8

Quadratic residue codes

8.1 INTRODUCTION

Let p be an odd prime. Let Q denote the set of all quadratic residues mod p and N the set of all quadratic non-residues mod p. Let s be another prime which is a quadratic residue mod p. Then $s \in Q$ and it follows (from Proposition 5.6) that Q is closed with respect to multiplication by s. Therefore, Q is partitioned as a disjoint union of cyclotomic cosets modulo p under multiplication by s. Similarly, N is partitioned as a union of cyclotomic cosets modulo p under multiplication by s. Let α be a primitive pth root of unity in some extension of the field GF(s). By Euler's theorem, there exists a positive integer m such that $s^m \equiv 1 \pmod p$. Let ρ be a primitive element of an extension GF(s^m) of GF(s) of degree m. We may then take

$$\alpha = \rho^{(s^m - 1)/p}$$

It follows from Theorem 7.3 that

$$q(x) = \prod_{i \in Q} (x - \alpha^i) \qquad n(x) = \prod_{j \in N} (x - \alpha^j) \tag{8.1}$$

are polynomials with coefficients in GF(s).

Lemma 8.1

$$x^p - 1 = (x - 1)q(x)n(x)$$

Proof

As every α^i is a pth root of unity, every root of $q(x)$ and every root of $n(x)$ is a root of $x^p - 1$. Therefore, $q(x)$ and $n(x)$ divide $x^p - 1$. Also $Q \cap N = \phi$ and $q(x)n(x) | x^p - 1$. Clearly $x - 1 | x^p - 1$ and 1 is neither a root of $q(x)$ nor of $n(x)$. Therefore

$$(x - 1)q(x)n(x) | (x^p - 1)$$

But both polynomials are monic and of the same degree p. Therefore

$$x^p - 1 = (x-1)q(x)n(x)$$

Set

$$\mathscr{R} = \mathrm{GF(s)}[x]/\langle x^p - 1\rangle$$

where $\langle x^p - 1\rangle$ denotes the ideal of $\mathrm{GF}(s)[x]$ generated by $x^p - 1$.

Definition 8.1

Quadratic residue codes $\mathscr{F}, \mathscr{N}, \bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ are the cyclic codes of length p over $\mathrm{GF}(s)$ generated by the polynomials $q(x)$, $n(x)$, $(x-1)q(x)$ and $(x-1)n(x)$ respectively, i.e. these are the ideals in $\mathscr{R}$ generated by the respective polynomials.

It is clear that

$$\bar{\mathscr{F}} \subseteq \mathscr{F} \quad \text{and} \quad \bar{\mathscr{N}} \subseteq \mathscr{N}$$

As

$$\text{degree of } q(x) = \text{degree of } n(x) = \frac{p-1}{2}$$

both $\mathscr{F}$ and $\mathscr{N}$ are linear codes over $\mathrm{GF}(s)$ of dimension

$$p - \frac{p-1}{2} = \frac{p+1}{2}$$

each. Similarly, $\bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ are linear codes over $\mathrm{GF}(s)$ of dimension $(p-1)/2$ each.

Let $s = 2$ and $p = 7$. Then, 1, 2, 4 are quadratic residues mod 7 and 3, 5, 6 are quadratic non-residues mod 7. Consider the field

$$\mathbb{B}[x]/\langle x^3 + x + 1\rangle$$

of order 8. Then

$$\alpha = x + \langle x^3 + x + 1\rangle$$

is a primitive 7th root of unity having $x^3 + x + 1$ as its minimal polynomial over $\mathbb{B}$. Now

$$\begin{aligned} q(x) &= (x+\alpha)(x+\alpha^2)(x+\alpha^4) \\ &= x^3 + x^2(\alpha + \alpha^2 + \alpha^4) + x(\alpha^3 + \alpha^5 + \alpha^6) + 1 \\ &= x^3 + x[\alpha^3 + \alpha^2(\alpha+1) + (\alpha+1)^2] + 1 \\ &= x^3 + x(\alpha^2 + \alpha^2 + 1) + 1 \\ &= x^3 + x + 1 \end{aligned}$$

So, the quadratic residue code $\mathscr{F}$ of length 7 over $\mathbb{B}$ is generated by

$$x^3 + x + 1 + \langle x^7 + 1\rangle = q(x) + \langle x^7 + 1\rangle$$

Observe that

$$x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)$$

and, therefore, the other quadratic residue code $\mathcal{N}$ is generated by

$$x^3+x^2+1=n(x)$$

Now

$$\begin{aligned}
q(x^3)+\langle x^7+1\rangle &= (x^3)^3+x^3+1+\langle x^7+1\rangle\\
&= x^3+x^2+1+\langle x^7+1\rangle\\
&= n(x)+\langle x^7+1\rangle \in \mathcal{N}\\
q(x^5)+\langle x^7+1\rangle &= (x^5)^3+x^5+1+\langle x^7+1\rangle\\
&= x^5+x+1+\langle x^7+1\rangle\\
&= (x^5+x^4+x^2)+(x^4+x^3+x)\\
&\quad +x^3+x^2+1+\langle x^7+1\rangle\\
&= (x^3+x^2+1)(x^2+x+1)+\langle x^7+1\rangle\\
q(x^6)+\langle x^7+1) &= x^4+x^6+1+\langle x^7+1\rangle\\
&= (x^3+x^2+1)^2+\langle x^7+1\rangle
\end{aligned}$$

Thus

$$q(x^n)+\langle x^7+1\rangle \in \mathcal{N}$$

whenever n is any quadratic non-residue mod 7.

