Korean J. Math. **24** (2016), No. 3, pp. 567–572
http://dx.doi.org/10.11568/kjm.2016.24.3.567

QUADRATIC RESIDUE CODES OVER GALOIS RINGS

Young Ho Park

Abstract. 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. In this article we introduce the generalization of quadratic residue codes defined over Galois rings using the Galois theory.

1. Introduction

Let R be a ring and n a positive integer. A (linear) code over R of length n is an R-submodule of R^n. A code C is cyclic if $a_0a_1\cdots a_{n-1} \in C$ implies $a_{n-1}a_0\cdots a_{n-2} \in C$. A cyclic code is isomorphic to an ideal of $R[x]/(x^n-1)$ via $a_0a_1\cdots a_{n-1} \mapsto a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$.

Quadratic residue codes have been defined over finite fields. See [4] for generality of codes and quadratic residue codes over fields. Being cyclic codes, quadratic residue codes over the prime finite field $\mathbb{F}_p = \mathbb{Z}_p$ can be lifted to codes over $\mathbb{Z}_{p^e}$ and to the ring $\mathcal{O}_p$ of p-adic integers using the Hensel lifting [1, 3, 8]. Quadratic residue codes can be also defined as duadic codes with idempotent generators and lifted to $\mathbb{Z}_{p^e}$ [2, 5, 9–11]. However, we have found a better way of constructing quadratic residue codes for Galois rings.

Received August 9, 2016. Revised September 18, 2016. Accepted September 19, 2016.

2010 Mathematics Subject Classification: 94B05, 11T71.

Key words and phrases: quadratic residue code, Galois rings, code over rings.

This work was supported by 2014 Research Grant from Kangwon National University (No. 120141505).

2. Galois Rings

$\mathbb{Z}_{p^e}$ is a local ring with maximal ideal $p\mathbb{Z}_{p^e}$ and residue field $\mathbb{Z}_p$. Let r be a positive integer and let

$$GR(p^e, r) = \mathbb{Z}_{p^e}[X]/\langle h(X)\rangle \simeq \mathbb{Z}_{p^e}[\zeta],$$

where $h(X)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^e}[X]$ of degree r that divides $X^{p^r-1} - 1$. The polynomial $h(X)$ is chosen so that $\zeta = X + \langle h(X)\rangle$ is a primitive $(p^r - 1)$st root of unity. $GR(p^e, r)$ is the Galois extension of degree r over $\mathbb{Z}_{p^e}$, called a *Galois ring.* We refer [1, 7] for details. Galois extensions are unique up to isomorphism. $GR(p^e, r)$ is a finite chain rings with ideals of the form $\langle p^i\rangle$ for $0 \le i \le e - 1$, and residue field $\mathbb{F}_{p^r}$.

The set $T_r = \{0, 1, \zeta, \dots, \zeta^{p^r-2}\}$ is a complete set, known as Teichmüller set, of coset representatives of $GR(p^e, r)$ modulo $\langle p\rangle$. Any element of $GR(p^e, r)$ can be uniquely written as a p-adic sum $c_0 + c_1 p + c_2 p^2 + \cdots + c_{e-1}p^{e-1}$ with $c_i \in T_r$. It can also be written in the ζ-adic expansion $b_0 + b_1\zeta + \cdots + b_{r-1}\zeta^{r-1}$ with $b_i \in \mathbb{Z}_{p^e}$.

The Galois group of isomorphisms of $GR(p^e, r)$ over $\mathbb{Z}_{p^e}$ is a cyclic group of order r generated by the Frobenius automorphism $\mathtt{Fr}$ given by $\mathtt{Fr}\left(\sum_{i=0}^{r-1} b_i\zeta^i\right) = \sum_{i=0}^{r-1} b_i\zeta^{ip}$ $(b_i \in \mathbb{Z}_{p^e})$ in ζ-adic expansion and $\mathtt{Fr}\left(\sum_{i=0}^{e-1} c_i p^i\right) = \sum_{i=0}^{e-1} c_i^p p^i$, $(c_i \in T_r)$ in p-adic expansion. We recall that $GR(p^e, l) \subset GR(p^e, m)$ if and only if $l \mid m$. Moreover, the Galois group of $GR(p^e, rs)$ over $GR(p^e, r)$ is generated by $\mathtt{Fr}^r$ and hence

$$GR(p^e, r) = \{a \in GR(p^e, rs) \mid \mathtt{Fr}^r(a) = a\}. \tag{1}$$

Here the map $\mathtt{Fr}^r$ is explicitly given as

$$\mathtt{Fr}^r(a_0 + a_1 p + \cdots + a_t p^t + \cdots) = a_0^{p^r} + a_1^{p^r} p + \cdots + a_t^{p^r} p^t + \cdots$$

where $a_i \in T_r$. In particular, if α is any nth of unity in the extension $GR(p^e, rs)$, where $n \mid p^{rs} - 1$, then

$$\mathtt{Fr}^r(\alpha) = \alpha^{p^r} \tag{2}$$

3. Quadratic residue codes for Galois rings

Now we are going to define quadratic residue codes over the Galois ring $GR(p^e, r)$. We fix an odd prime (length) n, and another prime power p^r which is a quadratic residue modulo n. Let α be a primitive nth root of unity in an extension $GR(p^e, rs)$ of $GR(p^e, r)$. Let Q be quadratic residues mod n, N quadratic nonresidues mod n. Define

$$q_e(X) = \prod_{i \in Q}(X - \alpha^i), \quad n_e(X) = \prod_{j \in N}(X - \alpha^j) \tag{3}$$

