Remark 8.3
A close look at the proof of Theorem 8.9 suggests the following working rule for obtaining the idempotents of the quadratic residue codes of $\mathscr{F}$, $\mathscr{N}$, $\bar{\mathscr{F}}$ and $\bar{\mathscr{N}}$ (not necessarily binary).

If $f(x)$ is a polynomial over GF(s) and

$$q(x) \mid f(x)$$

$x-1$ does not divide it and

$$(x-1)n(x) \mid (1-f(x))$$

then $f(x)$ is the idempotent of the QR code $\mathscr{F}$ and $1-f(x)$ is the idempotent of the QR code $\bar{\mathscr{N}}$.

When $s=2$, $p=4k\pm 1$ and, so, in either case $\theta^2=1$. When $s=3$, $p=12k\pm 1$ and again, in either case $\theta^2=1$. Since $\theta \in \mathrm{GF}(s)$, in both the cases $\theta=1$ or $\theta=-1$ (for $s=2$ it is always $\theta=1$).

Lemma 8.3
In

$$\mathscr{R}=F[x]/\langle x^p-1\rangle$$

where $F=\mathrm{GF}(3)$ and $p=12k-1$

$$\left(\sum_{r\in Q} x^r\right)^2 = -\sum_{r\in Q} x^r$$

$$\left(\sum_{n\in N} x^n\right)^2 = -\sum_{n\in N} x^n$$

and

$$\left(\sum_{r\in Q} x^r\right)\left(\sum_{n\in N} x^n\right) = -(1+x+\cdots+x^{p-1})$$

Proof
For any residue t, it follows (from Perron's Theorem 8.3) that $\{r+t/r\in Q\}$ contains $3k-1$ residues and $3k$ non-residues. Therefore in $\{r+t/r, t\in Q\}$ every residue appears $3k-1$ times and every non-residue appears $3k$ times. Hence

$$\left(\sum_{r\in Q} x^r\right)^2 = (3k-1)\sum_{r\in Q} x^r + 3k\sum_{n\in N} x^n = -\sum_{r\in Q} x^r$$

Thus

$$-\sum_{r\in Q} x^r$$

is an idempotent. That

$$-\sum_{n\in N} x^n$$

is an idempotent follows as above using the observation that for any non-residue t, $\{t+n/n\in N\}$ contains $3k$ residues and $3k-1$ non-residues.

In the present case, i.e. $p=12k-1$, -1 is a non-residue and so $\forall n\in N$ there is an $r\in Q$ such that $r+n=0$ and for every $r\in Q$, there is an $n\in N$ such that $r+n=0$. Therefore for every non-residue n, $\{r+n/r\in Q\}$ has $3k$ residues (including 0) and $3k-1$ non-residues. Therefore, in $\{r+n/r\in Q,\ n\in N\}$ every residue or non-residue occurs $3k-1$ times and 0 also occurs $3k-1$ times. Hence

$$\left(\sum_{r\in Q} x^r\right)\left(\sum_{n\in N} x^n\right)=(3k-1)\sum_{i=0}^{p-1} x^i=-\sum_{i=0}^{p-1} x^i$$

Using parts (iii) and (iv) of Theorem 8.3, we can similarly prove the following Lemma.

Lemma 8.4
In

$$\mathscr{R}=F[x]/\langle x^p-1\rangle$$

where $F=\mathrm{GF}(3)$ and $p=12k+1$

$$\left(\sum_{r\in Q} x^r\right)^2=-\sum_{r\in Q} x^r$$

$$\left(\sum_{n\in N} x^n\right)^2=-\sum_{n\in N} x^n$$

and

$$\left(\sum_{r\in Q} x^r\right)\left(\sum_{n\in N} x^n\right)=0$$

Let

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

$$E_n(x)=-\sum_{n\in N} x^n$$

$$F_q(x)=1-E_n(x)$$

and

$$F_n(x)=1-E_q(x)$$

Using the above lemma and proceeding as in the proof of Lemma 8.2, we can prove the next lemma.

