Irreducible Cyclic Codes of Length 2^n

Anuradha Sharma*, Gurmeet K. Bakshi ,
V.C.Dumir and Madhu Raka
Centre for Advanced Study in Mathematics
Panjab University
Chandigarh
INDIA

Abstract

Explicit expressions for all the primitive idempotents in the ring $R_{2^n} = \mathrm{F}_q[x]/(x^{2^n}-1)$, where q is an odd prime power, are obtained. Some lower bounds on the minimum distances of the irreducible cyclic codes of length 2^n over F_q are also obtained.

Keywords : Minimal cyclic codes, primitive idempotents, cyclotomic cosets.
2000 Mathematics Subject Classification : 11T71, 94B15.

1. Introduction.

Let F_q be a field of prime power order q. Let $m \geq 1$ be an integer with $\gcd(q,m) = 1$. A q-ary cyclic code $\mathcal{C}$ of length m is an ideal in the principal ideal ring $R_m = \mathrm{F}_q[x]/(x^m-1)$. The ideal $\mathcal{C}$ is generated by a *generating polynomial* $g(x)$ that is the unique monic divisor of (x^m-1). The ideal $\mathcal{C}$ is also generated by an *idempotent* $e(x)$ which is the unique polynomial in $\mathcal{C}$ that generates $\mathcal{C}$ and satisfies $(e(x))^2 = e(x)$. (For reference see chapter 5 of [4] and chapter 8 of [5]). Every ideal in R_m can be expressed uniquely as a sum of minimal ideals. The generator idempotent of a minimal ideal (also known as irreducible cyclic code) is called the primitive idempotent. Thus it is of interest

*Research supported by N.B.H.M., India is gratefully acknowledged.

to determine the primitive idempotents.

When $q = 2$, all the idempotents in R_m can be constructed directly from the cyclotomic cosets. For non-binary cyclic codes, Berman [3, p.22] gave explicit expression for all the primitive idempotents in R_{p^n}, where p, q are distinct odd primes, $n \geq 1$, q a primitive root mod p^n. The authors [6] generalized the result of Berman, by taking q to be an odd prime power, not necessarily a primitive root mod p^n and gave an algorithm to compute explicitly all the primitive idempotents in the ring R_{p^n} making use of cyclotomic numbers. In another paper [7], Sharma, Bakshi and Raka determined all the primitive idempotents in the ring R_{2p^n} explicitly. Earlier, Bakshi and Raka [1] derived all the primitive idempotents in the ring $R_{p^n l}$, where p, l are distinct odd primes, q a primitive root mod p^n and also modulo l, with $\gcd(\frac{\phi(p^n)}{2}, \frac{\phi(l)}{2}) = 1$.

The primitive idempotents of irreducible cyclic codes of length 2^n, $n \geq 3$, were determined by Bakshi and Raka [2] under the conditions that $q \equiv 3$ or $5 \pmod 8$. In this paper, we drop this condition on q and for all odd prime power q, derive explicit expressions for all the primitive idempotents in R_{2^n}, $n \geq 3$ (see Theorems 1 and 2). We give two examples to illustrate it. These explicit expressions have been used in our another paper [8] to compute the idempotent generators of polyadic codes of prime power length. We also find some lower bounds on the minimum distances of the minimal cyclic codes of length 2^n (see Section 4).

2. q-cyclotomic cosets modulo 2^n, $n \geq 3$.

For any integer $m \geq 1$, the set $\{0, 1, 2, \cdots, m-1\}$ is divided into disjoint cyclotomic cosets $C_s = \{s, sq, sq^2, \cdots, sq^{m_s-1}\}$, where m_s is the smallest positive integer such that $sq^{m_s} \equiv s \pmod m$. In this section we determine cyclotomic cosets modulo 2^n, $n \geq 3$.

Since $q \equiv \pm 1 \pmod 4$, we write $q = 1 + 2^d c$ or $-1 + 2^d c$, where $d \geq 2$ and c is odd. Note that if $q \equiv 3$ or $5 \pmod 8$, d is always equal to 2. Let $O_m(q)$ denotes

the order of q modulo m. For every positive integer ℓ, $\ell \geq 2$,

$$O_{2^\ell}(q) = \begin{cases} 2^{\ell-d} & \text{if } \ell \geq d+1, \ q = \pm 1 + 2^d c\,; \\ 1 & \text{if } 2 \leq \ell \leq d, \ q = \ 1 + 2^d c\,; \\ 2 & \text{if } 2 \leq \ell \leq d, \ q = -1 + 2^d c. \end{cases} \tag{1}$$

Therefore the q-cyclotomic coset modulo 2^n containing $2^{n-\ell}r$, $2 \leq \ell \leq n$, r odd, is given by

$$C_{2^{n-\ell}r} = \begin{cases} \{2^{n-\ell}r, 2^{n-\ell}rq, \cdots, 2^{n-\ell}rq^{(2^{\ell-d}-1)}\} & \text{if } d+1 \leq \ell \leq n \\ & \text{and } q = \pm 1 + 2^d c\,; \\ \{2^{n-\ell}r\} & \text{if } 2 \leq \ell \leq d \\ & \text{and } q = 1 + 2^d c\,; \\ \{2^{n-\ell}r, 2^{n-\ell}rq\} = \{2^{n-\ell}r, -2^{n-\ell}r\} & \text{if } 2 \leq \ell \leq d \\ & \text{and } q = -1 + 2^d c. \end{cases} \tag{2}$$

Clearly $C_0 = \{0\}$, $C_{2^{n-1}} = \{2^{n-1}\}$.

Proposition.

