Kangweon-Kyungki Math. Jour. **11** (2003), No. 1, pp. 57–64

QUADRATIC RESIDUE CODES OVER $\mathbb{Z}_{16}$

Sung Jin Kim

Abstract. We define Z_{16} quadratic residue codes in term of their idempotent generators and show that these codes also have many good properties which are analogous in many respects to properties of quadratic residue codes over a field.

1. Introduction

Let $\mathbb{Z}_{16}$ denote the integers modulo 16. A set of n-tuples over $\mathbb{Z}_{16}$ is called a code over $\mathbb{Z}_{16}$ or a $\mathbb{Z}_{16}$-code if it is a $\mathbb{Z}_{16}$ module.

A particularly interesting family of $\mathbb{Z}_{16}$-cyclic codes are quadratic residue codes. Quadratic residue codes were first defined by Andrew Gleason. The minimum weights of many modest quadratic residue codes are quite high for the code's lengths, making this class of codes promising. We define Z_{16} quadratic residue codes in term of their idempotent generators and show that these codes also have many good properties which are analogous in many respects to properties of quadratic residue codes over a field.

2. Idempotent Generators of Cyclic Codes

An idempotent in $\mathbb{Z}_{p^m}/(x^n-1)$, where p is a prime number, is defined to be a polynomial $e(x)$ such that $e(x)^2 \equiv e(x) \pmod{x^n-1}$.

Theorem 2.1. *Let C be a $\mathbb{Z}_{p^m}$ cyclic code of odd length n. If $C = (f)$, where $fg = x^n - 1$ for some g such that f and g are coprime, then C has an idempotent generator in $\mathbb{Z}_{p^m}[x]/(x^n - 1)$. Moreover, the idempotent generator of a cyclic code is unique.*

Received January 10, 2003.
2000 Mathematics Subject Classification: 94B15.
Key words and phrases: cyclic codes, quadratic residue codes.

THEOREM 2.2. *If a $\mathbb{Z}_{p^m}[x]$ cyclic code C has the idempotent generator $e(x)$, then $C^{\perp}$ has the idempotent generator $1 - e(x^{-1})$.*

THEOREM 2.3. *Let C_1 and C_2 be cyclic codes with $\mathbb{Z}_{16}$-idempotent generators e_1 and e_2; then $C_1 \cap C_2$ has the $\mathbb{Z}_{16}$-idempotent e_1e_2 and $C_1 + C_2$ has $\mathbb{Z}_{16}$-idempotent generator $e_1 + e_2 - e_1e_2$.*

3. Idempotent Generators of QR Codes

Let $e_1 = \Sigma_{i\in Q}x^i$ and $e_2 = \Sigma_{i\in N}x^i$, where Q is the set of quadratic residues and N is the set of non-residues for a prime $p \equiv \pm 1(\text{mod } 8)$. When $p \equiv -1(\text{mod } 8)$, e_1 and e_2 are idempotents of binary $[p, (p+1)/2]$ QR codes. When $p \equiv 1(\text{mod } 8)$, they are idempotents of binary $[p, (p-1)/2]$ QR codes.

LEMMA 3.1. *Let x and y be both in Q or both in N, and let $\alpha \neq 0$ in $\mathbb{Z}_p$. Then the number of pairs x, y such that $x + y = \alpha$ is $(p+1)/8$ if $p \equiv -1(\text{mod } 8)$ and $(p-1)/8$ if $p \equiv 1(\text{mod } 8)$.*

Let the map μ_a a be defined as

$$\mu_a : i \to ai \pmod{p}$$

for any nonzero $a \in GF(p)$. It is not hard to show that $\mu_a(fg) = \mu_a(f)\mu_a(g)$ for f and g polynomials in $R_p = \mathbb{Z}_{16}[x]/(x^p - 1)$.

We know that in the binary case, the all one vector $1+e_1+e_2$, denoted by h, is an idempotent in $\mathbb{Z}_2[x]/(x^p - 1)$. In $\mathbb{Z}_{16}[x]/(x^p - 1)$,

$$h^2 = (1 + e_1 + e_2)h = h + \tfrac{p-1}{2}h + \tfrac{p-1}{2}h = h + (p-1)h = ph$$

Therefore, when $p \equiv 1(\text{mod } 8)$, h and $9h$ is an idempotent in $\mathbb{Z}_{16}[x]/(x^p - 1)$ and $(h) = (9h)$; when $p \equiv -1(\text{mod } 8)$, $15h$ denoted by $\tilde{h}$ and 7h are an idempotent in $\mathbb{Z}_{16}[x]/(x^p - 1)$. and $(15h) = (7h)$

In order to prove the next theorem, we first discuss the following results.

