

as a generator matrix of \mathcal{F} and

$$\mathbf{H}_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

as a generator matrix of \mathcal{N} . As

$$(x+1)q(x)(x+1)n(x) = (x+1)(x^{17}+1) = 0$$

in $\mathbb{B}[x]/I$, every one of the first eight rows of \mathbf{G}_1 is orthogonal to any one of the first eight rows of \mathbf{H}_1 . If we add a column to \mathbf{G}_1 and a column to \mathbf{H}_1 such that each of the first eight entries of these columns is zero, and the last entries are λ and μ respectively, then the above orthogonality property stays good. Each one of the first eight rows of \mathbf{G}_1 and of \mathbf{H}_1 being of even weight, this is equivalent to saying that if

$$a = (a_0, \dots, a_{16}) \in \mathcal{F}$$

then

$$a_{17} = \lambda \sum_{i=1}^{16} a_i$$

while if $a \in \mathcal{N}$, then

$$a_{17} = \mu \sum_{i=0}^{16} a_i$$

Taking $\lambda = \mu = 1$, we find that every row of $\hat{\mathbf{G}}_1$ is orthogonal to every row of $\hat{\mathbf{H}}_1$. Hence, the codes generated by $\hat{\mathbf{G}}_1$ and $\hat{\mathbf{H}}_1$ are orthogonal to each other. Therefore,

$$\hat{\mathcal{F}} \leq (\hat{\mathcal{N}})^\perp \quad \text{and} \quad \hat{\mathcal{N}} \leq (\hat{\mathcal{F}})^\perp \quad (8.4)$$

As on extending a code, the dimension remains unchanged, $\hat{\mathcal{F}}$ is an $[18, 9, -]$ code and so is $\hat{\mathcal{N}}$. For a code \mathcal{C} of dimension k

$$\dim \mathcal{C}^\perp = n - k$$

therefore

$$\dim(\hat{\mathcal{F}})^\perp = 9$$

and

$$\dim(\hat{\mathcal{N}})^\perp = 9$$

It then follows from the relation (8.4) that

$$(\hat{\mathcal{F}})^\perp = \hat{\mathcal{N}}$$

8.4 IDEMPOTENTS OF QUADRATIC RESIDUE CODES

We have studied idempotents of cyclic codes earlier. Recall that the idempotent in a cyclic code \mathcal{C} is the unique element e in \mathcal{C} which generates \mathcal{C} and $e^2 = e$. Quadratic residue codes being cyclic codes, we study idempotents for binary and ternary quadratic residue codes here.

Lemma 8.2

Let p be a prime congruent to $\pm 1 \pmod{8}$. Then there exists a primitive p th root α of unity in some extension field of $\mathbb{B} = \text{GF}(2)$ such that $E(\alpha) = 0$, where

$$E_q(x) = \sum_{r \in Q} x^r$$

Proof

Since Q is closed under multiplication by 2, $E_q(x)$ is an idempotent in the ring $\mathbb{B}[x]/\langle x^p - 1 \rangle$. Therefore, for every primitive p th root α of unity

$$E_q(\alpha)^2 = E_q(\alpha)$$

showing that $E_q(\alpha) \in \mathbb{B}$. Thus, either $E_q(\alpha) = 0$ or $E_q(\alpha) = 1$.

Suppose that $E_q(\alpha) = 1$ for every primitive p th root α of unity. As the primitive p th roots of unity are precisely the roots of the polynomial

$$f(x) = 1 + x + \cdots + x^{p-1}$$

$$f(x) | E_q(x) + 1$$

The polynomial $E_q(x)$ being of degree at most $p-1$, we must have

$$f(x) = E_q(x) + 1 \tag{8.5}$$

The right-hand side of this relation has $(p+1)/2$ non-zero terms while the left-hand side has $p-1$ non-zero terms. The relation (8.5) is as such not possible. Hence there is at least one primitive p th root α of unity such that

$$E_q(\alpha) = 0$$

Theorem 8.9

If $p \equiv -1 \pmod{8}$, then the primitive p th root α of unity in (8.1) can be suitably chosen so that the idempotents of the binary quadratic residue codes \mathcal{F} , \mathcal{N} , $\overline{\mathcal{F}}$ and $\overline{\mathcal{N}}$ are respectively

$$\begin{aligned} E_q(x) &= \sum_{r \in Q} x^r & E_n(x) &= \sum_{n \in N} x^n \\ 1 + E_n(x) & \quad \text{and} \quad & 1 + E_q(x) \end{aligned}$$

