Cyclic Codes

Although it will turn out that cyclic codes are not asymptotically good codes, they are an important class of codes which include many useful and widely implemented short length codes, most notably the Golay codes and the general class of BCH codes. BCH codes have a prescribed minimum distance which means that, by construction, we can bound from below the minimum distance and therefore guarantee some error-correction properties. Cyclic codes also provide examples of linear codes with few weights, which allows us to construct designs via Theorem 4.22. The cyclic structure of these codes will appear again in ▶ Chapter 10, when we consider p-adic codes.

5.1 Basic Properties

A linear code C is called **cyclic** if, for all $(c_1, \ldots, c_n) \in C$, the vector $(c_n, c_1, \ldots, c_{n-1}) \in C$.

The map

$$(c_1, \ldots, c_n) \mapsto c_1 + c_2 X + \cdots + c_n X^{n-1}$$

is a bijection between the vectors of $\mathbb{F}_q^n$ and the polynomials in

$$\mathbb{F}_q[X]/(X^n - 1).$$

We define the **weight** $\mathrm{wt}(u)$ of a polynomial $u(X) \in \mathbb{F}_q[X]/(X^n - 1)$ of degree less than n, as the weight of the corresponding vector of $\mathbb{F}_q^n$. In other words, the number of non-zero coefficients that it has.

An **ideal** I of a polynomial ring is a subspace with the property that if $f \in I$, then $Xf \in I$.

S. Ball, *A Course in Algebraic Error-Correcting Codes*, Compact Textbooks in Mathematics,
https://doi.org/10.1007/978-3-030-41153-4_5

Lemma 5.1 *A cyclic code C is mapped by the bijection to an ideal I in $\mathbb{F}_q[X]/(X^n - 1)$.*

Proof
This is precisely the condition that a linear code satisfies to be cyclic. □

We assume that $(n, q) = 1$ so that the polynomial $X^n - 1$ has no repeated factors in its factorisation, see ▶ Section 2.3.

5

The ring $\mathbb{F}_q[X]/(X^n - 1)$ is a principal ideal ring, so I in Lemma 5.1 is a principal ideal. Hence,

$$I = \langle g \rangle = \{fg \mid f \in \mathbb{F}_q[X]/(X^n - 1)\}$$

for some polynomial g, which is monic and of lowest degree in the ideal.

Therefore, a cyclic code C is mapped by the bijection to $\langle g \rangle$. We will from now on write $C = \langle g \rangle$, for some polynomial g.

Lemma 5.2 *If $C = \langle g \rangle$ is a cyclic code of length n, then g divides $X^n - 1$ and C has dimension at least $n - \deg g$.*

Proof
If $g(X)$ does not divide $X^n - 1$, then, using the Euclidean algorithm, we can find polynomials $a(X)$ and $b(X)$ such that

$$a(X)g(X) + b(X)(X^n - 1)$$

is equal to the greatest common divisor of $g(X)$ and $X^n - 1$, which has degree less than g. This contradicts the property that g has minimal degree in the ideal I. Therefore, g divides $X^n - 1$.

The polynomials $X^j g$, for $j = 0, \ldots, n - \deg(g) - 1$ are linearly independent polynomials in $\langle g \rangle$, so the dimension of C is at least $n - \deg g$. □

In fact, we shall see that the dimension k of C is precisely $n - \deg g$. This follows from the following theorem.

Theorem 5.3
Let $C = \langle g \rangle$ be a cyclic code of length n. The dual code $C^\perp$ is the cyclic code $\langle \overleftarrow{h} \rangle$, where $g(X)h(X) = X^n - 1$ and $\overleftarrow{h}(X) = X^k h(X^{-1})$.

