Kangweon-Kyungki Math. Jour. **13** (2005), No. 1, pp. 103–112

GENERATOR POLYNOMIALS OF THE p-ADIC QUADRATIC RESIDUE CODES

Sung Jin Kim

Abstract. Using the Newton's identities, we give the inductive formula for the generator polynomials of the p-adic quadratic residue codes.

1. Introduction

Let p be a prime. We use the symbol $\mathbb{Z}_{p^a}$ to denote the ring $\mathbb{Z}/p^a\mathbb{Z}$ of integers modulo p^a for any positive integer a, and $\mathbb{Z}_{p^\infty}$ for the ring of p-adic integers. An element $u \in \mathbb{Z}_{p^a}$ may be written uniquely as a finite sum

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

and any element of $\mathbb{Z}_{p^\infty}$ as an infinite sum

$$u = u_0 + pu_1 + p^2u_2 + \cdots ,$$

where $0 \le u_i \le p-1$. The units in $\mathbb{Z}_{p^a}$ or $\mathbb{Z}_{p^\infty}$ are precisely those u for which $u_0 \neq 0$. $\mathbb{Z}_{p^a}$ has characteristic p^a, and $\mathbb{Z}_{p^\infty}$ has characteristic 0. The finite field of $q = p^a$ elements will be denoted by $\mathbb{F}_q$.

For a positive integer m, the Galois extension of $\mathbb{Z}_q$ of degree m is denoted by $GR(q,m)$. It is called a Galois ring and it can be realized as

$$GR(q,m) = \mathbb{Z}_q[X]/\langle h(X)\rangle$$

for any monic polynomial of degree m in $\mathbb{Z}[X]$, which is irreducible over $\mathbb{Z}_p$. We may choose $h(X)$ so that its root ζ is a (p^m-1)th root of unity, and $GR(q,m) = \mathbb{Z}_q[\zeta]$. See [2, 6] for details. Thus any element $s \in GR(q,m)$ can be written as

$$s = b_0 + b_1\zeta + b_2\zeta^2 + \cdots + b_{m-1}\zeta^{m-1}, \quad b_i \in \mathbb{Z}_q.$$

Received January 9, 2005.
2000 Mathematics Subject Classification: 94B15.
Key words and phrases: quadratic residue codes, p-adic codes.

The map $\mathcal{F}r : GR(q,m) \to GR(q,m)$ defined by

$$\mathcal{F}r(b_0 + b_1\zeta + \cdots + b_{m-1}\zeta^{m-1}) = b_0 + b_1\zeta^p + \cdots + b_{m-1}\zeta^{p(m-1)}$$

is called the Frobenius map. It is the generator of the Galois group of $GR(q,m)$ over $\mathbb{Z}_q$. In particular, the elements of $GR(q,m)$ fixed under $\mathcal{F}r$ is $\mathbb{Z}_q$.

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

Let $n \neq 2, 3$ be a prime. Let $Q \subset \mathbb{Z}_n$ denote the set of nonzero quadratic residues modulo n and N denote the set of nonresidues modulo n.

Let $p < n$ be another prime which is a quadratic residue mod n. Let $q = p^a$, where a is a positive integer. Let m be the order of p modulo n. Then $n \mid p^m - 1$ and hence the Galois ring $GR(q,m)$ contains a primitive nth root of unity $\alpha = \zeta^{(p^m-1)/n}$.

Let

$$Q_q(X) = \prod_{i \in Q}(X - \alpha^i), \quad N_q(X) = \prod_{j \in N}(X - \alpha^j). \tag{1}$$

Then the degrees of $Q_q(x)$ and $N_q(x)$ are both $\frac{n-1}{2}$, and

$$X^n - 1 = \prod_{i=0}^{n-1}(X - \alpha^i) = (X-1)Q_q(X)N_q(X).$$

Since $pQ = Q$, we have that

$$\mathcal{F}rQ_q(X) = \prod_{i \in Q}(X - \alpha^{ip}) = \prod_{i \in pQ}(X - \alpha^i) = Q_q(X),$$

and similarly $pN = N$ implies that $\mathcal{F}rN_q(X) = N_q(X)$. Thus $Q_q(X)$ and $N_q(X)$ have coefficients from $\mathbb{Z}_q$. Furthermore,

$$Q_{p^b}(X) \equiv Q_{p^a}(X) \pmod{p^a}$$

for all $a \leq b < \infty$. We define Q_{p^∞} to be the p-adic limits of Q_{p^a}. In particular,

$$Q_{p^a}(X) \equiv Q_{p^\infty}(X) \pmod{p^a}. \tag{2}$$

The similar results hold for $N_q(X)$.