First assume that $p \equiv -1(\text{mod } 8)$ (i.e.,$p + 1 = 8r$).

1. $e_1^2 = (\Sigma_{i\in Q}x^i)^2 = \Sigma_{i\in Q}x^{2i} + \Sigma_{i\neq j, i,j\in Q}x^{i+j}$. Since $2 \in Q$ (so $i \in Q \Rightarrow 2i \in Q$), the first part of the above sum is e_1. Since $-1 \notin Q$, we have $-a \notin Q$ whenever $a \in Q$. By Lemma 3.1, the second part of the sum is $2[(r-1)e_1 + re_2] = 2re_1 + 2re_2 - 2e_1$. So

$$e_1^2 = e_1 + 2re_1 + 2re_2 - 2e_1 = 2re_1 + 2re_2 - e_1.$$

2. $e_2^2 = (\Sigma_{i\in N}x^i)^2 = \Sigma_{i\in N}x^{2i} + \Sigma_{i\neq j,i,j\in N}x^{i+j}$. Since $2 \in Q$ (so $i \in N \Rightarrow 2i \in N$), the first part of above sum is e_2. Since $-1 \notin Q$, we have $-a \notin N$ whenever $a \in N$. By Lemma 3.1, the second part of the sum is $2[re_1 + (r-1)e_2] = 2re_1 + 2re_2 - 2e_2$. So

$$e_2^2 = e_2 + 2re_1 + 2re_2 - 2e_2 = 2re_1 + 2re_2 - e_2.$$

3. Since $15h = 15(1 + e_1 + e_2)$ is an idempotent in $\mathbb{Z}_{16}[x]/(x^p - 1)$, then $(15h)^2 = 15h$, i.e.,

$$\begin{gathered}15+15e_1+15e_2 = (15+15e_1+15e_2)^2 = 1+e_1^2+e_2^2+2e_1+2e_2+2e_1e_2 \\ \Rightarrow 2e_1e_2 = 14 + 15e_1^2 + 15e_2^2 + 13e_1 + 13e_2.\end{gathered}$$

Next assume that $p \equiv 1 (\text{mod } 8)$ (i.e.,$p - 1 = 8r$).

1. $e_1^2 = (\Sigma_{i\in Q}x^i)^2 = \Sigma_{i\in Q}x^{2i} + \Sigma_{i\neq j,i,j\in Q}x^{i+j}$. Since $2 \in Q$ (so $i \in Q \Rightarrow 2i \in Q$), the first part of the above sum is e_1. Since $-1 \in Q$, we have $-a \in Q$ whenever $a \in Q$. By Lemma 3.1, the second part of the sum is $2[(r-1)e_1 + re_2] + 4r = 2re_1 + 2re_2 - 2e_1 + 4r$. So

$$e_1^2 = e_1 + 2re_1 + 2re_2 - 2e_1 + 4r = 2re_1 + 2re_2 - e_1 + 4r.$$

2. $e_2^2 = (\Sigma_{i\in N}x^i)^2 = \Sigma_{i\in N}x^{2i} + \Sigma_{i\neq j,i,j\in N}x^{i+j}$. Since $2 \in Q$ (so $i \in N \Rightarrow 2i \in N$), the first part of above sum is e_2. Since $-1 \in Q$, we have $-a \in N$ whenever $a \in N$. By Lemma 3.1, the second part of the sum is $2[re_1 + (r-1)e_2] + 4r = 2re_1 + 2re_2 - 2e_2 + 4r$. So

$$e_2^2 = e_2 + 2re_1 + 2re_2 - 2e_2 + 4r = 2re_1 + 2re_2 - e_2 + 4r.$$

3. Since $h = 1 + e_1 + e_2$ is an idempotent in $\mathbb{Z}_{16}[x]/(x^p - 1)$, then $h^2 = h$, i.e.,

$$\begin{gathered}1 + e_1 + e_2 = (1 + e_1 + e_2)^2 = 1 + e_1^2 + e_2^2 + 2e_1 + 2e_2 + 2e_1e_2 \\ \Rightarrow 2e_1e_2 = -e_1^2 - e_2^2 - e_1 - e_2 = 15e_1^2 + 15e_2^2 + 15e_1 + 15e_2.\end{gathered}$$

