Original Article

Minimum Distance Bounds for Some Cyclic Codes

Sheetal Chawla

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi - 110016
Email: chawlaasheetal@gmail.com

Abstract Generating polynomials, minimum distances and dimensions for the minimal cyclic codes of length $16p^n$ over the field $GF(q)$, where q is of the form $16k+1$, are obtained.

Keywords: Cyclotomiccosets, generating polynomials, minimum distances.

[*]**Address for Correspondence:**
Dr. Sheetal Chawla, Department of Mathematics, Indian Institute of Technology Delhi, New Delhi - 110016
Email: chawlaasheetal@gmail.com

Received Date: 20/09/2016 Revised Date: 18/10/2016 Accepted Date: 12/11/2016

Access this article online	
Quick Response Code:	Website: www.statperson.com
	DOI: 14 November 2016

INTRODUCTION

Let F be a finite field of prime power order q and G be a cyclic group of order m such that $g.c.d.(m,q)=1$. Then FG, the group algebra of the cyclic group G over F, is semi-simple and has only a finite number of primitive idempotents which equals the number of cyclotomiccosets modulo m. Let t be the multiplicative order of q modulo m, then $1 \le t \le \phi(m)$ [3]. If $t=\phi(m)$ and $m=2,4,p^n,2p^n$, the minimal cyclic codes were calculated by Pruthi and Arora [1, 6]. The minimal cyclic codes of length p^nq were discussed by Bakshi and Raka[2].Minimal cyclic codes of length $4p^n$ were obtained by Chawla and Singh[4] and those of length $8p^n$ were discussed by Singh and Arora[7].

The q-cyclotomiccosetsmodulo $16p^n$,where $p^n \equiv 1(\mathrm{mod}\,8)$ and q is of the form $16k+9$,are obtained in Section 2. In Section 3, we obtained the primitive idempotentsin FC_{16p^n} (Theorem 3.19).

CYCLOTOMIC COSETS

Let $S=\{1,2,\dots,16p^n\}$. For $a,b \in S$, say that a □ b iff $a \equiv bq^i(\mathrm{mod}\,16p^n)$ for some integer $i \ge 0$. This is an equivalence relation on set S. The equivalence classes due to this relation are called q-cyclotomiccosets modulo $16p^n$. The q-cyclotomiccosetcontaining $s \in S$ is $\Omega_s=\{s,sq,sq^2,\dots,sq^{t_s-1}\}$, where t_s is the smallest positive integer such that $sq^{t_s} \equiv s(\mathrm{mod}\,16p^n)$.

How to site this article: Sheetal Chawla. Minimum Distance Bounds for Some Cyclic Codes. *International Journal of Statistika and Mathemtika*. November to January 2016; 21(1): 01-06. http://www.statperson.com (accessed 16 November 2016).

Lemma 2.1. If $\phi(p^n)$ is the order of q modulo p^n then order of q modulo p^{n-i} is $\phi(p^{n-i})$, for all i, $0 \le i \le n-1$.
Proof is trivial.

Lemma 2.2. If q is an odd prime of the form $16k+1$ and $\phi(p^n)$ is the order of q modulo p^n, then for $0 \le i \le n-1$, the order of q modulo $2p^{n-i}$, $4p^{n-i}$, $8p^{n-i}$ and $16p^{n-i}$ is $\phi(p^{n-i})$.

Proof. Since $\phi(p^n)$ is the order of q modulo p^n, therefore, by lemma 2.1, order of q modulo p^{n-i} is $\phi(p^{n-i})$, $0 \le i \le n-1$. Hence $q^{\phi(p^{n-i})} \equiv 1 \pmod{p^{n-i}}$. Since $\phi(p^{n-i})$ is even, therefore, $\varphi(p^{n-i}) = 2t$ for some integer t and $q^{\phi(p^{n-i})} \equiv 1 \pmod{2}$. Also, $g.c.d.(2, p^{n-i}) = 1$, therefore, $q^{\phi(p^{n-i})} \equiv 1 \pmod{2p^{n-i}}$. As order of q modulo p^{n-i} is $\phi(p^{n-i})$, therefore, $\phi(p^{n-i})$ is the smallest integer for which $q^{\phi(p^{n-i})} \equiv 1 \pmod{p^{n-i}}$ holds. Hence the order of q modulo $2p^{n-i}$ is $\phi(p^{n-i})$. Similarly, the result holds for $4p^{n-i}$, $8p^{n-i}$ and $16p^{n-i}$.