Definition 2.1. The cyclic codes of $\mathbb{Z}_q[X]/(X^n-1)$ with generator polynomials $Q_q(X)$, $(X-1)Q_q(X)$, $N_q(X)$ and $(X-1)N_q(X)$, respectively, are called the quadratic residue codes over $\mathbb{Z}_q$ and denoted by $\mathcal{Q}_q$, $\overline{\mathcal{Q}}_q$, $\mathcal{N}_q$ and $\overline{\mathcal{N}}_q$, respectively. When $q=p^\infty$, then they are called the p-adic quadratic residue codes.

The *reciprocal polynomial* of a polynomial $h(X)=a_0+a_1X+\cdots+a_kX^k$ of degree k is the polynomial

$$\bar{h}(X)=a_k+a_{k-1}X+\cdots+a_0X^k=h(X^{-1})X^k.$$

If $\bar{h}(X)=h(X)$, it is called a *self reciprocal polynomial.*

Theorem 2.2. *Let $Q_q(X)$ and $N_q(X)$ be as in* (1).

(i) *If $n=4k-1$, then $N_q(X)$ is the reciprocal polynomial to $-Q_q(X)$.*
(ii) *If $n=4k+1$, then $Q_q(X)$ and $N_q(X)$ are self reciprocal polynomial.*

Proof. Let $\mathbb{Z}_n{}^*=\{1,2,3,\cdots n-1\}$. First note that

$$\sum_{i\in\mathbb{Z}_n{}^*} i=1+2+\cdots+(n-1)=n\cdot\frac{(n-1)}{2}\equiv 0 \pmod{n}.$$

On the other hand, for any $b\in N$ we have that $bQ=N$ and hence

$$\sum_{i\in\mathbb{Z}_n{}^*} i=\sum_{i\in Q} i+\sum_{j\in N} j=\sum_{i\in Q} i+\sum_{i\in Q} bi=(1+k)\sum_{i\in Q} i.$$

Taking $k\neq -1$, we obtain that

$$\sum_{i\in Q} i=0. \tag{3}$$

Furthermore, recall that $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$. Hence -1 is a quadratic residue modulo n iff $n\equiv 1 \pmod 4$.

(i) We have $|Q|=|N|=2k-1$. Also -1 is a nonresidue and hence $N=-Q$. We will show that $N_q(X)=-Q_q(X^{-1})\cdot X^{2k-1}$. Indeed,

$$\begin{aligned}-Q_q(X^{-1})\cdot X^{2k-1}&=-\left(\prod_{i\in Q}(X^{-1}-\alpha^i)\right)\cdot X^{2k-1}=-\prod_{i\in Q}(X^{-1}-\alpha^i)X\\&=\prod_{i\in Q}(\alpha^iX-1)=\prod_{i\in Q}\alpha^i\cdot\prod_{i\in Q}(X-\alpha^{-i})\\&=\alpha^0\cdot\prod_{i\in Q}(X-\alpha^{-i})=\prod_{j\in N}(X-\alpha^j)=N_q(X).\end{aligned}$$

Hence, $N_q(X)$ is the reciprocal polynomial to $-Q_q(X)$.

(ii) In this case we have that $|Q| = |N| = 2k$ and $Q = -Q$, $N = -N$. We have that

$$\begin{aligned} Q_q(X^{-1}) \cdot X^{2k} &= \left(\prod_{i\in Q}(X^{-1} - \alpha^i)\right) \cdot X^{2k} = \prod_{i\in Q}(X^{-1} - \alpha^i)X \\ &= \prod_{i\in Q}(1 - \alpha^i X) = \prod_{i\in Q}(\alpha^i X - 1) = \prod_{i\in Q}\alpha^i(X - \alpha^{-i}) \\ &= \prod_{i\in Q}\alpha^i \cdot \prod_{i\in Q}(X - \alpha^{-i}) = \alpha^0 \cdot \prod_{i\in Q}(X - \alpha^{-i}) = \prod_{i\in Q}(X - \alpha^i) \\ &= Q_q(X). \end{aligned}$$

