Irreducible cyclic codes of length $2p^n$

Anuradha Sharma*, Gurmeet K. Bakshi, and Madhu Raka
Centre for Advanced Study in Mathematics
Panjab University
Chandigarh - 160014
INDIA

April 27, 2005

Abstract

Let q be an odd prime power and p be an odd prime with $\gcd(p,q) = 1$. Let the order of q modulo p be f and $\gcd\left(\frac{p-1}{f}, q\right) = 1$. Here explicit expressions for all the primitive idempotents in the ring $R_{2p^n} = GF(q)[x]/(x^{2p^n} - 1)$, for any positive integer n, are obtained in terms of cyclotomic numbers, provided p does not divide $\frac{q^f-1}{2p}$, if $n \geq 2$. Some lower bounds on the minimum distances of irreducible cyclic codes of length $2p^n$ over $GF(q)$ are also obtained.

Keywords : Cyclic codes, cyclotomic numbers, idempotents, periods.

1. Introduction.

Let $GF(q)$ be a field of prime power order q, q odd. Let $m \geq 1$ be an integer with $\gcd(q,m) = 1$. Let $R_m = GF(q)[x]/(x^m - 1)$. A cyclic code of length m over $GF(q)$ is an ideal in the ring R_m. The ideal C is generated by a generating polynomial $g(x)$ that is the unique monic divisor of $(x^m - 1)$. The ideal C is also generated by a unique polynomial $e(x)$ which is an idempotent in R_m, i.e., $(e(x))^2 = e(x)$ (for reference, see Chapter 4 of [5] or Chapter 8 of [6]). Every ideal in R_m can be expressed uniquely as a sum of minimal ideals also known as irreducible cyclic codes. The generator idempotents of irreducible cyclic codes are called the primitive idempotents. Thus it is of interest to determine the primitive idempotents.

Construction of binary idempotents from the cyclotomic cosets is easy. In general, however, as stated by V. Pless [7, §3, p.95], "we do not have much information about the codes generated. Only in special situations do we know the dimension". We consider non-binary cyclic codes only, i.e., we take q to be always odd.

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

For non-binary cyclic codes, Berman [4, p.22] gave explicit expression (without proof) for all the primitive idempotents in R_{p^n}, where p, q are odd primes and q a primitive root modulo p^n; Pruthi and Arora [8] verified it. Let the order of q modulo p be f and $\gcd(\frac{p-1}{f}, q) = 1$. In a previous paper [9], the authors gave an algorithm to determine all the primitive idempotents in the ring $R_{p^n} = GF(q)[x]/(x^{p^n} - 1)$, for any positive integer n, with the condition that p does not divide $\frac{q^f-1}{p}$ if $n \geq 2$; thus generalizing a result of Berman [4].

In this paper, we give an algorithm to determine all the primitive idempotents in the ring $R_{2p^n} = GF(q)[x]/(x^{2p^n} - 1)$, (see Theorem 3). This is an extension of a result of Arora and Pruthi [1], where they obtained primitive idempotents in the ring R_{2p^n}, under the strong assumption that q is a primitive root mod $2p^n$, i.e., for $f = p - 1$ only. Our method of computing primitive idempotents in the ring R_{2p^n} is similar to that of computing primitive idempotents in the ring R_{p^n}, used in [9].

Earlier, Bakshi and Raka [2] have derived all the primitive idempotents in the ring $R_{p^n\ell}$, where p, q, ℓ are distinct odd primes, q a primitive root modulo p^n and also modulo ℓ, with $\gcd(\frac{\phi(p^n)}{2}, \frac{\phi(\ell)}{2}) = 1$. In [3], Bakshi and Raka obtained all the primitive idempotents in $R_{2^m}, m \geq 3$, when $q \equiv 3$ or $5 \pmod 8$.

2. Cyclotomic Cosets modulo $2p^n$.

For any integer $m \geq 1$ such that $\gcd(m, q) = 1$, 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 q-cyclotomic cosets modulo $2p^n$.

Throughout this paper, we assume that p is an odd prime, n is a positive integer, q is an odd prime power with $\gcd(p, q) = 1$. Let the order of q modulo p be $f = \frac{p-1}{e}$ for some positive integer e and let $q^f = 1 + 2p\lambda$. Further suppose that p does not divide λ, if $n \geq 2$. Let $O_m(q)$ denotes the order of q modulo m. The following two lemmas can be easily obtained as in [9].

Lemma 1: $O_{2p^n}(q) = fp^{n-1} = O_{p^n}(q)$ for all $n \geq 1$.

