ELSEVIER
Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 13 (2007) 1086–1095
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

The weight distributions of irreducible cyclic codes of length 2^m

Anuradha Sharma [1], Gurmeet K. Bakshi, Madhu Raka *

Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India

Received 7 February 2006; revised 21 July 2007

Available online 7 September 2007

Communicated by Gary L. Mullen

Abstract

Let m be a positive integer and q be an odd prime power. In this paper, the weight distributions of all the irreducible cyclic codes of length 2^m over F_q are determined explicitly.

Keywords: Irreducible cyclic codes; Cyclotomic cosets

1. Introduction

Let F_q be the finite field with q elements and n be a positive integer coprime to q. A cyclic code $\mathcal{C}$ of length n over F_q is a linear subspace of F_q^n with the property that if $(a_0, a_1, a_2, \dots, a_{n-1}) \in \mathcal{C}$, then the cyclic shift $(a_{n-1}, a_0, a_1, \dots, a_{n-2})$ is also in $\mathcal{C}$. The code $\mathcal{C}$ can also be regarded as an ideal in the principal ideal ring $R_n = \mathrm{F}_q[x]/\langle x^n - 1\rangle$ under the vector space isomorphism from F_q^n to R_n given by $(a_0, a_1, \dots, a_{n-1}) \mapsto a_0 + a_1 x + \dots + a_{n-1}x^{n-1}$. Every ideal $\mathcal{C}$ is generated by a unique monic polynomial $g(x)$, which is a divisor of $(x^n - 1)$, called the generating polynomial of $\mathcal{C}$. A minimal ideal in R_n is called an irreducible cyclic code of length n over F_q.

For any integer s, the q-cyclotomic coset of s modulo n is the set $C_s = \{s, sq, sq^2, \dots, sq^{n_s-1}\}$, where n_s is the least positive integer such that $sq^{n_s} \equiv s \pmod{n}$. There is a 1–1 corre-

* Corresponding author.
E-mail address: mraka@pu.ac.in (M. Raka).
[1] Research support by N.B.H.M., India, is gratefully acknowledged.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.07.004

spondence between irreducible cyclic codes of length n over F_q and q-cyclotomic cosets modulo n. Let α denote a primitive nth root of unity in some extension field of F_q. For any cyclotomic coset C_s, $M_{\alpha^s}(x) = \prod_{j \in C_s}(x - \alpha^j)$ is the minimal polynomial of α^s over F_q. The ideal, $\mathcal{M}_s^{(n)}$, generated by $\frac{x^n-1}{M_{\alpha^s}(x)}$ is a minimal ideal in R_n and it is the irreducible cyclic code corresponding to the cyclotomic coset C_s. For reference, see MacWilliams, Sloane [5, Chapters 7, 8].

The Hamming weight, $wt(v)$, of a vector $v \in \mathrm{F}_q^n$ is the number of non-zero coordinates in v. The minimum Hamming weight of a code is the smallest of all the non-zero weights of its codewords.

Let $\mathcal{C}$ be a code of length n over F_q. Let $A_i^{(n)}$ denote the number of codewords of Hamming weight i in $\mathcal{C}$. Then the list $A_0^{(n)}, A_1^{(n)}, \ldots, A_n^{(n)}$ is called the Hamming weight distribution (or weight spectrum) of $\mathcal{C}$. The knowledge of the weight distribution of a code enables one to calculate the probability of undetected errors when the code is used purely for error detection. The least value of i, $i > 0$, for which $A_i^{(n)}$ is non-zero is the minimum Hamming weight of $\mathcal{C}$, which gives a measure of how good a code is at error correcting. Thus the problem of determining the weight distribution of a code is of great interest.

Many authors have worked on the problem of determining the weight distributions of irreducible cyclic codes using different techniques. MacWilliams and Seery [4] gave a procedure to obtain the weight distributions of binary irreducible cyclic codes, which involves generation of a pseudorandom sequence, but it can be implemented only on a powerful computer. Van der Vlugt [8] connected the problem of computing weight distributions to the evaluation of certain sums involving Gauss sums, which are generally hard to determine explicitly. To evaluate these sums in some special cases, certain algorithms were given by Baumert and McEliece [2], Moisio and Väänänen [6], Fitzgerald and Yucas [3], etc., using various techniques. In [1], Augot used the theory of Grobner basis for a certain system of algebraic equations to give information about the minimum weight codewords.

Let $m \geqslant 1$ be an integer and q be an odd prime power. In this paper, we explicitly compute the weight distributions of all the irreducible cyclic codes of length $n = 2^m$ over F_q directly from their generating polynomials. In Section 2, we list all the q-cyclotomic cosets modulo 2^m. We also show that the weight distribution of an irreducible cyclic code corresponding to any q-cyclotomic coset modulo 2^m can be computed if we know the weight distribution of the irreducible cyclic code $\mathcal{M}_1^{(2^r)}$ of length 2^r, $1 \leqslant r \leqslant m$, which corresponds to the cyclotomic coset containing 1. In Section 3 (see Theorems 1–3), we explicitly compute the weight distribution of irreducible cyclic code $\mathcal{M}_1^{(2^r)}$ of length 2^r for $r \geqslant 1$.