Similarly, we can show that $N_q(X) = N_q(X^{-1}) \cdot X^{2k}$. Hence $Q_q(X)$ and $N_q(X)$ are self reciprocal polynomials. □

3. Generator polynomials of quadratic residue codes

As in the previous section, let $n \neq 2, 3$ be a prime, $Q \subset \mathbb{Z}_n$ denote the set of nonzero quadratic residues modulo n and N the set of nonresidues modulo n. Let

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

THEOREM 3.1. *Let* $R = \mathbb{Z}_q[X]/(X^n - 1)$.

(i) *Suppose* $n = 4k - 1$. *In* R, *we have*

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

(ii) *Suppose $n = 4k+1$. In R, we have*

$$f_Q{}^2 = \frac{(n-5)}{4} f_Q + \frac{(n-1)}{4} f_N + \frac{(n-1)}{2},$$
$$f_N{}^2 = \frac{(n-1)}{4} f_Q + \frac{(n-5)}{4} f_N + \frac{(n-1)}{2},$$
$$f_Q \cdot f_N = \frac{(n-1)}{4} f_Q + \frac{(n-1)}{4} f_N.$$

Proof. These follows from Perron's Theorem (p.519 in [7]). □

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

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

We define $s_0(X_1, X_2, \cdots, X_t) = 1$. It is clear that
(4)

$$(X - a_1) \cdots (X - a_t) = X^t - s_1(a) X^{t-1} + \cdots \pm s_t(a) = \sum_{i=0}^{t} (-1)^i s_i(a) X^{t-i},$$

where $s_i(a) = s_i(a_1, a_2, \cdots, a_t)$.

For all $i \geq 1$, the i-power symmetric polynomials are defined by

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

The following Newton's identities are well-known [4].

Theorem 3.2 (Newton's identities). *For each $i \geq 1$,*

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

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 $Q = \{q_1, q_2, \cdots q_t\}$, $N = \{n_1, n_2, \cdots, n_t\}$.

Theorem 3.3. *Let $\lambda = -f_Q(\alpha)$ and $\mu = -f_N(\alpha)$. Then*

(i) $\lambda + \mu = 1$.
(ii) *If $n = 4k-1$, then λ and μ satisfy $x^2 - x + k = 0$.*
(iii) *If $n = 4k+1$, then λ and μ satisfy $x^2 - x - k = 0$.*

Proof. (i) We have that

$$0 = \alpha^{n-1} + \alpha^{n-2} + \cdots + \alpha + 1 = f_Q(\alpha) + f_N(\alpha) + 1.$$

Thus $\lambda + \mu = 1$.

(ii) By Theorem 3.1(i) we have that

$$\begin{aligned}\lambda^2-\lambda &= f_Q(\alpha)^2+f_Q(\alpha)=\frac{4k-4}{4}f_Q(\alpha)+\frac{4k}{4}f_N(\alpha)+f_Q(\alpha)\\ &= k(f_Q(\alpha)+f_N(\alpha))=k(-1)=-k.\end{aligned}$$

Similarly, we have that

$$\begin{aligned}\mu^2-\mu &= f_N(\alpha)^2+f_N(\alpha)=\frac{4k}{4}f_Q(\alpha)+\frac{4k-4}{4}f_N(\alpha)+f_N(\alpha)\\ &= k(f_Q(\alpha)+f_N(\alpha))=k(-1)=-k.\end{aligned}$$

(iii) It can be proved in a similar manner. □

Let

$$\begin{aligned}s_i(\alpha^Q)&=s_i(\alpha^{q_1},\alpha^{q_2},\cdots,\alpha^{q_t}), \quad s_i(\alpha^N)=s_i(\alpha^{n_1},\alpha^{n_2},\cdots,\alpha^{n_t}),\\ p_i(\alpha^Q)&=p_i(\alpha^{q_1},\alpha^{q_2},\cdots,\alpha^{q_t}), \quad p_i(\alpha^N)=p_i(\alpha^{n_1},\alpha^{n_2},\cdots,\alpha^{n_t}).\end{aligned}$$