Proof

Since Q and N are closed under multiplication by 2, $E_q(x)$, $E_n(x)$ are idempotents in $\mathbb{B}[x]/\langle x^p - 1 \rangle$. But then $1 + E_n(x)$ and $1 + E_q(x)$ are also idempotents. As seen in Lemma 8.2, $E_q(\alpha) \in \mathbb{B}$. Similarly $E_q(\alpha) \in \mathbb{B}$. For any $i \in Q$

$$E_q(\alpha^i) = \sum_{r \in Q} \alpha^{ir} = \sum_{r \in Q} \alpha^r = E_q(\alpha)$$

while for any non-residue t

$$E_n(\alpha^t) = \sum_{n \in N} \alpha^{tn} = \sum_{r \in Q} \alpha^r = E_q(\alpha) \quad (8.6)$$

Choose α so that $E_q(\alpha) = 0$. Then α^i , $\forall i \in Q$, is a root of $E_q(x)$ so that

$$q(x) | E_q(x)$$

As $(p-1)/2$ is odd, 1 is not a root of $E_q(x)$ and

$$(x-1) \nmid E_q(x)$$

Now

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1} = 0$$

so that

$$E_q(\alpha) + E_n(\alpha) = 1$$

Therefore

$$E_n(\alpha) + 1 = 0 \quad \text{and} \quad E_q(\alpha^t) = 1$$

for every non-residue t . Thus

$$n(x) | (1 + E_q(x))$$

Also 1 is a root of $1 + E_q(x)$ and

$$(x-1) | (1 + E_q(x))$$

Let

$$1 + E_q(x) = n(x)(x-1)f_1(x)$$

then

$$1 = E_q(x) + n(x)(x-1)f_1(x) \quad (8.7)$$

Multiplying both sides of this relation by $q(x)$ gives

$$\begin{aligned} q(x) &= q(x)E_q(x) + q(x)n(x)(x-1)f_1(x) \\ &\equiv q(x)E_q(x) \quad \text{in } \mathbb{B}[x]/\langle x^p - 1 \rangle \end{aligned}$$

Thus, the ideal generated by $q(x)$ in $\mathbb{B}[x]/\langle x^p - 1 \rangle$ is contained in the ideal generated by $E_q(x)$. The reverse inclusion follows as $q(x) | E_q(x)$. Hence $E_q(x)$ is the idempotent of the cyclic code \mathcal{F} (Theorem 6.1).

Let

$$E_q(x) = q(x)f_2(x)$$

Multiplying the relation (8.7) by $n(x)(x-1)$, gives

$$\begin{aligned} n(x)(x-1) &= q(x)n(x)(x-1)f_2(x) + n(x)(x-1)(1+E_q(x)) \\ &= n(x)(x-1)(1+E_q(x)) \quad \text{in } \mathbb{B}[x]/\langle x^p-1 \rangle \end{aligned}$$

From this relation and the fact that

$$n(x)(x-1)|(1+E_q(x))$$

it follows that $1+E_q(x)$ is the idempotent of the cyclic code $\bar{\mathcal{N}}$.

Again, it follows from (8.6) and that $E_q(\alpha) = 0$ that

$$n(x)|E_n(x)$$

and the number of terms in $E_n(x)$ being odd

$$x-1 \nmid E_n(x)$$

The number of terms in $1+n(x)$ being even

$$(x-1) \nmid (1+n(x))$$

Also, for any quadratic residue i ,

$$E_n(\alpha^i) = E_n(\alpha) = E_q(\alpha) + 1 = 1$$

Therefore, every α^i is a root of $1+E_n(x)$. Hence

$$q(x)|(1+E_n(x))$$

Let

$$E_n(x) = n(x)g_1(x)$$

and

$$1+E_n(x) = q(x)(x-1)g_2(x)$$

Then

$$1 = E_n(x) + q(x)(x-1)g_2(x) = n(x)g_1(x) + (1+E_n(x)) \quad (8.8)$$

implies

$$n(x) \equiv E_n(x)n(x) \pmod{x^p-1}$$

Therefore, the cyclic code generated by $n(x)$ is contained in the cyclic code generated by $E_n(x)$. That $n(x)|E_n(x)$ shows that the cyclic code generated by $E_n(x)$ is contained in the cyclic code \mathcal{N} . Hence $E_n(x)$ is the idempotent of the cyclic code \mathcal{N} .

On multiplying the relation (8.8) by $(x-1)q(x)$, we can prove that $1+E_n(x)$ is the idempotent of the cyclic code $\bar{\mathcal{N}}$.

Using a similar argument, we can prove the following theorem.

Theorem 8.10

If $p \equiv 1 \pmod{8}$, then the primitive p th root α in (8.1) can be suitably chosen so that the idempotents of the binary quadratic residue codes \mathcal{F} , $\bar{\mathcal{F}}$, \mathcal{N} , $\bar{\mathcal{N}}$ are $1 + E_q(x)$, $E_n(x)$, $1 + E_n(x)$ and $E_q(x)$ respectively.