(*a*) Let $q = 1 + 2^d c$, $d \geq 2$, c odd. All the distinct q – cyclotomic cosets modulo 2^n are given by C_0, $C_{2^{n-1}}$ and $C_{2^{n-\ell}r}$ for $\ell = 2, 3, \cdots, n$ and r running over S_ℓ for each ℓ, where

$$S_\ell = \begin{cases} \{\pm 1, \pm 3, \cdots, \pm 3^{(2^{d-2}-1)}\} & \text{if } d+1 \leq \ell \leq n, \\ \{\pm 1, \pm 3, \cdots, \pm 3^{(2^{\ell-2}-1)}\} & \text{if } 2 \leq \ell \leq d. \end{cases} \tag{3}$$

(*b*) Let $q = -1 + 2^d c$, $d \geq 2$, c odd. All the distinct q–cyclotomic cosets modulo 2^n are given by C_0, $C_{2^{n-1}}$ and $C_{2^{n-\ell}r}$ for $\ell = 2, 3, \cdots, n$ and r running over T_ℓ for each ℓ, where

$$T_\ell = \begin{cases} \{1, 3, 3^2, \cdots, 3^{(2^{d-1}-1)}\} & \text{if } d+1 \leq \ell \leq n, \ d \geq 3\,; \\ \{1, 3, 3^2, \cdots, 3^{(2^{\ell-2}-1)}\} & \text{if } 2 \leq \ell \leq d, \ d \geq 2\,; \\ \{1, -1\} & \text{if } 3 \leq \ell \leq n, \ d = 2. \end{cases} \tag{4}$$

Proof. We first note that $O_{2^\ell}(3) = 2^{\ell-2}$ for $\ell \geq 3$ and $q^2 \equiv 1 (\text{mod } 2^{d+1})$ for any q. Also for any r, r' odd, it is clear that $C_{2^{n-\ell}r} \neq C_{2^{n-\ell'}r'}$ if $\ell \neq \ell'$.

First we consider the case when $q = 1 + 2^d c$, $d \geq 2$.

Suppose, if possible, $C_{2^{n-\ell}r} = C_{2^{n-\ell}r'}$ for some ℓ, $2 \leq \ell \leq n$ and $r, r' \in S_\ell$. This means

$$2^{n-\ell}3^t \equiv \pm 2^{n-\ell}3^{t'}q^u (\text{mod } 2^n)$$

for some t, t', $0 \leq t, t' \leq 2^{\min(\ell,\, d)-2} - 1$ and for some u. Then $3^{t-t'} \equiv \pm q^u (\mathrm{mod}\ 2^\ell)$. This implies $3^{2(t-t')} \equiv q^{2u} \equiv 1 (\mathrm{mod}\ 2^{\min(\ell,\, d)+1})$. Since the order of 3 modulo $2^{\min(\ell,\, d)+1}$ is $2^{\min(\ell,\, d)-1}$, we get that $2^{\min(\ell,\, d)-1}$ divides $2(t-t')$ which is possible only if $t = t'$ and hence $r = r'$. Thus the cosets $C_{2^n-\epsilon r}$, $2 \leq \ell \leq n$ and $r \in S_\ell$, are disjoint modulo 2^n.

When $q = -1 + 2^2 c$, working in a same way, one finds that the cosets $C_{2^n-\epsilon r}$, $r \in T_\ell = \{1, -1\}$ for $3 \leq \ell \leq n$, are disjoint modulo 2^n.

Let now $q = -1 + 2^d c$, $d \geq 3$.

Suppose, if possible, $C_{2^n-\epsilon r} = C_{2^n-\epsilon r'}$ for some ℓ, $3 \leq \ell \leq n$ and $r, r' \in T_\ell$. This gives

$$3^{t-t'} \equiv q^u (\mathrm{mod}\ 2^\ell) \tag{5}$$

for some t, t', $0 \leq t' \leq t \leq 2^{\min(\ell-1,\, d)-1} - 1$ and for some u.

For $d+1 \leq \ell \leq n$, working as above, we get that it is possible only if either $t - t' = 0$ or $t - t' = 2^{d-2}$. If $t - t' = 2^{d-2}$, write $3^{t-t'} = 3^{2^{d-2}} = 1 + 2^d \lambda$, λ odd. Then (5) gives $3^{t-t'} = 1 + 2^d \lambda \equiv q^u (\mathrm{mod}\ 2^{d+1})$ which is not possible, as $q^u \equiv 1 (\mathrm{mod}\ 2^{d+1})$ if u is even, $q^u \equiv -1 (\mathrm{mod}\ 2^d)$ if u is odd. Thus we must have $t = t'$.

For $3 \leq \ell \leq d$, we have, by (2), that $u = 0$ or 1.

If $u = 0$, then we have $3^{t-t'} \equiv 1 (\mathrm{mod}\ 2^\ell)$ which implies $2^{\ell-2}$ divides $t - t'$. This gives $t = t'$. If $u = 1$, we have $3^{t-t'} \equiv -1 + 2^d c (\mathrm{mod}\ 2^\ell)$, and hence $3^{2(t-t')} \equiv 1 (\mathrm{mod}\ 2^{\ell+1})$. This implies $2^{\ell-2}$ divides $t - t'$. So $t = t'$, as $t - t' < 2^{\ell-2}$. Therefore the cosets $C_{2^n-\epsilon r}$, $3 \leq \ell \leq n$ and $r \in T_\ell$, are disjoint modulo 2^n.