THEOREM 3.4. *Let $Q_{p^\infty}(X)=a_0X^t+a_1X^{t-1}+\cdots+a_t$. Then $a_0=1$, $a_1=\lambda$ and the other coefficients $a_i\in\mathbb{Z}_{p^\infty}$ can be determined inductively by the formula*

$$a_i=-\frac{p_ia_0+p_{i-1}a_1+p_{i-2}a_2+\cdots+p_1a_{i-1}}{i},$$

where $a_i=s_i(\alpha^Q)$ and $p_i=p_i(\alpha^Q)$. Moreover each a_i is linear in λ, i.e. has the form $\alpha_i\lambda+\beta_i$. Analogous statements hold for $N_{p^\infty}(X)=b_0X^t+b_1X^{t-1}+\cdots+b_t$ with $b_0=1$, $b_1=\mu$. In particular, $N_{2^\infty}(X)$ can be obtained by replacing λ in $Q_{p^\infty}(X)$ by $\mu=1-\lambda$.

Proof. The formula for a_i follows from the Newton's identities (5) and the fact that $a_i=(-1)^is_i$. We will use the induction to prove that each a_i is linear in λ. $a_1=\lambda$ has the right form. Suppose a_j all are linear in λ. Then $s_j=(-1)^ja_j$ is linear in λ. Note that each p_{i-j} is linear in λ by Lemma 4.1. Since λ^2 is linear in λ by Theorem 3.3, each $p_{i-j}s_j$ is linear, and thus it is now clear from the formula that a_i is linear in λ. □

4. Examples

PROPOSITION 4.1. (i) $p_i(\alpha^Q)=\begin{cases}-\lambda, & i\in Q,\\ \lambda-1, & i\in N.\end{cases}$

(ii) $p_i(\alpha^N) = \begin{cases} -\mu, & i \in Q, \\ \mu - 1, & i \in N. \end{cases}$

Proof. (i) If $i \in Q$, then $p_i(\alpha^Q) = f_Q(\alpha) = -\lambda$. If $i \in N$, then $p_i(\alpha^Q) = f_N(\alpha) = \lambda - 1$.

(ii) If $i \in Q$, then $p_i(\alpha^N) = f_N(\alpha) = -\mu$. If $i \in N$, then $p_i(\alpha^N) = f_Q(\alpha) = 1 - \mu$. □

EXAMPLE 4.2. We consider the case $n = 7$, $p = 2$. Then $k = 2$ so that $7 = 4k - 1$, and λ is a 2-adic number satisfying

$$\lambda^2 - \lambda + k = \lambda^2 - \lambda + 2 = 0.$$

Its 2-adic expansion is chosen to be

$$\lambda = 0 + 2^1 + 2^2 + 2^5 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{11} + 2^{12} + 2^{15} + 2^{16} + 2^{17} + \cdots .$$

We have $Q = \{1, 4, 2\}$ and $N = \{3, 5, 6\}$. Thus $p_1 = p_2 = p_4 = -\lambda$, and $p_3 = p_5 = p_6 = \lambda - 1$. Write

$$Q_{2^\infty}(X) = X^3 + a_1X^2 + a_2X + a_3.$$

Then $a_1 = \lambda$ and

$$a_2 = -\frac{p_2a_0 + p_1a_1}{2} = -\frac{-\lambda - \lambda^2}{2} = \frac{\lambda + \lambda^2}{2} = \lambda - 1$$

$$a_3 = -\frac{p_3a_0 + p_2a_1 + p_1a_2}{3} = -\frac{\lambda - 1 - \lambda^2 - \lambda^2 + \lambda}{3} = -1,$$

and hence

$$Q_{2^\infty}(X) = X^3 + \lambda X^2 + (\lambda - 1)X - 1.$$

The polynomial $Q_{2^\infty}(X)$ is a generator for the 2-*adic Hamming code* of length 7. By Theorem 2.2 or Theorem 3.4,

$$N_{2^\infty}(X) = -\bar{Q}_{2^\infty}(X) = X^3 - (\lambda - 1)X^2 - \lambda X - 1,$$

and

$$X^7 - 1 = (X - 1)Q_{2^\infty}(X)N_{2^\infty}(X).$$

EXAMPLE 4.3. We next consider the case $n = 23$, $p = 2$. Then $k = 6$ so that $23 = 4k - 1$, and λ is a 2-adic number satisfying

$$\lambda^2 - \lambda + 6 = 0.$$

Its 2-adic expansion is chosen to be

$$\lambda = 0 + 2^1 + 2^3 + 2^5 + 2^6 + 2^7 + 2^8 + 2^{11} + 2^{14} + 2^{16} + 2^{17} + \cdots .$$

