of $\alpha$ is of degree 3. Thus $q(x)$ must equal the minimal polynomial $x^3 + x + 1$ of $\alpha$. The quadratic residue code being the polynomial code of length 7 generated by $1 + x + x^3$ it has a generator matrix

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

The code generated by $\mathbf{G}_1$ is the same as the code generated by

$$\mathbf{G}_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

or the same as that generated by (interchanging the first and fourth rows)

$$\mathbf{G}_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

The permutation $\sigma = (1 \quad 7 \quad 3 \quad 4 \quad 2 \quad 5)$ applied to the columns of $\mathbf{G}_3$ gives the generator matrix $\mathbf{G}$ of the Hamming code. Hence the $[7, 4, 3]$ binary Hamming code is equivalent to the binary quadratic residue code of length 7 generated by $x^3 + x + 1$.

Let $p = 23$. As $5^2 \equiv 2 (\text{mod } 23)$, 2 is a quadratic residue modulo 23. As seen in Case (i) of Examples 7.4,

$$x^{23} + 1 = (x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \times (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)$$

and each of the two factors of degree 11 is irreducible. Therefore, either may be taken as $q(x)$ (Theorem 8.1). Let

$$q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

If $d$ denotes the minimum distance of the quadratic residue code generated by $q(x)$, then $d \leq 7$. We shall prove two theorems about the minimum distance of quadratic residue codes from which it will follow that $d = 7$. Thus we have a $[23, 12, 7]$ code.

Given a code word $c = c_1 c_2 \cdots c_{23}$, the number of binary words of length 23 which are at distance at most 3 from $c$ is

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 1 + 23(1 + 11 + 11 \times 7)$$

$$= 1 + 23 \times 89 = 2048 = 2^{11}$$

i.e.

$$O(\mathscr{S}(c,3)) = 2^{11}$$

and so

$$O\left(\bigcup_{c\in\mathscr{F}} \mathscr{S}(c,3)\right) = 2^{12} \times 2^{11} = 2^{23} = O(V(23,2))$$

Hence the code under consideration is perfect.

**Definition 8.2**
The binary quadratic residue code of length 23 is called the **Golay code** and is denoted by $\mathscr{G}_{23}$.

Consider the case when $s = 3$ and $p = 11$. As $5^2 \equiv 3 \pmod{11}$, 3 is a quadratic residue modulo 11. We have proved in Case (ii) of Examples 7.4 that

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1)$$

and both the factors of degree 5 are irreducible. Therefore, either of the two may be taken as $q(x)$ (Theorem 8.1). Let

$$q(x) = x^5 + x^4 - x^3 + x^2 - 1$$

Then the minimum distance $d$ of the code is at most 5. Again, as an application of the two theorems to be proved, we shall find that $d = 5$.

Let $c$ be a fixed code word of the code. Then the number of ternary words which are at distance at most 2 from $c$ is

$$1 + \binom{11}{1} \times 2 + \binom{11}{2} \times 2^2 = 1 + 22 + 55 \times 4 = 243 = 3^5$$

i.e.

$$O(\mathscr{S}(c,2)) = 3^5$$

Therefore

$$O\left(\bigcup_{c\in\mathscr{F}} \mathscr{S}(c,2)\right) = 3^6 \times 3^5 = 3^{11} = O(V(11,3))$$

Hence the code under consideration is perfect.

**Definition 8.3**
The [11, 6, 5] ternary quadratic residue code is the Golay code $\mathscr{G}_{11}$.

Let $p = 13$, $s = 3$. Observe that 3 is a quadratic residue modulo 13. We have seen in Case (iii) of Examples 7.4 that

$$x^{13} - 1 = (x-1)(x^3 - x^2 - x + 1)(x^3 + x^2 + x - 1)(x^3 + x^2 - 1)(x^3 - x - 1)$$

where all the four factors of degree 3 are irreducible over GF(3) = $F$. Consider the extension

$$F[x]/\langle x^3 - x - 1\rangle$$

of $F$ and let

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

Then $x^3 - x - 1$ is the minimal polynomial of $\alpha$. Now

$$\alpha^3 - \alpha - 1 = 0$$

or

$$\alpha^3 = \alpha + 1 \neq 0$$

and, so

$$\begin{aligned}\alpha^{12} &= \alpha^4 + \alpha^3 + \alpha + 1\\ &= \alpha(\alpha + 1) + 2(\alpha + 1)\\ &= \alpha^2 + 2\end{aligned}$$

then

$$\alpha^{13} = \alpha^3 - \alpha = 1$$

Thus, $\alpha$ is a primitive 13th root of unity in

$$F[x]/\langle x^3 - x - 1\rangle$$

Now

$$Q = \{1, 4, 9, 3, 12, 10\} \quad \text{and} \quad N = \{2, 5, 6, 7, 8, 11\}$$

As $\alpha, \alpha^3, \alpha^9$ have the same minimal polynomial, these are the roots of the polynomial $x^3 - x - 1$.