Lemma 2.3. For $0 \le i \le n-1$ and $0 \le k \le \phi(p^{n-i})-1$, $2^r\left(1+2sp^n\right) \not\equiv q^k \pmod{16p^{n-i}}$,for $0 \le r \le 2$ and $1 \le s \le 7$ .Equivalently, $p^i(1+2sp^n) \not\equiv p^i q^k \pmod{16p^n}$.
Proof can be obtained using lemma 2.1 - 2.2.

Theorem 2.4. The q-cyclotomiccosets modulo $16p^n$ are

$$\Omega_{lp^n} = \left\{lp^n\right\} \text{ for } 0 \le l \le 15;$$

and $\Omega_{tp^j} = \{tp^j, tp^j q, ..., tp^j q^{\phi(p^{n-j})-1}\}$,for $0 \le j \le n-1$,

$t = 1, 2, 4, 8, \lambda = 1+2p^n, 2\lambda, 4\lambda, \mu = 1+4p^n, 2\mu, \nu = 1+6p^n, 2\nu, \chi = 1+8p^n, \psi = 1+10p^n,$
$\xi = 1+12p^n, \tau = 1+14p^n.$

Proof. $\Omega_0 = \left\{0\right\}$ is trivial.

Since $q \equiv 1\left(\bmod 16\right)$, therefore, $lp^n q \equiv lp^n \left(\bmod 8p^n\right)$. Hence $\Omega_{lp^n} = \left\{lp^n\right\}$.

By lemma 2.2, $q^{\phi(p^{n-i})} \equiv 1\left(\bmod 16p^{n-i}\right)$, equivalently, $p^i q^{\phi(p^{n-i})} \equiv p^i \left(\bmod 16p^n\right)$.

Therefore, $\Omega_{p^i} = \{p^i, p^i q, ..., p^i q^{\phi(p^{n-i})-1}\}$.

Similarly, $\Omega_{tp^i} = \{tp^i, tp^i q, ..., tp^i q^{\phi(p^{n-i})-1}\}$.

Obviously, $|\Omega_{lp^n}| = 1$ and $|\Omega_{tp^i}| = \phi(p^{n-i})$ for $0 \le j \le n-1$.

Therefore, $\sum_{i=0}^{n-1}\left|\Omega_{p^i}\right| = \sum_{i=0}^{n-1}\phi(p^{n-i}) = \varphi(p^n) + \varphi(p^{n-1}) + \varphi(p^{n-2}) + ... + \varphi(p) = p^n - 1$.

$$\sum_{i=0}^{15}|\Omega_{tp^n}| + \sum_{i=0}^{n-1}\left\{\sum_{t=1,2,4,8,16,\lambda,2\lambda,4\lambda,\mu,2\mu,\nu,2\nu,\chi,\psi,\xi,\tau}|\Omega_{tp^i}|\right\} = 8p^n.$$

Thus, it follows that these are the only distinct q-cyclotomiccosetsmodulo $16p^n$.

GENERATING POLYNOMIALS

If α is a primitive $16p^n$ th root of unity, then $m_s(x)=\prod_{s\in\Omega_s}\left(x-\alpha^s\right)$ denotes the minimal polynomial for α^s, $s\in\Omega_s$, and so the generating polynomial for cyclic code of length $16p^n$ corresponding to the cyclotomiccoset Ω_s is $\frac{x^{16p^n}-1}{m_s(x)}$. The dimension of minimal cyclic code M_s is equal to the cardinality of the class Ω_s. Thus, the dimensions of the codes M_{lp^n} and $\mathrm{M}_{\mathrm{tp}^j}$ are $1$and$\phi\left(p^{n-j}\right)$ respectively.**.**Let m be the smallest integer such that $p^m\equiv 1(\bmod n)$, then GF(p^{m}) is the smallest field containing all the nth roots of unity. [5]