Proof
Suppose that

$$g(X) = \sum_{j=0}^{n-k} g_j X^j$$

and

$$h(X) = \sum_{i=0}^{k} h_i X^i.$$

The code $\langle g \rangle$ contains the row span of the $k \times n$ matrix

$$\mathrm{G} = \begin{pmatrix} g_0 & \dots & g_{n-k} & 0 & \dots & \dots & 0 \\ 0 & g_0 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & \dots & 0 & g_0 & \dots & g_{n-k} \end{pmatrix}$$

and the code $\langle \overleftarrow{h} \rangle$ contains the row span of the $(n-k) \times n$ matrix

$$\mathrm{H} = \begin{pmatrix} h_k & \dots & h_0 & 0 & \dots & \dots & 0 \\ 0 & h_k & \dots & h_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \dots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & \dots & 0 & h_k & \dots & h_0 \end{pmatrix}.$$

The scalar product between the s-th row of G and the r-th row of H, where $s \in \{1, \dots, k\}$ and $r \in \{1, \dots, n-k\}$ is

$$\sum_{i=s}^{k+r} g_{i-s} h_{k+r-i},$$

which is the coefficient of X^{k+r-s} in gh. Since $1 \leqslant k + r - s \leqslant n - 1$, this coefficient is zero and so $\mathrm{GH}^t = 0$.

Since

$$n = \dim C + \dim C^{\perp} \geqslant \operatorname{rank}(\mathrm{G}) + \operatorname{rank}(\mathrm{H}) = n, \tag{5.1}$$

the theorem follows. □

Corollary 5.4 *The code $C = \langle g \rangle$ of length n has dimension $n - \deg g$.*

Proof

Let G and H be as in the previous proof. Equation (5.1) implies that the dimension of C is the rank of G, which is k. □

Example 5.5 (perfect ternary Golay code)
Consider the factorisation of $X^{11} - 1$ over $\mathbb{F}_3$. As in ▶ Section 2.3, we calculate the cyclotomic subsets of the multiples of 3 modulo 11,

$$\{0\}, \{1, 3, 9, 5, 4\}, \{2, 6, 7, 10, 8\}.$$

According to Lemma 2.12, there are two factors of degree 5 which are

$$(X - \alpha)(X - \alpha^3)(X - \alpha^9)(X - \alpha^5)(X - \alpha^4)$$

and

$$(X - \alpha^2)(X - \alpha^6)(X - \alpha^7)(X - \alpha^{10})(X - \alpha^8),$$

where α is a primitive 11-th root of unity in $\mathbb{F}_{3^5}$.

Suppose that

$$X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$$

is the first of these factors. Then $a_0 = -\alpha^{22} = -1$. Since the roots of the first factor are the reciprocals of the roots of the second factor, the second factor is

$$X^5 - a_1X^4 - a_2X^3 - a_3X^2 - a_4X - 1.$$

It is fairly easy to deduce from this that the factorisation is

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

The cyclic code $C = \langle X^5 - X^3 + X^2 - X - 1\rangle$ over $\mathbb{F}_3$ is the perfect ternary Golay code of length 11. To prove that this is a perfect code we need to show that the minimum weight of a non-zero codeword is 5 (and hence the minimum distance is 5 according to Lemma 4.1) and observe that

$$\left(1 + 2\binom{11}{1} + 4\binom{11}{2}\right)3^6 = 3^{11},$$

so the sphere-packing bound of Theorem 3.9 is attained.

Adding a column of 1's to the generator matrix

$$\begin{pmatrix}
-1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & -1 & 0 & 1
\end{pmatrix}$$

we get a generator matrix of a self-dual code $\overline{C}$ of length 12. This we can check by computing the scalar product of any two rows and verifying that it is zero (modulo 3). Since this code is self-dual, the codewords have weights which are multiples of 3. If we can rule out the possibility that a codeword has weight 3, which we will in ▶ Section 5.3, then the minimum weight of a non-zero codeword of $\overline{C}$ is 6, which implies that the minimum weight of a non-zero codeword of the cyclic code $\langle X^5 - X^3 + X^2 - X - 1\rangle$ is 5. Therefore, C is a $[11, 6, 5]_3$ code and $\overline{C}$ is a $[12, 6, 6]_3$ code. ■

5.2 Quadratic Residue Codes

Let n and q be primes for which q is a square in $\mathbb{F}_n$, where we consider the field $\mathbb{F}_n \cong \mathbb{Z}/n\mathbb{Z}$ to be addition and multiplication modulo n, defined on the set $\{0, 1, \ldots, n-1\}$.

Let α be a primitive n-th root of unity in some extension field of $\mathbb{F}_q$.

Define

$$g(X) = \prod (X - \alpha^r),$$

where the product runs over the non-zero squares r in $\mathbb{F}_n$.

