and so the space generated by these two vectors is not a self dual code. However, the code

$$\mathscr{C} = \{0000, 1100, 0011, 1111\}$$

generated by 1100 and 0011 is self dual. Following are the other self dual codes of length 4:

$$\{0000, 0101, 1010, 1111\} \qquad \{0000, 1001, 0110, 1111\}$$

Exercises 5.3

1. Construct a binary self dual code of length 6.
2. Construct a binary self dual code of length 8.
3. Prove that 1201 and 1012 generate a ternary self dual code of length 4. Also find all the code words of this code.
4. Prove that the weight of every code word of a ternary self dual is divisible by 3.
5. Prove that the (4, 7) binary Hamming code is not a polynomial code. Is this code equivalent to a polynomial code?

Next, we consider self dual codes over GF(q), q an odd prime. First we have a couple of number theoretic results which we again need in Chapter 8 when we study quadratic residue codes.

Definition 5.7
Let p be an odd prime. Recall that a positive integer a is called a **quadratic residue modulo p** if $x^2 \equiv a(\text{mod}\, p)$ for some integer x. If there is no such x, then a is called a **quadratic non-residue modulo p**. If b is another positive integer such that $b \equiv a(\text{mod}\, p)$, then b is a quadratic residue modulo p iff a is a quadratic residue modulo p. We may thus think of a as an element of the field $F = \text{GF}(p)$ rather than as an integer. We may similarly regard x as an element of F. Let λ denote a primitive element of F. Every non-zero element of F is then a power of λ and it follows that $a \in F$ is a residue mod p if $a = \lambda^{2k}$ for some k and a is a non-residue mod p if $a = \lambda^{2k+1}$ for some k. As a consequence we have the following proposition.

Proposition 5.6
If Q denotes the set of all quadratic residues modulo p and N the set of all quadratic non-residues modulo p, then:

(i) order of Q = order of $N = (p-1)/2$
(ii) $ab \in Q$ if both $a, b \in Q$ or $a, b \in N$
(iii) $ab \in N$ if one of a, b is in Q and the other is in N
(iv) $-1 \in Q$ if p is of the form $4k+1$ and $-1 \in N$ if p is of the form $4k-1$.

Proof
We need only to prove item (iv).
Let

$$\beta = \lambda^{(p-1)/2}$$

Then

$$\beta^2 = \lambda^{p-1} = 1$$

so that

$$(\beta - 1)(\beta + 1) = 0$$

The element λ being primitive, $\beta \neq 1$. Therefore, $\beta + 1 = 0$, i.e.

$$-1 = \beta = \lambda^{(p-1)/2}$$

which is an even power of λ if $p = 4k + 1$ while it is an odd power of λ if $p = 4k - 1$.

Proposition 5.7
If p is a prime of the form $4k + 1$ then there exist integers a and b such that $p = a^2 + b^2$.

Proof
Since $p \equiv +1 (\text{mod } 4)$, -1 is a quadratic residue mod p. Let s be an integer such that $s^2 \equiv -1 (\text{mod } p)$. Consider the set

$$S = \{(u, v) | 0 \leq u \leq \sqrt{p}, 0 \leq v \leq \sqrt{p}\}$$

of ordered pairs with u, v integers. This set contains $(1 + [\sqrt{p}])^2$ elements, where $[x]$ denotes the number of non-negative integers at most x. Now

$$(1 + [\sqrt{p}])^2 = 1 + 2[\sqrt{p}] + [\sqrt{p}]^2$$

Also

$$\sqrt{p} = [\sqrt{p}] + x \quad 0 < x < 1$$

and

$$\begin{aligned}(1 + [\sqrt{p}])^2 &= 1 + 2(\sqrt{p} - x) + p - 2\sqrt{p}x + x^2 \\ &= (1 - x)^2 + p + 2(1 - x)\sqrt{p} > p\end{aligned}$$

Therefore, $\{u - sv | (u, v) \in S\}$ has more than p numbers and, therefore, we have

$$u_2 - sv_2 \equiv u_1 - sv_1 (\text{mod } p)$$

for some $(u_1, v_1) \neq (u_2, v_2)$ in S.

Let $u_0 = u_2 - u_1$, $v_0 = v_2 - v_1$. Then $|u_0| < \sqrt{p}$, $|v_0| < \sqrt{p}$ and both $|u_0|$, $|v_0|$ cannot be simultaneously zero. Hence,

$$1 \leq u_0^2 + v_0^2 < 2p \tag{5.1}$$

Also

$$u_0^2 + v_0^2 \equiv s^2 v_0^2 + v_0^2 \pmod p$$
$$\equiv 0 \pmod p \qquad (5.2)$$

It follows from (5.1) and (5.2) that $u_0^2 + v_0^2 = p$.

Proposition 5.8
Given any positive integer m and a prime p of the form $4k+1$, there always exists a self dual code of length $2m$ and dimension m over $\mathrm{GF}(p)$.