Further, these are all the q-cyclotomic cosets modulo 2^n, because in each case, the number of elements in the listed cosets sums upto to 2^n. For example, in Case (a),

$$|C_0| + |C_{2^n-1}| + \sum_{\ell=2}^{n} \sum_{r \in S_\ell} |C_{2^n-\epsilon r}| = 1 + 1 + \sum_{\ell=d+1}^{n} 2^{d-1} 2^{\ell-d} + \sum_{\ell=2}^{d} 2^{\ell-1} = 2^n. \qquad \square$$

For any ℓ, $2 \le \ell \le n$, we note that

$$\bigcup_r C_{2^{n-\ell}r} = \{j : 1 \le j \le 2^n - 1 \text{ such that } 2^{n-\ell} \| j\}, \tag{6}$$

where r runs over S_ℓ or T_ℓ according as $q = 1 + 2^d c$ or $q = -1 + 2^d c$, (By $2^{n-\ell} \| j$, we mean that $2^{n-\ell} | j$ but $2^{n-\ell+1} \nmid j$).

Throughout this paper, empty sums are assumed to be zero.

3. Primitive Idempotents in R_{2^n}, $n \ge 3$.

If α denotes a primitive 2^nth root of unity in some extension field of F_q, then the polynomial $M^{(s)}(x) = \prod_{i \in C_s} (x - \alpha^i)$ is the minimal polynomial of α^s over F_q and the ideal $\mathcal{M}_s$ generated by $\frac{x^{2^n}-1}{M^{(s)}(x)}$ is a minimal ideal in R_{2^n}. The idempotent generator of the ideal $\mathcal{M}_s$, i.e. the primitive idempotent will be denoted by $\theta_s(x)$.

Theorem 1. Let $q = 1 + 2^d c$, $d \ge 2$, c odd and let ζ be an arbitrary primitive 2^dth root of unity in F_q. Then we can choose α, a primitive 2^nth root of unity, suitably, so that all the primitive idempotents in the ring R_{2^n} are given by

$$\begin{aligned} \theta_0(x) &= \tfrac{1}{2^n}(1 + x + x^2 + \cdots + x^{2^n-1}), \\ \theta_{2^{n-1}}(x) &= \tfrac{1}{2^n}(1 - x + x^2 - \cdots - x^{2^n-1}), \end{aligned}$$

and for $2 \le \ell \le n$, $r \in S_\ell$,

$$\theta_{2^{n-\ell}r}(x) = \frac{|C_{2^{n-\ell}r}|}{2^n} \left\{ \sum_{\substack{i=0 \\ 2^\ell | i}}^{2^n-1} x^i - \sum_{\substack{i=1 \\ 2^{\ell-1} \| i}}^{2^n-1} x^i + \sum_{j=2}^{\min(\ell,d)} \sum_{s \in S_{n-\ell+j}} \zeta^{rs2^{d-j}} \{ \sum_{i \in C_{s2^{\ell-j}}} x^i \} \right\}.$$

Theorem 2. Let $q = -1 + 2^d c$, $d \ge 2$, c odd. Let ω be an arbitrary primitive 2^{d+1}th root of unity in F_{q^2}. Then we can choose α, a primitive 2^nth root of unity, suitably, so that all the primitive idempotents in the ring R_{2^n} are given by

$$\begin{aligned} \theta_0(x) &= \tfrac{1}{2^n}(1 + x + x^2 + \cdots + x^{2^n-1}), \\ \theta_{2^{n-1}}(x) &= \tfrac{1}{2^n}(1 - x + x^2 - \cdots - x^{2^n-1}), \end{aligned}$$

and for $2 \le \ell \le n$, $r \in T_\ell$,

$$\theta_{2^n-\epsilon_r}(x) = \frac{|C_{2^n-\epsilon_r}|}{2^n}\left\{\sum_{\substack{i=0\\ 2^\ell|i}}^{2^n-1} x^i - \sum_{\substack{i=1\\ 2^{\ell-1}||i}}^{2^n-1} x^i\right\}$$

$$+ \frac{|C_{2^n-\epsilon_r}|}{2^{n+1}} \sum_{j=3}^{\min(\ell,\, d+1)} \sum_{s\in T_{n-\ell+j}} \{\omega^{rs2^{d+1-j}} + (-\omega)^{-rs2^{d+1-j}}\}\{\sum_{i\in C_{s2^{\ell-j}}} x^i\}.$$

Remark. Theorems 1 and 2 do not depend upon the choice of ζ and ω respectively. If ζ is a primitive 2^dth root of unity, then ζ^k, $k \in \{\pm 1, \pm 3, \cdots, \pm 3^{2^{d-2}-1}\}$ are all the primitive 2^dth roots of unity. Changing ζ to ζ^k just changes $\theta_{2^n-\epsilon_r}(x)$ to $\theta_{2^n-\epsilon_{rk}}(x)$ for $rk \in S_\ell$ modulo 2^ℓ. Similarly, changing ω to ω^k, where $k \in \{1, 3, 3^2, \cdots, 3^{2^{d-1}-1}\}$, changes $\theta_{2^n-\epsilon_r}(x)$ to $\theta_{2^n-\epsilon_{rk}}(x)$.

Corollary.

(*a*) If $q \equiv 5 (\text{mod } 8)$, all the primitive idempotents in R_{2^n} are given by $\theta_0(x)$, $\theta_{2^{n-1}}(x)$ and $\theta_{2^n-\epsilon_r}(x)$ for $2 \le \ell \le n$, $r \in \{1, -1\}$, where

$$\theta_{2^n-\epsilon_r}(x) = \tfrac{1}{2^{n-\ell+2}}\left\{\sum_{\substack{i=0\\ 2^\ell|i}}^{2^n-1} x^i - \sum_{\substack{i=1\\ 2^{\ell-1}||i}}^{2^n-1} x^i\right\} + \tfrac{r\sqrt{-1}}{2^{n-\ell+2}}\left\{\sum_{i\in C_{2^{\ell-2}}} x^i - \sum_{i\in C_{-2^{\ell-2}}} x^i\right\}.$$