The minimal polynomial of $\alpha^4$ is

$$\begin{aligned}&(x - \alpha^4)(x - \alpha^{10})(x - \alpha^{12})\\ &= x^3 - x^2(\alpha^4 + \alpha^{10} + \alpha^{12}) + x(\alpha^{14} + \alpha^{16} + \alpha^{22}) - 1\\ &= x^3 - x^2(\alpha^2 + \alpha + \alpha(\alpha + 1)^3 + (\alpha^2 + \alpha)^3) + x(\alpha + \alpha^3 + \alpha^9) - 1\\ &= x^3 - x^2(\alpha^2 + \alpha + \alpha(\alpha^3 + 1) + \alpha^6 + \alpha^3) + x(2\alpha + 1 + (\alpha + 1)^3) - 1\\ &= x^3 - x^2(\alpha^2 + \alpha + \alpha^2 + 2\alpha + (\alpha + 1)^2 + \alpha + 1) + x(2\alpha + 1 + \alpha^3 + 1) - 1\\ &= x^3 - x^2(2\alpha^2 + \alpha + 1 + \alpha^2 + 2\alpha + 1) + x(2\alpha + 1 + \alpha + 1 + 1) - 1\\ &= x^3 + x^2 - 1\end{aligned}$$

Hence

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

Then $\mathscr{F}$ is the code of length 13 generated by $q(x)$, its dimension is 7 and the minimum distance $d \leq 6$. It will follow from Theorem 8.8 that $d = 5$ or 6. The code is, therefore, capable of correcting any two errors. Observe that

$$O(\mathscr{S}(c, 2)) = 1 + 13 \times 2 + 13 \times 6 \times 4 = 339$$

and, so

$$O\left(\bigcup_{C \in \mathscr{F}} \mathscr{S}(c, 2)\right) = 339 \times 3^7 \neq 3^{13} = O(V(13, 3))$$

Hence $\mathscr{F}$ is not perfect.

## 8.3 EXTENDED QUADRATIC RESIDUE CODES AND DISTANCE PROPERTIES

We are interested in finding some information about the minimum distance of quadratic and extended quadratic residue codes. For that we first need to obtain duals of quadratic residue codes.

**Theorem 8.2**

$$\mathscr{F}^{\perp} = \bar{\mathscr{F}}, \mathscr{N}^{\perp} = \bar{\mathscr{N}} \quad \text{if } p = 4k - 1$$

and

$$\mathscr{F}^{\perp} = \bar{\mathscr{N}}, \mathscr{N}^{\perp} = \bar{\mathscr{F}} \quad \text{if } p = 4k + 1$$

Moreover, $\mathscr{F}$ is always generated by $\bar{\mathscr{F}}$ and

$$\sum_{i=0}^{p-1} x^i$$

while $\mathscr{N}$ is always generated by $\bar{\mathscr{N}}$ and

$$\sum_{i=0}^{p-1} x^i$$

***Proof***

The check polynomial of $\mathscr{F}$ is

$$h(x) = (x - 1)n(x)$$

and, therefore, the dual code $\mathscr{F}^{\perp}$ is generated by

$$\rho(x) = x^{(p+1)/2}(x^{-1} - 1)n(x^{-1}) = (x - 1) \prod_{n \in N} (1 - x\alpha^n)$$

(Theorem 6.2) which is a constant multiple of

$$(x - 1) \prod_{n \in N} (x - \alpha^{-n})$$

Now if $p$ is of the form $4k + 1$, then $-1$ is a quadratic residue mod $p$ so that

$-n \in N\ \forall n \in N$. Hence,

$$(x-1)\prod_{n\in\mathcal{N}}(x-\alpha^{-n}) = (x-1)n(x)$$

Therefore $\mathcal{F}^{\perp}$ is the code generated by $(x-1)n(x)$ and so is $\bar{\mathcal{N}}$.