THEOREM 3.2. *Let p be a prime $\equiv \pm 1$ (mod 8). Let f_{ij}, g_{ij} as in the table below for $1 \leq i \neq j \leq 2$. Then $f_{12}, f_{21}, g_{12}, g_{21}$ are idempotents over $\mathbb{Z}_{16}[x]/(x^p - 1)$.*

1. *Case* $p+1=8r$.

$r \pmod 8$	f_{ij}	g_{ij}
0	$15e_i$	$1+e_i$
1	$12+10e_i+13e_j$	$5+3e_i+6e_j$
2	$8+3e_i+12e_j$	$9+4e_i+13e_j$
3	$4+e_i+6e_j$	$13+10e_i+15e_j$
4	$7e_i+8e_j$	$1+8e_i+9e_j$
5	$12+2e_i+5e_j$	$5+11e_i+14e_j$
6	$8+4e_i+11e_j$	$9+5e_i+12e_j$
7	$4+9e_i+14e_j$	$13+2e_i+7e_j$

2. *Case* $p-1=8r$.

$r \pmod 8$	f_{ij}	g_{ij}
0	$1+e_i$	$15e_i$
1	$13+2e_i+7e_j$	$4+9e_i+14e_j$
2	$9+5e_i+12e_j$	$8+4e_i+11e_j$
3	$5+11e_i+14e_j$	$12+2e_i+5e_j$
4	$1+8e_i+9e_j$	$7e_i+8e_j$
5	$13+10e_i+15e_j$	$4+e_i+6e_j$
6	$9+4e_i+13e_j$	$8+3e_i+12e_j$
7	$5+3e_i+6e_j$	$12+10e_i+13e_j$

Proof. 1. Suppose $p+1=8r,\ r=8k+1$. Then

$$
\begin{aligned}
&(12{+}10e_1+13e_2)^2\\
&\quad=4e_1^2+9e_2^2+8e_2+4e_1e_2\\
&\quad=4e_1^2+9e_2^2+8e_2+2(14+15e_1^2+15e_2^2+13e_1+13e_2)\\
&\quad=12+10e_1+2e_2+2e_1^2+7e_2^2\\
&\quad=12+10e_1+2e_2+2(2re_1+2re_2-e_1)+7(2re_1+2re_2-e_2)\\
&\quad=12+8e_1+11e_2+2re_1+2re_2\\
&\quad=12+8e_1+11e_2+2(8k+1)e_1+2(8k+1)e_2\\
&\quad=12+10e_1+13e_2
\end{aligned}
$$

and

$$\begin{aligned}
&(5{+}3e_1+6e_2)^2\\
&\quad=9+14e_1+12e_2+9e_1^2+4e_2^2+4e_1e_2\\
&\quad=9+14e_1+12e_2+9e_1^2+4e_2^2+2(14+15e_1^2+15e_2^2+13e_1+13e_2)\\
&\quad=5+8e_1+6e_2+7e_1^2+2e_2^2\\
&\quad=5+8e_1+6e_2+7(2re_1+2re_2-e_1)+2(2re_1+2re_2-e_2)\\
&\quad=5+e_1+4e_2+2re_1+2re_2\\
&\quad=5+e_1+4e_2+2(8k+1)e_1+2(8k+1)e_2\\
&\quad=5+3e_1+6e_2.
\end{aligned}$$

The proof of other cases are similar.

2. Suppose $p-1=8r,\ r=8k+1$. Then

$$\begin{aligned}
&(4+9e_1+14e_2)^2\\
&=8e_1+e_1^2+4e_2^2+12e_1e_2\\
&=8e_1+e_1^2+4e_2^2+6(15e_1^2+15e_2^2+15e_1+15e_2)\\
&=2e_1+10e_2+11e_1^2+14e_2^2\\
&=2e_1+10e_2+11(2re_1+2re_2-e_1+4r)+14(2re_1+2re_2-e_2+4r)\\
&=4r+7e_1+12e_2+2re_1+2re_2\\
&=4(8k+1)+7e_1+12e_2+2(8k+1)e_1+2(8k+1)e_2\\
&=4+9e_1+14e_2
\end{aligned}$$