We have $Q = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ and recall that $p_i = -\lambda$ for $i \in Q$ and $p_i = \lambda - 1$ for $i \in N$. Write

$$\begin{aligned} Q_{2^\infty}(X) = X^{11} + a_1 X^{10} + a_2 X^9 + a_3 X^8 + a_4 X^7 + a_5 X^6 \\ + a_6 X^5 + a_7 X^4 + a_8 X^3 + a_9 X^2 + a_{10} X + a_{11}. \end{aligned}$$

Then $a_1 = \lambda$ and

$$\begin{aligned} a_2 &= -\frac{p_2 a_0 + p_1 a_1}{2} = -\frac{-\lambda - \lambda^2}{2} = \frac{\lambda + \lambda^2}{2} = \lambda - 3 \\ a_3 &= -\frac{p_3 a_0 + p_2 a_1 + p_1 a_2}{3} = -\frac{-\lambda + (-\lambda)\lambda + (-\lambda)(\lambda - 3)}{3} = -4 \\ a_4 &= -\frac{p_4 a_0 + p_3 a_1 + p_2 a_2 + p_1 a_3}{4} \\ &= -\frac{-\lambda + (-\lambda)\lambda + (-\lambda)(\lambda - 3) + (-\lambda)(-4)}{4} = -\lambda - 3 \\ &\vdots \end{aligned}$$

and

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

The polynomial $Q_{2^\infty}(X)$ is a generator for the 2-*adic Golay code* of length 23. By Theorem 2.2,

$$\begin{aligned} N_{2^\infty}(X) = -\bar{Q}_{2^\infty}(X) = X^{11} - (\lambda - 1)X^{10} - (\lambda + 2)X^9 - 4X^8 + (\lambda - 4)X^7 \\ +(2\lambda - 3)X^6 + (2\lambda + 1)X^5 + (\lambda + 3)X^4 + 4X^3 - (\lambda - 3)X^2 - \lambda X - 1, \end{aligned}$$

and

$$X^{23} - 1 = (X - 1)Q_{2^\infty}(X)N_{2^\infty}(X).$$

EXAMPLE 4.4. Case $n = 11$, $p = 3$. Then $k = 3$ so that $11 = 4k - 1$, and λ is a 3-adic number satisfying

$$\lambda^2 - \lambda + 3 = 0.$$

Its 3-adic expansion is chosen to be

$$\lambda = 0 + 3^1 + 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 2\cdot 3^6 + 3^8 + 2\cdot 3^9 + 2\cdot 3^{11} + 2\cdot 3^{13} + 3^{14} + 2\cdot 3^{15} + \cdots .$$

We have $Q = \{1, 3, 4, 5, 9\}$ and $N = \{2, 6, 7, 8, 10\}$. Thus $p_1 = p_3 = p_4 = p_5 = -\lambda$, and $p_2 = \lambda - 1$. Write

$$Q_{3^\infty}(X) = X^5 + a_1 X^4 + a_2 X^3 + a_3 X^2 + a_4 X + a_5.$$

$$\begin{aligned}
a_1 &= \lambda \\
a_2 &= -\frac{p_2 a_0 + p_1 a_1}{2} = -\frac{(\lambda-1)+(-\lambda)\lambda}{2} = -1 \\
a_3 &= -\frac{p_3 a_0 + p_2 a_1 + p_1 a_2}{3} = -\frac{-\lambda+(\lambda-1)\lambda+(-\lambda)(-1)}{3} = 1 \\
a_4 &= -\frac{p_4 a_0 + p_3 a_1 + p_2 a_2 + p_1 a_3}{4} \\
&= -\frac{-\lambda+(-\lambda)\lambda+(\lambda-1)(-1)+(-\lambda)}{4} = \lambda - 1 \\
a_5 &= -\frac{p_5 a_0 + p_4 a_1 + p_3 a_2 + p_2 a_3 + p_1 a_4}{5} \\
&= -\frac{-\lambda+(-\lambda)\lambda+(-\lambda)(-1)+(\lambda-1)+(-\lambda)(\lambda-1)}{5} = -1
\end{aligned}$$