THEOREM 3.1. *We have the factorization in* $GR(p^r, e)[X]$*:*

$$X^n - 1 = (X - 1)q_e(X)n_e(X)$$

Proof. $\mathtt{Fr}^r(q_e(X)) = \prod_{i \in Q}(X - \alpha^{ip^r}) = \prod_{i \in Q}(X - \alpha^i)$ by (2) and the fact that $p^r Q = Q$. Hence $q_e(X) \in GR(p^r, e)$ by (1). □

DEFINITION 3.2. The **quadratic residue codes** $\mathcal{Q}_e, \mathcal{Q}_{e1}, \mathcal{N}_e, \mathcal{N}_{e1}$ (respectively) over the Galois ring $GR(p^e, r)$ are cyclic codes of length n with generator polynomials (respectively)

$$q_e(X), \quad (X - 1)q_e(X), \quad n_e(X), \quad (X - 1)n_e(X).$$

We now explain how to get the polynomials in the definition. First we define

$$\lambda = \sum_{i \in Q} \alpha^i, \quad \mu = \sum_{j \in N} \alpha^j.$$

Since λ and μ are invariant under the Frobenius map, they lie in the ring $GR(p^e, r)$. Notice that a different choice (for example α^j for $j \in N$) of the root α may interchange λ and μ. We have the following theorem [6,8].

THEOREM 3.3. *If* $n = 4k \pm 1$ *then* λ *and* μ *are roots of* $x^2 + x = \pm k$ *in the ring* $GR(p^e, r)$.

The elementary symmetric polynomials $s_0, s_1, s_2, \cdots, s_t$ in the polynomial ring $S[X_1, X_2, \cdots, X_t]$ over a ring S are given by

$$s_i(X_1, X_2, \cdots, X_t) = \sum_{i_1 < i_2 < \cdots < i_t} X_{i_1} X_{i_2} \cdots X_{i_t}, \quad \text{for } i = 1, 2, \cdots, t.$$

We define $s_0(X_1, X_2, \cdots, X_t) = 1$. For all $i \geq 1$, the i-power symmetric polynomials are defined by

$$p_i(X_1, X_2, \cdots, X_t) = X_1^i + X_2^i + \cdots + X_t^i.$$

THEOREM 3.4 (Newton's identities). *For each* $1 \leq i \leq t$

$$p_i = p_{i-1}s_1 - p_{i-2}s_2 + \cdots + (-1)^i p_1 s_{i-1} + (-1)^{i+1} i s_i, \tag{4}$$

where $s_i = s_i(X_1, X_2, \cdots, X_t)$ *and* $p_i = p_i(X_1, X_2, \cdots, X_t)$.

Let $Q = \{q_1, q_2, \cdots q_t\}$, $N = \{n_1, n_2, \cdots, n_t\}$. The followings hold:

(i) $p_i(\alpha^{q_1}, \alpha^{q_2}, \cdots, \alpha^{q_t}) = \begin{cases} \lambda, & i \in Q, \\ \mu, & i \in N. \end{cases}$

(ii) $p_i(\alpha^{n_1}, \alpha^{n_2}, \cdots, \alpha^{n_t}) = \begin{cases} \mu, & i \in Q, \\ \lambda, & i \in N. \end{cases}$

We use these identities together with Newton's identity to get the formula for $q_e(X)$ and $n_e(X)$ [6,8].

THEOREM 3.5. *Let $t = (n-1)/2$ and*

$$q_e(X) = a_0 X^t + a_1 X^{t-1} + \cdots + a_t.$$

Then

1. $a_0 = 1$, $a_1 = -\lambda$.
2. a_i *can be determined inductively by the formula*

$$a_i = -\frac{p_i a_0 + p_{i-1} a_1 + p_{i-2} a_2 + \cdots + p_1 a_{i-1}}{i},$$

where $p_i = p_i(\alpha^{q_1}, \alpha^{q_2}, \cdots, \alpha^{q_t})$.

Analogous statements hold for $n(X)$ with $a_1 = -\mu$.

