International Journal of Mathematics Trends and Technology
ISSN: 2231-5373 / https://doi.org/10.14445/22315373/IJMTT-V68I5P507

Volume 68 Issue 5, 40-43, May 2022
©2022 Seventh Sense Research Group®

Original Article

Generating, Minimal Polynomial and Minimum Distance of Quadratic Residue Codes (QR-Codes) of Length $4p^n$

Ranbir Singh[1], Manoj Kumar[2], Vinod Bhatia[3]

[1,2,3] *Deptt. of Mathematics, Baba Mast Nath University, Rohtak*

Received: 16 March 2022 Revised: 11 May 2022 Accepted: 17 May 2022 Published: 07 June 2022

Abstract - *Generating, Minimal polynomial and Minimum distance of all 3(2n+1) quadratic residue codes(QR-Codes) of length* $4p^n$ *over GF(l), where* p, l *are distinct odd primes,* $o(l)_{p^n} = \frac{\varphi(p^n)}{2}, o(l)_4 = \varphi(4)$, $gcd(\varphi(p^n), \varphi(4)) = 2$, *p does not divide* 3 , *are obtained.*

Keywords - *Generating polynomials, Minimal polynomial and Minimum distance.*

MSC(2010): *11A03;15A07;11R09;11T06;11T22;11T71;94B05;94B15*

1. Introduction

Let $F = GF(l)$ be a field of odd prime order l and k ≥ 1 be an integer such that $\gcd(l, k) = 1$. Let $o(l)_k$ denotes the order of l modulo k. Many authors have obtained the complete set of primitive idempotents of the minimal cyclic codes of various lengths. Sahni and Sehgal [1] described the minimal cyclic codes of length $p^n q$, p, q are distinct odd primes and $o(l)_{p^n} = \varphi(p^n)$, $o(l)_q = \varphi(q)$, $gcd(\varphi(p^n), \varphi(q))$ = d, p does not divide $q - 1$.

In this paper, we extend the results of Rani S. Singh I.J and Kumar P. [13]. We consider the case when $k = 4p^n$, where p, l are distinct odd primes, $o(l)_{2p^n} = \varphi(2p^n)/d = \varphi(p^n)$, $o(l)_4 = \varphi(4)$, $gcd(\varphi(2p^n), \varphi(4))$ = d, p does not divide 3. In Section 2 (Lemmas 2.1 – 2.4 and Theorem 2.5), we obtain the generating polynomials, minimal polynomial and minimum distance of all 3(2n+1) quadratic residue codes (QR-Codes) of length $4p^n$.

2. Dimension, generating polynomial and minimum distance of minimal cyclic codes of length $4p^n$

The dimension of minimal cyclic code Ω_s is the number of non-zeros of the generating idempotent θ_s; which is the cardinality of the cyclotomic coset C_s that is dim (Ω_s) = | C_s |. We denote the minimum distance of Ω_s by d (Ω_s).

2.1 Theorem Let p, l be distinct odd primes and n, $d \geq 1$ be integers. If $o(l)_{p^{n-j}} = \varphi(p^{n-j})/2$ and $o(l)_4 = \varphi(4)$ with $gcd\left(\varphi(p^{n-j}), \varphi(4)\right) = 2$ and p does not divide 3,, then for the integer $n \geq 1$, there are $3(2n + 1)$ cyclotomic cosets (mod $4p^n$) given by

(i) $C_0 = \{0\}$,

(ii) $C_{p^n} = \{p^n, p^n l\}$,

(iii) $C_{2p^n} = \{2p^n\}$

For $0 \leq j \leq n - 1, 0 \leq k \leq 1$,

(iv) $C_{g^k p^j} = \{g^k p^j,\ g^k p^j l,\ g^k p^j l^2,\ . . ., g^k p^j l^{\varphi(4p^{n-j})/2-1}\}$,

(v) $C_{2g^k p^j} = \{2g^k p^j,\ 2g^k p^j l,\ 2g^k p^j l^2,\ . . ., 2g^k p^j l^{\varphi(2p^{n-j})/2-1}\}$,

(vi) $C_{4g^k p^j} = \{4g^k p^j,\ 4g^k p^j l,\ 4g^k p^j l^2,\ . . ., 4g^k p^j l^{\varphi(p^{n-j})/2-1}\}$

where g is fixed integer

2.2. Lemma If C is the cyclic code of length m generated by g(x) and is of minimum distance d, then the code Ĉ is of length mk generated by $g(x)(1 + x^m + x^{2m} + \ldots + x^{(k-1)m})$ is a repetition code of C repeated k times and minimum distance is kd.