Lemma 5.6 *The polynomial $g(X)$ divides $X^n - 1$ in $\mathbb{F}_q[X]$.*

Proof

Since q is a square in $\mathbb{F}_n$, the map

$$r \mapsto qr$$

is a bijection from the squares of $\mathbb{F}_n$ to the squares of $\mathbb{F}_n$, for all non-zero squares $r \in \mathbb{F}_n$.

Hence,

$$g(X) = \prod (X - \alpha^r) = \prod (X - \alpha^{rq}),$$

where the product runs over the non-zero squares r in $\mathbb{F}_n$.

Lemma 2.11 implies that $g(X) \in \mathbb{F}_q[X]$ and note that the roots of $g(X)$ are distinct n-th roots of 1. □

Since $g(X)$ is a factor of $X^n - 1$, we can define the cyclic code $\langle g\rangle$ of length n over $\mathbb{F}_q$. This code is called the **quadratic residue code**.

We can obtain evidence that the minimum distance of a quadratic residue code is quite good from the following theorems.

Theorem 5.7
If $u \in \langle g\rangle$ and $u(1) \neq 0$, then $\mathrm{wt}(u)^2 \geqslant n$.

Proof

Since $u \in \langle g \rangle$, the n-th roots of unity α^r of $\mathbb{F}_q$, where r is a non-zero square in $\mathbb{F}_n$, are zeros of $u(X)$.

Let t be a non-square of $\mathbb{F}_n$. The n-th roots of unity α^s of $\mathbb{F}_q$, where s is a non-square in $\mathbb{F}_n$, are zeros of $u(X^t)$, since the product of two non-squares is a square. Therefore, all the n-th roots of unity of $\mathbb{F}_q$, except 1, are zeros of $u(X)u(X^t)$. Hence,

$$u(X)u(X^t) = (1 + X + \cdots + X^{n-1})v(X),$$

for some polynomial $v(X)$. Since $u(1) \neq 0$, we have that $v(1) \neq 0$.

Therefore, in the ring $\mathbb{F}_q[X]/(X^n - 1)$,

$$u(X)u(X^t) = (1 + X + \cdots + X^{n-1})v(1),$$

since $v(X) = v(1) + (X - 1)v_1(X)$, for some polynomial $v_1(X)$.

Since $u(X)$ has $\mathrm{wt}(u)$ terms, this implies that $\mathrm{wt}(u)^2 \geqslant n$. □

Theorem 5.8

If $n \equiv -1$ mod 4, $u \in \langle g \rangle$ and $u(1) \neq 0$, then $\mathrm{wt}(u)^2 - \mathrm{wt}(u) + 1 \geqslant n$.

Proof

If $n \equiv -1 \bmod 4$, then -1 is a non-square in $\mathbb{F}_n$, since $(-1)^{(n-1)/2} = -1$. Therefore, in the proof of Theorem 5.7, we can take $t = -1$. Then,

$$u(X)u(X^{-1}) = (1 + X + \cdots + X^{n-1})v(1).$$

In the product there are at least $\mathrm{wt}(u)$ terms of $u(X)$ which multiply with a term of $u(X^{-1})$ to give a constant term, since $X^j X^{-j} = 1$. Hence,

$$\mathrm{wt}(u)^2 - \mathrm{wt}(u) \geqslant n - 1.$$

□

Example 5.9 (perfect binary Golay code)

Consider the quadratic residue code with $n = 23$ and $q = 2$. Let ϵ be a primitive element of $\mathbb{F}_{2^{11}} \cong \mathbb{F}_2[X]/(X^{11} + X^2 + 1)$ and let $\alpha = \epsilon^{89}$. Then α is a primitive 23-rd root of unity. By Lemma 5.6, the factorisation of $X^{23} - 1$ in $\mathbb{F}_2[X]$ has a factor

$$g(X) = \prod_{r \in S} (X - \alpha^r),$$

where $S = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$ is the set of non-zero squares of $\mathbb{F}_{23}$.

If α^j is a root of $g(X)$, then α^{-j} is not, which implies that

$$X^{23} - 1 = (X - 1)g(X)\overleftarrow{g}(X).$$

Solving this polynomial identity we deduce that one of $g(X)$ or $\overleftarrow{g}(X)$ is

$$X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1.$$

By checking that the sum of the roots of $g(X)$ is zero, we deduce that this polynomial is $g(X)$.

The quadratic residue code $\langle g \rangle$ is the perfect binary Golay code of length 23. By Corollary 5.4, it has dimension 12.