and

$$\begin{aligned}
&(13+2e_1+7e_2)^2\\
&\quad=9+4e_1^2+e_2^2+4e_1+6e_2+12e_1e_2\\
&\quad=9+4e_1^2+e_2^2+4e_1+6e_2+6(15e_1^2+15e_2^2+15e_1+15e_2)\\
&\quad=9+14e_1+14e_1^2+11e_2^2\\
&\quad=9+14e_1+14(2re_1+2re_2-e_1+4r)+11(2re_1+2re_2-e_2+4r)\\
&\quad=9+4r+5e_2+2re_1+2re_2\\
&\quad=9+4(8k+1)+5e_2+2(8k+1)e_1+2(8k+1)e_2\\
&\quad=13+2e_1+7e_2.
\end{aligned}$$

The proof of other cases are similar. □

DEFINITION 3.3. A $\mathbb{Z}_{16}$-cyclic code is $\mathbb{Z}_{16}$-quadratic residue (QR) code if it is generated by one of the idempotent in above theorem. Hence μ_a is in the group of any $\mathbb{Z}_{16}$-QR code for any $a \in Q$

4. Properties of QR Codes

THEOREM 4.1. *Let p be a prime with $p+1 = 8r$. Following the notations in the Theorem 3.2, let $Q_1 = (f_{12})$, $Q_2 = (f_{21})$, $Q_1' = (g_{12})$, $Q_2' = (g_{21})$.*

Then the following holds for $\mathbb{Z}_{16}$-QR codes Q_1, Q_2, Q_1', and Q_2'.

1. *Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent;*
2. *$Q_1 \cap Q_2 = (\tilde{h})$ and $Q_1 + Q_2 = R_p = \mathbb{Z}_{16}[x]/(x^p - 1)$, where $\tilde{h} = 15h = 15(1 + e_1 + e_2)$;*
3. *$|Q_1| = 16^{(p+1)/2} = |Q_2|$;*
4. *$Q_1 = Q_1' + (\tilde{h})$, $Q_2 = Q_2' + (\tilde{h})$;*
5. *$|Q_1'| = 16^{(p-1)/2} = |Q_2'|$;*
6. *Q_1' and Q_2' are self-orthogonal and $Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$.*

Proof. First we prove the case $r = 8k + 1$. Let x be an element in N; then the map μ_x interchanges e_1 and e_2, i.e.,$\mu_x e_1 = e_2$, $\mu_x e_2 = e_1$. Hence $\mu_x(12+10e_1+13e_2) = (12+10e_2+13e_1)$ and $\mu_x(5+3e1+6e2) = (5 + 3e - 2 + 6e - 1)$. This proves 1. Since $(\tilde{h}) = (15h) = (7h)$ and $7h = 7 + 7e_1 + 7e_2 = 15 + (12 + 10e_1 + 13e_2) + (12 + 13e_1 + 10e_2)$,

$$
\begin{aligned}
&(12 + 10e_1 + 13e_2)7h \\
&= (12 + 10e_1 + 13e_2)[15 + (12 + 10e_1 + 13e_2) + (12 + 13e_1 + 10e_2)] \\
&= 15(12 + 10e_1 + 13e_2) + (12 + 10e_1 + 13e_2)^2 \\
&\quad + (12 + 10e_1 + 13e_2)(12 + 13e_1 + 10e_2) \\
&= (12 + 10e_1 + 13e_2)(12 + 13e_1 + 10e_2).
\end{aligned}
$$

On the other hand, $(12 + 10e_1 + 13e_2)7h = 12(7h) + 10 \cdot \frac{p-1}{2}(7h) + 13 \cdot \frac{p-1}{2}(7h) = (12 + 7 \cdot \frac{p-1}{2})(7h) = 7h$ because $12 + 7 \cdot (p-1)/2 = 12 + 7 \cdot (8r - 1 - 1)/2 = 12r + 5 = 12(8k + 1) + 5 = 17 \equiv 1 \pmod{16}$. Hence $(12 + 10e_1 + 13e_2)(12 + 13e_1 + 10e_2) = 7h$.