2. Some lemmas

Since q is odd, we write $q = 1 + 2^b c$ or $-1 + 2^b c$ for some integers $b, c, b \geqslant 2$ and c odd, according as $q \equiv 1 \pmod 4$ or $-1 \pmod 4$. For any integer $k \geqslant 1$, let $O_k(q)$ denote the multiplicative order of q modulo k. We have, for any positive integer $r, r \geqslant 2$,

$$O_{2^r}(q) = \begin{cases} 2^{r-b} & \text{if } r \geqslant b+1,\ q = \pm 1 + 2^b c, \\ 1 & \text{if } 2 \leqslant r \leqslant b,\ q = 1 + 2^b c, \\ 2 & \text{if } 2 \leqslant r \leqslant b,\ q = -1 + 2^b c. \end{cases} \tag{1}$$

Lemma 1.

(a) *Let $q = 1 + 2^b c$, $b \geqslant 2$, c odd. All the distinct q-cyclotomic cosets modulo 2^m are given by C_0, $C_{2^{m-1}}$ and $C_{2^{m-r}s}$ for $2 \leqslant r \leqslant m$ and s runs over S_r for each r, where*

$$S_r = \begin{cases} \{\pm 1, \pm 3, \ldots, \pm 3^{(2^{b-2}-1)}\} & \text{if } b+1 \leqslant r \leqslant m, \\ \{\pm 1, \pm 3, \ldots, \pm 3^{(2^{r-2}-1)}\} & \text{if } 2 \leqslant r \leqslant b. \end{cases}$$

(b) *Let $q = -1 + 2^b c$, $b \geqslant 2$, c odd. All the distinct q-cyclotomic cosets modulo 2^m are given by C_0, $C_{2^{m-1}}$ and $C_{2^{m-r}s}$ for $2 \leqslant r \leqslant m$ and s runs over T_r for each r, where*

$$T_r = \begin{cases} \{1, 3, 3^2, \ldots, 3^{(2^{b-1}-1)}\} & \text{if } b+1 \leqslant r \leqslant m, b \geqslant 3, \\ \{1, 3, 3^2, \ldots, 3^{(2^{r-2}-1)}\} & \text{if } 2 \leqslant r \leqslant b, b \geqslant 2, \\ \{1, -1\} & \text{if } 3 \leqslant r \leqslant m, b = 2. \end{cases}$$

This is Proposition 2 *of* [7].

Let α be a primitive 2^mth root of unity in some extension field of F_q. For $1 \leqslant r \leqslant m$ and s odd, let $\mathcal{M}^{(2^m)}_{2^{m-r}s}$ be the irreducible cyclic code of length 2^m over F_q corresponding to the cyclotomic coset $C_{2^{m-r}s}$. As s is odd, the code $\mathcal{M}^{(2^m)}_{2^{m-r}s}$ is equivalent to the code $\mathcal{M}^{(2^m)}_{2^{m-r}}$. Also $\mathcal{M}^{(2^m)}_0$ (which corresponds to the coset C_0) is a 1-dimensional subspace spanned by $\frac{x^{2^m}-1}{x-\alpha^0} = 1 + x + \cdots + x^{2^m-1}$. Thus every non-zero codeword in $\mathcal{M}^{(2^m)}_0$ has weight 2^m. Hence, it is enough to study the weight distribution of the irreducible codes, $\mathcal{M}^{(2^m)}_{2^{m-r}}$, corresponding to the cosets $C_{2^{m-r}}$, $1 \leqslant r \leqslant m$.

The following lemma shows that the weight distribution of $\mathcal{M}^{(2^m)}_{2^{m-r}}$, $1 \leqslant r \leqslant m$, can be computed from the weight distribution of the irreducible cyclic code $\mathcal{M}^{(2^r)}_1$ of length 2^r.

Lemma 2. *Let $1 \leqslant r \leqslant m$. The code $\mathcal{M}^{(2^m)}_{2^{m-r}}$ is the repetition code of the irreducible cyclic code $\mathcal{M}^{(2^r)}_1$ of length 2^r, repeated 2^{m-r} times. As a consequence,*

$$A^{(2^m)}_i = \begin{cases} 0 & \text{if } 2^{m-r} \text{ does not divide } i, \\ A^{(2^r)}_j & \text{if } i = 2^{m-r}j,\ 0 \leqslant j \leqslant 2^r, \end{cases} \tag{2}$$

where $A^{(2^m)}_0, A^{(2^m)}_1, A^{(2^m)}_2, \ldots$ is the weight distribution of $\mathcal{M}^{(2^m)}_{2^{m-r}}$ and $A^{(2^r)}_0, A^{(2^r)}_1, A^{(2^r)}_2, \ldots$ is the weight distribution of $\mathcal{M}^{(2^r)}_1$.

