}(1 - x^{2^{i-1}})\left\{\sum_{k=0}^{2^{m-i}-1}(x^{2^i})^k\right\} \\
&= \frac{1}{2^{m-i+1}}(1 - x^{2^{i-1}})\{1 + S_{i+1} + \cdots + S_m\} \\
&= \frac{1}{2^{m-i+1}}g_i(x).
\end{aligned}$$

Thus for $1 \le i \le m$, $e_i(x)$ is a constant multiple of $g_i(x)$. Also by definition $e_0(x)$ is a constant multiple of $g_0(x)$. Hence $g_i(\alpha^j) = 0$ iff $e_i(\alpha^j) = 0$.

To prove the Fact 3.2, consider for $0 \le i \le m$,

$$\begin{aligned}
1 - x^{2^m} &= 1 - (x^{2^i})^{2^{m-i}} = (1 - x^{2^i})\{(x^{2^i})^{2^{m-i}-1} + (x^{2^i})^{2^{m-i}-2} + \cdots + (x^{2^i}) + 1\} \\
&= (1 + x^{2^{i-1}})(1 - x^{2^{i-1}})\{1 + S_{i+1} + \cdots + S_m\} \\
&= (1 + x^{2^{i-1}})g_i(x).
\end{aligned}$$

Thus $g_i(x)$ is a factor of $(1 - x^{2^m})$. Hence the assertion follows.

Theorem 3.3. *E_i is a* $[2^m, 2^{i-1}, 2^{m-i+1}]$ *cyclic code over* $GF(q)$.

Proof. By Corollary 3 ([3], p. 218) (generalized to non binary case) for $0 \le i \le m$, $\dim E_i = \#\alpha^j$ such that $e_i(\alpha^j) = 1$.

By Theorem 2.5, we have $e_i(\alpha^j) = 1$ only if $j \in S_{m-i+1}$. So $\dim E_i = \#S_{m-i+1} = 2^{i-1}$.

As shown in [5, 6, 1] it is easy to prove that the repetition code E_i generated by $g_i(x)$ has the minimum distance 2^{m-i+1} and $d(E_0) = 2^m = \#$ non-zero terms in $g_0(x)$.

4. q-Cyclotomic cosets (modulo 2^m) when order $(q) = 2^{m-2}$

First note that such a q exists due to the following facts [2]. Obviously in this case $m \ge 3$. So throughout this section assume that $m \ge 3$.

Fact 4.1. The integer 2^m has no primitive root.

Fact 4.2. Let a be any odd integer, then it is always true that $a^{2^{m-2}} \equiv 1 \pmod{2^m}$.

Fact 4.3. If $\mathrm{ord}(a) = 2 \pmod{2^3}$ and $a^2 \not\equiv 1 \pmod{2^4}$, then $\mathrm{ord}(a) = 2^{m-2} \pmod{2^m}$ for every $m \geq 3$.

Computation of q-cyclotomic cosets (modulo 2^m) depend upon the following facts:

Fact 4.4. If $\mathrm{ord}(q) = 2^{m-2}$ (modulo 2^m) for every $m \geq 3$, (Fact 4.3), then $q^t \not\equiv -1$ (mod 2^m) for $1 \leq t \leq 2^{m-2}$.

Proof. For $t \geq 2^{m-2}$, we have $q^t \equiv 1 \pmod{2^m}$.

If possible let $q^t \equiv -1 \pmod{2^m}$ for some non-negative integer $t < 2^{m-2}$, then $q^{2t} \equiv 1 \pmod{2^m}$. But $\mathrm{ord}(q) = 2^{m-2}$ implies that $2^{m-2} | 2t$ or $2^{m-3} | t \Rightarrow t = 2^{m-3}a$, but $t < 2^{m-2}$. So we must have $a = 1$. So we have

$$\Rightarrow q^{2^{m-3}} \equiv -1 (\text{mod } 2^m)$$
$$\Rightarrow q^{2^{m-3}} \equiv -1 (\text{mod } 2^{m-1}). \tag{3}$$

But we are assuming that $\mathrm{ord}(q) = 2^{m-2}$ for all $m \geq 3$. So we have

$$q^{2^{m-3}} \equiv 1 (\text{mod } 2^{m-1}). \tag{4}$$

From (3) and (4)

$$-1 \equiv 1 (\text{mod } 2^{m-1}) \quad \text{for all } m \geq 3$$

which is not possible. Hence the result follows.

