Korean J. Math. **20** (2012), No. 4, pp. 525–532
http://dx.doi.org/10.11568/kjm.2012.20.4.525

LIFTS OF THE TERNARY QUADRATIC RESIDUE CODE OF LENGTH 24 AND THEIR WEIGHT ENUMERATORS

Young Ho Park

Abstract. We study the extended quadratic residue code of length 24 over $\mathbb{Z}_3$ and its lifts to rings $\mathbb{Z}_{3^e}$ for all e including 3-adic integers ring. We completely determine the weight enumerators of all these lifts.

1. Introduction

Let R be a ring. A *linear code* of length n over R is a R-submodule of R^n. We define an inner product on R^n by $(x,y) = \sum_{i=1}^n x_i y_i$ where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. The *dual code* $C^\perp$ of a code C of length n is defined to be $C^\perp = \{y \in R^n \mid (y,x) = 0 \text{ for all } x \in C\}$. C is *self-dual* if $C = C^\perp$.

For $v \in R^n$, the weight $wt(v)$ of v is defined to be the number of nonzero components of v. The minimum distance of a code C is the minimum of $wt(v)$ for nonzero $v \in C$. For generality on codes over fields, we refer [5] and [8]. For codes over $\mathbb{Z}_m$, see [12], and for self dual codes, see [11].

Now we define the quadratic residue codes over $\mathbb{Z}_3$ [8]. Let

$$Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

Received November 10, 2012. Revised December 7, 2012. Accepted December 10, 2012.

2010 Mathematics Subject Classification: 94B05, 11T71.

Key words and phrases: quadratic residue code, code over rings, self-dual code, p-adic code, weight enumertaor.

© The Kangwon-Kyungki Mathematical Society, 2012.

This is an Open Access article distributed under the terms of the Creative commons Attribution Non-Concercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

be the set of nonzero quadratic residues modulo 23, N the set of quadratic nonresidues modulo 23. Note that 3 is a quadratic residue modulo 23. Since $3 \nmid 23$, there exists a 23^{rd} primitive root ζ of 1 over $\mathbb{Z}_3$. Let

$$Q(x) = \prod_{i \in Q}(x - \zeta^i), \quad N(x) = \prod_{i \in N}(x - \zeta^i).$$

The order of 3 modulo 23 is 11. Hence the cyclotomic cosets modulo 23 over $\mathbb{Z}_3$ are given by $\{0\}, Q, N$. Therefore, $Q(x)$ and $N(x)$ are polynomials in $\mathbb{Z}_3[x]$. See [7] for detail. Indeed, we can choose an ζ such that

$$Q(x) = x^{11} - x^8 - x^6 + x^4 + x^3 - x^2 - x - 1,$$

$$N(x) = x^{11} - 2x^{10} - 2x^9 - x^8 - x^7 + x^5 + x^3 - 1.$$

We have that

$$x^{23} - 1 = (x - 1)Q(x)N(x).$$

Notice that the choice of $Q(x)$ and $N(x)$ depends on the choice of the primitive root ζ. In fact, the replacement of ζ by ζ^i with $i \in N$ interchanges $Q(x)$ and $N(x)$.

Definition 1.1. Cyclic codes $\mathcal{Q}, \mathcal{Q}_1, \mathcal{N}, \mathcal{N}_1$ of length 23 with generator polynomials

$$Q(x), \quad (x-1)Q(x), \quad N(x), \quad (x-1)N(x),$$

respectively, are called **quadratic residue codes** defined over $\mathbb{Z}_3$.

We extend $\mathcal{Q}$ and $\mathcal{N}$ by adding the overall parity check 1. The resulting extended codes will be denoted by $\hat{\mathcal{Q}}$ and $\hat{\mathcal{N}}$.

We have the following well-known results on quadratic residue codes defined over the field $\mathbb{Z}_3$.

