Korean J. Math. **23** (2015), No. 1, pp. 163–169
http://dx.doi.org/10.11568/kjm.2015.23.1.163

QUADRATIC RESIDUE CODES OVER p-ADIC INTEGERS AND THEIR PROJECTIONS TO INTEGERS MODULO p^e

Young Ho Park

Abstract. We give idempotent generators for quadratic residue codes over p-adic integers and over the rings $\mathbb{Z}_{p^e}$.

1. Introduction

Let R be a ring. A *code* of length n over R is a R-submodule of R^n. For generality on codes over fields, we refer [5] and [8]. For codes over $\mathbb{Z}_m$, see [3, 12], and for self dual codes, see [11]. See [1, 4] for codes over p-adic numbers.

Quadratic residue codes are cyclic codes of prime length n defined over a finite field $\mathbb{F}_{p^e}$, where p^e is a quadratic residue mod n. They comprise a very important family of codes. Examples of quadratic residue codes include the binary [7,4,3] Hamming code, the binary [23,12,7] Golay code, the ternary [11,6,5] Golay code and the quaternary Hexacode. Quadratic residue codes have rate close to 1/2 and tend to have high minimum distance. Extended quadratic residue codes are self-dual.

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

Received March 6, 2015. Revised March 15, 2015. Accepted March 15, 2015.
2010 Mathematics Subject Classification: 94B05.
Key words and phrases: quadratic residue code, p-adic code, idempotent generator.
This study was supported by 2013 Research Grant from Kangwon National University (No. C1009751-01-01).

residue codes over the field $\mathbb{F}_p$ to rings $\mathbb{Z}_{p^e}$ and to the p-adic integers $\mathbb{Z}_{p^\infty}$.

In early papers [2,5,6,10,13], authors tried to generalize the quadratic residue codes to the rings $\mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_{16}, \mathbb{Z}_9$ by giving idempotent generators. In [7], author defined quadratic residue codes over the rings $\mathbb{Z}_{p^e}$ and p-adic integer ring $\mathbb{Z}_{p^\infty}$ in general and gave generating polynomials. In this article, we give their idempotent generators.

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

In the earlier works by several authors, quadratic residue codes over $\mathbb{Z}_{p^e}$ are usually defined by giving idempotent generators. See [2, 10] for quadratic residue codes over $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ and [13] for codes over $\mathbb{Z}_9$ for example. However it is generally difficult to give a formula for such generators and hard to understand. We will define quadratic residue codes over $\mathbb{Z}_{p^e}$ in a similar way as in the field case. The p-adic case ($e = \infty$) is also included here. For codes over p-adic integers, we refer [1, 3, 4].

Let p be a prime and let n be a prime such that p is a quadratic residue modulo n. Let Q be the set of quadratic residues modulo n, and N the set of quadratic nonresidues modulo n.

Let $\mathbb{Q}_p$ denote the field of p-adic numbers. Let K be the splitting field of $x^n - 1$ over $\mathbb{Q}_p$. Since the roots of $x^n - 1$ in K form a multiplicative group of order n, it is clear that there exists an element ζ such that $K = \mathbb{Q}_p[\zeta]$. By considering the map $\Psi_e : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^e}$ defined by $\Psi_e(a) = a \pmod{p^e}$ and extending it to $\mathbb{Z}_{p^\infty}[\zeta]$, we can easily see that

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

$\mathbb{Z}_{p^e}[\zeta]$ is a Galois ring defined over $\mathbb{Z}_{p^e}$. Elements in $\mathbb{Z}_{p^e}[\zeta]$ can be written uniquely as a ζ-adic expansion $u = \sum_{i=0}^{p-1} v_i \zeta^i$, $v_i \in \mathbb{Z}_{p^e}$ or in a p-adic expansion

$$u = u_0 + pu_1 + p^2 u_2 + \cdots + p^{e-1} u_{e-1}$$

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

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

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 $p \in Q$ we have

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

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

$$x^n - 1 = (x-1)Q_e(x)N_e(x)$$

and for all $e' \geq e$,

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

$Q_\infty(x)$ and $N_\infty(x)$ may be defined as p-adic limits of $Q_e(x)$ and $N_e(x)$.

Definition 2.1. Cyclic codes $\mathcal{Q}^e, \mathcal{Q}_1^e, \mathcal{N}^e, \mathcal{N}_1^e$ of length n 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 $\mathbb{Z}_{p^e}$.