Lemma 8.5
Let p be a prime congruent to $\pm 1 \pmod{12}$. Then there exists a primitive pth root α of unity in some extension field of $F=\mathrm{GF}(3)$ such that $E_n(\alpha)=0$.

Theorem 8.13
If $p \equiv 1 \pmod{12}$, then the primitive pth root α in (8.1) can be suitably chosen so that the idempotents of the ternary quadrative residue codes $\mathscr{F}$, $\bar{\mathscr{F}}$, $\mathscr{N}$ and $\bar{\mathscr{N}}$ are $1 - E_q(x)$, $E_n(x)$, $1 - E_n(x)$ and $E_q(x)$ respectively.

Proof
Choose α such that $E_n(\alpha) = 0$. Then

$$1 - E_q(\alpha) - E_n(\alpha) = 0 \Rightarrow 1 - E_q(\alpha) = 0$$

For $t \in Q$

$$E_q(\alpha^t) = -\sum_{r \in Q} \alpha^{rt} = -\sum_{r \in Q} \alpha^r = E_q(\alpha) = 1$$

Therefore

$$q(x) \mid (1 - E_q(x))$$

Also

$$E_q(1) = \frac{p-1}{2} \equiv 0 \pmod 3$$

Therefore

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

For any $n \in N$

$$E_q(\alpha^n) = -\sum_{r \in Q} \alpha^{rn} = -\sum_{t \in N} \alpha^t = E_n(\alpha) = 0$$

It then follows that

$$n(x) \mid E_q(x)$$

Thus

$$(x-1)n(x) \mid E_q(x)$$

and it follows from Remark 8.3 that $1 - E_q(x)$ is the idempotent of $\mathscr{F}$, while $E_q(x)$ is the idempotent of $\bar{\mathscr{N}}$. We can similarly prove that $1 - E_n(x)$ is the idempotent of $\mathscr{N}$ and $E_n(x)$ is the idempotent of $\bar{\mathscr{F}}$. ∎

Proceeding similarly, we have the following theorem.

Theorem 8.14
If $p \equiv -1 \pmod{12}$, then the primitive pth root α in (8.1) can be suitably chosen so that the idempotents of the ternary quadratic residue codes $\mathscr{F}$, $\bar{\mathscr{F}}$, $\mathscr{N}$ and $\bar{\mathscr{N}}$ are $E_q(x)$, $1 - E_n(x)$, $E_n(x)$ and $1 - E_q(x)$ respectively.

Remark 8.4
If $p = 12k - 1$, we have observed that the minimum distance d of a QR code satisfies

$$d \equiv 2(\text{mod } 4) \quad \text{or} \quad d \equiv 3(\text{mod } 4)$$

and

$$d \equiv 0(\text{mod } 3) \quad \text{or} \quad d \equiv 2(\text{mod } 3)$$

Then

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

and so

$$d \equiv m + 2 \quad \text{or} \quad d \equiv m(\text{mod } 3)$$

For $d \equiv 0(\text{mod } 3)$ then shows that

$$m \equiv 1(\text{mod } 3) \quad \text{or} \quad m \equiv 0(\text{mod } 3)$$

But then

$$d \equiv 3(\text{mod } 12) \quad \text{or} \quad d \equiv 6(\text{mod } 12)$$

For $d \equiv 2(\text{mod } 3)$ shows that

$$m \equiv 0(\text{mod } 3) \quad \text{or} \quad m \equiv 2(\text{mod } 3)$$

so that

$$d \equiv 2(\text{mod } 12) \quad \text{or} \quad d \equiv 11(\text{mod } 12)$$

Thus the minimum distance of a ternary QR code of length $p = 12k - 1$ is always congruent to 2, 3, 6 or 11 modulo 12 and hence the minimum distance of extended ternary QR code is always congruent to 0 or 3 or 6 modulo 12.