Fact 4.5. Thus in this case q cyclotomic cosets modulo 2^m are given by:

For $1 \leq i \leq m$,

$$X_i = \{2^{i-1}, 2^{i-1}q, 2^{i-1}q^2, \ldots, 2^{i-1}q^{2^{m-(i+1)}-1}\},$$
$$X_i^* = \{-2^{i-1}, -2^{i-1q}, -2^{i-1}q^2, \ldots, -2^{i-1}q^{2^{m-(i+1)}-1}\}.$$

Remark 4.6. By definition of S_i it is clear that for $1 \leq i \leq m$,

$$S_i = X_i \cup X_i^*.$$

Note that integers of the type $q = 8\lambda + 3 (\lambda \geq 0)$ satisfy the above facts. In particular we may consider $q = 3$, then order $(3) = 2^{m-2}$ (modulo 2^m) for all $m \geq 3$. In this case observe the following.

Fact 4.7. For $1 \leq i \leq m - 2$,

$$3^{2^{m-(i+1)}} \equiv 1 (\text{mod } 2^{m-i+1})$$

or

$$2^{i-1} 3^{2^{m-(i+1)}} \equiv 2^{i-1} (\text{mod } 2^m).$$

Fact 4.8. Since 3 is primitive root of unity modulo 4

$$3^2 \equiv 1 (\text{mod } 2^2) \Rightarrow 2^{m-2}3^2 \equiv 2^{m-2} (\text{modulo } 2^m).$$

Fact 4.9. Since $3 \equiv -1$ (mod 2^2),

$$2^{m-2}.3 \equiv -2^{m-2} (\text{mod } 2^m)$$

and

$$2^{m-2}.3^2 \equiv -2^{m-2}.3 (\text{modulo } 2^m).$$

Fact 4.10.

$$\begin{aligned} & 1 \equiv -1 (\text{mod } 2), \\ \Rightarrow & 2^{m-1} \equiv -2^{m-1} (\text{mod } 2^m). \end{aligned}$$

Using the facts of §4, the 3-cyclotomic cosets modulo 2^m are given as follows:
For $1 \leq i \leq m-2$,

$$\begin{aligned} X_i &= \{2^{i-1}, 2^{i-1}.3, 2^{i-1}3^2, \ldots, 2^{i-1}3^{2^{m-(i+1)}-1}\}, \\ X_i^* &= \{-2^{i-1}, -2^{i-1}3, -2^{i-1}3^2, \ldots, -2^{i-1}3^{2^{m-(i+1)}-1}\} \end{aligned}$$

and

$$\begin{aligned} X_{m-1} &= X_{m-1}^* = \{2^{m-2}, 2^{m-2}.3\} = \{-2^{m-2}, -2^{m-2}.3\}, \\ X_m &= X_m^* = \{2^{m-1}\}. \end{aligned}$$

Example. Consider $q = 5$ and C_{2^5} be a cyclic group of order 2^5 generated by x. Then the q-cyclotomic cosets (modulo 2^5) are given by

$$\begin{aligned} X_1 &= \{1, 5, 25, 29, 17, 21, 9, 13\}, \\ X_1^* &= \{-1, -5, -25, -29, -17, -21, -9, -13\} \\ &= \{31, 27, 7, 3, 15, 11, 23, 19\}, \\ X_2 &= \{2, 10, 18, 26\}, \\ X_2^* &= \{30, 22, 14, 6\} \\ X_3 &= \{4, 20\}, \\ X_3^* &= \{28, 12\}, \\ X_4 &= \{8\}, \\ X_4^* &= \{24\}, \\ X_5 &= \{6\} = X_5^*. \end{aligned}$$

By Remark 4.6,

$$\begin{aligned} S_1 &= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}, \\ S_2 &= \{2, 6, 10, 14, 18, 22, 26, 30\}, \\ S_3 &= \{4, 12, 20, 28\}, \\ S_4 &= \{8, 24\}, \\ S_5 &= \{16\}. \end{aligned}$$

The six distinct idempotents in this case can be read as follows:

$$
\begin{aligned}
e_0(x) &= \frac{1}{2^5}\{1 + S_1 + S_2 + S_3 + S_4 + S_5\}(x),\\
e_1(x) &= \frac{1}{2^5}\{1 + S_2 + S_3 + S_4 + S_5 - S_1\}(x),\\
e_2(x) &= \frac{1}{2^4}\{1 + S_3 + S_4 + S_5 - S_2\}(x),\\
e_3(x) &= \frac{1}{2^3}\{1 + S_4 + S_5 - S_3\}(x),\\
e_4(x) &= \frac{1}{2^2}\{1 + S_5 - S_4\}(x),\\
e_5(x) &= \frac{1}{2}\{1 - S_5\}(x).
\end{aligned}
$$

The important parameters of the codes E_0, E_1, E_2, E_3, E_4, E_5 of length 2^5 over the field GF(5) are listed in the table below.

Code	Non-zero	Dimension K	Minimum distance, d	Generator polynomial, $g_i(x)$
E_0	$\alpha^0 = 1$	1	2^5	$1 + x + x^2 + \cdots + x^{31}$
E_1	α^{16}	1	2^5	$(1 - x)\{1 + S_2 + S_3 + S_4 + S_5\}$
E_2	α^8, α^{24}	2	2^4	$(1 - x^2)\{1 + S_3 + S_4 + S_5\}$
E_3	$\alpha^4, \alpha^{12}, \alpha^{20}, \alpha^{28}$	4	2^3	$(1 - x^4)\{1 + x^8 + x^{24} + x^{16}\}$
E_4	$\alpha^2, \alpha^6, \alpha^{10}, \alpha^{14}, \alpha^{18}, \alpha^{22}, \alpha^{26}, \alpha^{30}$	8	2^2	$(1 - x^8)\{1 + x^{16}\}$
E_5	$\alpha^j, j \in S_1$	16	2	$(1 - x^{16})$

Example. Consider $q = 3$ and C_2^3 be a cyclic group of order 2^3 generated by x. Then the q-cyclotomic cosets (modulo 2^3) are given by

$$
\begin{aligned}
X_1 &= \{1, 3\},\\
X_1^* &= \{5, 7\},\\
X_2 &= \{2, 6\},\\
X_3 &= \{4\},\\
X_0 &= \{0\}.
\end{aligned}
$$

The five primitive idempotents in the group algebra GF(3) C_2^3 are given with their non-zeroes:

Primitive idempotents	Non-zeroes
$e_0(x) = \frac{1}{2^3}\{1 + X_1 + X_1^* + X_2 + X_3\}(x)$	α^0
$e_1(x) = \frac{1}{2^3}\{1 + X_3 + X_2 - (X_1 + X_1^*)\}(x)$	$\alpha^j, j \in X_3$
$e_2(x) = \frac{1}{2^2}\{1 + X_3 - X_2\}(x)$	$\alpha^j, j \in X_2$
$e_3(x) = \frac{1}{2^2}\{(1 - X_3) - (X_1 - X_1^*)\}(x)$	$\alpha^j, j \in X_1$
$e_4(x) = \frac{1}{2^2}\{(1 - X_3) + (X_1 - X_1^*\}(x)$	$\alpha^j, j \in X_1^*$

References

[1] Arora S K and Pruthi Manju, Minimal cyclic codes of length $2p^n$, Finite fields and their applications, **5** (1999) 177–187
[2] Burton David M, Elementary number theory, 2nd ed. (University of New Harsheri)
[3] Mac Williams F J and Sloane N J A, Theory of error-correcting codes (Amsterdam: North Holland) (1977)
[4] Pless V, Introduction to the theory of error correcting codes (New York: Wiley-Interscience) (1981)
[5] Pruthi Manju and Arora S K, Minimal codes of prime power length, Finite fields and their applications, **3** (1997) 99–113
[6] Vermani Lekh R, Elements of algebraic coding theory (UK: Chapman and Hall) (1992)