and hence

$$Q_{3^\infty}(X) = X^5 + \lambda X^4 - X^3 + X^2 + (\lambda-1)X - 1.$$

The polynomial $Q_{3^\infty}(X)$ is a generator for *the* 3-*adic Golay code* of length 11. By Theorem 2.2,

$$N_{3^\infty}(X) = -\bar{Q}_{3^\infty}(X) = X^5 - (\lambda-1)X^4 - X^3 + X^2 - \lambda X - 1,$$

and

$$X^{11} - 1 = (X-1)Q_{3^\infty}(X)N_{3^\infty}(X).$$

EXAMPLE 4.5. Case $n = 41$, $p = 2$. Then $k = 10$ so that $41 = 4k+1$, and λ is a 2-adic number satisfying

$$\lambda^2 - \lambda - 10 = 0.$$

Its 2-adic expansion is chosen to be

$$\lambda = 0 + 2^1 + 2^3 + 2^4 + 2^7 + 2^{10} + 2^{11} + 2^{14} + 2^{15} + \cdots$$

and we can compute that

$$\begin{aligned}
Q_{2^\infty}(X) =& X^{20} + \lambda X^{19} + (\lambda+5)X^{18} + (2\lambda+7)X^{17} \\
&+ (4\lambda+5)X^{16} + (3\lambda+13)X^{15} + (4\lambda+13)X^{14} + (6\lambda+8)X^{13} \\
&+ (4\lambda+16)X^{12} + (4\lambda+15)X^{11} + (6\lambda+7)X^{10} + (4\lambda+15)X^{9} \\
&+ (4\lambda+16)X^{8} + (6\lambda+8)X^{7} + (4\lambda+13)X^{6} + (3\lambda+13)X^{5} \\
&+ (4\lambda+5)X^{4} + (2\lambda+7)X^{3} + (\lambda+5)X^{2} + \lambda X + 1
\end{aligned}$$

and by Theorem 3.4

$$\begin{aligned} N_{2^\infty}(X) = & X^{20} - (\lambda - 1)X^{19} - (\lambda - 6)X^{18} - (2\lambda - 9)X^{17} \\ & - (4\lambda - 9)X^{16} - (3\lambda - 16)X^{15} - (4\lambda - 17)X^{14} - (6\lambda - 14)X^{13} \\ & - (4\lambda - 20)X^{12} - (4\lambda - 19)X^{11} - (6\lambda - 13)X^{10} - (4\lambda - 19)X^{9} \\ & - (4\lambda - 20)X^{8} - (6\lambda - 14)X^{7} - (4\lambda - 17)X^{6} - (3\lambda - 16)X^{5} \\ & - (4\lambda - 9)X^{4} - (2\lambda - 9)X^{3} - (\lambda - 6)X^{2} - (\lambda - 1)X + 1. \end{aligned}$$

The polynomial $Q_{2^\infty}(X)$ is a generator for the 2-adic quadratic residue code of length 41.

References

[1] A.R. Calderbank and N.J.A. Sloane, *Modular and p-adic cyclic codes*, Des., Codes Cryptogr. **6** (1995), 21-35.
[2] S.T. Dougherty and Y.H. Park *Modular cyclic codes* (2004), submitted.
[3] P. Kanwar and S.R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields Appl. **3** (1997), 334–352.
[4] W.K.Nicholson, Introduction to Abstract Algera, PWS, Boston, 1993.
[5] S.Y. Kim, *Liftings of the ternary Golay code*, Master's Thesis, Kangwon National University, 2004.
[6] B.R. McDonald, *Finite rings with identity*, Dekker, New York, 1974.
[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-correcting Codes*, North-Holland, Amsterdam, 1977.
[8] V.S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over* $\mathbb{Z}_4$, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.

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