Proof. Trivial.

2.3. Theorem (i) Ω_0 and Ω_{2p^n} are equivalent codes, each of length $4p^n$, dimension 1 and minimum distance $4p^n$.

(ii) Ω_{p^n} and Ω_{3p^n} are equivalent codes, each of length $4p^n$, dimension $\varphi(4)$ and minimum distance $4p^n$.

(iii) Ω_{2p^j} and Ω_{2gp^j}, for $0 \le j \le n-1$ are equivalent codes, each of length $4p^n$, dimension $4p^n$ and minimum distance $8p^j$.

Proof (i) Clearly, the minimal polynomial of $\alpha^0 = 1$ is x - 1, therefore the generating polynomial of Ω_0 is $\frac{x^{4p^n}-1}{x-1} = 1 + x + x^2 + \ldots + x^{4p^n-1}$ and the minimal polynomial of α^{2p^n} is x + 1. Therefore, the generating polynomial of Ω_{2p^n} is $\frac{x^{4p^n}-1}{x+1} = x^{4p^n-1} - x^{4p^n-2} + \ldots - x + 1$. These obviously imply that Ω_0 and Ω_{2p^n} are equivalent codes, each of length $4p^n$, dimension 1 and minimum distance $4p^n$.

(ii) The minimal polynomial of α^{p^n} and α^{3p^n} are

$M^{(p^n)}(x) = x^2 + 1$

and

$M^{(3p^n)}(x) = 1 + x^2$ respectively.

Therefore, $\frac{x^{4p^n}-1}{M^{(p^n)}(x)} = (x^2 - 1)(1 + x^4 + x^8 + \ldots + x^{4(p^n-1)})$

and

$\frac{x^{4p^n}-1}{M^{(3p^n)}(x)} = (x^2 - 1)(1 + x^4 + x^8 + \ldots + x^{4(p^n-1)})$

are generating polynomials of the minimal cyclic codes Ω_{p^n} and Ω_{3p^n}. This implies that Ω_{p^n} and Ω_{3p^n} are equivalent codes. Trivially, the dimension of each code is 2.

The minimal cyclic code Ω_{p^n} is p^n times repetition of a code generated by $(x^2 - 1)$ and of minimum distance 2. Therefore, by Lemma 2.2, the minimum distance of Ω_{p^n} is $2p^n$.

Analogously, the minimal cyclic code Ω_{3p^n} is p^n times repetition of a code generated by same generating polynomial $(x^2 - 1)$ and of minimum distance 2. Therefore, again by Lemma 2.2, the minimum distance of Ω_{3p^n} is $2p^n$.

(iii) For $0 \le i \le n-1$, the minimal polynomial of $\alpha^{2p^j}, \alpha^{2gp^j}$ over GF (*l*) is

$M^{(2p^j)}(x) M^{(2gp^j)}(x) = 1 - x^{p^{n-j-1}} + x^{2p^{n-j-1}} - \ldots + x^{(p-1)p^{n-j-1}}$.

Also,

$x^{4p^n} - 1 = (x^{2p^{n-j}} - 1)(1 + x^{2p^{n-j}} + x^{4p^{n-j}} + \ldots + x^{(2p^j-1)2p^{n-j}})$

$= (x^{p^{n-j}} - 1)(x^{p^{n-j-1}} + 1)(1 - x^{p^{n-j-1}} + x^{2p^{n-j-1}} - \ldots + x^{(p-1)p^{n-j-1}})$

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

Thus, generating polynomial of cyclic code Ω_{2p^j} is

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

Similarly, the minimal polynomial of α^{4p^j} over GF (*l*) is

$M^{(4p^j)}(x) M^{(4gp^j)}(x) = 1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}}$.