Lemma 2 : Let g be a primitive root mod $2p$ such that $\gcd(\frac{g^{p-1}-1}{p}, p) = 1$, then g is a primitive root mod $2p^n$, and hence a primitive root modulo p^n also, for all integers $n \geq 1$.

Remark 1: On replacing g by $g + 2p$ (if necessary), we can always ensure that $\gcd(\frac{g^{p-1}-1}{p}, p) = 1$, so there always exist a primitive root g mod $2p^n$ for all $n \geq 1$.

Theorem 1 : For each integer $n \geq 1$, there are $2(en + 1)$ distinct

q-cyclotomic cosets mod $2p^n$ given by

$$\begin{aligned} C_0 &= \{0\}, \\ C_{p^n} &= \{p^n\}, \\ C_{2^i p^j g^k} &= \{2^i p^j g^k, 2^i p^j g^k q, 2^i p^j g^k q^2, \cdots, 2^i p^j g^k q^{fp^{n-j-1}-1}\}, \end{aligned}$$

for $0 \le i \le 1$, $0 \le j \le n-1$ and $0 \le k \le e-1$, where g is a primitive root mod $2p^n$.

Proof is similar to that of Theorem 1 of [9].

3. Cyclotomic numbers and Periods.

The results of this section are explicitly stated and proved in [9]. For the sake of completeness, we give some definitions and results we need. The reduced residue system modulo p given by $\{1, g, g^2, \cdots, g^{p-2}\}$ is divided into e disjoint classes $\hat{C}_i$, for $i = 0, 1, 2, \cdots, e-1$, where

$$\hat{C}_i = \{g^{es+i} : s = 0, 1, 2, \cdots, f-1\} = \{g^i, g^i q, g^i q^2, \cdots, g^i q^{f-1}\}.$$

If $n = 1$, the class $\hat{C}_i$ is same as C_{g^i}, defined earlier.

For fixed i and j, $0 \le i, j \le e-1$, the cyclotomic number A_{ij} is defined to be the number of solutions of the equation

$$z_i + 1 = z_j, \quad \text{where} \quad z_i \in \hat{C}_i, \ z_j \in \hat{C}_j.$$

For $0 \le k \le e-1$, the period η_k is defined as

$$\eta_k = \sum_{t=0}^{f-1} \beta^{g^k q^t} = \sum_{t=0}^{f-1} \beta^{g^{et+k}} = \sum_{j \in \hat{C}_k} \beta^j, \tag{1}$$

where β is a primitive p^{th} root of unity in some extension field of $GF(q)$. Let $\mathcal{A}$ denote the $e \times e$ matrix given by

$$\begin{bmatrix} A_{00}-f & A_{01}-f & A_{02}-f & \cdots & A_{0(e-1)}-f \\ A_{10} & A_{11} & A_{12} & \cdots & A_{1(e-1)} \\ A_{20} & A_{21} & A_{22} & \cdots & A_{2(e-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)} \end{bmatrix}, \text{ if } f \text{ is even}$$

and is given by

$$\begin{bmatrix} A_{00} & A_{01} & A_{02} & \cdots & A_{0(e-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ A_{(\frac{e}{2}-1)0} & A_{(\frac{e}{2}-1)1} & A_{(\frac{e}{2}-1)2} & \cdots & A_{(\frac{e}{2}-1)(e-1)} \\ A_{(\frac{e}{2})0}-f & A_{(\frac{e}{2})1}-f & A_{(\frac{e}{2})2}-f & \cdots & A_{(\frac{e}{2})(e-1)}-f \\ A_{(\frac{e}{2}+1)0} & A_{(\frac{e}{2}+1)1} & A_{(\frac{e}{2}+1)2} & \cdots & A_{(\frac{e}{2}+1)(e-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)} \end{bmatrix}, \text{ if } f \text{ is odd.}$$

Let $X = (x_0, x_1, x_2, \cdots, x_{e-1})^T$, where '$T$' stands for the transpose of a matrix, be an eigen vector of $\mathcal{A}$. We say that X has cyclic property if for each k, $0 \leq k \leq e-1$, $\sigma^k(X)$, the kth cyclic shift of X, is also an eigen vector of $\mathcal{A}$.

The following theorem, proved in [9], is a crucial step towards the main result.

Theorem 2 : Let $\gcd(e, q) = 1$.

(*i*) The period η_i is an eigenvalue of the matrix $\mathcal{A}$ with $P_i = (\eta_i, \eta_{i+1}, \eta_{i+2}, \cdots, \eta_{i-1})^T$ as a corrosponding eigen vector with first entry η_i, for each i, $0 \leq i \leq e-1$.
(Thus the eigen vector P_i, for each i, has the cyclic property.)