(*b*) If $q \equiv 3 (\text{mod } 8)$, all the primitive idempotents other than $\theta_0(x)$ and $\theta_{2^{n-1}}(x)$, are given by $\theta_{2^n-\epsilon_r}(x)$ for $3 \le \ell \le n$, $r \in \{1, -1\}$ and $\theta_{2^n-2}(x)$, where

$$\theta_{2^n-\epsilon_r}(x) = \tfrac{1}{2^{n-\ell+2}}\left\{\sum_{\substack{i=0\\ 2^\ell|i}}^{2^n-1} x^i - \sum_{\substack{i=1\\ 2^{\ell-1}||i}}^{2^n-1} x^i\right\} + \tfrac{r\sqrt{-2}}{2^{n-\ell+3}}\left\{\sum_{i\in C_{2^{\ell-3}}} x^i - \sum_{i\in C_{-2^{\ell-3}}} x^i\right\}$$

and

$$\theta_{2^n-2}(x) = \frac{1}{2^{n-1}}\left\{1 - x^2 + x^4 - x^6 + \cdots - x^{2^n-2}\right\}.$$

Proof. If $q \equiv 5 \pmod 8$, then $q = 1 + 2^d c$ with $d = 2$. Part (a), therefore, follows from Theorem 1, by taking $\zeta = \sqrt{-1} \in F_q$. If $q \equiv 3 (\text{mod } 8)$, then $q = -1 + 2^d c$ with $d = 2$. Part (b) follows from Theorem 2, by taking $\omega = \frac{\sqrt{2}+\sqrt{-2}}{2} \in F_{q^2}$. □

Lemma 1. Let α be a primitive 2^nth root of unity in some extension field of F_q. Then

$$\sum_{i=0}^{2^{\ell-d}-1} \alpha^{2^{n-\ell} r q^i} = 0$$

for any r odd and any ℓ satisfying $d+1 \le \ell \le n$ or $d+2 \le \ell \le n$ according as $q = 1+2^d c$ or $q = -1+2^d c$.

Proof. Let $\beta = \alpha^{2^{n-\ell} r}$. Then β is a primitive 2^ℓth root of unity and the required sum is equal to $\sum_{i=0}^{2^{\ell-d}-1} \beta^{q^i}$.

Case I. Let $q = 1+2^d c$.

For each i, $0 \le i \le 2^{\ell-d}-1$, $q^i \equiv 1 \pmod{2^d}$, so $(\beta^{q^i-1})^{2^{\ell-d}} = 1$. Further $\beta^{q^i-1} = \beta^{q^j-1}$ if and only if $q^i \equiv q^j \pmod{2^\ell}$ if and only if $i \equiv j \pmod{2^{\ell-d}}$, as the order of q modulo 2^ℓ is $2^{\ell-d}$ for $\ell \ge d+1$. Therefore β^{q^i-1}, $0 \le i \le 2^{\ell-d}-1$, are all the distinct $2^{\ell-d}$th roots of unity and hence their sum is zero. Therefore the required sum, being equal to $\beta(\sum_{i=0}^{2^{\ell-d}-1} \beta^{q^i-1})$, is also zero.

Case II. Let $q = -1+2^d c$.

The required sum is equal to $\beta(\sum_{i=0}^{2^{\ell-d-1}-1} \beta^{q^{2i}-1}) + \beta^q(\sum_{i=0}^{2^{\ell-d-1}-1} \beta^{q^{2i+1}-q})$ which is further equal to $\beta(\sum_{i=0}^{2^{\ell-d-1}-1} \beta^{q^{2i}-1}) + \beta^q(\sum_{i=0}^{2^{\ell-d-1}-1} \beta^{q^{2i}-1})^q$. Since $q^2 \equiv 1 \pmod{2^{d+1}}$, we have $q^{2i} \equiv 1 \pmod{2^{d+1}}$ and so $(\beta^{q^{2i}-1})^{2^{\ell-d-1}} = 1$. As before, $\beta^{q^{2i}-1}$ for $0 \le i \le 2^{\ell-d-1}-1$, are all the distinct $2^{\ell-d-1}$th roots of unity and hence their sum is zero. Therefore the required sum is zero. □

Proof of Theorem 1. In view of Theorem 6 (generalized to non-binary case) of Chapter 8 by MacWilliams & Sloane [5], we have

$$\theta_s(x) = \sum_{i=0}^{2^n-1} \epsilon_i^{(s)} x^i, \text{ where } \epsilon_i^{(s)} = \frac{1}{2^n} \sum_{j \in C_s} \alpha^{-ij}.$$

Clearly

$\epsilon_i^{(0)} = \frac{1}{2^n}$ for every i, and $\epsilon_i^{(2^n-1)} = \frac{1}{2^n} \sum_{j \in C_{2^n-1}} \alpha^{-ij} = \frac{1}{2^n} \alpha^{-i2^n-1} = \frac{(-1)^i}{2^n}$.

Thus

$$\theta_0(x) = \tfrac{1}{2^n}(1 + x + x^2 + \cdots + x^{2^n-1}) \quad \text{and}$$

$$\theta_{2^n-1}(x) = \tfrac{1}{2^n}(1 - x + x^2 - \cdots - x^{2^n-1}).$$

To compute the primitive idempotents $\theta_{2^n-\ell_r}(x)$, we write

$$\begin{aligned}\theta_{2^n-\ell_r}(x) &= \sum_{i=0}^{2^n-1} \epsilon_i^{(2^n-\ell_r)} x^i \\ &= \sum_{\substack{i=0 \\ 2^\ell | i}}^{2^n-1} \epsilon_i^{(2^n-\ell_r)} x^i + \sum_{\substack{i=1 \\ 2^{\ell-1} || i}}^{2^n-1} \epsilon_i^{(2^n-\ell_r)} x^i + \sum_{t=0}^{\ell-2} \sum_{\substack{i=1 \\ 2^t || i}}^{2^n-1} \epsilon_i^{(2^n-\ell_r)} x^i, \quad (7)\end{aligned}$$

where for any $i \geq 0$, we have, using (2),

$$\epsilon_i^{(2^n-\ell_r)} = \frac{1}{2^n} \sum_{j \in C_{2^n-\ell_r}} \alpha^{-ij} = \begin{cases} \frac{1}{2^n} \sum_{j=0}^{2^{\ell-d}-1} \alpha^{-i2^{n-\ell}rq^j} & \text{if} \quad d+1 \leq \ell \leq n, \\ \frac{1}{2^n}\, \alpha^{-i2^{n-\ell}r} & \text{if} \quad 2 \leq \ell \leq d. \end{cases} \quad (8)$$