Proposition 8.10

If $s = 2$ and $p \equiv -1 \pmod{4}$, the weight of every code word in $\hat{\mathcal{F}}$ is divisible by 4, and the weight of every code word in \mathcal{F} is congruent to 0 or 3 modulo 4.

Proof

For quadratic residue codes s is a quadratic residue mod p . Thus 2 is a quadratic residue mod p and so

$$p \equiv \pm 1 \pmod{8}$$

But

$$p \equiv -1 \pmod{4}$$

Therefore,

$$p = 8k - 1$$

for some natural number k . The number of residues or non-residues is then $4k - 1$. The idempotent of the expurgated QR code $\bar{\mathcal{F}}$ is

$$1 + \sum_{n \in N} x^n$$

which has $4k$ non-zero terms. In the corresponding generator matrix $\bar{\mathbf{G}}$ of this code, every row has $4k$ non-zero terms. A generator matrix for \mathcal{F} is then

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

Since $\hat{\mathcal{F}}$ is obtained from \mathcal{F} by adding an overall parity check, the weight of every row of the generator matrix $\hat{\mathbf{G}}$ corresponding to \mathbf{G} of $\hat{\mathcal{F}}$ is divisible by 4. The code $\hat{\mathcal{F}}$ being self dual, any two rows of $\hat{\mathbf{G}}$ agree in an even number of terms. Therefore, the sum of any two rows of $\hat{\mathbf{G}}$ again has weight divisible by 4 and the result follows. ■

Let p be a prime of the form $12n + b$. Then $b = 1, 5, 7$ or 11 . By the law of quadratic reciprocity

$$\begin{aligned} \left(\frac{3}{12n+b} \right) \left(\frac{12n+b}{3} \right) &= (-1)^{(12n+b-1)/2} = (-1)^{(b-1)/2} \\ (-1)^{(b-1)/2} &= \begin{cases} 1 & \text{if } b = 4k + 1 \Rightarrow b = 1 \text{ or } b = 5 \\ -1 & \text{if } b = 4k - 1 \Rightarrow b = 7 \text{ or } b = 11 \end{cases} \end{aligned}$$

Thus when $b = 1$ or $b = 5$

$$\left(\frac{3}{12n+b} \right) = \left(\frac{b}{3} \right) = \begin{cases} 1 & \text{if } b = 1 \\ -1 & \text{if } b = 5 \end{cases}$$

198 Quadratic residue codes

When $b = 7$ or $b = 11$

$$\left(\frac{3}{12n+b}\right) = -\left(\frac{b}{3}\right) = \begin{cases} -1 & \text{if } b = 7 \\ 1 & \text{if } b = 11 \end{cases}$$

Hence, 3 is a quadratic residue for primes of the form $12n \pm 1$ and non-residue for primes of the form $12n \pm 5$.

We can thus talk of ternary quadratic residue codes of length p when p is of the form $12n \pm 1$. Also, -1 is a non-residue for $p = 12n - 1$ and a residue for $p = 12n + 1$.

Theorem 8.11

Suppose that $p \equiv -1 \pmod{12}$ and that

$$c(x) = \sum_{i=1}^d c_i x^{e_i}$$

is a code word of weight d in the ternary QR code of length p . Then

$$d \equiv 2 \pmod{4} \quad \text{or} \quad d \equiv 3 \pmod{4}$$

Proof

Let $\hat{c}(x)$ be the word obtained from $c(x)$ by replacing x by x^{-1} . The product

$$c(x)\hat{c}(x) = \sum_{i=1}^d c_i^2 + \sum_{\substack{i \neq j \\ i, j}} c_i c_j x^{e_i - e_j}$$

will have less than $d^2 - d + 1$ terms if some of the terms cancel, i.e. if

$$e_i - e_j = e_k - e_l$$

for some i, j, k, l . The number of such terms is of the form $4t$ and so

$$d^2 - d + 1 - 4t = p$$

which implies that

$$d \equiv 2 \pmod{4} \quad \text{or} \quad d \equiv 3 \pmod{4}$$

If we recall that 2 is a quadratic residue for primes of the form $8n \pm 1$, we have the following theorem.

Theorem 8.12

If $p \equiv 1 \pmod{8}$ and c is a code word of odd weight d in the binary QR code with generator $q(x)$, then $d \equiv 3 \pmod{4}$.

Remark 8.2

Observe that the conclusion of Theorem 8.11 is valid for any quadratic residue code of prime length p provided $p \equiv -1 \pmod{4}$.