(*ii*) The matrix $P = (P_0\ P_1\ P_2 \cdots P_{e-1})$ having the eigen vector P_i as its $(i+1)$th column is nonsingular, so that η_0, η_1, η_2, $\cdots$, η_{e-1} are all the eigenvalues of $\mathcal{A}$, counted with multiplicity.

(*iii*) If $X = (\rho_0, \rho_1, \rho_2, \cdots, \rho_{e-1})^T$ is another eigen vector of $\mathcal{A}$ with cyclic property, then $X = \alpha P_j$ for some j, $0 \leq j \leq e-1$ and for some scalar $\alpha \in GF(q)$.
In addition, if $\sum_{i=0}^{e-1} \rho_i = -1$, then $X = P_j$ for some j.

Lemma 3 : Let $\gcd(a, 2p) = 1$, $p = 1 + ef$.

(i) For $\ell = 0$ or 1, a is an e^{th} power residue mod $2^\ell p^k$, where k is any positive integer, if and only if

$$a^{fp^{k-1}} \equiv 1 \pmod{2^\ell p^k}.$$

(ii) If a is an e^{th} power residue mod $2p$, then $a + 2\mu p$, for any μ, is an e^{th} power residue mod $2p^k$, for all $k \geq 1$.

(iii) The set $S = \left\{ a + 2\mu p : \begin{array}{c} a \text{ runs over } e^{th} \text{ power residues mod } 2p \\ \mu \text{ runs over complete residue system} \\ \text{mod } p^{k-1} \end{array} \right\}$
consists of all the fp^{k-1} incongruent e^{th} power residues mod $2p^k$ for all $k \geq 2$.

Proof is similar to that of Lemma 10 of [9].

Lemma 4: The cyclotomic number A_{0j} is even or odd according as $2 \in \hat{C}_j$ or not. In particular, exactly one of the numbers A_{0j}, say A_{0t}, is odd.

This is Lemma 4 of [10, Part I].

Lemma 5 : Let $2 \in \hat{C}_t$ for some t, $0 \leq t \leq e-1$. Then, for every s, $0 \leq s \leq n-1$, $2 \equiv g^t q^{u_s} \pmod{p^{n-s}}$, for some u_s, $0 \leq u_s \leq fp^{n-s-1} - 1$.

Proof : $2 \in \hat{C}_t$ implies $2g^{-t}$ is an e^{th} power residue mod p, which by Lemma 3(i), gives $(2g^{-t})^f \equiv 1 \pmod{p}$. Then for every s, $0 \leq s \leq n-1$,

we have

$$(2g^{-t})^{fp^{n-s-1}} \equiv 1 \pmod{p^{n-s}}.$$

This, by Lemma 3(i) again, gives that $2g^{-t}$ is an e^{th} power residue mod p^{n-s}. As $1, q, q^2, \cdots, q^{fp^{n-s-1}-1}$ are all the e^{th} power residues mod p^{n-s}, we get the required result.

Lemma 6 : Let ℓ be either 0 or 1. Let $S_i^{(\ell)}$, $0 \le i \le e-1$, denote the sum

$$S_i^{(\ell)} = \gamma^{2^\ell g^i} + \gamma^{2^\ell g^i q} + \gamma^{2^\ell g^i q^2} + \cdots + \gamma^{2^\ell g^i q^{fp^{k-1}-1}},$$

where γ is a primitive $(2p^k)$th, $k \ge 1$, root of unity. Then for a suitable choice of γ, we have

$$S_i^{(\ell)} = \begin{cases} \eta_i & \text{if } k=1 \text{ and } \ell=1 \\ -\eta_{i-t} & \text{if } k=1 \text{ and } \ell=0 \\ 0 & \text{if } k \ge 2. \end{cases}$$

Proof : If $k=1$ and $\ell=1$, then choosing γ such that $\gamma^2=\beta$, we have

$$S_i^{(1)} = \sum_{u=0}^{f-1} \gamma^{2g^i q^u} = \sum_{u=0}^{f-1} \beta^{g^i q^u} = \eta_i.$$

Let now $k=1$ and $\ell=0$. We know, by Lemma 5, that $2 \equiv g^t q^{u_{n-1}} \pmod p$, for some u_{n-1}, $0 \le u_{n-1} \le f-1$ which is equivalent to $2 \equiv g^t q^{u_{n-1}} + p \pmod{2p}$. Since $\gamma^p = -1$, we have

$$\begin{aligned} \eta_i &= \sum_{u=0}^{f-1} \gamma^{2g^i q^u} = \sum_{u=0}^{f-1} \gamma^{(g^t q^{u_{n-1}}+p)g^i q^u} = \sum_{u=0}^{f-1} \gamma^{g^{t+i} q^{u_{n-1}+u}} \gamma^{pg^i q^u} \\ &= -\sum_{v=0}^{f-1} \gamma^{g^{t+i} q^v} = -S_{i+t}^{(0)} \end{aligned}$$

which implies $S_i^{(0)} = -\eta_{i-t}$.