3. Main Theorem

Let

$$f_Q(x) = \sum_{i \in Q} x^i, \quad f_N(x) = \sum_{i \in N} x^i.$$

the polynomials in $\mathbb{Z}_{p^e}[x]/(x^n - 1)$, where $e = 1, 2, \ldots, \infty$.

Theorem 3.1. *1. Suppose $n = 4k - 1$.*

$$\begin{aligned} f_Q^2 &= \frac{n-3}{4} f_Q + \frac{n+1}{4} f_N \\ f_N^2 &= \frac{n+1}{4} f_Q + \frac{n-3}{4} f_N \\ f_Q f_N &= \frac{n-1}{2} + \frac{n-3}{4} f_Q + \frac{n-3}{4} f_N \end{aligned}$$

2. Suppose $n = 4k + 1$.

$$f_Q^2 = \frac{n-5}{4} f_Q + \frac{n-1}{4} f_N + \frac{n-1}{2}$$
$$f_N^2 = \frac{n-1}{4} f_Q + \frac{n-5}{4} f_N + \frac{n-1}{2}$$
$$f_Q f_N = \frac{n-1}{4} f_Q + \frac{n-1}{4} f_N$$

Proof. It follows from the Perron's theorem. □

Let

$$\lambda = f_Q(\zeta) = \sum_{i \in Q} \zeta^i, \quad \mu = f_N(\zeta) = \sum_{i \in N} \zeta^i$$

Diffenrent choice of the root ζ may interchange λ and μ. Let

$$\theta = \lambda - \mu.$$

Then

$$\theta^2 = \pm n$$

for $n = 4k \pm 1$, where double signs are in the same order.

Theorem 3.2. *1. If $n = 4k - 1$, then λ and μ are roots of $x^2 + x + k = 0$.*
2. If $n = 4k + 1$, then λ and μ are roots of $x^2 + x - k = 0$.

Note that $\mu + \lambda = -1$. For details, we refer [7].

Theorem 3.3. *Let $p > 2$ be a prime and and $n = 4k \pm 1$ be a prime such that p is a quadratic residue modulo n. Let $\theta^2 \equiv \pm 1 \pmod p$, where double signs are in the same order as in $n = 4k \pm 1$. The idempotent generators of the p-adic quadratic residue codes $\langle Q_\infty(x) \rangle, \langle (x-1)Q_\infty(x) \rangle, \langle N_\infty(x) \rangle, \langle (x-1)N_\infty(x) \rangle$ of length n are given as follows, respectively:*

$$E_q(x) = a + b f_Q(x) + c f_N(x)$$
$$F_q(x) = a' - c f_Q(x) - b f_N(x)$$
$$E_n(x) = a + c f_Q(x) + b f_N(x)$$
$$F_n(x) = a' - b f_Q(x) - c f_N(x)$$

where

$$a = \frac{n+1}{2n}, \quad a' = \frac{n-1}{2n}, \quad b = \frac{1 \mp \theta}{2n}, \quad c = \frac{1 \pm \theta}{2n}.$$

The idempotent generators of quadratic residue codes over $\mathbb{Z}_{p^e}$ can be obtained by projecting these generators modular p^e.

Proof. We prove the formula for $E_q(x)$ in the case that $n = 4k - 1$. Let

$$E = 1 + f_Q(x) + f_N(x) + n + \theta(f_Q(x) - f_N(x)).$$

It is a lengthy but straightforward computation to show that $E^2 = 2nE$ using Theorem 3.1 and $\theta^2 = -n$. Therefore $(\frac{E}{2n})^2 = \frac{E}{2n}$. But $\frac{E}{2n} = E_q(x)$. Thus $E_q(x)$ is idempotent. Next, note that $1 + f_Q(x) + f_N(x) = Q_\infty(x)N_\infty(x)$. Thus for all $i \in Q$, we have $E(\zeta^i) = 0 + n + \theta(\lambda - \mu) = n + \theta^2 = 0$. For all $i \in N$, we have $E(\zeta^i) = 0 + n + \theta(\mu - \lambda) = n - \theta^2 = 2n$. Thus $E_q(\zeta^i) = 0$ if $i \in Q$ and $E_q(\zeta^i) = 1$ if $i \in N$. We also have that $E_q(1) = 1$. Thus $E_q(x) = V(x)Q_\infty(x)$ for some $V(x)$ and $E_q(x)$ is relatively prime to $N_\infty(x)(x-1)$. Therefore there exist $A(x), B(x)$ such that $A(x)E_q(x) + B(x)N_\infty(x)(x-1) = 1$. From this we get $A(x)E_q(x)Q(x) = Q(x)$. Hence $\langle E_q(x)\rangle = \langle Q_\infty(x)\rangle$.