Also, $x^{4p^n} - 1 = (x^{p^{n-j}} - 1)(1 + x^{p^{n-j}} + x^{2p^{n-j}} + \ldots + x^{(4p^j-1)p^{n-j}})$

$= (x^{p^{n-j-1}} - 1)(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}})$

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

Thus, generating polynomial of cyclic code Ω_{4p^j} is

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

This obviously implies that Ω_{2p^j} and Ω_{4p^j} are equivalent codes, each of length $4p^n$ and dimension $4p^n$. By Lemma 2.2, minimum distance of each is $8p^j$.

2.4. Lemma Let χ_j be the code of length $2p^{n-j}$ over GF(l) generated by $g(x) = (x^{2p^{n-j-1}} - 1)(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}})$. Then the minimum distance of χ_j is 4.

Proof. Trivial.

2.5. Lemma Let $\tilde{\chi}_j$ be the code of length $4p^{n-j}$ over GF(l) generated by

$g(x) = (x^{2p^{n-j}} + 1)(x^{2p^{n-j-1}} - 1)(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}})$. Then the minimum distance of $\tilde{\chi}_j$ is 8.

Proof. It is easy to see that $\tilde{\chi}_j$ is repetition code of χ_j repeated twice as defined in Lemma 2.4, which is a cyclic code of length $2p^{n-j}$ and minimum distance 4. Then by Lemma 2.2, $\tilde{\chi}_j$ is the cyclic code of length $4p^{n-j}$ and minimum distance 8.

We shall further discuss some results for finding out the minimum distance of the minimal cyclic codes $\Omega_{2g^k p^j}$, for $0 \le j \le n-1$ and $0 \le k \le 1$.

2.6. Theorem For each j, $0 \le j \le n-1$ and $0 \le k \le 1$

(i) $\Omega_{2g^k p^j}$ are equivalent codes.

(ii) The minimum distance of $\Omega_{2g^k p^j}$ is at least $8p^j$.

Proof. (i) Trivial..

(ii) Let $0 \le j \le n-1$ and $0 \le k \le 1$.

We observe that, $M^{(2p^l)}(x)M^{(2gp^l)}(x) = (1 + x^{2p^{n-j-1}} + x^{4p^{n-j-1}} + \ldots + x^{(p-1)2p^{n-j-1}})$.

Also, $x^{4p^n} - 1 = (x^{4p^{n-j}} - 1)(1 + x^{4p^{n-j}} + x^{8p^{n-j}} + \ldots + x^{(p^j-1)4p^{n-j}})$

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

$= (x^{2p^{n-j}} + 1)(x^{2p^{n-j-1}} - 1)(1 + x^{2p^{n-j-1}} + x^{4p^{n-j-1}} + \ldots + x^{(p-1)2p^{n-j-1}})$

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

Therefore, we have

$$\frac{x^{4p^n}-1}{\prod_{k=0}^{1} M^{(2g^k p^j)}(x)} = (x^{2p^{n-j}} + 1)(x^{2p^{n-j-1}} - 1)(1 + x^{p^{n-j-1}} + x^{2p^{n-j-1}} + \ldots + x^{(p-1)p^{n-j-1}})$$

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

Let χ_j^* be the cyclic code of length $4p^n$, generated by $\frac{x^{4p^n}-1}{\prod_{k=0}^{1} M^{(2g^k p^j)}(x)}$.

Then, by Lemma 2.2, χ_j^* is a repetition code of $\tilde{\chi}_j$ repeated p^j times and its minimum distance is $8p^j$. Further, $\chi_j^* = \oplus_{k=0}^{1} \Omega_{2g^k p^j}$, thus $\Omega_{2g^k p^j}$ is sub code of χ_j^* .Therefore, the minimum distance of $\Omega_{2g^k p^j}$ is at least $8p^j$.

Theorem 2.7 For each j, $0 \le j \le n-1$ and $0 \le k \le 1$

(i) $\Omega_{g^k p^j}$ are equivalent codes.

(ii) The minimum distance of each $\Omega_{g^k p^j}$ is at least $8p^j$.

Proof. The proof follows on the similar lines as Theorem 2.6.

3. Conclusion

We have discussed three parameters viz generating polynomial, minimal polynomial and minimum distance of quadratic residue codes (QR-Codes) of length $4p^n$. These parameters are useful to detect and correct the transmission errors.