Let now $k \ge 2$. As the set $\{1, q, q^2, \cdots, q^{fp^{k-1}-1}\}$ consists of all the e^{th} power residues mod $2p^k$, using Lemma 3(iii) and working as in Lemma 11 of [9], we get that $S_i^{(\ell)} = 0$ for each i, $0 \le i \le e-1$ and $k \ge 2$.

4. Primitive idempotents of the irreducible codes of length $2p^n$.

If α denotes a primitive $(2p^n)$th root of unity in some extension field of $GF(q)$, then the polynomial $M^{(s)}(x) = \prod_{i \in C_s} (x - \alpha^i)$ is the minimal polynomial of α^s over $GF(q)$ and the ideal $\mathcal{M}_s$ generated by $\frac{x^{2p^n}-1}{M^{(s)}(x)}$ is a

minimal ideal in R_{2p^n}. The primitive idempotent of the ideal $\mathcal{M}_s$ will be denoted by $\theta_s(x)$. It is known that

$$\theta_s(\alpha^j) = \begin{cases} 1 & if \quad j \in C_s \\ 0 & if \quad j \notin C_s. \end{cases} \tag{2}$$

Clearly, the irreducible (or minimal) cyclic codes $\mathcal{M}_0$ and $\mathcal{M}_{p^n}$ have their generator polynomials as $h(x) = 1 + x + x^2 + x^3 + \cdots + x^{2p^n-1}$ and $j(x) = 1 - x + x^2 - x^3 + \cdots - x^{2p^n-1}$ respectively and their primitive idempotents are $\theta_0(x) = \frac{1}{2p^n}h(x)$ and $\theta_{p^n}(x) = \frac{1}{2p^n}j(x)$ respectively. It is clear that both the minimal codes $\mathcal{M}_0$ and $\mathcal{M}_{p^n}$ have minimum distance equal to $2p^n$ and dimension equal to 1.

For a fixed s, define the polynomial

$$\Omega_s(x) = \sum_{j \in C_{p^n-s-1}} x^j.$$

All the polynomials in this paper are considered mod $(x^{2p^n} - 1)$.

An algorithm to compute non-trivial primitive idempotents in the ring R_{2p^n}.

- Step I : Find a primitive root g mod $2p$ such that $gcd(\frac{g^{p-1}-1}{p}, p) = 1$.
- Step II : Evaluate all the e^2 cyclotomic numbers A_{ij}, $0 \le i, j \le e-1$.
- Step III : Find all the eigenvalues of matrix $\mathcal{A}$.
- Step IV : Fix an eigen value ρ_0 of $\mathcal{A}$. Corresponding to ρ_0, find an eigen vector $P_0 = (\rho_0, \rho_1, \rho_2, \cdots, \rho_{e-1})$, whose first entry is ρ_0 and other entries ρ_i, $1 \le i \le e-1$, are the remaining eigenvalues of $\mathcal{A}$ with $\sum_{i=0}^{e-1} \rho_i = -1$, and P_0 having cyclic property. (Such a P_0 exists uniquely by Theorem 2).
- Step V : Choose t, $0 \le t \le e-1$, for which A_{0t} is odd (such a t is unique by Lemma 4).
- Step VI : Compute the following polynomials over $GF(q)$, for $0 \le j \le n-1$,

$$\theta_{p^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}-1)\{f \sum_{\substack{i=0, i \text{ odd} \\ p^{n-j} \mid i}}^{2p^n-1} x^i + \rho_{e-t}\Omega_j(x) + \rho_{e-t+1}\Omega_j(x^g) + \cdots + \rho_{e-t-1}\Omega_j(x^{g^{e-1}})\},$$

$$\theta_{gp^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}-1)\{f \sum_{\substack{i=0,i \text{ odd} \\ p^{n-j}|i}}^{2p^n-1} x^i + \rho_{e-t+1}\Omega_j(x) + \rho_{e-t+2}\Omega_j(x^g) + \cdots + \rho_{e-t}\Omega_j(x^{g^{e-1}})\},$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$\theta_{g^{e-1}p^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}-1)\{f \sum_{\substack{i=0,i \text{ odd} \\ p^{n-j}|i}}^{2p^n-1} x^i + \rho_{e-t-1}\Omega_j(x) + \rho_{e-t}\Omega_j(x^g) + \cdots + \rho_{e-t-2}\Omega_j(x^{g^{e-1}})\},$$