If $2^\ell | \, i$, then we have

$$\epsilon_i^{(2^n-\ell_r)} = \begin{cases} \frac{2^{\ell-d}}{2^n} = \frac{1}{2^{d+n-\ell}} & \text{if} \quad d+1 \leq \ell \leq n, \\ \frac{1}{2^n} & \text{if} \quad 2 \leq \ell \leq d. \end{cases} \quad (9)$$

If $2^{\ell-1} || \, i$, then as $\alpha^{2^{n-1}} = -1$, we have

$$\epsilon_i^{(2^n-\ell_r)} = \begin{cases} \frac{-1}{2^{d+n-\ell}} & \text{if} \quad d+1 \leq \ell \leq n, \\ \frac{-1}{2^n} & \text{if} \quad 2 \leq \ell \leq d. \end{cases} \quad (10)$$

If $2^t || \, i$ for some t, $0 \leq t \leq \ell - 2$, then by (6), we have $i \in \bigcup_{s \in S_{n-t}} C_{2^t s}$, i.e., $i \in C_{2^t s}$ for some s, $s \in S_{n-t}$. Since $\epsilon_i^{(2^n-\ell_r)}$ has the same value for all i varying over a cyclotomic coset, we have, from (8),

$$\epsilon_i^{(2^n-\ell_r)} = \epsilon_{2^t s}^{(2^n-\ell_r)} = \begin{cases} \frac{1}{2^n} \sum_{j=0}^{2^{\ell-d}-1} \alpha^{-2^{n-\ell+t}rsq^j} & \text{if} \quad d+1 \leq \ell \leq n, \\ \frac{1}{2^n}\, \alpha^{-2^{n-\ell+t}rs} & \text{if} \quad 2 \leq \ell \leq d. \end{cases} \quad (11)$$

Now $\alpha^{-2^{n-\ell+t}rsq^j} = \alpha^{-2^{n-\ell+t}rsq^u}$ if and only if $q^j \equiv q^u \pmod{2^{\ell-t}}$. In view of (1), for $\ell - t \geq d+1$, this is so if and only if $j \equiv u \pmod{2^{\ell-t-d}}$, and for

$\ell - t \le d$, this is so if and only if $j \equiv u (\mathrm{mod}\ 1)$. Thus

$$\sum_{j=0}^{2^{\ell-t-d}-1} \alpha^{-2^{n-\ell+t} rsq^j} = \begin{cases} 2^t \sum_{j=0}^{2^{\ell-t-d}-1} \alpha^{-2^{n-\ell+t} rsq^j} & \text{if} \quad \ell - t \ge d+1, \\ 2^{\ell-d} \alpha^{-2^{n-\ell+t} rs} & \text{if} \quad \ell - t \le d. \end{cases} \tag{12}$$

Also for $\ell - t \ge d+1$, i.e., for $0 \le t \le \ell - d - 1$, the sum on the right hand side of (12) is zero, by Lemma 1. Therefore from (11) and (12), we have

$$\epsilon_{2^t s}^{(2^{n-\ell} r)} = \begin{cases} 0 & \text{if} \quad d+1 \le \ell \le n \text{ and } 0 \le t \le \ell - d - 1, \\ \frac{1}{2^{d+n-\ell}} \alpha^{-2^{n-\ell+t} rs} & \text{if} \quad d+1 \le \ell \le n \text{ and } \ell - d \le t \le \ell - 2, \\ \frac{1}{2^n} \alpha^{-2^{n-\ell+t} rs} & \text{if} \quad 2 \le \ell \le d \quad \text{and } 0 \le t \le \ell - 2. \end{cases} \tag{13}$$

Choose α, a primitive 2^nth root of unity such that $\alpha^{-2^{n-d}} = \zeta$, then ζ is a primitive 2^dth root of unity. Note that $\alpha^{-2^{n-\ell+t} rs} = \zeta^{rs 2^{d-\ell+t}}$. Substituting the values of $\epsilon_i^{(2^{n-\ell} r)}$ from (9), (10) and (13) in (7), we get that for $d+1 \le \ell \le n$,

$$\theta_{2^{n-\ell} r}(x) = \frac{1}{2^{d+n-\ell}} \left\{ \sum_{\substack{i=0 \\ 2^\ell | i}}^{2^n-1} x^i - \sum_{\substack{i=1 \\ 2^{\ell-1} || i}}^{2^n-1} x^i \right\} + \sum_{t=0}^{\ell-2} \sum_{s \in S_{n-t}} \epsilon_{2^t s}^{(2^{n-\ell} r)} \sum_{i \in C_{2^t s}} x^i$$

$$= \frac{1}{2^{d+n-\ell}} \left\{ \sum_{\substack{i=0 \\ 2^\ell | i}}^{2^n-1} x^i - \sum_{\substack{i=1 \\ 2^{\ell-1} || i}}^{2^n-1} x^i \right\} + \frac{1}{2^{d+n-\ell}} \sum_{t=\ell-d}^{\ell-2} \sum_{s \in S_{n-t}} \zeta^{rs 2^{d-\ell+t}} \sum_{i \in C_{2^t s}} x^i$$

and for $2 \le \ell \le d$,

$$\theta_{2^{n-\ell} r}(x) = \frac{1}{2^n} \left\{ \sum_{\substack{i=0 \\ 2^\ell | i}}^{2^n-1} x^i - \sum_{\substack{i=1 \\ 2^{\ell-1} || i}}^{2^n-1} x^i \right\} + \frac{1}{2^n} \sum_{t=0}^{\ell-2} \sum_{s \in S_{n-t}} \zeta^{rs 2^{d-\ell+t}} \sum_{i \in C_{2^t s}} x^i.$$

Putting $\ell - t = j$, we obtain the required expression as stated in Theorem 1.