References

[1] S.K. Arora and Manju Pruthi, Minimal Cyclic Codes Length $2p^n$, Finite Field and Their Applications, 5 (1999) 177-187.
[2] Gurmeet K. Bakshi and Madhu Raka, Minimal Cyclic Codes of Length $P^n q$, Finite Fields Appl. 9(4) (2003) 432-448.
[3] Sudhir Batra and S.K. Arora, Minimal Quadratic Residue Cyclic Codes of Length P^n (P Odd Prime), Korean J. Comput & Appl. Math. 8(3) (2001) 531-547.
[4] Sudhir Batra and S.K. Arora, Some Cyclic Codes of Length $2p^n$ (P Odd Prime), Design Codes Cryptography , 57(3) (2010).
[5] F.J. Mac Williams & N.J.A. Sloane ; the Theory of Error Correcting Codes Bell Laboratories Murray Hill Nj 07974 U.S.A.
[6] Manju Pruthi and S.K. Arora, Minimal Cyclic Codes of Prime Power Length, Finite Field and Their Application, 3 (1997) 99-113.
[7] Raka, M., Bakshi ,G.K.; Sharma,A.,Dumir,V.C. Cyclotomic Numbers and Primitive Idempotents In the Ring $\frac{GF(q)[x]}{(x^{p^n}-1)}$, Finite Field & Their Appl.3, 2 (2004) 653-673.
[8] Ferraz,R.A.,Millies,C.P., Idempotents In Group Algebras and Minimal Abelian Codes, Finite Fields and Their Appl,13(2) (2007) 982-993
[9] A.Sahni and P.T.Sehgal,Minimal Cyclic Codes of Length $P^n q$, Finite Fields Appl. 18 (2012) 1017-1036.
[10] Ranjeet Singh and Manju Pruthi, Primitive Idempotents of Quadratic Residue Codes of Length $P^n Q^m$, Int.J.Algebra, 5(2011) 285-294.
[11] S. Batra and S.K. Arora,Minimal Quadratic Residue Cyclic Codes of Length P^n(P Odd Prime),Korean J. Comput and Appl. Math, 8(3)(2001) 531- 547.
[12] S.Rani, I.J.Singh and S.K. Arora, Minimal Cyclic Codes of Length 2 $P^n q$ (P Odd Prime), Bull.Calcutta.Math Society ,106(4) (2014)281-296.
[13] S. Rani, P,Kumar and I.J.Singh, Minimal Cyclic Codes of Length 2 P^n,Int. J.Algebra 7, 1- 4 (2013) 79 - 90.
[14] S. Rani, P,Kumar and I.J.Singh, Quadratic Residues Codes of Prime Power Length Over Z4,J.Indian Math.Soc.New Series ,78(1-4) (2011) 155 -161.
[15] S. Rani, I.J.Singh and S.K.Arora,Primitive Idempotents of Irre-Ducible Cyclic Code sof Length $P^n q^m$,Far East Journal of Math. Sciences, 77(1) (2013) 17 - 32.
[16] R. Singh, V. Kumar and I.J. Singh,`` Generalized Cyclotomic Cosets Modulo $4p^n$ Aryabhatta J.of Maths & Info. 10(1) (2020) 93-96.
[17] Vanlint, J.H. Generalised Quadratic Residue Macwilliams, F.J. Codes, Ieee Trans. Infor. Theory, 24(6) (1978) 730- 737.
[18] Vanlint, J.H. Introduction to Coding Theory, Springer- Verlag, (1999).
[19] Vanlint, J.H. on the Minimum Distance of Wilson, Richard M. Cyclic Codes Ieee Trans. Infor. Theory, 32(1) (1986) 23-40.
[20] Vermani, L.R. Elements of Algebraic Coding Theory, Chapman & Hall.
[21] Ward, H.N. Quadratic Residue Codes and Symplectic Group, Journal of Algebra 29,150-171 (1974) 168- 173.
[22] Mc Coy, N.H. the Theory of Numbers, the Mcmillan Company, New York, (1971).
[23] Niven, I., Zuckerman, H.S. an Introduction To the Theory of Numbers, John Wiley & Sons, Inc, New York, (1960).
[24] Huffman, D.G. Coding Theory, Marcel Dekker, Inc. New York, (1991).
[25] Jenson, R.A. Information Sets As Permutation Cycles for Quadratic Residue Codes, Internat.J. Math. Sci, 5 (1982).