$$\theta_{2p^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}+1)\ \{f \sum_{\substack{i=0 \\ p^{n-j}|i}}^{p^n-1} x^i + \rho_0\Omega_j(x) + \rho_1\Omega_j(x^g) + \cdots + \rho_{e-1}\Omega_j(x^{g^{e-1}})\},$$

$$\theta_{2gp^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}+1)\ \{f \sum_{\substack{i=0 \\ p^{n-j}|i}}^{p^n-1} x^i + \rho_1\Omega_j(x) + \rho_2\Omega_j(x^g) + \cdots + \rho_0\Omega_j(x^{g^{e-1}})\},$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$\theta_{2g^{e-1}p^j}(x) = \frac{1}{2p^{j+1}}(x^{p^n}+1)\ \{f \sum_{\substack{i=0 \\ p^{n-j}|i}}^{p^n-1} x^i + \rho_{e-1}\Omega_j(x) + \rho_0\Omega_j(x^g) + \cdots + \rho_{e-2}\Omega_j(x^{g^{e-1}})\}.$$

Theorem 3 : Let p be an odd prime and q be an odd prime power, with $\gcd(p,q)=1$. Let the order of q modulo p be f and $q^f = 1+2p\lambda$. Further suppose that p does not divide λ if $n \geq 2$. Let $\gcd(e,q)=1$, where $p = 1+ef$. Then we can choose α, a primitive $(2p^n)$th root of unity, suitably, so that step V of the above Algorithm gives all the $2en$ non-trivial primitive idempotents in the ring R_{2p^n}.

Proof : For $0 \leq j \leq n-1$, j fixed, we have, by Theorem 6 of [6, Ch. 8], generalized to non-binary case, that

$$\theta_{p^j}(x) = \sum_{i=0}^{2p^n-1} \epsilon_i^{(p^j)} x^i, \quad \text{where } \epsilon_i^{(p^j)} = \frac{1}{2p^n} \sum_{h \in C_{p^j}} \alpha^{-ih} = \frac{1}{2p^n} \sum_{u=0}^{fp^{n-j-1}-1} \alpha^{-ip^j q^u}.$$

As the value of $\epsilon_i^{(p^j)}$ remain the same for all i in a cyclotomic coset, we have

$$\theta_{p^j}(x) = \epsilon_0^{(p^j)} + \sum_{\ell=0}^{1} \sum_{r=0}^{e-1} \sum_{s=0}^{n-1} \epsilon_{2\ell g^r p^s}^{(p^j)} \sum_{i \in C_{2\ell g^r p^s}} x^i \ + \ \epsilon_{p^n}^{(p^j)} x^{p^n}.$$

Now

$$\epsilon_0^{(p^j)} = \frac{1}{2p^n} \sum_{h=0}^{p^{n-j-1}f-1} \alpha^{-0p^j q^h} = \frac{f}{2p^{j+1}}\ , \ \epsilon_{p^n}^{(p^j)} = \frac{1}{2p^n} \sum_{h \in C_{p^j}} \alpha^{-p^n h} = \frac{-f}{2p^{j+1}}.$$

If $s \geq n-j$,

$$\epsilon_{2^\ell g^r p^s}^{(p^j)} = \frac{1}{2p^n} \sum_{h=0}^{p^{n-j-1}f-1} \alpha^{-2^\ell g^r p^{s+j} q^h} = \begin{cases} \frac{-f}{2p^{j+1}} & \text{if} \quad \ell = 0 \\ \frac{f}{2p^{j+1}} & \text{if} \quad \ell = 1. \end{cases}$$

If $0 \leq s \leq n-j-1$, then

$$\epsilon_{2^\ell g^r p^s}^{(p^j)} = \frac{1}{2p^n} \sum_{h=0}^{p^{n-j-1}f-1} \gamma^{2^\ell g^r q^h}, \tag{3}$$

where $\gamma = \alpha^{-p^{s+j}}$ is a primitive $(2p^{n-s-j})$th root of unity.

Now $\gamma^{2^\ell g^r q^h} = \gamma^{2^\ell g^r q^{h'}}$ if and only if $q^h \equiv q^{h'} \pmod{p^{n-s-j}}$ if and only if $h \equiv h' \pmod{fp^{n-s-j-1}}$, as $O_{p^{n-s-j}}(q) = fp^{n-s-j-1}$.
Thus from (2), we get

$$\epsilon_{2^\ell g^r p^s}^{(p^j)} = \frac{1}{2p^n} \frac{p^{n-j-1}}{p^{n-s-j-1}} \sum_{h=0}^{p^{n-j-s-1}f-1} \gamma^{2^\ell g^r q^h}. \tag{4}$$

If $k = n-s-j \geq 2$, i.e., if $0 \leq s \leq n-j-2$, then the sum on the right hand side of (3), which is $S_r^{(\ell)}$, is zero by Lemma 6. If $s = n-j-1$, by (3), we have

$$\epsilon_{2^\ell g^r p^{n-j-1}}^{(p^j)} = \frac{1}{2p^{j+1}} \sum_{h=0}^{f-1} \gamma^{2^\ell g^r q^h} = \frac{1}{2p^{j+1}} S_r^{(\ell)} = \begin{cases} \frac{-1}{2p^{j+1}} \eta_{r-t} & \text{if} \quad \ell = 0 \\ \frac{1}{2p^{j+1}} \eta_r & \text{if} \quad \ell = 1. \end{cases}$$

We choose α and hence β suitably to have $\eta_r = \rho_r$. Therefore $\theta_{p^j}(x)$ is given by

$$\frac{f}{2p^{j+1}} \left\{ 1 - x^{p^n} + \sum_{r=0}^{e-1} \sum_{s=n-j}^{n-1} \sum_{i \in C_{2g^r p^s}} x^i - \sum_{r=0}^{e-1} \sum_{s=n-j}^{n-1} \sum_{i \in C_{g^r p^s}} x^i \right\}$$

$$+ \frac{1}{2p^{j+1}} \left\{ \sum_{r=0}^{e-1} \rho_r \sum_{i \in C_{2g^r p^{n-j-1}}} x^i - \sum_{r=0}^{e-1} \rho_{r-t} \sum_{i \in C_{g^r p^{n-j-1}}} x^i \right\}.$$

Further, since by Lemma 5, $2g^r p^s \equiv g^{t+r} p^s q^{u_s} (\bmod\ p^n)$, we have $2g^r p^s \equiv g^{t+r} p^s q^{u_s} + p^n (\bmod\ 2p^n)$. Therefore

$$\sum_{i \in C_{2g^r p^s}} x^i = x^{p^n} \sum_{i \in C_{g^{t+r} p^s}} x^i.$$

Hence $\theta_{p^j}(x)$ is given by

$$\frac{f}{2p^{j+1}}\{x^{p^n}(x^{p^n}-1) \;+\; (x^{p^n}-1)\sum_{r=0}^{e-1}\sum_{s=n-j}^{n-1}\sum_{i\in C_{g^r p^s}} x^i\}$$

$$+\quad \frac{1}{2p^{j+1}}(x^{p^n}-1)\sum_{r=0}^{e-1}\rho_{r-t}\sum_{i\in C_{g^r p^{n-j-1}}} x^i$$

which can further be written as

$$\frac{1}{2}(x^{p^n}-1)\{\frac{f}{p^{j+1}}\sum_{\substack{i=0\\ p^{n-j}|i\\ i \text{ odd}}}^{2p^n-1} x^i+\frac{1}{p^{j+1}}[\rho_{e-t}\Omega_j(x)+\rho_{e-t+1}\Omega_j(x^g)+\cdots+\rho_{e-t-1}\Omega_j(x^{g^{e-1}})]\}.$$

Working in a similar way, one can obtain that

$$\theta_{2p^j}(x)=\frac{1}{2}(x^{p^n}+1)\{\frac{f}{p^{j+1}}\sum_{\substack{i=0\\ p^{n-j}|i}}^{p^n-1} x^i+\frac{1}{p^{j+1}}[\rho_0\Omega_j(x)+\rho_1\Omega_j(x^g)+\cdots+\rho_{e-1}\Omega_j(x^{g^{e-1}})]\}.$$

Further since for any j and ℓ,

$$\theta_{2^\ell g^k p^j}(x)=\theta_{2^\ell p^j}(x^{g^{-k}})$$

for each k, $0\le k\le e-1$, Theorem 3 is proved.

The result of Arora and Pruthi [1] follows as a corollary of Theorem 3.

Corollary : Let p be an odd prime, q an odd prime power such that q is a primitive root mod $2p^n$, $n\ge 1$ an integer. Then there are $2(n+1)$ primitive idempotents in R_{2p^n}, given by

$$\begin{aligned}
\theta_0(x) &= \tfrac{1}{p^n}\left\{1+x+x^2+\cdots+x^{2p^n-1}\right\},\\
\theta_{p^n}(x) &= \tfrac{1}{p^n}\left\{1-x+x^2-\cdots-x^{2p^n-1}\right\},\\
\theta_{p^j}(x) &= \tfrac{1}{2p^{j+1}}(x^{p^n}-1)\{(p-1)\sum_{\substack{i=0,\ i \text{ odd}\\ p^{n-j}|i}}^{2p^n-1} x^i-\sum_{i\in C_{p^{n-j-1}}} x^i\},\\
\theta_{2p^j}(x) &= \tfrac{1}{2p^{j+1}}(x^{p^n}+1)\{(p-1)\sum_{\substack{i=0\\ p^{n-j}|i}}^{p^n-1} x^i-\sum_{i\in C_{p^{n-j-1}}} x^i\}
\end{aligned}$$

for $0\le j\le n-1$.

6. Some Lower bounds on the minimum distance of irreducible cyclic codes.

Lemma 7:

- (i) For fixed j and k, $0 \leq j \leq n-1$, $0 \leq k \leq e-1$, the minimum distance of the minimal code $\mathcal{M}_{g^k p^j}$ is at least $2p^j$ and the minimum distance of the minimal code $\mathcal{M}_{2g^k p^j}$ is at least $4p^j$.
- (ii) For fixed ℓ and j, all the minimal codes $\mathcal{M}_{2^\ell g^k p^j}$, for $0 \leq k \leq e-1$, have the same minimum distance.
- (iii) The minimal cyclic code $\mathcal{M}_{2g^k p^j}$ of length $2p^n$ has twice the minimum distance to that of a minimal code $\mathcal{M}_{g^k p^j}$ of length p^n.

Proof (i) : Consider the code $\mathcal{C}_j = \bigoplus_{\ell=0}^{1} \bigoplus_{k=0}^{e-1} \mathcal{M}_{2^\ell g^k p^j}$, generated by

$$\frac{x^{2p^n}-1}{\prod_{\ell=0}^{1}\prod_{k=0}^{e-1} M^{(2^i g^k p^j)}(x)} = (x^{2p^{n-j-1}}-1)(1+x^{2p^{n-j}}+x^{4p^{n-j}}+\cdots+x^{2p^{n-j}(p^j-1)}).$$

Let $\mathcal{C}'_j$ be a code of length $2p^{n-j}$ generated by $g_j(x) = x^{2p^{n-j-1}} - 1$ with minimum distance 2. Then by Lemma 12 of [9], the code $\mathcal{C}_j$ is a repetition code of $\mathcal{C}'_j$ repeated p^j times and its minimum distance is $2p^j$. As $\mathcal{M}_{g^k p^j}$ is a subcode of $\mathcal{C}_j$, it has minimum distance at least $2p^j$.

Similarly $\mathcal{M}_{2g^k p^j}$ is a sub code of the code $\mathcal{D}_j = \bigoplus_{k=0}^{e-1} \mathcal{M}_{2g^k p^j}$, which is generated by

$$\frac{x^{2p^n}-1}{\prod_{k=0}^{e-1} M^{(2g^k p^j)}(x)} = (x^{p^{n-j-1}}-1)(1+x^{p^{n-j}}+x^{2p^{n-j}}+\cdots+x^{(p^j-1)p^{n-j}})(x^{p^n}+1).$$

Let $\mathcal{D}'_j$ be a cyclic code of length p^{n-j} generated by $g'_j(x) = x^{p^{n-j-1}} - 1$ and of minimum distance 2. Then by Lemma 12 of [9], the code $\mathcal{D}''_j$ of length p^n generated by $g''_j(x) = g'_j(x)(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \cdots + x^{(p^j-1)p^{n-j}})$ is a repetition code of $\mathcal{D}'_j$ repeated p^j times and its minimum distance is $2p^j$. Applying the same lemma again, the code $\mathcal{D}_j$ of length $2p^n$ generated by $g''_j(x)(1 + x^{p^n})$ is a repetition code of $\mathcal{D}''_j$ repeated twice and its minimum distance is $2(2p^j) = 4p^j$.

Therefore minimum distance of $\mathcal{M}_{2g^kp^j}$ is at least $4p^j$.

(ii): As the code $\mathcal{M}_{2\ell_{g^kp^j}}$ is transformed to $\mathcal{M}_{2\ell_{g^{k+1}p^j}}$ by the coordinate permutation $i \to ig^{-1}$, all the minimal codes $\mathcal{M}_{2\ell_{g^kp^j}}$, for $0 \leq k \leq e-1$, are equivalent and hence have the same minimum distance.