1. $\dim \mathcal{Q} = \dim \mathcal{N} = 12$, $\dim \mathcal{Q}_1 = \dim \mathcal{N}_1 = 11$.
2. $\mathcal{Q}^\perp = \mathcal{Q}_1$, $\mathcal{N}^\perp = \mathcal{N}_1$.
3. Extended codes $\hat{\mathcal{Q}}$, $\hat{\mathcal{N}}$ are **self-dual**.
4. $Aut\hat{\mathcal{Q}}$ contains $PSL_2(24)$.

Denote by $\mathbb{Z}_{3^e}$ the ring of integers modulo 3^e, and $\mathbb{Z}_{3^\infty}$ the ring of 3-adic integers. In next section we are going to lift these quadratic residue codes over $\mathbb{Z}_{3^e}$ and to the 3-adic integers $\mathbb{Z}_{3^\infty}$.

2. Quadratic residue codes over $\mathbb{Z}_{3^e}$

Quadratic residue codes over $\mathbb{Z}_{3^e}$ are usually defined by giving their idempotent generators. See [10] for quadratic residue codes over $\mathbb{Z}_{16}$ and [15] for codes over $\mathbb{Z}_9$ for example. However it is generally difficult to give general formulas for such generators. We will define quadratic residue codes over $\mathbb{Z}_{3^e}$ in a similar way as in the field case. The 3-adic case ($e = \infty$) is also included here. The idempotent generators for quadratic residue codes over $\mathbb{Z}_{3^e}$ can be obtained from idempotent generators of quadratic residue codes over $\mathbb{Z}_{3^\infty}$. For codes over p-adic integers, we refer [3].

Let $\mathbb{Q}_3$ denote the field of 3-adic numbers. Let K be the splitting field of $x^{23} - 1$ over $\mathbb{Q}_3$. Since the roots of $x^{23} - 1$ in K form a multiplicative group of order 23, it is clear that there exists an element ζ such that $K = \mathbb{Q}_3[\zeta]$. By considering the map

$$\Psi_e : \mathbb{Z}_{3^\infty} \to \mathbb{Z}_{3^e}, \quad \Psi_e(a) = a \pmod{3^e}$$

and extending it to $\mathbb{Z}_{3^\infty}[\zeta]$, we can easily see that

$$\mathbb{Z}_{3^e}[\zeta] \simeq \mathbb{Z}_{3^\infty}[\zeta]/(3^e).$$

$\mathbb{Z}_{3^e}[\zeta]$ is a Galois ring defined over $\mathbb{Z}_{3^e}$. Elements in $\mathbb{Z}_{3^e}[\zeta]$ can be written uniquely in a ζ-adic expansion $u = \sum_{i=0}^{22} v_i\zeta^i,\ v_i \in \mathbb{Z}_{3^e}$ or in a 3-adic expansion

$$u = u_0 + 3u_1 + 3^2u_2 + \cdots + 3^{e-1}u_{e-1}$$

where $u_i \in \{0, 1, \zeta, \cdots, \zeta^{22}\} \simeq \mathbb{Z}_{23}$, the finite field of 23 elements. In 3-adic integer case, this sum is infinite. The automorphism group of $\mathbb{Z}_{3^e}[\zeta]$ over $\mathbb{Z}_{3^e}$ is the cyclic group generated by the Frobenius automorphism

$$\mathcal{F}(\sum_{i=0}^{e-1} 3^i u_i) = \sum_{i=0}^{e-1} 3^i u_i^3.$$

We refer [1] or [9] for details. As in the field case, we let

$$Q_e(x) = \prod_{i\in Q}(x - \zeta^i), \quad N_e(x) = \prod_{i\in N}(x - \zeta^i).$$

Since $3 \in Q$ we have

$$\mathcal{F}(Q_e(x)) = \prod_{i\in Q}(x - \zeta^{3i}) = \prod_{i\in Q}(x - \zeta^i) = Q_e(x)$$

and similarly $\mathcal{F}(N_e(x)) = N_e(x)$. Thus $Q(x)$ and $N(x)$ are polynomials in $\mathbb{Z}_{3^e}[x]$. We certainly have that

$$x^{23} - 1 = (x-1)Q_e(x)N_e(x)$$

and for all $e' \geq e$,

$$Q_{e'}(x) \equiv Q_e(x) \pmod{3^e}, \quad N_{e'}(x) \equiv N_e(x) \pmod{3^e}.$$

DEFINITION 2.1. Cyclic codes $\mathcal{Q}^e, \mathcal{Q}_1^e, \mathcal{N}^e, \mathcal{N}_1^e$ of length 23 with generator polynomials

$$Q_e(x), \quad (x-1)Q_e(x), \quad N_e(x), \quad (x-1)N_e(x),$$

respectively, are called **quadratic residue codes** over $\mathbb{Z}_{3^e}$.