All remaining cases can be proved in a similar way. □

Note that an idempotent generator for the binary case is given in [1].

4. An example

In this section, we use our Theorem 3.3 to find idempotent generators of the quadratic residue codes over $\mathbb{Z}_9$ as in [13].

First we note that $\left(\dfrac{n}{3}\right) = 1$ iff $n = 12r \pm 1$ for some r. In order to solve $\theta^2 \equiv \pm n \pmod 9$, we need to separate cases further according to r modulo 3. We compute everything modulo 9.

Case I. $n = 12r - 1$.

1. $r = 3j$: $(n = 36j - 1)$.

   In this case $n = 36j - 1 = -1$. Inverse of $2n = -2$ is 4. Thus $a = 4(n+1) = 0$, $a' = 4(n-1) = 1$. Solving $\theta^2 = -n = 1$, we obtain $\theta = \pm 1$. Thus $b, c = 4(1 \pm \theta) = 8, 0$. Hence the idempotent generators of quadratic residue codes are

   $$8f_Q, \quad 8f_N, \quad 1 - 8f_Q, \quad 1 - 8f_N.$$

2. $r = 3j + 1$: $(n = 36j + 11)$.

   In this case $n = 2$, and the inverse of $2n$ is 7. Thus $a = 3$ and $a' = 7$. From $\theta^2 = -n = 7$, we get $\theta = \pm 4$. Thus $b, c = 7(1 \pm 4) =$

$8, 6$. Thus the idempotent generators of quadratic residue codes are

$$3 + 8f_Q + 6f_N, \quad 3 + 6f_Q + 8f_N, \quad 7 + f_Q + 3f_N, \quad 7 + 3f_Q + f_N.$$

3. $r = 3j + 2$: $(n = 36j + 23)$.
   Similarly, we find that the idempotent generators of quadratic residue codes for this case are

$$6 + 3f_Q + 8f_N, \quad 6 + 8f_Q + 3f_N, \quad 4 + 6f_Q + 1f_N, \quad 4 + 1f_Q + 6f_N.$$

Case II. $n = 12r + 1$.

1. $r = 3j$: $(n = 36j + 1)$.
   In this case $n = 1$. Inverse of $2n = 2$ is 5. Thus $a = 1$, $a' = 0$. Solving $\theta^2 = n$, we obtain $\theta = \pm 1$. Thus $b, c = 5(1 \pm \theta) = 0, 1$. Hence the idempotent generators of quadratic residue codes are

$$1 + f_N, \quad 1 + f_Q, \quad 8f_N, \quad 8f_Q.$$

2. $r = 3j + 1$: $((n = 36j + 13)$.
   The idempotent generators of quadratic residue codes are

$$4 + 6f_Q + f_N, \quad 4 + f_Q + 6f_N, \quad 6 + 3f_Q + 8f_N, \quad 6 + 8f_Q + 3f_N.$$

3. $r = 3j + 2$: $(n = 36j + 25)$.
   The idempotent generators of quadratic residue codes for this case are

$$7 + f_Q + 3f_N, \quad 7 + 3f_Q + f_N, \quad 3 + 8_Q + 6f_N, \quad 3 + 6f_Q + 8f_N.$$

References

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

[2] M.H Chiu, S. S.-T. Yau and Y. Yu, *$\mathbb{Z}_8$-cyclic codes and quadratic residue codes*, Advances in Algebra **25** (2000), 12–33.

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

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

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003.

[6] S.J. Kim, *Quadratic residue codes over $\mathbb{Z}_{16}$*, Kangweon-Kyungki Math. J. **11** (2003), 57–64.

[7] S.J. Kim, *Generator polynomials of the p-adic quadratic residue codes*, Kangweon-Kyungki Math. J. **13** (2005), 103–112.

[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] B. Taeri, *Quadratic residue codes over* $\mathbb{Z}_9$, J. Korean Math Soc. **46** (2009), 13–30.

Young Ho Park
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
E-mail: yhpark@kangwon.ac.kr