8.5 SOME EXAMPLES

Case (i)
In Case (v) of Examples 7.4, we obtained the irreducible factors of $x^{37} - 1$ over GF(3):

$$x^{37} - 1 = (x - 1)f(x)g(x)$$

where $f(x), g(x)$ are irreducible factors of degree 18 each. We may take either of these as a generator polynomial of the QR code. The weight of the polynomial (word) $g(x)$ being 10, it follows that the minimum distance d of the code is at most 10. As $d^2 \geq 37$, we have

$$7 \leq d \leq 10$$

Case (ii) – ternary QR code of length 61

Let $\alpha = x + \langle h_2(x) \rangle$ be the primitive 61st root of unity in the field F as constructed in Case (vi) of Examples 7.4. A generator polynomial of the QR code is

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

where $Q = C_1 \cup C_4 \cup C_5$ is the set of all quadratic residues modulo 61. Here C_0, C_1, C_2, C_4, C_5, C_8 and C_{10} are the cyclotomic cosets relative to 3 modulo 61 as obtained in Case (vi) of Examples 7.4. Thus $q(x)$ is the product of the minimal polynomials of α, α^4 and α^5. Factorization of $x^{61} - 1$ as a product of irreducible polynomials over GF(3) has been obtained in Case (vi) of Examples 7.4. We find that α^5 satisfies the irreducible factor $f_2(x)$ and so $f_2(x)$ is its minimal polynomial. We have already proved in Case (vi) of Examples 7.4 that $g_1(x)$ is the minimal polynomial of α^4. Therefore,

$$\begin{aligned} q(x) &= f_2(x) g_1(x) h_2(x) \\ &= x^{30} + x^{29} - x^{28} + x^{27} - x^{25} - x^{21} - x^{20} - x^{19} - x^{15} - x^{11} \\ &\quad - x^{10} - x^9 - x^5 + x^3 - x^2 + x + 1 \end{aligned}$$

which is a word of weight 17. Let d denote the minimum distance of the QR code. Then $d^2 \geq 61$ and so we have $8 \leq d \leq 17$. Observe that

$$\begin{aligned} (x^6 - x^5 - x^4 - x^3 + x^2 + 1)q(x) = x^{36} - x^{27} + x^{23} + x^{18} + x^{17} + x^{13} \\ + x^9 - x^8 - x^5 + x^3 + x + 1 \end{aligned}$$

which is a word of weight 12. Hence $d \leq 12$.

Taking

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

where $N = C_2 \cup C_8 \cup C_{10}$ is the set of all quadratic non-residues modulo 61, we find that

$$\begin{aligned} n(x) &= f_1(x) g_2(x) h_1(x) \\ &= x^{30} - x^{28} + x^{27} - x^{26} - x^{25} + x^{21} - x^{19} + x^{18} + x^{17} - x^{16} \\ &\quad + x^{15} - x^{14} + x^{13} + x^{12} - x^{11} + x^9 - x^5 - x^4 + x^3 - x^2 + 1 \end{aligned}$$

Also, on direct computation we find that

$$\begin{aligned} (x^9 + x^7 - x^6 - x^5 + x^4 + x^3 - 1)n(x) = x^{39} - x^{27} + x^{25} - x^{21} - x^{20} - x^{18} \\ + x^{14} + x^6 - x^5 + x^2 - 1 \end{aligned}$$

which is a word of weight 11. As the codes generated by $q(x)$ and $n(x)$ are equivalent and equivalent codes have the same minimum distance, the minimum distance of the ternary quadratic residue code of length 61 is at most 11.

Case (iii)–QR code of length 11 over GF(5)

We have obtained the factorization of $x^{11}-1$ over GF(5) as a product of irreducible polynomials in Case (iv) of Examples 7.4

$$x^{11}-1=(x-1)f(x)g(x)$$

where

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

and

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

As one of the equivalent QR codes $\mathscr{F}$ and $\mathscr{N}$ is generated by $f(x)$ and the other by $g(x)$, we find that the minimum distance ∂ of the QR code $\mathscr{F}$ is at most 6. Also

$$(x+1)g(x)=x^6+3x^5+x^4+2x^2-1$$

and, so, $\partial \le 5$. As $\partial^2 \ge 11$, we have $4 \le \partial \le 5$.