Observe that

$$\left(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}\right)2^{12} = 2^{23},$$

so the bound in Theorem 3.9 is attained.

The following matrix is a generator matrix for the code $\langle g \rangle$:

$$\begin{pmatrix}
1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1
\end{pmatrix}$$

Adding a column of 1's to this matrix we get a generator matrix for a 12-dimensional linear code $\overline{C}$ of length 24. One can verify that all codewords of $\overline{C}$ have weights which are multiples of four, see Exercise 5.3. We shall prove in ▶ Section 5.3 that the cyclic code $\langle g \rangle$ has minimum weight at least 5. Therefore, the minimum weight of a non-zero codeword of $\overline{C}$ is 8, which implies that the minimum weight of a non-zero codeword of $\langle g \rangle$ is 7. By Lemma 4.1, the minimum distance of $\langle g \rangle$ is 7. Hence, $\langle g \rangle$ is a $[23, 12, 7]_2$ code and $\overline{C}$ is a $[24, 12, 8]_2$ code. ■

5.3 BCH Codes

Let α be a primitive n-th root of unity in $\mathbb{F}_{q^m}$. BCH codes are a class of cyclic codes in which we choose α so that $\alpha, \alpha^2, \ldots, \alpha^{d_0-1}$ are roots of a low degree polynomial g of $\mathbb{F}_q[X]$, for some $d_0 < n$. This allows us to bound the minimum distance of the code $\langle g \rangle$. The lower the degree of g, the larger the dimension (and hence the size) of the code.

Suppose that $g(X) \in \mathbb{F}_q[X]$ is the polynomial of minimal degree such that

$$g(\alpha^j) = 0,$$

for $j = 1, \ldots, d_0 - 1$.

The code $\langle g \rangle$ is called a **BCH code**, after Bose, Ray-Chaudhuri and Hocquenghem who introduced this family of cyclic codes. The parameter d_0 is called the **prescribed minimum distance** because of the following theorem.

Theorem 5.10
The dimension of the BCH code $\langle g \rangle$ is at least $n - m(d_0 - 1)$ and its minimum distance is at least d_0.

Proof
Let $j \in \{1, \ldots, d_0 - 1\}$. By Lemma 2.11, the polynomial

$$(X - \alpha^j)(X - \alpha^{jq}) \cdots (X - \alpha^{jq^{m-1}})$$

is in $\mathbb{F}_q[X]$. Clearly, it is zero at α^j. Since this polynomial has degree m this implies that there is a polynomial of degree $m(d_0 - 1)$ in $\mathbb{F}_q[X]$ which is zero at α_j, for all $j = 1, \ldots, d_0 - 1$.

Thus, the degree of g is at most $m(d_0 - 1)$ so, by Corollary 5.4, the dimension of $\langle g \rangle$ is at least $n - m(d_0 - 1)$.

Suppose that there is an $f \in \langle g \rangle$ for which $\mathrm{wt}(f)$ is at most $d_0 - 1$. Then

$$f(X) = b_1 X^{k_1} + \cdots + b_{d_0-1} X^{k_{d_0-1}},$$

for some $k_1, \ldots, k_{d_0-1}$.

Since $f \in \langle g \rangle$,

$$f(\alpha^j) = 0$$

for all $j = 1, \ldots, d_0 - 1$. Writing this in matrix form these equations are

$$\begin{pmatrix} \alpha^{k_1} & \alpha^{k_2} & \ldots & \alpha^{k_{d_0-1}} \\ \alpha^{2k_1} & \alpha^{2k_2} & \ldots & \alpha^{2k_{d_0-1}} \\ . & . & . & . \\ \alpha^{(d_0-1)k_1} & \alpha^{(d_0-1)k_2} & \ldots & \alpha^{(d_0-1)k_{d_0-1}} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_{d_0-1} \end{pmatrix} = 0.$$

The determinant of the matrix is

$$\prod_{i \neq j} (\alpha^{k_i} - \alpha^{k_j}),$$

which is non-zero. This implies that the only solution to the above system is $f(X) = 0$. Hence, the minimum weight of a non-zero codeword of the cyclic code $\langle g \rangle$ is at least d_0. The lemma follows since, by Lemma 4.1, the minimum weight of a non-zero codeword of a linear code is equal to its minimum distance. □