Proof. The generating polynomial of $\mathcal{M}^{(2^m)}_{2^{m-r}}$ is $\frac{x^{2^m}-1}{M_{\alpha^{2^{m-r}}}(x)}$, where $M_{\alpha^{2^{m-r}}}(x) = \prod_{j \in C_{2^{m-r}}} (x - \alpha^j)$. We have

$$x^{2^m} - 1 = \left(x^{2^r} - 1\right)\left(1 + x^{2^r} + \left(x^{2^r}\right)^2 + \cdots + \left(x^{2^r}\right)^{2^{m-r}-1}\right).$$

Note that α^j, $j \in C_{2^{m-r}}$, are roots of $x^{2^r}-1$ and therefore $M_{\alpha^{2^{m-r}}}(x)$ is an irreducible factor of $x^{2^r}-1$ over F_q and we have

$$\frac{x^{2^m}-1}{M_{\alpha^{2^{m-r}}}(x)} = \frac{x^{2^r}-1}{M_{\alpha^{2^{m-r}}}(x)}\left(1+x^{2^r}+\left(x^{2^r}\right)^2+\cdots+\left(x^{2^r}\right)^{2^{m-r}-1}\right).$$

It is now clear from this expression that the code of length 2^m with generating polynomial $\frac{x^{2^m}-1}{M_{\alpha^{2^{m-r}}}(x)}$ is the repetition of the code of length 2^r having generating polynomial $\frac{x^{2^r}-1}{M_{\alpha^{2^{m-r}}}(x)}$, repeated 2^{m-r} times. But the code of length 2^r with generating polynomial $\frac{x^{2^r}-1}{M_{\alpha^{2^{m-r}}}(x)}$ is the irreducible code of length 2^r corresponding to the cyclotomic coset containing 1. From this, (2) follows immediately. This proves the lemma. □

The following lemma is needed in the proof of Theorem 3.

Lemma 3. *Let $r \geqslant 3$ and $q = -1 + 2^b c$, $b \geqslant 2$, c odd. Let $t = \min(r, b+1)$ and γ be a primitive 2^tth root of unity in some extension field of F_q. Let $\epsilon = \gamma^{1+q}$. Let $\{b_i\}$, $0 \leqslant i \leqslant 2^t-2$, be a finite sequence of elements of F_q satisfying the linear homogeneous recurrence relation*

$$b_i - \left(\epsilon\gamma + \gamma^{-1}\right)b_{i-1} + \epsilon b_{i-2} = 0 \quad \textit{for } 2 \leqslant i \leqslant 2^t - 2 \tag{3}$$

with initial conditions $b_0 = -\epsilon$, $b_1 = -(\gamma + \gamma^q) = -(\gamma + \epsilon\gamma^{-1})$ and end conditions $b_{2^t-3} = (\gamma + \gamma^q)$, $b_{2^t-2} = 1$.

Then

(i) $b_i \neq 0$ *for* $0 \leqslant i \leqslant 2^{t-1}-2$ *and* $2^{t-1} \leqslant i \leqslant 2^t-2$,
(ii) $b_{2^{t-1}-1} = 0$,
(iii) $b_{i+2^{t-1}} = -b_i$ *for* $0 \leqslant i \leqslant 2^{t-1}-2$,
(iv) $b_u b_{v-1} - b_v b_{u-1} \neq 0$ *for* $1 \leqslant u < v \leqslant 2^{t-1}-2$.

Proof. Since $\gamma^{2^{t-1}} = -1$, we have

$$\epsilon = \gamma^{1+q} = \gamma^{2^b c} = \left(\gamma^{2^{t-1}}\right)^{2^{b-t+1}c} = (-1)^{2^{b+1-t}} = \begin{cases} -1 & \text{if } r \geqslant b+1, \\ 1 & \text{if } r \leqslant b. \end{cases} \tag{4}$$

Further, since $q^2 \equiv 1 \pmod{2^t}$ and $\gamma^{2^t} = 1$, we get that $\gamma^{q^2-1} = 1$. Thus $\gamma \in \mathrm{F}_{q^2}$, which yields $\gamma + \gamma^q$ and $\gamma.\gamma^q \in \mathrm{F}_q$. Therefore $\epsilon\gamma + \gamma^{-1} = \epsilon(\gamma + \epsilon\gamma^{-1}) = \epsilon(\gamma + \gamma^q) \in \mathrm{F}_q$, as $\epsilon = \pm 1$. Thus the recurrence relation (3) has coefficients in F_q. The characteristic equation of this recurrence relation is given by $y^2 - (\epsilon\gamma + \gamma^{-1})y + \epsilon = (y - \epsilon\gamma)(y - \gamma^{-1}) = 0$. The two characteristic roots $\epsilon\gamma$ and γ^{-1} are distinct, as $t \geqslant 3$. Therefore, the general solution of (3) is $b_i = c_1(\epsilon\gamma)^i + c_2\gamma^{-i}$ for some constants $c_1, c_2 \in \mathrm{F}_q$. Using $b_0 = -\epsilon$, $b_1 = -(\gamma + \gamma^q)$, we get that $b_0 = -\epsilon = c_1 + c_2$ and $b_1 = -(\gamma + \epsilon\gamma^{-1}) = c_1\epsilon\gamma + c_2\gamma^{-1}$. Solving these, we get $c_1 = \frac{-\gamma}{\epsilon\gamma - \gamma^{-1}}$, $c_2 = \frac{\epsilon\gamma^{-1}}{\epsilon\gamma - \gamma^{-1}}$.