Finally we use this theorem to give some examples. We take the Galois ring $GR(3^2, 2)$ with $p = 3, r = 2$. Since 3^2 is a quadratic residue for every n, there are quadratic residue codes of any length $n \neq 2, 3$. Now $GR(9, 2) \simeq \mathbb{Z}_9[\zeta]$ where ζ is the $p^r - 1 = 8$th root of unity satisfying $\zeta^2 = \zeta + 1$. We note that $\mathbb{F}_9 \simeq \mathbb{Z}_3[\zeta]$ also. There exists an integer $s \leq n-1$ such that $n \mid 9^s - 1$ by Fermat's little theorem. Then the nth root α of unity exists in $GR(9, 2s)$.

Let $n = 4k \pm 1$. According to Theorem 3.3 we first need to solve $x^2 + x = \pm k$ in $GR(9, 2) = \{a + b\zeta \mid a, b \in \mathbb{Z}_9\}$. In fact, we obtain $x = \frac{1}{2}(-1 \pm \sqrt{\pm n})$ for λ and μ. Thus we need to solve $(a + b\zeta)^2 = \pm n$, equivalently, $a^2 + b^2 = \pm n$ and $b(2a + b) = 0$. Solving these for small values of $n < 40$, we obtain the following table.

n	5	7	11	13	17	19	23	29	31	37
λ	8ζ	$5+7\zeta$	6	5	$6+5\zeta$	$6+5\zeta$	5	$5+7\zeta$	8ζ	0

We can compute the $q_e(X)$ and $n_e(X)$ by Theorem 3.5 for each n as follows. Replace r with λ and $\mu = -1 - \lambda$ to get $q_e(X)$ and $n_e(X)$ in the given polynomial in the Table 1.

n	$q_e(X)$ or $n_e(X)$
5	$1 - rX + X^2$
7	$-1 + (-1 - r)X - rX^2 + X^3$
11	$-1 + (-1 - r)X + X^2 - X^3 - rX^4 + X^5$
13	$1 - rX + 2X^2 + (-1 - r)X^3 + 2X^4 - rX^5 + X^6$
17	$1 - rX + (2 - r)X^2 + (3 - r)X^3 + (1 - 2r)X^4 + (3 - r)X^5 +$ $(2 - r)X^6 - rX^7 + X^8$
19	$-1 + (-1 - r)X + 2X^2 + (-1 + r)X^3 + (-3 - r)X^4 + (2 - r)X^5 +$ $(2 + r)X^6 - 2X^7 - rX^8 + X^9$
23	$-1 + (-1 - r)X + (2 - r)X^2 + 4X^3 + (4 + r)X^4 + (3 + 2r)X^5 +$ $(-1 + 2r)X^6 + (-3 + r)X^7 - 4X^8 + (-3 - r)X^9 - rX^{10} + X^{11}$
29	$1 - rX + 4X^2 + (-2 - r)X^3 + (1 + r)X^4 - X^5 + (1 - r)X^6 + (4 - r)X^7 +$ $(1 - r)X^8 - X^9 + (1 + r)X^{10} + (-2 - r)X^{11} + 4X^{12} - rX^{13} + X^{14}$
31	$-1 + (-1 - r)X + (3 - r)X^2 + (6 + r)X^3 + 2rX^4 - 4X^5 + (1 - r)X^6 +$ $(3 + r)X^7 + (-2 + r)X^8 + (-2 - r)X^9 + 4X^{10} + 2(1 + r)X^{11} +$ $(-5 + r)X^{12} + (-4 - r)X^{13} - rX^{14} + X^{15}$
37	$1 - rX + 5X^2 + (-3 - 2r)X^3 + (8 + r)X^4 + (-4 - 3r)X^5 + (9 + r)X^6 +$ $(-5 - 2r)X^7 + (6 + r)X^8 + (-3 - 2r)X^9 + (6 + r)X^{10} + (-5 - 2r)X^{11} +$ $(9 + r)X^{12} + (-4 - 3r)X^{13} + (8 + r)X^{14} + (-3 - 2r)X^{15} + 5X^{16} - rX^{17} + X^{18}$

TABLE 1. Generator polynomials of $q_e(X)$ and $n_e(X)$

References

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

[2] M.H. Chiu, S.S.Yau and Y. Yu, *$\mathbb{Z}_8$-cyclic codes and quadratic residue codes*, Advances in Applied Math. **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] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003.

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

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

[7] B. McDonald, *Finite rings with identity*, Marcel Dekker, 1974.

[8] Y.H. Park, *Quadratic residue codes over p-adic integers and their projections to integers modulo p^e*, Korean J. Math. **23** (2015), 163–169.

[9] V.S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory. **42** (1996), 1594–1600.

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

[11] X. Tan, *A family of quadratic residue codes over $\mathbb{Z}_{2^m}$*, preprint, 2011.

Young Ho Park
Department of Mathematics
Kangwon National University
Chun Cheon 24341, Korea
E-mail: yhpark@kangwon.ac.kr