3.1 Theorem. The generating polynomials for the codes M_0, M_{p^n}, $\mathrm{M}_{2\mathrm{p}^n}$, M_{3p^n}, M_{4p^n}, M_{5p^n}, M_{6p^n}, M_{7p^n}, M_{8p^n}, M_{9p^n}, M_{10p^n}, M_{11p^n}, M_{12p^n}, M_{13p^n}, M_{14p^n} and M_{15p^n} are $\left(1+x+x^2+\ldots+x^{16p^n-1}\right)$,

$$(x^8-1)(x^4+\beta_1)(x^2+\beta)\left(x+\delta\right)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$$(x^{12}-x^8+x^4-1)(x^2+\beta_1)(x+\beta)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$$\left(x+\delta_1\right)\left(x^2+\beta_2\right)\left(x^4-\beta_1\right)\left(x^8-1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right),$$

$$(x^{14}-x^{12}+x^{10}-x^8+x^6-x^4+x^2-1)\left(x+\beta_1\right)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$$\left(x^8-1\right)\left(x+\delta_2\right)\left(x^2-\beta\right)\left(x^4+\beta_1\right)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$$\left(x+\beta_2\right)\left(x^2-\beta_1\right)\left(x^4-1\right)\left(x^8+1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right),$$

$$\left(x^8-1\right)\left(x+\delta_3\right)\left(x^2-\beta_2\right)\left(x^4-1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right),$$

$$(x^{15}-x^{14}+x^{13}-x^{12}+x^{11}-x^{10}+x^9-x^8+x^7-x^6+x^5-x^4+x^3-x^2+x-1)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$$\frac{\left(x^{16}-1\right)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right)}{\left(x+\delta\right)},\frac{\left(x^{16}\ -1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right)}{\left(x+\beta\right)},$$

$$\left(x-\delta_1\right)\left(x^2+\beta_2\right)\left(x^4-\beta_1\right)\left(x^8-1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right),\ \frac{\left(x^{16}-1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right)}{\left(x+\beta_1\right)},$$

$$\left(x^8-1\right)\left(x-\delta_2\right)\left(x^2-\beta\right)\left(x^4+\beta_1\right)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right),$$

$\left(x-\beta_2\right)\left(x^2-\beta_1\right)\left(x^4-1\right)\left(x^8+1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right)$ and

$\left(x^8-1\right)\left(x-\delta_3\right)\left(x^2-\beta_2\right)\left(x^4-1\right)\left(1+x^{16}+\ldots+x^{16(p^n-1)}\right)$ respectively, where $\alpha^{p^n}=\delta$, $\alpha^{2p^n}=\beta,\alpha^{3p^n}=\delta_1,\alpha^{4p^n}=\beta_1,\alpha^{5p^n}=\delta_2,\alpha^{6p^n}=\beta_2,\alpha^{7p^n}=\delta_3$.

Proof. The minimal polynomial for α^{lp^n} is $x-\alpha^{lp^n}$ and so the corresponding generating polynomialis $\dfrac{x^{16p^n}-1}{x-\alpha^{lp^n}}$, for $0\le l\le 15$.

3.2 Theorem. The generating polynomial for M_{8p^j} and M_{16p^j} are

$\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$ and

$\left(x^{p^{n-j-1}}-1\right)\left(x^{p^{n-j}}+1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$respectively.

Proof. The minimal polynomial for α^{8p^j} and α^{16p^j} are $\dfrac{x^{p^{n-j}}+1}{x^{p^{n-j-1}}+1}$ and $\dfrac{x^{p^{n-j}}-1}{x^{p^{n-j-1}}-1}$respectively. Using these we can obtain the required generating polynomials for M_{8p^j} and M_{16p^j}.

3.3 Theorem. The generating polynomial for $M_{p^j}\oplus M_{2p^j}\oplus M_{4p^j}\oplus M_{\lambda p^j}\oplus M_{\mu p^j}\oplus M_{\nu p^j}\oplus M_{\chi p^j}\oplus M_{\psi p^j}\oplus M_{\xi p^j}\oplus M_{\tau p^j}$ is

$\left(x^{2p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{8p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$.