Proof of Theorem 2. Here $q = -1 + 2^d c$, $O_{2^d}(q) = 2 = O_{2^{d+1}}(q)$.

For $2 \le \ell \le n$, $r \in T_\ell$, working as in proof of Theorem 1, we can write $\theta_{2^{n-\ell} r}(x)$, as in (7), where now, for any $i \ge 0$, $\epsilon_i^{(2^{n-\ell} r)}$ has instead of (8), the following values :

$$\epsilon_i^{(2^{n-\ell} r)} = \frac{1}{2^n} \sum_{j \in C_{2^{n-\ell} r}} \alpha^{-ij} = \begin{cases} \frac{1}{2^n} \sum_{j=0}^{2^{\ell-d}-1} \alpha^{-i 2^{n-\ell} rq^j} & \text{if } d+1 \le \ell \le n, \\ \frac{1}{2^n} (\alpha^{-i 2^{n-\ell} r} + \alpha^{i 2^{n-\ell} r}) & \text{if } 2 \le \ell \le d. \end{cases} \tag{14}$$

Clearly, if $2^\ell | i$, then we have

$$\epsilon_i^{(2^{n-\ell}r)} = \frac{|C_{2^{n-\ell}r}|}{2^n}. \tag{15}$$

If $2^{\ell-1} || i$, then we get

$$\epsilon_i^{(2^{n-\ell}r)} = -\frac{|C_{2^{n-\ell}r}|}{2^n}. \tag{16}$$

And if $2^t || i$, $0 \le t \le \ell-2$, then by (6), $i \in \bigcup_{s \in T_{n-t}} C_{2^t s}$. Therefore we have

$$\epsilon_i^{(2^{n-\ell}r)} = \epsilon_{2^t s}^{(2^{n-\ell}r)} = \begin{cases} \frac{1}{2^n} \sum_{j=0}^{2^{\ell-d}-1} \alpha^{-2^{n-\ell+t}rsq^j} & \text{if } d+1 \le \ell \le n, \\ \frac{1}{2^n}(\alpha^{-2^{n-\ell+t}rs} + \alpha^{2^{n-\ell+t}rs}) & \text{if } 2 \le \ell \le d. \end{cases} \tag{17}$$

The value of $\sum_{j=0}^{2^{\ell-d}-1} \alpha^{-2^{n-\ell+t}rsq^j}$ is same as that given in (12) when $\ell - t \ge d+1$; but when $\ell - t \le d$, its value is $2^{\ell-d-1}(\alpha^{-2^{n-\ell+t}rs} + \alpha^{-2^{n-\ell+t}rsq})$. This is so because for $\ell - t \le d$, $\alpha^{-2^{n-\ell+t}rsq^j} = \alpha^{-2^{n-\ell+t}rsq^u}$ if and only if $j \equiv u \pmod 2$. Further for $\ell - t \ge d+2$, i.e., for $0 \le t \le \ell - d - 2$, by Lemma 1, the sum $\sum_{j=0}^{2^{\ell-t-d}-1} \alpha^{-2^{n-\ell+t}rsq^j} = 0$. Thus in this case

$$\epsilon_{2^t s}^{(2^{n-\ell}r)} = \begin{cases} 0 & \text{if } 0 \le t \le \ell-d-2, \\ & d+1 \le \ell \le n ; \\ \frac{|C_{2^n-\ell_r}|}{2^{n+1}}(\alpha^{-2^{n-\ell+t}rs} + \alpha^{-2^{n-\ell+t}rsq}) & \text{if } t \ge \ell-d-1, \\ & d+1 \le \ell \le n ; \\ \frac{|C_{2^n-\ell_r}|}{2^{n+1}}(\alpha^{-2^{n-\ell+t}rs} + \alpha^{2^{n-\ell+t}rs}) & \text{if } 2 \le \ell \le d, \\ & 0 \le t \le \ell-2. \end{cases} \tag{18}$$

Choose α, a primitive 2^nth root of unity such that $\alpha^{-2^{n-d-1}} = \omega$. Since $q = -1 + 2^d c$, $\omega^{2^d} = -1$, one finds that $\omega^q = -\omega^{-1}$. Then for $t \ge \ell - d - 1$ and $d+1 \le \ell \le n$, we have

$$\begin{aligned} \alpha^{-2^{n-\ell+t}rs} + \alpha^{-2^{n-\ell+t}rsq} &= \omega^{rs2^{d+1-\ell+t}} + \omega^{rs2^{d+1-\ell+t}q} \\ &= \omega^{rs2^{d+1-\ell+t}} + (-\omega)^{-rs2^{d+1-\ell+t}}. \end{aligned}$$

Also for $2 \le \ell \le d$, $0 \le t \le \ell - 2$,

$$\begin{aligned} \alpha^{-2^{n-\ell+t}rs} + \alpha^{2^{n-\ell+t}rs} &= \omega^{rs2^{d+1-\ell+t}} + \omega^{-rs2^{d+1-\ell+t}} \\ &= \omega^{rs2^{d+1-\ell+t}} + (-\omega)^{-rs2^{d+1-\ell+t}}. \end{aligned}$$

Also observe that when $t = \ell - 2$, $\omega^{rs2^{d-1}} + \omega^{-rs2^{d-1}} = 0$. Substituting the values of $\epsilon_i^{(2^{n-\ell}r)}$ in (7) and putting $\ell - t = j$, we obtain the required idempotents as stated in Theorem 2. □

4. The minimum distance of minimal cyclic codes of length 2^n.

The minimum distance of the minimal cyclic codes $\mathcal{M}_0$ and $\mathcal{M}_{2^n-1}$ is clearly 2^n and their generating polynomials are $1+x+x^2+\cdots+x^{2^n-1}$ and $(x-1)\{1+x^2+x^4+\cdots+(x^2)^{2^{n-1}-1}\}$ respectively.