Example 5.11
Let α be a primitive 31-st root of unity in $\mathbb{F}_{32}$. By Lemma 2.12, we obtain the factorisation of $X^{31} - 1$ over $\mathbb{F}_2$ by considering the cyclotomy classes

$$\{1, 2, 4, 8, 16\},\ \{3, 6, 12, 24, 17\},\ \{5, 10, 20, 9, 18\},\ \{7, 14, 28, 25, 19\},$$
$$\{11, 22, 13, 26, 21\}.$$

The i-th cyclotomy class gives a polynomial $f_i(X)$ in $\mathbb{F}_2[X]$ which is zero at α^j for j in the cyclotomy class. For example,

$$f_1(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)(X - \alpha^{16})$$

is in $\mathbb{F}_2[X]$ and is zero at α^j for $j \in \{1, 2, 4, 8, 16\}$.

Let

$$g(X) = f_1(X) f_2(X) f_3(X).$$

According to Corollary 5.4, the cyclic code $\langle g \rangle$ is a 16-dimensional linear code.

Since 1, 2, 3, 4, 5 and 6 appear in the first three cyclotomic subsets,

$$g(\alpha^j) = 0,$$

for $j = 1, \ldots, 6$. Theorem 5.10 implies that $\langle g \rangle$ is a $[31, 16, \geqslant 7]_2$ code. It is in fact a $[31, 16, 7]_2$ code. Since there exists a $[31, 16, 8]_2$ code, $\langle g \rangle$ is not an optimal linear code for this length and dimension. ■

Example 5.12 (shortened Reed–Solomon code)
Let α be a primitive $(q-1)$-st root of unity in $\mathbb{F}_q$. By Theorem 2.4, the polynomial $X^{q-1} - 1$ factorises into linear factors over $\mathbb{F}_q$. Each cyclotomy class has size 1 and the factors are

$$f_i(X) = X - \alpha^i,$$

for $i = 0, \ldots, q - 2$.

Let

$$g(X) = f_1(X)f_2(X)\cdots f_{d-1}(X).$$

According to Corollary 5.4, $\langle g \rangle$ is a $(n - d + 1)$-dimensional linear code of length n. According to Theorem 5.10, $\langle g \rangle$ has minimum distance at least d. This is an example of an MDS code, which we will study in more depth in ▶ Chapter 6. ■

5

Example 5.13

In Example 5.9, the numbers 1, 2, 3 and 4 appear in the same cyclotomy class, so Theorem 5.10 implies that the binary Golay code has weight at least 5. As observed in Example 5.9, this implies that the extended binary Golay code $\overline{C}$ has no codewords of weight 4, which implies that the minimum distance of $\overline{C}$ is 8. This, in turn, implies that the minimum distance of the binary Golay code is 7. ■

Example 5.14

Theorem 5.10 generalises in a straightforward way to Exercise 5.5. We can now establish that the minimum distance of the ternary Golay code is 5. By Exercise 5.5, since 3, 4 and 5 appear in the same cyclotomy class (and 6, 7 and 8 appear in the same cyclotomy class), the ternary Golay code in Example 5.5 has minimum distance at least 4. Therefore, the extended code $\overline{C}$ has no codewords of weight three, so the weight of a non-zero codeword of the extended code is either 6, 9 or 12. As observed in Example 5.5, this implies that the minimum distance of the ternary Golay code is 5.

■

The following theorem, which we quote without proof, states that there is no sequence of asymptotically good BCH codes.

Theorem 5.15

There is no infinite sequence of $[n.k, d]_q$ BCH codes for which both $\delta = d/n$ and $R = k/n$ are bounded away from zero.

5.4 Comments

The introduction of cyclic codes and quadratic residue codes is widely accredited to Eugene Prange and Andrew Gleason who proved the automorphism group of an extended quadratic residue code has a subgroup which is isomorphic to either PSL(2, p) or SL(2, p), see [12]. The Golay codes were discovered by Golay [27]. The BCH codes were introduced by Bose and Ray-Chaudhuri in [13] and independently by Hocquenghem in [38]. The fact that long BCH codes are asymptotically bad is proven by Lin and Welden in [47]. The code in Exercise 5.7 is a Zetterberg code, one of a family of $[4^m + 1, 4^m + 1 - 4m, 5]_2$ codes.