Proof
Let $a, b \in \mathrm{GF}(p)$ such that $a^2 + b^2 = p$. For any i, $1 \le i \le m$, let

$$e^i = e_1^i e_2^i \cdots e_{2m}^i$$

be the word of length $2m$ with

$$e_{2i-1}^i = a$$
$$e_{2i}^i = b$$
$$e_j^i = 0 \quad \text{for every other } j$$

Then $e^1, e^2, \ldots, e^m$ are linearly independent, and e^i, e^j for any i, j, $1 \le i$, $j \le m$, are orthogonal. Therefore, these generate a self dual code of dimension m and length $2m$ over $\mathrm{GF}(p)$.

Examples 5.4

Case (i)
Consider the ternary words

2 0 2 1 0 0 0 0	1 1 2 0 0 0 0 0
0 0 0 0 0 1 1 1	2 1 0 2 0 0 0 0

of length 8. These words are self-orthogonal and any two of these are orthogonal to each other. Therefore, these words generate a ternary self dual code of length 8 and dimension 4.

Case (ii)
The ternary words

1 1 2 0 0 0 0 0	0 0 0 0 1 1 2 0
2 1 0 2 0 0 0 0	0 0 0 0 2 1 0 2

of length 8 are self-orthogonal and any two of these are orthogonal to each other. These, thus, generate a ternary self dual code of length 8 and dimension 4.

Case (iii)

Observe that 112000, 211000, 000111 generate a ternary self dual code of length 6 and dimension 3.

Case (iv)

1211, 0123 generate a self dual code of length 4 and dimension 2 over GF(7).

Case (v)

12110000, 01230000, 00001211, 00000123 generate a self dual code of length 8 and dimension 4 over GF(7).

Exercises 5.4

1. Does there exist a self dual code of length 6 and dimension 3 over GF(7)?
2. Given an odd prime p, does there exist a self dual code of length
   (i) 8 and dimension 4, and
   (ii) 16 and dimension 8 over GF(p)?

(Hint: Every odd prime can be expressed as a sum of four squares.)

3. Given an odd prime p and a positive integer m, does there always exist a self dual code of length $4m$ and dimension $2m$ over GF(p)?
4. Find all possible self dual codes of length
   (i) 4;
   (ii) 6;
   over the field of four elements.
5. Does there exist a self dual code of length 6 over the field of 9 elements?
6. Describe (if possible) a self dual code of length 8 over GF(4).

5.3 WEIGHT DISTRIBUTION OF THE DUAL CODE OF A BINARY LINEAR CODE

In this section, we prove one of the most important results in algebraic coding theory. This is a result of F. J. MacWilliams (MacWilliams and Sloane, 1978) which says that the weight enumerator of the dual code $\mathscr{C}^\perp$ is completely determined once the weight enumerator of $\mathscr{C}$ is known.

Definition 5.8

Let $\mathscr{C}$ be an $[n, k, d]$ linear code over a finite field F and let $\mathscr{C}^\perp$ be its dual code. Recall that $\mathscr{C}^\perp$ is a linear $[n, n-k, -]$ code over F. Let A_i denote the number of code words in $\mathscr{C}$ which are of weight i. We call the polynomial

$$\sum_{i=0}^{n} A_i x^{n-i} y^i$$

the **weight enumerator** of $\mathscr{C}$ and denote it by $W_{\mathscr{C}}(x, y)$. This is a homogeneous polynomial of degree n in the variables x and y. Observe that we can rewrite this polynomial as

$$W_{\mathscr{C}}(x, y) = \sum_{u \in \mathscr{C}} x^{n - \mathrm{wt}(u)} y^{\mathrm{wt}(u)}$$

We denote by A'_i the number of code words of weight i in the dual code $\mathscr{C}^{\perp}$. Then we can similarly have the weight enumerator of the dual code $\mathscr{C}^{\perp}$ by

$$W_{\mathscr{C}^{\perp}}(x, y) = \sum_{i=0}^{n} A'_i x^{n-i} y^i$$

Examples 5.5

Case (i)
The weight enumerator of the code of Case (iv)(a) of Examples 5.1 is

$$W_{\mathscr{C}}(x, y) = x^4 + x^3 y + 3x^2 y^2 + 3xy^3$$

while that of its dual (refer to Case (i) of Examples 5.2) is

$$W_{\mathscr{C}^{\perp}} = x^4 + xy^3$$

Case (ii)
The weight enumerator of $[7, 4, 3]$ Hamming code is (refer to Case (ii) of Examples 5.2):

$$W_{\mathscr{C}}(x, y) = x^7 + 7x^4 y^3 + 7x^3 y^4 + y^7$$

while that of its dual is

$$W_{\mathscr{C}^{\perp}}(x, y) = x^7 + 7x^3 y^4$$

Case (iii)
The weight enumerator of $(4, 7)$ polynomial code $\mathscr{C}$ generated by the polynomial $1 + X + X^3$ (refer to Case (iii) of Examples 2.1) is given by

$$W_{\mathscr{C}}(x, y) = x^7 + 7x^4 y^3 + 7x^3 y^4 + y^7$$

which is the same as that of the $[7, 4, 3]$ Hamming code. The weight enumerator of its dual code is

$$W_{\mathscr{C}^{\perp}}(x, y) = x^7 + 7x^3 y^4$$

again the same (as it should be in view of MacWilliams's Identity to be proved later) as that of the dual of $[7, 4, 3]$ Hamming code.