For a fixed integer ℓ, $2 \le \ell \le n$, and r varying over S_ℓ or T_ℓ as the case may be, all the minimal cyclic codes $\mathcal{M}_{2^n-\epsilon_r}$ are equivalent, and hence have the same minimum distance.

For any ℓ, $2 \le \ell \le n$, we have

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

Note that, for r varying over S_ℓ or T_ℓ, by (6), we have

$$\prod_r M^{(2^{n-\ell}r)}(x) = \prod_r \prod_{i \in C_{2^n-\epsilon_r}} (x - \alpha^i) = \prod_{\substack{j=1 \\ 2^{n-\ell} \nmid j}}^{2^n-1} (x - \alpha^i) = x^{2^{\ell-1}} + 1.$$

Let $\mathcal{C}_\ell$ be the code of length 2^ℓ generated by $x^{2^{\ell-1}} - 1$. Then by Lemma 12 of [6], $\hat{\mathcal{C}}_\ell$, the code of length 2^n generated by $\dfrac{x^{2^n}-1}{\prod_r M^{(2^{n-\ell}r)}(x)}$ is the repetition of code $\mathcal{C}_\ell$ repeated $2^{n-\ell}$ times and its minimum distance is $2.2^{n-\ell} = 2^{n-\ell+1}$. The minimal code $\mathcal{M}_{2^n-\epsilon_r}$, being the subcode of the code $\hat{\mathcal{C}}_\ell = \bigoplus_r \mathcal{M}_{2^n-\epsilon_r}$, has minimum distance at least $2^{n-\ell+1}$.

Example 1. Let $n = 4$, $q = 3 = -1 + 2^2$ so that $d = 2$. The 3-cyclotomic cosets mod 16 are

$$\begin{array}{llll} C_0 = \{0\}, & & C_4 = \{4,12\}, & \\ C_1 = \{1,3,9,11\}, & & C_{-1} = \{5,7,13,15\}, & \\ C_2 = \{2,6\}, & & C_{-2} = \{10,14\}, & \\ C_8 = \{8\}. & & & \end{array}$$

Also $x^2 \equiv -2 \pmod 3$ has the solutions ± 1. If we take $\sqrt{-2} = 1$ in F_3, the seven ternary primitive idempotents mod 16 are given by

$$\begin{aligned}
\theta_0(x) &= (1 + x + x^2 + \cdots + x^{15}),\\
\theta_1(x) &= 1 - x^2 - x^6 - x^8 + x^{10} + x^{14},\\
\theta_2(x) &= -1 + x + x^3 + x^4 - x^5 - x^7 - x^8 + x^9 + x^{11} + x^{12} - x^{13} - x^{15},\\
\theta_4(x) &= -1 + x^2 - x^4 + x^6 - x^8 + x^{10} - x^{12} + x^{14},\\
\theta_{-1}(x) &= 1 + x^2 + x^6 - x^8 - x^{10} - x^{14},\\
\theta_8(x) &= 1 - x + x^2 - \cdots - x^{15},\\
\theta_{-2}(x) &= -1 - x - x^3 + x^4 + x^5 + x^7 - x^8 - x^9 - x^{11} + x^{12} + x^{13} + x^{15}.
\end{aligned}$$

The minimal ternary cyclic codes of length 16 have the following parameters:

Code	*dimension*	*minimum distance*	*generating polynomial*
$\mathcal{M}_0$	1	16	$(x^{15} + x^{14} + \cdots + x + 1)$,
$\mathcal{M}_1$	4	6	$(x^{12} + x^{10} - x^8 - x^4 - x^2 + 1)$,
$\mathcal{M}_2$	2	12	$(x^{14} + x^{13} - x^{12} - x^{10} - x^9 + x^8$ $+x^6 + x^5 - x^4 - x^2 - x + 1)$,
$\mathcal{M}_4$	2	8	$(x^{14} - x^{12} + x^{10} - x^8 + x^6 - x^4 + x^2 - 1)$,
$\mathcal{M}_{-1}$	4	6	$(x^{12} - x^{10} - x^8 - x^4 + x^2 + 1)$,
$\mathcal{M}_8$	1	16	$(x^{15} - x^{14} + \cdots + x - 1)$,
$\mathcal{M}_{-2}$	2	12	$(x^{14} - x^{13} - x^{12} - x^{10} + x^9 + x^8$ $+x^6 - x^5 - x^4 - x^2 + x + 1)$.