(If the end conditions $b_{2^t-3} = (\gamma + \gamma^q)$ and $b_{2^t-2} = 1$ are used, one finds that the values of constants c_1, c_2 remain the same.) Thus

$$b_i = \frac{-\epsilon^i \gamma^{i+1} + \epsilon \gamma^{-(i+1)}}{\epsilon\gamma - \gamma^{-1}}. \tag{5}$$

Therefore

$$b_i = 0 \quad \text{if and only if} \quad \gamma^{2i+2} = \epsilon^{i-1}. \tag{6}$$

If i is even, (6) cannot occur. This is because, in that case, we have $\gamma^{2i+2} = \epsilon$, which gives $\gamma^{4i+4} = 1$. This further implies that $2^t | 4i + 4$, i.e., $2^{t-2} | i + 1$, which is not possible for $t \geqslant 3$.

If i is odd, (6) gives $\gamma^{2i+2} = 1$, i.e., $2^{t-1} | i + 1$. For $0 \leqslant i \leqslant 2^t - 2$, this can happen if and only if $i = 2^{t-1} - 1$. This proves (i) and (ii). As $\gamma^{2^{t-1}} = -1$ and $\epsilon^{2^{t-1}} = 1$, (iii) is immediate from (5). Substituting the values of b_i from (5) and simplifying, we get

$$b_u b_{v-1} - b_v b_{u-1} = \frac{\epsilon^v \gamma^{v-u} - \gamma^{-(v-u)} \epsilon^u}{\epsilon\gamma - \gamma^{-1}} = -\epsilon^{u-1} b_{v-u-1},$$

which, by (i), is non-zero for $1 \leqslant u < v \leqslant 2^{t-1} - 2$. □

3. The weight distribution of $\mathcal{M}_1^{(2^r)}$, r a positive integer

Throughout this section, α denotes a primitive 2^rth root of unity in some extension of F_q.

Theorem 1. *Let $q = 1 + 2^b c$, $b \geqslant 2$, c odd.*

If $r \leqslant b$, the only possible non-zero weight in $\mathcal{M}_1^{(2^r)}$ is 2^r, which is attained by all its $q - 1$ non-zero codewords.

If $r \geqslant b + 1$, the weight distribution of $\mathcal{M}_1^{(2^r)}$ is given by

$$A_i^{(2^r)} = \begin{cases} 0 & \text{if } 2^b \text{ does not divide } i, \\ \binom{2^{r-b}}{j}(q-1)^j & \text{if } i = 2^b j,\ 0 \leqslant j \leqslant 2^{r-b}. \end{cases}$$

Proof.

Case 1. $r \leqslant b$.

In this case, 2^r divides $q - 1$. Therefore $\alpha^{2^r} = 1$ implies $\alpha^{q-1} = 1$. Hence $\alpha \in F_q$. Also in this case, the q-cyclotomic coset modulo 2^r containing 1 is $\{1\}$. Hence $\mathcal{M}_1^{(2^r)}$ is a 1-dimensional subspace of $F_q^{2^r}$ spanned by $\frac{x^{2^r}-1}{x-\alpha} = \alpha^{2^r-1} + \alpha^{2^r-2}x + \alpha^{2^r-3}x^2 + \cdots + \alpha x^{2^r-2} + x^{2^r-1}$. Thus every codeword of $\mathcal{M}_1^{(2^r)}$ is a scalar multiple of $\alpha^{2^r-1} + \alpha^{2^r-2}x + \alpha^{2^r-3}x^2 + \cdots + \alpha x^{2^r-2} + x^{2^r-1}$. Therefore, the only possible non-zero weight is 2^r, which is attained by all its $(q - 1)$ non-zero codewords.

Case 2. $r \geqslant b + 1$.

Let $\beta = \alpha^{-2^{r-b}}$. Since $\beta^{2^b} = 1$ and $2^b | q-1$, we have $\beta^{q-1} = 1$. Therefore $\beta \in \mathrm{F}_q$. In this case, by (1), the q-cyclotomic coset modulo 2^r containing 1 is $\{1, q, q^2, \dots, q^{2^{r-b}-1}\}$. Therefore $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{2^{r-b}-1}}$ are precisely all the roots of the minimal polynomial of α over F_q. But all of $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{2^{r-b}-1}}$ satisfy the polynomial $x^{2^{r-b}} - \beta^{-1} \in \mathrm{F}_q[x]$. Therefore $x^{2^{r-b}} - \beta^{-1}$ is the minimal polynomial of α over F_q. Consequently, the generating polynomial $g(x)$ of $\mathcal{M}_1^{(2^r)}$ is

$$\frac{x^{2^r} - 1}{x^{2^{r-b}} - \beta^{-1}} = \beta + \beta^2 x^{2^{r-b}} + \beta^3 x^{2^{r-b+1}} + \cdots + \beta^{2^b-1} x^{(2^b-2)2^{r-b}} + x^{(2^b-1)2^{r-b}}.$$