On the other hand, if $p$ is of the form $4k-1$, then $-1$ is a quadratic non-residue modulo $p$ and $-n \in Q\ \forall n \in N$. Hence, in this case

$$(x-1)\prod_{n\in N}(x-\alpha^{-n}) = (x-1)q(x)$$

and, therefore, $\mathcal{F}^{\perp}$ is $\bar{\mathcal{F}}$.

The proof for the dual of $\mathcal{N}$ follows on the same lines. As

$$\sum_{i=0}^{p-1} x^i = q(x)n(x)$$

the ideal in $F[x]/\langle x^p - 1\rangle$ generated by

$$\sum_{i=0}^{p-1} x^i \quad \text{and} \quad (x-1)q(x)$$

is contained in the ideal generated by $q(x)$. Also $x-1$ and $n(x)$ do not have a common root and so are relatively coprime. Therefore

$$1 = (x-1)a(x) + n(x)b(x)$$

for some $a(x), b(x) \in F[x]$. But then

$$\begin{aligned} q(x) &= (x-1)q(x)a(x) + q(x)n(x)b(x) \\ &= (x-1)q(x)a(x) + \left(\sum_{i=0}^{p-1} x^i\right)b(x) \end{aligned}$$

From this, it follows that the ideal of $F[x]/\langle x^p - 1\rangle$ generated by $q(x)$ is contained in the ideal generated by

$$\sum_{i=0}^{p-1} x^i \quad \text{and} \quad (x-1)q(x)$$

As $\bar{\mathcal{F}}$ is generated by $(x-1)q(x)$, $\mathcal{F}$ is generated by $\bar{\mathcal{F}}$ and

$$\sum_{i=0}^{p-1} x^i$$

**Corollary**

(i) If $\bar{\mathbf{G}}$ is a generator matrix for $\bar{\mathcal{F}}$, then

$$\left(\begin{array}{c|ccc} \bar{\mathbf{G}} & & & \\ \hline 1 & 1 & \cdots & 1 \end{array}\right)$$

is a generator matrix for $\mathcal{F}$.

(ii) If $\bar{\mathbf{G}}_1$ is a generator matrix for $\bar{\mathcal{N}}$, then

$$\left(\begin{array}{c|ccc} \bar{\mathbf{G}}_1 & & & \\ \hline 1 & 1 & \cdots & 1 \end{array}\right)$$

is a generator matrix for $\mathcal{N}$.

**Remark 8.1**
Let

$$(x-1)q(x) = a_0 + a_1 x + \cdots + a_m x^m$$

where $m = (p+1)/2$. The code $\bar{\mathcal{F}}$ being generated by $(x-1)q(x)$, it follows that

$$\bar{\mathbf{G}} = \left(\begin{array}{cccccccc} a_0 & a_1 & \cdots & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ \multicolumn{8}{c}{\text{---------- (dashed) ----------}} \\ 0 & 0 & \cdots & 0 & a_0 & \cdots & \cdots & a_m \end{array}\right)$$

which is an $(m-1) \times p$ matrix is a generator matrix of $\bar{\mathcal{F}}$ and clearly every row of $\bar{\mathbf{G}}$ is orthogonal to the all ones vector. Similarly, $\bar{\mathcal{N}}$ being a polynomial code generated by $(x-1)n(x)$, every row of the corresponding generator matrix $\bar{\mathbf{G}}_1$ is orthogonal to the all ones vector.

**Definition 8.4**
Recall that the Legendre symbol $\chi(i)$ is defined by

$$\chi(i) = \begin{cases} 0 & \text{if } i \text{ a multiple of } p \\ 1 & \text{if } i \text{ is a quadratic residue mod } p \\ -1 & \text{if } i \text{ is a non-residue mod } p \end{cases}$$

Since the product of two residues or two non-residues is a residue while the product of a residue and a non-residue is a non-residue, we have

$$\chi(i)\chi(j) = \chi(ij)$$

We then define the **Gaussian sum** by

$$\theta = \sum_{i=1}^{p-1} \chi(i)\alpha^i \tag{8.2}$$

As $s$ is a prime, $s \neq p$, and $\alpha$ belongs to an extension of the field GF($s$), it follows that

$$\theta^s = \sum_{i=1}^{p-1} \chi(i)^s \alpha^{is}$$

Now

$$\chi(i)^s = \chi(i)$$