Observe that the map $x \to x^5$ maps

$$x^6+x^2+1+\langle x^7+1\rangle=(x^3+x+1)^2+\langle x^7+1\rangle \in \mathcal{F}$$

onto

$$\begin{aligned}
(x^5)^6+(x^5)^2+1+\langle x^7+1\rangle &= x^2+x^3+1+\langle x^7+1\rangle\\
&= x^3+x^2+1+\langle x^7+1\rangle
\end{aligned}$$

which generates $\mathcal{N}$ and the map $x \to x^6$ maps

$$x^5+x^4+1+\langle x^7+1\rangle=(x^3+x+1)(x^2+x+1)+\langle x^7+1\rangle \in \mathcal{F}$$

onto the generator

$$x^3+x^2+1+\langle x^7+1\rangle$$

of $\mathcal{N}$. Thus for every non-residue n modulo 7, there is an element

$$a(x)+\langle x^7+1\rangle \in \mathcal{F}$$

which maps onto the generator

$$x^3+x^2+1+\langle x^7+1\rangle$$

of $\mathcal{N}$. Also the map $x \to x^n$ determines a permutation

$$\boldsymbol{\sigma}:\{0,1,2,\ldots,6\} \to \{0,1,2,\ldots,6\}$$

as g.c.d.$(n, 7) = 1$. For example, for $n = 3$, the permutation determined is

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix} = (1 \quad 3 \quad 2 \quad 6 \quad 4 \quad 5)$$

In general

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \end{pmatrix}$$

where for $1 \leq i \leq 6$, $\bar{i}$ denotes the least non-negative remainder on dividing ni by 7. The degrees of the generators of $\mathscr{F}$ and $\mathscr{N}$ being 3 each, the number of elements in the two codes are the same. Hence, it follows that the quadratic residue codes $\mathscr{F}$ and $\mathscr{N}$ are equivalent. Similarly, the expurgated quadratic residue codes $\bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ generated by

$$(x + 1)(x^3 + x + 1) \quad \text{and} \quad (x + 1)(x^3 + x^2 + 1)$$

respectively are also equivalent.

Theorem 8.1

The quadratic residue codes $\mathscr{F}$ and $\mathscr{N}$ of length p over GF(s) generated by $q(x)$ and $n(x)$ are equivalent. Also the expurgated quadratic residue codes $\bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ of length p over GF(s) are equivalent.

Proof

Let n be a fixed quadratic non-residue mod p. Then there exists a positive integer r such that

$$nr \equiv 1 \pmod{p}$$

As 1 is always a quadratic residue, nr is a quadratic residue. But, then n being a non-residue it follows that r is a quadratic non-residue mod p. For any $i \in Q$, it follows that ir is a non-residue mod p. Now

$$q(x^n) = \prod_{i \in Q} (x^n - \alpha^i)$$

where α is a primitive pth root of unity in some extension of GF(s). Also

$$nr \equiv 1 \pmod{p} \Rightarrow \alpha^i = \alpha^{nri} = (\alpha^{ri})^n$$

so that α^{ir} is a root of $q(x^n)$. This is so for every $i \in Q$ and so

$$n(x) \mid q(x^n)$$

Hence the map induced by $x \to x^n$ maps code words from $\mathscr{F}$ onto code words in $\mathscr{N}$. Again

$$1 = nr + pt$$

for some integer t and, therefore,

$$x + \langle x^p - 1 \rangle = x^{nr + pt} + \langle x^p - 1 \rangle$$

If $t < 0$, then $-t > 0$ and

$$\begin{aligned} x^{-pt} + \langle x^p - 1\rangle &= (x^p)^{-t} + \langle x^p - 1\rangle \\ &= 1 + \langle x^p - 1\rangle \end{aligned}$$

and so

$$\begin{aligned} x + \langle x^p - 1\rangle &= (x^{nr+pt} + \langle x^p - 1\rangle)(x^{-pt} + \langle x^p - 1\rangle) \\ &= x^{nr} + \langle x^p - 1\rangle \\ &= (x^n)^r + \langle x^p - 1\rangle \end{aligned}$$

It follows that the map

$$F[x]/\langle x^p - 1\rangle \to F[x]/\langle x^p - 1\rangle$$

induced by $x \to x^n$ is onto and hence one–one as well. Therefore, the restriction of this map to

$$:\mathscr{F} \to \mathscr{N}$$

is also one–one and the two spaces being of the same dimension, the map is onto as well. Furthermore, the map $x \to x^n$ determines the permutation $\boldsymbol{\sigma}$ of the set $\{0, 1, 2, \ldots, p-1\}$ given by

$$\boldsymbol{\sigma} = \begin{pmatrix} 0 & 1 & 2 & \cdots & p-1 \\ 0 & \bar{1} & \bar{2} & \cdots & \overline{p-1} \end{pmatrix}$$

where for $1 \leq i \leq p-1$, $\bar{i}$ denotes the least non-negative remainder where ni is divided by p. Thus $\mathscr{F}$ and $\mathscr{N}$ are equivalent.

Equivalence of $\bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ follows similarly.

8.2 SOME EXAMPLES OF QUADRATIC RESIDUE CODES

Consider the $[7, 4, 3]$ binary Hamming code $\mathscr{C}$. A generator matrix of this code is (see p. 115)

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Consider the field

$$\mathrm{GF}(2^3) = \mathbb{B}[X]/\langle x^3 + x + 1\rangle$$

Then,

$$\alpha = x + \langle x^3 + x + 1\rangle$$

is a primitive 7th root of unity. Now $1, 2, 4$ are quadratic residues modulo 7 and so $q(x)$ is a cubic polynomial having α as a root. Also, the minimal polynomial