Proof. The product of minimal polynomial satisfied by $\alpha^{p^j},\alpha^{2p^j},\alpha^{4p^j},\alpha^{\lambda p^j},\alpha^{\mu p^j},\alpha^{\nu p^j},\alpha^{\chi p^j},\alpha^{\psi p^j},\alpha^{\xi p^j},\alpha^{\tau p^j}$ is $\dfrac{\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)}{\left(x^{2p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{8p^{n-j-1}}+1\right)}$.Therefore, thecorresponding generating polynomial for $M_{p^j}\oplus M_{2p^j}\oplus M_{4p^j}\oplus M_{\lambda p^j}\oplus M_{\mu p^j}\oplus M_{\nu p^j}\oplus M_{\chi p^j}\oplus M_{\psi p^j}\oplus M_{\xi p^j}\oplus M_{\tau p^j}$ is

$\left(x^{2p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{8p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$.

MINIMUM DISTANCE

If l is a cyclic code of length m generated by $g\left(x\right)$ and its minimum distance is d, then the code $\widehat{l}$ of length mk generated by $g(x)\left(1+x^m+x^{2m}+\ldots+x^{(k-1)m}\right)$ is a repetition code of l repeated k times and its minimum distance is dk .[2]

4.1 Theorem. Each of the codes M_{lp^n}, $0\le l\le 15$, are of minimum distance $16p^n$.

Proof. Since the generating polynomial for the code M_0 is $\left(1+x+\ldots+x^{16p^n-1}\right)$, which is itself a polynomial of length $16p^n$, hence its minimum distance is $16p^n$.

Also, the generating polynomial for the cyclic code M_{p^n} is $(x^8-1)(x^4+\beta_1)\left(x^2+\beta\right)(x+\delta)\left(1+x^{16}+\ldots+x^{16\left(p^n-1\right)}\right)$. If we take a cyclic code of length 16 generated by the polynomial $(x^8-1)(x^4+\beta_1)\left(x^2+\beta\right)(x+\delta)$, then the minimum distance of this code is 16. Since the cyclic code of length $16p^n$ with generating polynomial $(x^8-1)(x^4+\beta_1)\left(x^2+\beta\right)(x+\delta)\left(1+x^{16}+...+x^{16\left(p^n-1\right)}\right)$, is a repetition of the cyclic code of length 16 with generating polynomial $(x^8-1)(x^4+\beta_1)\left(x^2+\beta\right)(x+\delta)$, repeated p^n times, thereforeits minimum distance is $16p^n$.

Expressionsfor M_{lp^n}, $2\le l\le 15$ can be obtained similarly.

4.2 Theorem. For $0\le j\le n-1,$ the minimum distance for the codes $M_{p^j}, M_{2p^j}, M_{4p^j}, M_{\lambda p^j}, M_{\mu p^j}, M_{\nu p^j}, M_{\chi p^j}, M_{\psi p^j}, M_{\xi p^j}$ and $M_{\tau p^j}$ are greater than or equal to $16p^j$.

Proof. Since the product of generating polynomial for the cyclic codes $M_{p^j}, M_{2p^j}, M_{4p^j}, M_{\lambda p^j}, M_{\mu p^j}, M_{\nu p^j}, M_{\chi p^j}, M_{\psi p^j}, M_{\xi p^j}$ and $M_{\tau p^j}$ is

$$\left(x^{8p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{2p^{n-j-1}}+1\right)\left(x^{p^{n-j}}+1\right)\left(x^{p^{n-j}}-1\right)\left(1+x^{16p^{n-j}}+...+x^{16p^{n-j}\left(p^j-1\right)}\right),$$

therefore, if we take a code l oflength$16p^{n-j}$ generated by the polynomial $\left(x^{8p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{2p^{n-j-1}}+1\right)\left(x^{p^{n-j}}+1\right)\left(x^{p^{n-j}}-1\right)$, then the minimum distance of this code is 16. Since the cyclic code $\widehat{l}$ of length $16p^n$ generated by the polynomial $\left(x^{8p^{n-j-1}}+1\right)\left(x^{4p^{n-j-1}}+1\right)\left(x^{2p^{n-j-1}}+1\right)\left(x^{p^{n-j}}+1\right)\left(x^{p^{n-j}}-1\right)\left(1+x^{16p^{n-j}}+...+x^{16p^{n-j}\left(p^j-1\right)}\right)$ is a repetition codes of the code l, repeated p^j times. Hence its minimum distance is $16p^j$.