As a vector subspace of R_{2^r}, $\mathcal{M}_1^{(2^r)}$ is spanned by $g(x), xg(x), \dots, x^{2^{r-b}-1} g(x)$. Therefore, under the standard isomorphism from R_{2^r} to $\mathrm{F}_q^{2^r}$, the code $\mathcal{M}_1^{(2^r)}$ has the following 2^{r-b} vectors as its basis

$$\begin{aligned}
R_1 &= \big(\beta, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^2, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^3, \dots, \beta^{2^b-1}, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^{2^b}, \underbrace{0, \dots, 0}_{2^{r-b}-1}\big), \\
R_2 &= \big(0, \beta, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^2, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^3, \dots, \beta^{2^b-1}, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^{2^b}, \underbrace{0, \dots, 0}_{2^{r-b}-2}\big), \\
&\ \vdots \\
R_{2^{r-b}} &= \big(\underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^2, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^3, \dots, \beta^{2^b-1}, \underbrace{0, \dots, 0,}_{2^{r-b}-1} \beta^{2^b}\big).
\end{aligned}$$

Note that the weight of each R_i, $1 \leqslant i \leqslant 2^{r-b}$, is 2^b.

Any codeword $C \in \mathcal{M}_1^{(2^r)}$ is of the type

$$\begin{aligned}
C &= \sum_{i=1}^{2^{r-b}} \alpha_i R_i \\
&= \big(\alpha_1\beta, \alpha_2\beta, \dots, \alpha_{2^{r-b}}\beta, \alpha_1\beta^2, \alpha_2\beta^2, \dots, \alpha_{2^{r-b}}\beta^2, \dots, \alpha_1\beta^{2^b}, \alpha_2\beta^{2^b}, \dots, \alpha_{2^{r-b}}\beta^{2^b}\big),
\end{aligned}$$

for some $\alpha_1, \alpha_2, \dots, \alpha_{2^{r-b}} \in \mathrm{F}_q$. It is now clear from the expression of C that the weight of C is $2^b j$, where j is the number of non-zero α_i's. Thus $A_i^{(2^r)} = 0$ if 2^b does not divide i. Moreover a codeword in $\mathcal{M}_1^{(2^r)}$ has weight $2^b j$ if and only if it is a linear combination of any j vectors over F_q out of a total of 2^{r-b} basis vectors R_i's. Thus there are $\binom{2^{r-b}}{j}(q-1)^j$ codewords having weight $2^b j$. This proves the theorem. □

To find the weight distribution of $\mathcal{M}_1^{(2^r)}$ when $q = -1 + 2^b c$, $b \geqslant 2$, c odd, we discuss two cases, i.e. $r \leqslant 2$ and $r \geqslant 3$, separately in Theorems 2 and 3, respectively.

Theorem 2. *Let $q = -1 + 2^b c$, $b \geqslant 2$, c odd. The weight distribution of $\mathcal{M}_1^{(2)}$ is given by $A_0^{(2)} = 1$, $A_1^{(2)} = 0$, $A_2^{(2)} = q - 1$ and the weight distribution of $\mathcal{M}_1^{(4)}$ is given by $A_0^{(4)} = 1$, $A_1^{(4)} = 0$, $A_2^{(4)} = 2(q-1)$, $A_3^{(4)} = 0$, $A_4^{(4)} = (q-1)^2$.*

Proof. $\mathcal{M}_1^{(2)}$ is a 1-dimensional subspace of F_q^2 spanned by $\frac{x^2-1}{x+1} = x - 1$. Since every codeword of $\mathcal{M}_1^{(2)}$ is a scalar multiple of $x - 1$, the only possible non-zero weight is 2, which is attained by all its $q - 1$ non-zero codewords.

As $O_4(q) = 2$ by (1), $\mathcal{M}_1^{(4)}$ is a 2-dimensional subspace of F_q^4 spanned by $g(x) = \frac{x^4-1}{x^2+1} = x^2 - 1$ and $xg(x) = x(x^2-1)$. Let $C \in \mathcal{M}_1^{(4)}$ be a non-zero codeword. Then $C = \alpha(x^2-1) + \beta(x^3 - x) = -\alpha - \beta x + \alpha x^2 + \beta x^3$, for $\alpha, \beta \in F_q$. Therefore, the weight of C is 2 (when exactly one of α or β is non-zero) or 4 (when both α and β are non-zero). Consequently, there are $2(q-1)$ and $(q-1)^2$ codewords in $\mathcal{M}_1^{(4)}$ having the weights 2 and 4, respectively. □

Theorem 3. *Let $r \geqslant 3$, $q = -1 + 2^b c$, $b \geqslant 2$, c odd and $t = \min(r, b+1)$. Then the weight distribution $A_\ell^{(2^r)}$, $0 \leqslant \ell \leqslant 2^r$, of $\mathcal{M}_1^{(2^r)}$ is given by*

$$A_\ell^{(2^r)} = \sum n(\ell_1) n(\ell_2) \ldots n(\ell_{2^{r-t}}),$$

where the summation runs over all tuples $(\ell_1, \ell_2, \ldots, \ell_{2^{r-t}})$ satisfying $\ell_1 + \ell_2 + \cdots + \ell_{2^{r-t}} = \ell$, $\ell_i \geqslant 0$, for each i, and

$$n(\ell_i) = \begin{cases} 1 & \text{if } \ell_i = 0, \\ (q-1)2^{t-1} & \text{if } \ell_i = 2^t - 2, \\ (q-1)(q - 2^{t-1} + 1) & \text{if } \ell_i = 2^t, \\ 0 & \text{otherwise}. \end{cases} \tag{7}$$