5.5 Exercises

5.1 *Let $\overline{C}$ be the extended ternary Golay code from Example 5.5.*

i. Verify that the factorisation of $X^{11} - 1$ in $\mathbb{F}_3[X]$ is as in Example 5.5.

ii. Prove that the weight enumerator of $\overline{C}$ is

$$A(X) = 1 + 264X^6 + 440X^9 + 24X^{12}.$$

iii. Let S be the set of 12 points of PG(5, 3) obtained from the set of columns of a generator matrix of the code $\overline{C}$. Label the points of S by the elements of $\{1, \ldots, 12\}$ and define a set D of 6-subsets to be the points of S which are dependent (i.e. are contained in a hyperplane of PG(5, 3)). Prove that D is a 5-(12, 6, 1) design.

iv. Verify that Theorem 4.22 implies that the set of supports of the codewords of weight 6 of $\overline{C}$ is a 5-(12, 6, 1) design.

5.2 *Prove that in Example 5.9 the code $\langle \overleftarrow{g} \rangle$ is equivalent to the code $\langle g \rangle$.*

5.3

i. Prove that the extended Golay code over $\mathbb{F}_2$, the code $\overline{C}$ in Example 5.9, is self-dual and that the weights of the codewords of $\overline{C}$ are multiples of 4.

ii. Prove that the weight enumerator of the code $\overline{C}$ is

$$A(X) = 1 + 759X^8 + 2576X^{12} + 759X^{16} + X^{24}.$$

iii. Apply Theorem 4.22 to construct a 5-(24, 8, 1) design.

5.4 *Investigate the observation that if $n \equiv -1$ modulo 4 and $\langle g \rangle$ is a quadratic residue code, then the reverse of the polynomial $(X^n - 1)/(X - 1)g(X)$ is $g(X)$. Does this imply that the extension of the code $\langle g \rangle$ is self-dual?*

5.5 *Suppose that $g(X) \in \mathbb{F}_q[X]$ is the polynomial of minimal degree such that*

$$g(\alpha^j) = 0,$$

for $j = \ell + 1, \ldots, \ell + d_0 - 1$.

Prove that the dimension of $\langle g \rangle$ is at least $n - m(d_0 - 1)$ and the minimum distance of $\langle g \rangle$ is at least d_0.

5.6 *Construct the largest possible BCH code with the following parameters.*

i. A binary code of length 15 with minimum distance at least 5.

ii. A binary code of length 31 with minimum distance at least 11.

iii. A ternary code of length 13 with minimum distance at least 7.

Compare the dimension of the codes with the Griesmer bound, the sphere-packing bound and the Gilbert–Varshamov bound.

5.7

i. *Prove that* $X^{17}+1$ *factorises in* $\mathbb{F}_2[X]$ *as* $(X+1)f(X)g(X)$*, where*

$$f(X) = \overleftarrow{f}(X) = X^8 + X^7 + X^6 + \cdots$$

and $g(X) = \overleftarrow{g}(X)$.

ii. *Construct a* $[17, 9, 5]_2$ *code.*

ii. *Construct a* $[18, 9, 6]_2$ *code.*

5.8

i. *Prove that the polynomial* $X^{11}+1$ *factorises in* $\mathbb{F}_4[X]$ *into two irreducible factors of degree* 5 *and one of degree* 1.

ii. *Using one of the factors of degree* 5*, construct a* $[11, 6, d]_4$ *code* C.

iii. *Prove that* C *is a* $[11, 6, \geqslant 4]_4$ *code.*

iv. *With the aid of a computer, or not, verify that* C *is a* $[11, 6, 5]_4$ *code.*

5.9

i. *Prove that the polynomial* $X^{17}+1$ *factorises in* $\mathbb{F}_4[X]$ *into four irreducible factors of degree* 4 *and one of degree* 1.

ii. *Construct a* $[17, 9, \geqslant 7]_4$ *code.*

iii. *Let* $g(X) = X^8 + eX^7 + X^6 + X^5 + (1+e)X^4 + X^3 + X^2 + eX + 1$*, where* e *is an element of* $\mathbb{F}_4$ *such that* $e^2 = e+1$*. Prove that* g *divides* $X^{17}+1$.

iv. *Assuming that the code in ii. is* $\langle g \rangle$*, prove that the minimum distance of the code constructed in ii. is* 7.