Example 2. Let $n = 4$, $q = 5 = 1 + 2^2$ so that $d = 2$. The 5-ary cyclotomic cosets mod 16 are

$$\begin{aligned}
C_0 &= \{0\}, & C_8 &= \{8\},\\
C_1 &= \{1,5,9,13\}, & C_{-1} &= \{3,7,11,15\},\\
C_2 &= \{2,10\}, & C_{-2} &= \{6,14\},\\
C_4 &= \{4\}, & C_{-4} &= \{12\}.
\end{aligned}$$

Also $x^2 \equiv -1 \pmod 5$ has the solutions ± 2. If we take $\sqrt{-1} = 2$ in F_5, the eight 5-ary primitive idempotents mod 16 are given by

$$\begin{aligned}
\theta_0(x) &= (1 + x + x^2 + \cdots + x^{15}),\\
\theta_1(x) &= -1 + 2x^4 + x^8 - 2x^{12},\\
\theta_2(x) &= 2 + x^2 - 2x^4 - x^6 + 2x^8 + x^{10} - 2x^{12} - x^{14},\\
\theta_{-1}(x) &= -1 - 2x^4 + x^8 + 2x^{12},\\
\theta_4(x) &= 1 - x - x^2 + x^3 + x^4 - x^5 - x^6 + x^7 + x^8 - x^9 - x^{10} + x^{11}\\
&\quad +x^{12} - x^{13} - x^{14} + x^{15},\\
\theta_{-2}(x) &= 2 - x^2 - 2x^4 + x^6 + 2x^8 - x^{10} - 2x^{12} + x^{14},\\
\theta_8(x) &= 1 - x + x^2 - \cdots - x^{15},\\
\theta_{-4}(x) &= 1 + x - x^2 - x^3 + x^4 + x^5 - x^6 - x^7 + x^8 + x^9 - x^{10} - x^{11}\\
&\quad +x^{12} + x^{13} - x^{14} - x^{15}.
\end{aligned}$$

The minimal 5-ary cyclic codes of length 16 have the following parameters :

Code	*dimension*	*minimum distance*	*generating polynomial*
$\mathcal{M}_0$	1	16	$(x^{15}+x^{14}+\cdots+x+1)$,
$\mathcal{M}_1$	4	4	$(x^{12}+2x^8-x^4-2)$,
$\mathcal{M}_2$	2	8	$(x^{14}+2x^{12}-x^{10}-2x^8+x^6+2x^4-x^2-2)$,
$\mathcal{M}_{-1}$	4	4	$(x^{12}-2x^8-x^4+2)$,
$\mathcal{M}_4$	1	16	$(x^{15}+2x^{14}-x^{13}-2x^{12}+x^{11}+2x^{10}-x^9$ $-2x^8+x^7+2x^6-x^5-2x^4+x^3+2x^2-x-2)$,
$\mathcal{M}_{-2}$	2	8	$(x^{14}-2x^{12}-x^{10}+2x^8+x^6-2x^4-x^2+2)$,
$\mathcal{M}_8$	1	16	$(x^{15}-x^{14}+\cdots+x-1)$,
$\mathcal{M}_{-4}$	1	16	$(x^{15}-2x^{14}-x^{13}+2x^{12}+x^{11}-2x^{10}-x^9$ $+2x^8+x^7-2x^6-x^5+2x^4+x^3-2x^2-x+2)$.

Given below is a table of irreducible cyclic codes of length 2^n, $3 \leq n \leq 7$, with good dimension and minimum distance :

$q=3$				$q=5$			
Length	Code	dimension	minimum distance	Length	Code	dimension	minimum distance
8	$\mathcal{M}_1$	2	6	8	$\mathcal{M}_1$	2	4
16	$\mathcal{M}_1$	4	6	16	$\mathcal{M}_1$	4	4
16	$\mathcal{M}_2$	2	12	16	$\mathcal{M}_2$	2	8
32	$\mathcal{M}_1$	8	6	32	$\mathcal{M}_1$	8	4
32	$\mathcal{M}_2$	4	12	32	$\mathcal{M}_2$	4	8
32	$\mathcal{M}_4$	2	24	32	$\mathcal{M}_4$	2	16
64	$\mathcal{M}_1$	16	6	64	$\mathcal{M}_1$	16	4
64	$\mathcal{M}_2$	8	12	64	$\mathcal{M}_2$	8	8
64	$\mathcal{M}_4$	4	24	64	$\mathcal{M}_4$	4	16
64	$\mathcal{M}_8$	2	48	64	$\mathcal{M}_8$	2	32
128	$\mathcal{M}_1$	32	6	128	$\mathcal{M}_1$	32	4
128	$\mathcal{M}_2$	16	12	128	$\mathcal{M}_2$	16	8
128	$\mathcal{M}_4$	8	24	128	$\mathcal{M}_4$	8	16
128	$\mathcal{M}_8$	4	48	128	$\mathcal{M}_8$	4	32
128	$\mathcal{M}_{16}$	2	96	128	$\mathcal{M}_{16}$	2	64

Their idempotent generators are explicitly stated in the Corollary with $r=1$, on taking $\sqrt{-2}=1$ in F_3 and $\sqrt{-1}=2$ in F_5.

References.

1. G. K. Bakshi and M. Raka, Minimal cyclic codes of length $p^n q$, Finite Fields Appl. 9, no.4 (2003) 432-448.

2. G. K. Bakshi and M. Raka, Minimal cyclic codes of length 2^m , Ranchi University Math. Journal 33 (2002) 1-18.

3. D. Berman, "Semisimple cyclic and abelian code.II.", Cybernatics 3(3) (1967) 17-23.

4. W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press (2003).

5. F.J. MacWilliams and N.J.A. Sloane, Theory of Error-Correcting Codes, North-Holland, Amsterdam (1977).

6. A. Sharma, G.K. Bakshi, V.C. Dumir and M. Raka, Cyclotomic Numbers and Primitive Idempotents in the Ring $GF(q)[x]/(x^{p^n} - 1)$, Finite Fields and their Appl. 10, no.4, (2004) 653-673.

7. A. Sharma, G.K. Bakshi and M. Raka, Irreducible Cyclic Codes of Length $2p^n$, accepted in ARS Combinatoria, 2005.

8. A. Sharma, G.K. Bakshi and M. Raka, Polyadic codes of prime power length, submitted in Journal of Combinatorial Theory, Series A.