Since, the codes corresponding to

$$\Omega_{p^j}, \Omega_{2p^j}, \Omega_{4p^j}, \Omega_{\lambda p^j}, \Omega_{\mu p^j}, \Omega_{\nu p^j}, \Omega_{\chi p^j}, \Omega_{\psi p^j}, \Omega_{\xi p^j} \text{ and } \Omega_{\chi p^j}$$

are the sub codes of above code so their minimum distance is greater than or equal to $16p^j$.

4.3 Theorem. For $0 \le j \le n-1$, the minimum distance of the cyclic codes M_{8p^j} and M_{16p^j} are $32p^j$

Proof. Consider the cyclic code M_{8p^j}. Since the generating polynomial of the cyclic code of length $16p^j$ is

$$\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+...+x^{16p^{n-j}\left(p^j-1\right)}\right),$$

therefore, if we take a cyclic code C of length p^{n-j} generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)$, then the minimum distance of this code is 2. Now consider the cyclic code C^1 of length $2p^{n-j}$ generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)$, and then the minimum distance of this code is 4, as it is 2 time repetition of the code C. Further, the minimum distance of the code C^2 of length $4p^{n-j}$ generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)$, and then the minimum distance of this code is 8, as it is 2 time repetition of the code C^1. Further, the minimum distance of the code C^3 of length $8p^{n-j}$ generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)$ is 16, as it is 2 time repetition of the code C^2.Hence, the minimum distance of the code C^4 of length $16p^{n-j}$ generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)$ is 32, as it is 2 time repetition of the code C^3.Since, the cyclic code of length $16p^n$ generated by the polynomial $\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$ is a repetition code of the cyclic code C^4, repeated p^j times, therefore, its minimum distance is $32p^j$.

Similarly, the minimum distance of the cyclic code M_{16p^j} of length $16p^n$ with generating polynomial

$$\left(x^{p^{n-j-1}}+1\right)\left(x^{p^{n-j}}-1\right)\left(x^{2p^{n-j}}+1\right)\left(x^{4p^{n-j}}+1\right)\left(x^{8p^{n-j}}+1\right)\left(1+x^{16p^{n-j}}+\ldots+x^{16p^{n-j}\left(p^j-1\right)}\right)$$

is also $32p^j$.

REFERENCES

1. Arora, S.K.,Pruthi, M.: Minimal Cyclic Codes of Length 2p^n, Finite Fields Appl.,(1999), 5, 177-187.
2. Bakshi, G.K.,Raka, M.: Minimal Cyclic Codes of Length p^{n}q, Finite Fields Appl.,(2003), 9, 432-448.
3. Berman, S.D.: Semisimple Cyclic and Abelian Codes, II, Cybernatics,(1967), 3, 17-23.
4. Chawla, S., Singh, J.: Cyclic Codes of Length $4p^n$ over $GF(q)$, where q is prime power of the form $4k+1$, ABJMI, (2014), 6(2), 373-380.
5. Pless, V.: Introduction of the Theory of Error Correcting Codes, Wiley, New York (1981)
6. Pruthi, M., Arora, S.K.: Minimal Codes of Prime-Power Length, Finite Fields Appl., (1997), 3, 99-113.
7. Singh, J., Arora, S.K., Minimal Cyclic Codes of Length $8p^n$ over $GF(q)$, where q is prime power of the form $8k+5$,J. Appl. Math. Comp., (2015), 48 (1-2), 55-69.

Source of Support: None Declared
Conflict of Interest: None Declared