(iii): We have

$$\frac{x^{2p^n}-1}{M^{(2g^kp^j)}(x)} = (x^{p^n}+1)\frac{(x^{p^n}-1)}{M^{(2g^kp^j)}(x)}.$$

In the ring R_{p^n}, the minimal polynomial $M^{(g^kp^j)}(x)$ is same as the minimal polynomial $M^{(2g^kp^j)}(x)$ in ring R_{2p^n}. Therefore by Lemma 12 of [9], the minimal code $\mathcal{M}_{2g^kp^j}$ of length $2p^n$ has twice the minimum distance to that of the corresponding minimal code $\mathcal{M}_{g^kp^j}$ of length p^n.

Example :

Let $p = 13$, $q = 5$. Since $5^4 \equiv 1 (\text{mod } 13)$, but $\gcd(\frac{5^4-1}{13}, 13) = 1$, we have $e = 3$, $f = 4$. Here $g = 7$ is a primitive root mod 26. The 5-cyclotomic cosets mod 26 are

$$\begin{array}{llll} C_0 = \{0\}, & & C_{13} = \{13\}, & \\ C_1 = \{1,5,21,25\}, & & C_2 = \{2,10,16,24\}, & \\ C_7 = \{7,9,17,19\}, & & C_{2.7} = \{8,12,14,18\}, & \\ C_{7^2} = \{3,11,15,23\}, & & C_{2.7^2} = \{4,6,20,22\}. & \end{array}$$

The characteristic equation of matrix

$$A = \begin{bmatrix} -4 & -2 & -3 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

is given by

$$x^3 + x^2 + x + 1 = 0;$$

so that eigenvalues of A are 2,3,4. Also $(2,3,4)^T$ is an eigen vector corresponding to the eigenvalue 2. Therefore by Theorem 2, we can take $\eta_0 = 2$, $\eta_1 = 3$, $\eta_2 = 4$. Since the cyclotomic number A_{02} is odd, therefore $t = 2$. Thus the six 5-ary nontrivial primitive idempotents mod 26 are given by

$$
\begin{aligned}
\theta_1(x) &= (x^{13}-1)\{-x^{13}+3(x+x^5+x^{21}+x^{25})+4(x^7+x^9+x^{17}+x^{19}) \\
&\quad +2(x^3+x^{11}+x^{15}+x^{23})\}, \\
\theta_7(x) &= (x^{13}-1)\{-x^{13}+4(x+x^5+x^{21}+x^{25})+2(x^7+x^9+x^{17}+x^{19}) \\
&\quad +3(x^3+x^{11}+x^{15}+x^{23})\}, \\
\theta_{7^2}(x) &= (x^{13}-1)\{-x^{13}+2(x+x^5+x^{21}+x^{25})+3(x^7+x^9+x^{17}+x^{19}) \\
&\quad +4(x^3+x^{11}+x^{15}+x^{23})\}, \\
\theta_2(x) &= (x^{13}+1)\{-1+2(x+x^5+x^{21}+x^{25})+3(x^7+x^9+x^{17}+x^{19}) \\
&\quad +4(x^3+x^{11}+x^{15}+x^{23})\}, \\
\theta_{2.7}(x) &= (x^{13}+1)\{-1+3(x+x^5+x^{21}+x^{25})+4(x^7+x^9+x^{17}+x^{19}) \\
&\quad +2(x^3+x^{11}+x^{15}+x^{23})\}, \\
\theta_{2.7^2}(x) &= (x^{13}+1)\{-1+4(x+x^5+x^{21}+x^{25})+2(x^7+x^9+x^{17}+x^{19}) \\
&\quad +3(x^3+x^{11}+x^{15}+x^{23})\}.
\end{aligned}
$$

Each of the codes $\mathcal{M}_1$, $\mathcal{M}_7$, $\mathcal{M}_{7^2}$, $\mathcal{M}_2$, $\mathcal{M}_{2.7}$, $\mathcal{M}_{2.7^2}$, of length 26, has dimension 4 and minimum distance 16.

Acknowledgements

The authors are grateful to Prof. V.C.Dumir for many valuable discussions during the preparation of this paper.

References

1. S.K. Arora and M. Pruthi, Minimal cyclic codes of length $2p^n$, Finite Fields Appl.5 (1999), no.2, 177-187.

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

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

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

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

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

7. V. Pless, Cyclotomy and cyclic codes, Proceedings of Symposia in Applied Mathematics, Vol.46, (1992), 91-104.

8. M. Pruthi and S.K. Arora, Minimal codes of prime-power length, Finite Fields Appl.3(1997), no.2, 99-113.

9. 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(2004), no.4, 653-673.

10. T. Storer, Cyclotomy and Difference Sets, Markham Publishing Company, Chicago (1967).