By Theorem 2.3, $Q_1 \cap Q_2$ has idempotent generator 7h. Therefore $|Q_1 \cap Q_2| = |(7h)| = |(15h)| = |(\tilde{h})| = 16$. Also by Theorem 2.3, $Q_1 + Q_2$ has idempotent generator $(12+10e_1+13e_2)+(12+13e_1+10e_2)-(12+10e_1+13e_2)(12+13e_1+10e_2) = 8 + 7e_1 + 7e_2 - (7 + 7e_1 + 7e_2) = 1$.

Hence $Q_1 + Q_2 = R_p$, and $|Q_1 + Q_2| = 16^p$. Because $|Q_1 + Q_2| = |Q_1| \cdot |Q_2|/|Q_1 \cap Q_2|$, $|Q_1| = |Q_2| = 16^{(p+1)/2}$. This proves 2 and 3. Observe that $(5+3e_1+6e_2)7h = 3h+5e_1h+10e_2h = 3h+5\cdot(p-1)/2\cdot h+10\cdot(p-1)/2\cdot h = 0$, because $3+15\cdot(p-1)/2 = 3+15\cdot(8r-1-1)/2 = 12r-12 = 12(8k+1)-12 = 0 \pmod{16}$. This implies $Q_1' \cap (7h) = Q_1' \cap (\tilde{h}) = \{0\}$. By Theorem 2.3, $Q_1' + (\tilde{h})$ has the idempotent generator $(5+3e_1+6e_2)+7h-(5+3e_1+6e_2)7h = 5+3e_1+6e_2+7+7e_1+7e_2 = 12+10e_1+13e_2$. Hence $Q_1' + (7h) = Q_1' + (\tilde{h}) = (12 + 10e_1 + 13e_2) = Q_1$. Similarly, $Q_2' + (\tilde{h}) = Q_2$, and $16^{(p+1)/2} = |Q_1| = |Q_1' + (\tilde{h})| = |Q_1'| \cdot |(\tilde{h})| = 16|Q_1'|$. Hence $Q_1' = 16^{(p-1)/2}$. This proves 4 and 5. Finally, by Theorem 2.2. and the fact that -1 is not a square, i.e., $-1 \in N$, $Q_1^{\perp}$ has the idempotent generator $1 - [5 + 3e_1(x^{-1}) + 6e_2(x^{-1})] = 12 + 13e_1(x^{-1}) + 10e_2(x^{-1}) = 12 + 10e_1 + 13e_2$. Hence $Q_1^{\perp} = Q_1'$ and $Q_1' \subseteq Q_1 = Q_1'^{\perp}$, so that Q_1' is self-orthogonal. Similarly, we can show that $Q_2^{\perp} = Q_2'$ and Q_2' is self-orthogonal. The proofs of other cases are similar. □

THEOREM 4.2. *Let p be a prime with $p - 1 = 8r$. Following the notations in the Theorem 3.2, let $Q_1 = (f_{12})$, $Q_2 = (f_{21})$, $Q_1' = (g_{12})$, $Q_2' = (g_{21})$. Then the following holds for $\mathbb{Z}_{16}$-QR codes Q_1, Q_2, Q_1', and Q_2'.*

1. *Q_1 and Q_2 are equivalent and Q_1' and Q_2' are equivalent;*
2. *$Q_1 \cap Q_2 = (h)$ and $Q_1 + Q_2 = R_p = \mathbb{Z}_{16}[x]/(x^p - 1)$.*
3. *$|Q_1| = 16^{(p+1)/2} = |Q_2|$;*
4. *$Q_1 = Q_1' + (h)$, $Q_2 = Q_2' + (h)$;*
5. *$|Q_1'| = 16^{(p-1)/2} = |Q_2'|$;*
6. *$Q_1^{\perp} = Q_1'$ and $Q_2^{\perp} = Q_2'$.*

Proof. First we prove the case $r = 8k + 1$. Let x be an element in N; then the map μ_x interchanges e_1 and e_2, i.e.,$\mu_x e_1 = e_2$, $\mu_x e_2 = e_1$. Hence $\mu_x(13 + 7e_1 + 2e_2) = (13 + 7e_2 + 2e_1)$ and $\mu_x(4 + 14e1 + 9e2) = (4 + 14e - 2 + 9e - 1)$. This proves 1. Since $(h) = (9h)$ and $9h = 9 + 9e_1 + 9e_2 = 15 + (13 + 7e_1 + 2e_2) + (13 + 2e_1 + 7e_2)$,

$$
\begin{aligned}
&(13 + 7e_1 + 2e_2)9h \\
&\quad = (13 + 7e_1 + 2e_2)[15 + (13 + 7e_1 + 2e_2) + (13 + 2e_1 + 7e_2)] \\
&\quad = 15(13 + 7e_1 + 2e_2) + (13 + 7e_1 + 2e_2)^2 \\
&\qquad + (13 + 7e_1 + 2e_2)(13 + 2e_1 + 7e_2) \\
&\quad = (13 + 7e_1 + 2e_2)(13 + 2e_1 + 7e_2).
\end{aligned}
$$