Proof. The q-cyclotomic coset modulo 2^r containing 1 is $\{1, q, q^2, \ldots, q^{2^{r-t+1}-1}\}$. Therefore $\alpha, \alpha^q, \ldots, \alpha^{q^{2^{r-t+1}-1}}$ are precisely all the zeros of the minimal polynomial of α over F_q. Let $\gamma = \alpha^{2^{r-t}}$. Then $\gamma^{2^t} = 1$ and $2^t | (q^2 - 1)$ implies $\gamma^{q^2-1} = 1$. Hence $\gamma \in F_{q^2}$ which yields that $\gamma + \gamma^q$ and $\gamma . \gamma^q \in F_q$. Observe that $\alpha, \alpha^{q^2}, \ldots, \alpha^{q^{2^{r-t+1}-2}}$ are all the zeros of $x^{2^{r-t}} - \gamma \in F_{q^2}[x]$ and $\alpha^q, \alpha^{q^3}, \ldots, \alpha^{q^{2^{r-t+1}-1}}$ are all the zeros of $x^{2^{r-t}} - \gamma^q \in F_{q^2}[x]$. Therefore the polynomial

$$\left(x^{2^{r-t}} - \gamma\right)\left(x^{2^{r-t}} - \gamma^q\right) = x^{2^{r-t+1}} - \left(\gamma + \gamma^q\right)x^{2^{r-t}} + \epsilon$$

is the minimal polynomial of α over F_q, where $\epsilon = \gamma^{1+q}$. Thus the generating polynomial $g(x)$ of the minimal ideal $\mathcal{M}_1^{(2^r)}$ is $g(x) = \frac{x^{2^r}-1}{x^{2^{r-t+1}} - (\gamma+\gamma^q)x^{2^{r-t}} + \epsilon}$. Let $y = x^{2^{r-t}}$. Then

$$g(x) = \frac{y^{2^t} - 1}{y^2 - (\gamma + \gamma^q)y + \epsilon} = b_0 + b_1 y + b_2 y^2 + \cdots + b_{2^t-2} y^{2^t-2} \text{ (say)}.$$

Therefore,

$$y^{2^t} - 1 = \left(y^2 - \left(\gamma + \gamma^q\right)y + \epsilon\right)\left(b_0 + b_1 y + b_2 y^2 + \cdots + b_{2^t-2} y^{2^t-2}\right).$$

Comparing the coefficients of $y^0, y^1, \ldots, y^{2^t}$, we get

$$\begin{gathered} b_0 = -\epsilon, \qquad b_1 = -(\gamma + \gamma^q) = -(\gamma + \epsilon\gamma^{-1}), \\ \epsilon b_i - (\gamma + \gamma^q) b_{i-1} + b_{i-2} = 0 \quad \text{for } 2 \leqslant i \leqslant 2^t - 2, \end{gathered}$$

and

$$b_{2^t-3} = \gamma + \gamma^q, \qquad b_{2^t-2} = 1.$$

By (4), $\epsilon^2 = 1$. Therefore, $\epsilon b_i - (\gamma + \gamma^q) b_{i-1} + b_{i-2} = 0$ if and only if $b_i - (\epsilon\gamma + \gamma^{-1}) b_{i-1} + \epsilon b_{i-2} = 0$ for $2 \leqslant i \leqslant 2^t - 2$. It thus follows from Lemma 3 that $b_{2^{t-1}-1} = 0$ and all other b_i's are non-zero.

The code $\mathcal{M}_1^{(2^r)}$ is a vector subspace of $\mathrm{F}_q^{2^r}$ spanned by $g(x), xg(x), \ldots, x^{2^{r-t+1}-1} g(x)$. Therefore under the standard isomorphism from R_{2^r} to $\mathrm{F}_q^{2^r}$ this code has the following 2^{r-t+1} vectors as its basis

$$\begin{aligned}
R_1 &= (b_0, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_1, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_2, \ldots, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_{2^t-2}, \underbrace{0, \ldots, 0}_{2^{r-t+1}-1}), \\
R_2 &= (0, b_0, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_1, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_2, \ldots, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_{2^t-2}, \underbrace{0, \ldots, 0}_{2^{r-t+1}-2}), \\
&\vdots \\
R_i &= (\underbrace{0, \ldots, 0}_{i-1}, b_0, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_1, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_2, \ldots, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_{2^t-2}, \underbrace{0, \ldots, 0}_{2^{r-t+1}-i}), \\
&\vdots \\
R_{i+2^{r-t}} &= (\underbrace{0, \ldots, 0}_{2^{r-t}+i-1}, b_0, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_1, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_2, \ldots, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_{2^t-2}, \underbrace{0, \ldots, 0}_{2^{r-t}-i}), \\
&\vdots \\
R_{2^{r-t+1}} &= (\underbrace{0, \ldots, 0}_{2^{r-t+1}-1}, b_0, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_1, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_2, \ldots, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, b_{2^t-2}).
\end{aligned}$$

Let V_i be the subspace of $\mathrm{F}_q^{2^r}$ generated by R_i and $R_{i+2^{r-t}}$ for $1 \leqslant i \leqslant 2^{r-t}$. Any vector $c_i \in V_i$ is of the form

$$(\underbrace{0, \ldots, 0}_{i-1}, *, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, *, \underbrace{0, \ldots, 0}_{2^{r-t}-1}, *, \ldots, *, \underbrace{0, \ldots, 0}_{2^{r-t}-i}),$$

where the non-zero entries can occur only at the places marked $*$.

Consequently, if $i \neq j$, the non-zero entries of elements in V_i and V_j occur at distinct places. Hence $wt(c_i + c_j) = wt(c_i) + wt(c_j)$ for $c_i \in V_i$ and $c_j \in V_j$.

Thus if $C \in \mathcal{M}_1^{(2^r)}$ is a codeword, then C can be uniquely expressed as

$$C = c_1 + \cdots + c_{2^{r-t}}, \quad c_i \in V_i \quad \text{and} \quad wt(C) = wt(c_1) + \cdots + wt(c_{2^{r-t}}). \tag{8}$$

For any integer $\ell \geqslant 0$, we now find the number of elements in $\mathcal{M}_1^{(2^r)}$ having weight ℓ. For any tuple $(\ell_1, \ell_2, \ldots, \ell_{2^{r-t}})$ satisfying $\ell_1 + \ell_2 + \cdots + \ell_{2^{r-t}} = \ell$ and $\ell_i \geqslant 0$ for each i, define

$$\mathcal{S}_{(\ell_1,\ell_2,\ldots,\ell_{2^{r-t}})} = \left\{c_1 + c_2 + \cdots + c_{2^{r-t}} \;\middle|\; c_i \in V_i,\ wt(c_i) = \ell_i,\ 1 \leqslant i \leqslant 2^{r-t}\right\}.$$

From (8), it follows that $\bigcup \mathcal{S}_{(\ell_1,\ell_2,\ldots,\ell_{2^{r-t}})}$, where union runs over all tuples $(\ell_1, \ell_2, \ldots, \ell_{2^{r-t}})$ satisfying $\ell_1 + \ell_2 + \cdots + \ell_{2^{r-t}} = \ell$ and $\ell_i \geqslant 0$ for each i, consists of precisely all the elements in $\mathcal{M}_1^{(2^r)}$ having weight ℓ. As this union is disjoint,

$$A_\ell^{(2^r)} = \left|\bigcup \mathcal{S}_{(\ell_1,\ell_2,\ldots,\ell_{2^{r-t}})}\right| = \sum |\mathcal{S}_{(\ell_1,\ell_2,\ldots,\ell_{2^{r-t}})}| = \sum n(\ell_1)n(\ell_2)\cdots n(\ell_{2^{r-t}}),$$

where $n(\ell_i)$ denote the number of codewords in V_i having weight ℓ_i. (For any set X, $|X|$ denotes the number of elements in X.)

We claim that the only possible non-zero weights in V_i are $2^t - 2$ and 2^t and there are precisely $(q-1)2^{t-1}$ and $(q-1)(q-2^{t-1}+1)$ codewords in V_i having weight $2^t - 2$ and 2^t, respectively.

Let $c_i \in V_i$ be a non-zero codeword. Then $c_i = \alpha_1 R_i + \alpha_2 R_{i+2^{r-t}}$ for some $\alpha_1, \alpha_2 \in \mathrm{F}_q$, not both zero, which gives

$$\begin{aligned} c_i = (&\underbrace{0,\ldots,0,}_{i-1}\alpha_1, b_0 \underbrace{0,\ldots,0,}_{2^{r-t}-1}\alpha_1 b_1 + \alpha_2 b_0, \underbrace{0,\ldots,0,}_{2^{r-t}-1}\alpha_1 b_2 + \alpha_2 b_1, \ldots, \\ &\alpha_2 b_{2^{t-1}-2}, \underbrace{0,\ldots,0,}_{2^{r-t}-1}\alpha_1 b_{2^{t-1}}, \underbrace{0,\ldots,0,}_{2^{r-t}-1}\alpha_1 b_{2^{t-1}+1} + \alpha_2 b_{2^{t-1}}, \ldots, \\ &\alpha_1 b_{2^t-2} + \alpha_2 b_{2^t-3}, \underbrace{0,\ldots,0,}_{2^{r-t}-1}\alpha_2 b_{2^t-2}, \underbrace{0,\ldots,0}_{2^{r-t}-i}). \end{aligned}$$

Case 1. Either $\alpha_1 = 0$ or $\alpha_2 = 0$.

In this case $c_i = \alpha_1 R_i$ or $\alpha_2 R_{i+2^{r-t}}$. Therefore, $wt(c_i) = 2^t - 2$ and such codeword c_i has $2(q-1)$ choices, as α_1 and α_2 both have $q-1$ choices.

Case 2. α_1 and α_2 both non-zero.

Divide the possible non-zero entries $\alpha_1 b_u + \alpha_2 b_{u-1}$ of c_i into three sets

$$\begin{aligned} S_1 &= \{\alpha_1 b_0, \alpha_2 b_{2^{t-1}-2}, \alpha_1 b_{2^{t-1}}, \alpha_2 b_{2^t-2}\}, \\ S_2 &= \left\{\alpha_1 b_u + \alpha_2 b_{u-1}\colon\ 1 \leqslant u \leqslant 2^{t-1} - 2\right\}, \\ S_3 &= \left\{\alpha_1 b_u + \alpha_2 b_{u-1}\colon\ 2^{t-1} + 1 \leqslant u \leqslant 2^t - 2\right\}. \end{aligned}$$

By Lemma 3(i), no element of S_1 is zero. By Lemma 3(iii), some element $\alpha_1 b_u + \alpha_2 b_{u-1}$ of S_2 is zero if and only if the corresponding element $\alpha_1 b_{u+2^{t-1}} + \alpha_2 b_{u-1+2^{t-1}}$ of S_3 is zero.

Further, two elements of S_2 cannot be zero simultaneously, because if $\alpha_1 b_u + \alpha_2 b_{u-1} = 0$ and $\alpha_1 b_v + \alpha_2 b_{v-1} = 0$ for some u, v, $1 \leqslant u < v \leqslant 2^{t-1} - 2$, then $\alpha_1(b_u b_{v-1} - b_v b_{u-1}) = 0$, which is not possible by Lemma 3(iv), as $\alpha_1 \neq 0$.

Thus if α_1 and α_2 are both non-zero, then either none of the elements in $S_1 \cup S_2 \cup S_3$ is zero or exactly two of them are zero. Accordingly, the weight of c_i is either 2^t or $2^t - 2$. However $wt(c_i) = 2^t - 2$ if and only if $\alpha_2 = -\alpha_1 b_u b_{u-1}^{-1}$ for some u, $1 \leqslant u \leqslant 2^{t-1} - 2$. It follows from Lemma 3(iv) that $-\alpha_1 b_1 b_0^{-1}, -\alpha_1 b_2 b_1^{-1}, \ldots, -\alpha_1 b_{2^{t-1}-2} b_{2^{t-1}-3}^{-1}$ are all distinct. Therefore, for each choice of α_1, there are $2^{t-1} - 2$ choices of α_2. Hence there are $(q-1)(2^{t-1}-2)$ codewords c_i having weight $2^t - 2$. The remaining $(q-1)^2 - (q-1)(2^{t-1}-2)$ codewords all have weight 2^t.

Combining both the cases, our claim follows. This completes the proof of Theorem 3. □

Corollary. (i) *Let $q = 1 + 2^b c$, where $b \geqslant 2$, c is odd. Then the code $\mathcal{M}_1^{(2^r)}$ is a* $[2^r, 2^{r-b}, 2^b]$-*code if $r \geqslant b+1$, and for $r \leqslant b$, $\mathcal{M}_1^{(2^r)}$ is a* $[2^r, 1, 2^r]$-*code.*

(ii) *Let $q = -1 + 2^b c$, where $b \geqslant 2$, c is odd. Then the code $\mathcal{M}_1^{(2^r)}$ is a* $[2^r, 2^{r-t+1}, 2^t - 2]$-*code if $r \geqslant 3$, where $t = \min(r, b+1)$, $\mathcal{M}_1^{(2)}$ is a* $[2, 1, 2]$-*code and $\mathcal{M}_1^{(4)}$ is a* $[4, 2, 2]$-*code.*

Acknowledgments

The authors are grateful to the anonymous referees for their comments and suggestions which helped to write the paper in the present form.

References

[1] D. Augot, Description of minimum weight codewords of cyclic codes by algebraic systems, Finite Fields Appl. 2 (2) (1996) 138–152.
[2] L.D. Baumert, R.J. McEliece, Weights of irreducible cyclic codes, Inform. Control 20 (1972) 158–175.
[3] R.W. Fitzgerald, J.L. Yucas, Sums of Gauss sums and weights of irreducible codes, Finite Fields Appl. 11 (1) (2005) 89–110.
[4] F.J. MacWilliams, J. Seery, The weight distributions of some minimal cyclic codes, IEEE Trans. Inform. Theory 27 (6) (1981) 796–806.
[5] F.J. MacWilliams, N.J.A. Sloane, Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[6] M.J. Moisio, K.O. Väänänen, Two recursive algorithms for computing the weight distribution of certain irreducible cyclic codes, IEEE Trans. Inform. Theory 45 (4) (1999) 1244–1249.
[7] A. Sharma, G.K. Bakshi, V.C. Dumir, M. Raka, Irreducible cyclic codes of length 2^n, Ars Combin., in press.
[8] M. van der Vlugt, Hasse–Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes, J. Number Theory 55 (2) (1995) 145–159.