Theorem 8.15

The minimum distance of the code is 5.

Proof

An arbitrary code word is

$$\begin{gathered}a,\quad 2a+b,\quad -a+2b+c,\quad a-b+2c+d,\quad a+b-c+2d+e,\\ -a-b+c-d+2e+1,\quad -b+c+d-e+2,\\ -c+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1\end{gathered}$$

where $a, b, c, d, e \in \mathrm{GF}(5)$.

To prove that $\partial=5$, we consider the various possible cases:

Case A: $a=0$, $2a+b=0$ so that $b=0$ as well

The word becomes

$$\begin{gathered}0,\quad 0,\quad c,\quad 2c+d,\quad -c+2d+e,\quad c-d+2e+1,\quad c+d-e+2,\\ -c+d+e-1,\quad -d+e+1,\quad -e+1,\quad -1\end{gathered}$$

If $c=d=0$, it is fairly easy to see that the word is of weight at least 5.

Case A(i): $c=0$ but $2c+d\neq 0$

Then $d\neq 0$ and the word takes the form

$$\begin{gathered}0,\quad 0,\quad 0,\quad d,\quad 2d+e,\quad -d+2e+1,\quad d-e+2,\quad d+e-1,\\ -d+e+1,\quad -e+1,\quad -1\end{gathered}$$

If $2d + e = 0$, then among the entries

$$-d + 2e + 1 = 1 \qquad d - e + 2 = 3d + 2 \qquad d + e - 1 = -d - 1$$
$$-d + e + 1 = -3d + 1 \qquad 2d + 1$$

at least three are non-zero so that the word is of weight at least 5. If $2d + e \neq 0$, but $-d + 2e + 1 = 0$, then among the entries

$$d - e + 2 = e + 3 \qquad 3e - 2 \qquad -e \qquad -e + 1$$

at least two are non-zero.

If $2d + e \neq 0$, $-d + 2e + 1 \neq 0$ but $d - e + 2 = 0$, then $-d + e + 1 = 3 \neq 0$ and so again the word is of weight at least 5.

Case A(ii): $c \neq 0$ but $2c + d = 0$
The word becomes

$$0, \quad 0, \quad c, \quad 0, \quad b, \quad 3c + 2e + 1, \quad -c - e + 2, \quad -3c + e - 1, \quad 2c + e,$$
$$-e + 1, \quad -1$$

For $e = 0$, the entries $3c + 1$, $4c + 2$, $-3c - 1$, $2c, 1, -1$ have at least four non-zero terms.

For $e \neq 0$, but $3c + 2e + 1 = 0$, we have $c = e - 2$ and among

$$-c - e + 2 = -2e + 4 \qquad -3c + e - 1 = -2e \qquad 3e - 4$$
$$-e + 1 \qquad -1$$

at least three terms are non-zero.

Case A(iii): $c \neq 0$, $2c + d \neq 0$ but $-c + 2d + e = 0$
Then $c = 2d + e$ and the last six terms of the word are (among the first five there are two non-zero terms):

$$d + 3e + 1 \qquad 3d - 2e + 2 \qquad -d - 1 \qquad -d + e + 1 \qquad -e + 1 \qquad -1$$

For $e = 0$, among the terms

$$-d - 1, \quad -d + e + 1 = -d + 1, \quad -e + 1 = 1, \quad -1$$

at least three are non-zero.

For $e \neq 0$, but $d + 3e + 1 = 0$, we have $d = 2e - 1$ and the last five terms are

$$4e - 1, \quad -2e, \quad -e + 2, \quad -e + 1, \quad -1$$

out of which at least four are non-zero.

Case A(iv): $c \neq 0$, $2c + d \neq 0$, $-c + 2d + e \neq 0$ but $c - d + 2e + 1 = 0$
Then $c = d - 2e - 1$ and among the last five terms

$$2d - 3e + 1, \quad 3e, \quad -d + e + 1, \quad -e + 1, \quad -1$$

at least two are non-zero.

Thus, in Case (A) we always have a word of weight at least 5.