It can be shown that the polynomial $x^{23} - 1$ factors over $\mathbb{Z}_{3^\infty}[x]$ as follows:

$$x^{23} - 1 = (x-1)Q_\infty(x)N_\infty(x)$$

where

$$\begin{aligned} Q_\infty(x) = {} & x^{11} - \lambda x^{10} + (-\lambda - 3)x^9 - 4x^8 + (\lambda - 3)x^7 + (2\lambda - 1)x^6 \\ & + (2\lambda + 3)x^5 + (\lambda + 4)x^4 + 4x^3 - (\lambda - 2)x^2 - (\lambda + 1)x - 1, \end{aligned}$$

and λ is a root of $x^2 + x + 6 = 0$ in $\mathbb{Z}_{3^\infty}$ such that $\lambda \equiv 0 \pmod 3$. The polynomial $N_\infty(x)$ is obtained from $Q_\infty(x)$ by replacing λ by another root μ of $x^2 + x + 6 = 0$. Note that $\mu = -\lambda - 1$. For details, we refer [6], [13] and [14].

Then the generator polynomials over $\mathbb{Z}_{3^e}$ can be obtained by applying the projection Ψ_e:

$$Q_e(x) = \Psi_e(Q_\infty(x)), \quad N_e(x) = \Psi_e(N_\infty(x)).$$

3. Weight enumerators

Let p be a prime. Let $\mathcal{C}$ be a p-adic $[n,k]$ code, $\mathcal{C}^e = \Psi_e(\mathcal{C})$ be the projection of $\mathcal{C}$ over $\mathbb{Z}_{p^e}$ and A_i^e be the number of codewords of weight i in $\mathcal{C}^e$. Then

$$W_{\mathcal{C}^e}(x,y) = \sum_{i=0}^{n} A_i^e x^{n-i} y^i$$

is called the **weight enumerator** of $\mathcal{C}^e$.

Theorem 3.1 (MacWilliams Identity). *Let $q = p^e$ and $C = \mathcal{C}^e$. Then*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

The following theorem is essentially proved in [8] and [11].

Theorem 3.2 (Gleason's type theorem). *Suppose C is a self-dual code over $\mathbb{Z}_{p^e}$ of even length. Then $W_C(x, y)$ is a polynomial in $x^2 + (p^e - 1)y^2$ and $xy - y^2$.*

We know that the minimum distance of $\mathcal{C}^e$ is equal to the minimum distance of $\mathcal{C}^1$ for all e (see [2]). The following theorem is also proved in [2].

Theorem 3.3. *There is an integer N such that for every $d \le j < d_\infty$,*

$$A_j^e = A_j^N$$

for all $e \ge N$.

Moreover, the following theorem shows that we can stop the computation of A_i's at the appropriate stage without knowing the bound N given in the previous theorem..

Theorem 3.4. [14] *Suppose that $f \ge 2$ and $A_i^f = A_i^{f-1}$ for all $i \le j$. Then $A_j^e = A_j^f$ for all $e \ge f$.*

Let G_1 be the generator matrix for $\mathcal{Q}_1^\infty$.. Then the generator matrix of the extended quadratic residue code $\hat{\mathcal{Q}}^\infty$ is given by

$$\begin{pmatrix} G_1 & 0 \\ \mathbf{1} & \gamma n \end{pmatrix}$$

where $\mathbf{1} = (1, 1, \cdots, 1)$ of length 23 and $1 + 23\gamma^2 = 0$ in $\mathbb{Z}_{3^\infty}$. As before, $\hat{\mathcal{Q}}^e$ denotes $\Psi_e(\hat{\mathcal{Q}}^\infty)$. Theorem 3.2 gives the following:

Theorem 3.5. *Then the weight enumerator $W^e(x, y)$ of $\hat{\mathcal{Q}}^e$ is completely determined by $A_0^e, \cdots, A_{12}^e$ as follows:*

$$W^e(x, y) = \sum_{j=0}^{12} c_i \left(x^2 + (q-1)y^2\right)^j (xy - y^2)^{4-j}.$$

weight	0	9	10	11	12
$e = 1$	1	4048	0	0	61824
$e = 2$	1	4048	0	72864	717600
$e = 3$				72864	658352
$e = 4$					1956288
$e = 5$					2721360
$e = 6$					2721360

TABLE 1. Weights of $\hat{\mathcal{Q}}^e$

A computer calculation based on [4] gives us the Table 1 of weights of $\hat{\mathcal{Q}}^e$ for $e = 1, \cdots, 6$.

This table shows that $\hat{\mathcal{Q}}^e$ are $[24, 12, 9]$-code. The blank spaces in the table and weights $0 - 12$ for $e \geq 7$ can be filled by Theorem 3.4. Then Theorem 3.5 gives the weight enumerators as follows:

$$\begin{aligned} W^1(x,y) = {} & x^{24} + 4048x^{15}y^9 + 61824x^{12}y^{12} + 242880x^9y^{15} + \\ & 198352x^6y^{18} + 24288x^3y^{21} + 48y^{24}, \end{aligned}$$

$$\begin{aligned} W^2(x,y) = {} & x^{24} + 4048x^{15}y^9 + 72864x^{13}y^{11} + 717600x^{12}y^{12} + \\ & 4630176x^{11}y^{13} + 30530016x^{10}y^{14} + 164624064x^9y^{15} + \\ & 730206576x^8y^{16} + 2757647376x^7y^{17} + 8593159168x^6y^{18} + \\ & 21684544992x^5y^{19} + 43367486976x^4y^{20} + 66114704832x^3y^{21} + \\ & 72095794848x^2y^{22} + 50165446464xy^{23} + 16719966480y^{24}, \end{aligned}$$

$$\begin{aligned} W^3(x,y) = {} & x^{24} + 4048x^{15}y^9 + 72864x^{13}y^{11} + 658352x^{12}y^{12} + 59234016x^{11}y^{13} + \\ & 744038592x^{10}y^{14} + 14898518272x^9\ y^{15} + 213070985424x^8y^{16} + \\ & 2615794866432x^7y^{17} + 26432852979280x^6y^{18} + 217053362753568x^5y^{19} + \\ & 1410815464735248x^4y^{20} + 6986921266743616x^3y^{21} + 24771798631643712x^2y^{22} + \\ & 56005809423748608xy^{23} + 60672959726017088y^{24}, \end{aligned}$$

and

$$\begin{aligned}W^4(x,y) = {} & x^{24} + 4048x^{15}y^9 + 72864x^{13}y^{11} + 1956288x^{12}y^{12} + \\ & 205337376x^{11}y^{13} + 10843401888x^{10}y^{14} + 576780883008x^9y^{15} + \\ & 25945664318640x^8y^{16} + 977089931615952x^7y^{17} + 30396954242486656x^6y^{18} + \\ & 767926111835206368x^5y^{19} + 15358518289524481632x^4y^{20} + \\ & 234034567589881962816x^3y^{21} + 2553104372130271697760x^2y^{22} + \\ & 17760726067437170405568xy^{23} + 59202420224736156032496y^{24}.\end{aligned}$$

From Table 1, we have that $A_i^e = A_i^5$ for all $i = 0, \cdots, 12$ and for all $e \geq 5$. Theorem 3.5 then gives the following values of A_i^e for $i = 13, \cdots, 24$ with $q = 3^e$:

1. $A_{13}^e = 6624(-6999 + 452q)$
2. $A_{14}^e = 18216(16217 - 1808q + 111q^2)$
3. $A_{15}^e = 12144(-88651 + 13560q - 1665q^2 + 108q^3)$
4. $A_{16}^e = 2277(1132101 - 216960q + 39960q^2 - 5184q^3 + 323q^4)$
5. $A_{17}^e = 18216(-237270 + 54240q - 13320q^2 + 2592q^3 - 323q^4 + 19q^5$
6. $A_{18}^e = 1012(5170156 - 1366848q + 419580q^2 - 108864q^3 + 20349q^4 - 2394q^5 + 133q^6)$
7. $A_{19}^e = 6072(-761184 + 227808q - 83916q^2 + 27216q^3 - 6783q^4 + 1197q^5 - 133q^6 + 7q^7)$
8. $A_{20}^e = 1518(1951476 - 650880q + 279720q^2 - 108864q^3 + 33915q^4 - 7980q^5 + 1330q^6 - 140q^7 + 7q^8)$
9. $A_{21}^e = 2024(-664584 + 244080q - 119880q^2 + 54432q^3 - 20349q^4 + 5985q^5 - 1330q^6 + 210q^7 - 21q^8 + q^9)$
10. $A_{22}^e = 276(1489410 - 596640q + 329670q^2 - 171072q^3 + 74613q^4 - 26334q^5 + 7315q^6 - 1540q^7 + 231q^8 - 22q^9 + q^{10})$
11. $A_{23}^e = 24(-3165054 + 1372272q - 842490q^2 + 491832q^3 - 245157q^4 + 100947q^5 - 33649q^6 + 8855q^7 - 1771q^8 + 253q^9 - 23q^{10} + q^{11})$
12. $A_{24}^e = 6421278 - 2994048q + 2021976q^2 - 1311552q^3 + 735471q^4 - 346104q^5 + 134596q^6 - 42504q^7 + 10626q^8 - 2024q^9 + 276q^{10} - 24q^{11} + q^{12}$

Therefore we have completely determined all weight enumerators of the extended quadratic residue codes of length 24 over $\mathbb{Z}_{3^e}$.

References

[1] A.R. Calderbank and N.J.A. Sloane, *Modular and p-adic and cyclic codes*, DCC, **6** (1995), 21–35.

[2] S.T. Dougherty, S.Y. Kim and Y.H. Park, *Lifted codes and their weight enumerators*, Discrite Math. **305** (2005), 123–135.

[3] S.T. Dougherty and Y.H. Park, *Codes over the p-adic integers*, Des. Codes. Cryptogr. **39** (2006), 65–80.

[4] S. Han, *On the weight enumerators of the projections of the 2-adic Golay codes of length 24*, 2012, submitted.

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003.
[6] S.J. Kim, *Generator polynomials of the p-adic quadratic residue codes*, Kangweon-Kyungki Math. J, **13** (2005), 103–112.
[7] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge, 2003.
[8] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.
[9] B.R. McDonald, *Finite rings with identity*, Dekker, New York, 1974.
[10] K. Nagata, F. Nemenzo and H. Wada, *On self-dual codes over* $\mathbb{Z}_{16}$, Lecture Notes in Computer Science **5527**, 107–116, 2009.
[11] G. Nebe, E. Rains and N.J.A. Sloane, *Self-dual codes and invariant theory*, Springer-Verlag, 2006.
[12] Y.H. Park, *Modular independence and generator matrices for codes over* $\mathbb{Z}_m$, Des. Codes. Crypt **50** (2009), 147–162.
[13] Y.H. Park, *On lifted codes and p-adic codes - their weight enumerators*, KIAS international conference on coding theory and applications, 2012.
[14] Y.H. Park, *Quadratic residue codes over p-adic integers and their projections to integers modulo* p^e, in preparation, 2012.
[15] B. Taeri, *Quadratic residue codes over* $\mathbb{Z}_9$, J. Korean Math Soc., **46** (2009), 13–30.

Department of Mathematics
Kangwon National University
E-mail: yhpark@kangwon.ac.kr