On the other hand, $(13+7e_1+2e_2)9h = 13(9h)+7\cdot\frac{p-1}{2}(9h)+2\cdot\frac{p-1}{2}(9h) = (13+9\cdot\frac{p-1}{2})9h = 9h$ because $13+9\cdot(p-1)/2 = 13+9\cdot(8r+1-1)/2 = 4r+13 = 4(8k+1)+13 = 17 \equiv 1 \pmod{16}$. Hence $(13+7e_1+2e_2)(13+2e_1+7e_2) = 9h$ By Theorem 2.3, $Q_1 \cap Q_2$ has idempotent generator 9h. Therefore $|Q_1 \cap Q_2| = |(9h)| = |(h)| = 16$. Also by Theorem 2.3, Q_1+Q_2 has idempotent generator $(13+7e_1+2e_2)+(13+2e_1+7e_2)-(13+7e_1+2e_2)(13+2e_1+7e_2) = 10+9e_1+9e_2-(9+9e_1+9e_2) = 1$. Hence $Q_1+Q_2 = R_p$, and $|Q_1+Q_2| = 16^p$. Because $|Q_1+Q_2| = |Q_1|\cdot|Q_2|/|Q_1\cap Q_2|$, $|Q_1| = |Q_2| = 16^{(p+1)/2}$. This proves 2 and 3. Observe that $(4+14e_1+9e_2)9h = 4h+14e_1h+e_2h = 4h+14\cdot(p-1)/2\cdot h+(p-1)/2\cdot h = 0$, because $4+15\cdot(p-1)/2 = 4+15\cdot(8r+1-1)/2 = 12r+4 = 12(8k+1)+4 = 0 \pmod{16}$. This implies $Q_1'\cap(9h) = Q_1'\cap(h) = \{0\}$. By Theorem 2.3, $Q_1'+(9h)$ has the idempotent generator $(4+14e_1+9e_2)+9h-(4+14e_1+9e_2)9h = 4+14e_1+9e_2+9+9e_1+9e_2 = 13+7e_1+2e_2$. Hence $Q_1'+(9h) = Q_1'+(h) = (13+7e_1+2e_2) = Q_1$. Similarly, $Q_2'+(h) = Q_2$, and $16^{(p+1)/2} = |Q_1| = |Q_1'+(h)| = |Q_1'|\cdot|(h)| = 16|Q_1'|$. Hence $Q_1' = 16^{(p-1)/2}$. Similarly, $Q_2' = 16^{(p-1)/2}$ This proves 4 and 5. Finally, by Theorem 2.2. and the fact that -1 is a square, i.e., $-1 \in Q$, $Q_1^{\perp}$ has the idempotent generator $1-[13+7e_1(x^{-1})+2e_2(x^{-1})] = 4+9e_1(x^{-1})+14e_2(x^{-1}) = 4+14e_1+9e_2$ which is the idempotent generator of Q_2'; this proves that $Q_1^{\perp} = Q_2'$. Similarly, we can show that $Q_2^{\perp} = Q_1'$. The proofs of other cases are similar. □

References

[1] F.J.MacWilliams and N.J.A.Sloane, *Theory of error-correcting codes*, North-Holland, Amsterdam, 1978.

[2] V.Pless, *Introduction to the Theory of Error-Correcting Codes*, 2nd ed., Wiley-Interscience, New York, 1989

[3] Z.Qian, and V.Pless, Cyclic Codes and Quadratic Residue Codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **42** (1996), 1594–1600

[4] M.H.Chiu, S.S.T.Yau, and Y.Yu, $\mathbb{Z}_8$-*Cyclic Codes and Quadratic Residue Codes*, Advances in Applied Mathematics **25** (2000), 12-33

Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea