An Introduction to Coding Theory: Lecture Notes

Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA

http://www.math.mtu.edu/∼tonchev/Coding-Theory-Tohoku-June-09.pdf

May 16, 2009

Contents

Often, when I say my name, **Vladimir**, over the phone, I am asked the question:

- "Can you **spell** it, please?"

Often, when I say my name, **Vladimir**, over the phone, I am asked the question:

- "Can you **spell** it, please?"

Then I reply:

- V as in Victor
- L as in Lancing
- A as in Apple
- D as in David
- I as in Igor
- M as in Mary
- I as in Igor
- R as in Richard

The original **message** (essential information) is:

$$Vladimir$$

(8 **information symbols**).

The original **message** (essential information) is:

$$Vladimir$$

(8 **information symbols**).

The **encoded** message:

$$VictorLancingAppleDavidIgorMaryIgorRichard$$

(42 symbols).

The original **message** (essential information) is:

$$Vladimir$$

(8 **information symbols**).

The **encoded** message:

$$VictorLancingAppleDavidIgorMaryIgorRichard$$

(42 symbols).

The added symbols

ictor ancing pple avid gor ary gor ichard

are $42 - 8 = 34$ **redundancy symbols**.

Questions:

- Can we do better than that?

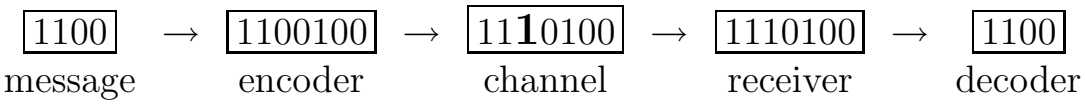
Questions:

- Can we do better than that?
- What is the smallest number of redundancy symbols that would insure the detection and correction of a single error?

Questions:

- Can we do better than that?
- What is the smallest number of redundancy symbols that would insure the detection and correction of a single error?
- What is the smallest number of redundancy symbols that would insure the detection and correction of a double error?

A basic model of a Communication Channel



1 Error-correcting codes

The mathematical theory of error-correcting codes originated in a paper by Claude Shannon [25] from 1948.

A *code* (or a *block code*) C of length n over a finite alphabet F_q of size q is a subset C of the set F_q^n of all n-letter words with components from F_q. We refer to the elements of C as words, codewords, or vectors. A code over F_q is called a *q-ary* code. A code is *binary* if $q = 2$, *ternary* if $q = 3$, etc.

The *Hamming distance* $d(x, y)$ between $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ is defined as the number of positions in which x and y differ:

$$d(x, y) = |\{i \mid x_i \neq y_i\}|.$$

The Hamming distance enjoys the usual properties of a distance function:

1. $d(x, y) \geq 0$, and $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y)$ for arbitrary $x, y, z \in F_q^n$; (the triangle inequality).

A Hamming *sphere* $S_r^{n,q}(x)$ of radius r with center $x \in F_q^n$ is defined as the set of all words being at distance at most r from x:

$$S_r^{n,q}(x) = \{y \mid y \in F_q^n,\ d(x, y) \leq r\}.$$

Exercise 1.1 Prove that a sphere of radius r in F_q^n is of size

$$\sum_{i=0}^{r} \binom{n}{i} (q-1)^i \tag{1}$$

The *minimum distance* d of a code C is defined as the smallest Hamming distance between pairs of words from C:

$$d = \min d(x, y) :\ x, y \in C,\ x \neq y.$$

A code can be thought as a collection of messages that are being transmitted over a communication channel. If the channel is subject to noise, some of the components of a message $x = (x_1, \ldots, x_n) \in C$ may be corrupted. Thus, the received message $y = (y_1, \ldots, y_n)$ may differ from x, and the distance $d(x, y)$ counts the number of *errors* in y.

The process of recovering the original message x from the received message y is called *decoding*.

Theorem 1.2 *If C is a code with minimum distance $d \geq 3$, there is a decoding algorithm that corrects up to $[(d-1)/2]$ errors.*

Proof. Assume that a message $x \in C$ is sent, and the number of positions of x that have been corrupted does not exceed $[(d-1)/2]$. The received vector y belongs to the sphere $S_r^{n,q}(x)$, where $r = [(d-1)/2]$.

It follows from the triangle inequality that the spheres of radius $r = [(d-1)/2]$ around all codewords from C are pairwise disjoint. Thus, the codeword x can be recovered from y as the unique word from C being at distance at most $[(d-1)/2]$ from y. □

The proof of Theorem 1.2 implies the following simple decoding algorithm, known as *maximum likelihood decoding*: the received vector y is decodes as $x \in C$ where x is the closest codeword to y:

$$\min_{z \in C} d(y,z) = d(y,x).$$

Exercise 1.3 Show that a code with minimum distance d can detect up to $d-1$ errors.

Exercise 1.4 Prove the triangle inequality for the Hamming distance.

Exercise 1.5 Give an example of a binary code of length 7, size 7, and minimum distance 4, or prove that such a code does not exist.

Exercise 1.6 Give an example of a binary code of length 7, size 17, and minimum distance 3, or prove that such a code does not exist.

2 Linear codes

A *field* is a set F with two operations, *addition* $+$, and *multiplication* $\cdot$, satisfying the following axioms:

a0. For every $a, b \in F$ there is a unique $c \in F$ such that $a + b = c$.
a1. $(a + b) + c = a + (b + c)$.
a2. $a + b = b + a$.
a3. There is an element $0 \in F$ such that $a + 0 = a$ for every $a \in F$.
a4. For every $a \in F$ there is an element $-a \in F$ such that $a + (-a) = 0$.
m0. For every $a, b \in F$ there is a unique $d \in F$ such that $ab = d$.
m1. $(ab)c = a(bc)$.
m2. $ab = ba$.
m3. There is an element $1 \in F$ such that $a \cdot 1 = a$ for every $a \in F$.
m4. For every $a \in F$, $a \neq 0$, there is an element $a^{-1} \in F$ such that $aa^{-1} = 1$.
d. $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

Equivalently, a set F with two operations $+, \cdot$ is a filed if $(F, +)$ and $(F \setminus \{0\}, \cdot)$ are commutative groups.

Familiar examples of fields are the filed of real numbers and the field of complex numbers. These fields contain infinitely many elements.

A field is *finite* if in contains a finite number of elements. The number of elements of a finite field F, $q = |F|$, is called the *order* of F.

Example 2.1 The smallest field of order 2 consists of two elements:

$$F_2 = \{0,\ 1\}.$$

Multiplication is the same as for real numbers:

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1.$$

Addition is modulo 2:

$$0 + 0 = 1 + 1 = 0,\ 0 + 1 = 1 + 0 = 1.$$

A finite field of order q is usually denoted by F_q or $GF(q)$ (Galois Field of order q). The order q of a finite field is necessarily a prime power. If q is a prime number, then $GF(q)$=Z_q=$\{0, 1, \ldots, q - 1\}$, and the operations are addition and multiplication modulo q.

If F_q is a field of order q, the set

$$F_q^n = \{ (x_1, \ldots, x_n) \mid x_i \in F_q \}$$

of all n-letter words with components from F_q is an n dimensional vector space, with addition of vectors and multiplication of vectors by a scalar performed in F_q:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n),\ \alpha \in F_q.$$

Definition 2.2 A *linear* code over F_q is a linear subspace of the n-dimensional vector space F_q^n.

Definition 2.3 A $k \times n$ matrix G whose rows form a basis of an $[n, k]$ code C is called a *generator matrix* of C.

Exercise 2.4 Find the number of distinct generator matrices of a q-ary linear $[n, k]$ code.

Definition 2.5 Given a code $C \subseteq F_q^n$, the *dual code* $C^\perp$ is defined as the orthogonal space of C:

$$C^\perp = \{y \in F_q^n \mid y \cdot x = 0 \text{ for every } x \in C\},$$

where $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n)$ and

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n \tag{2}$$

is the ordinary scalar product in F_q^n (note that other inner products are used sometimes).

If C is a linear $[n, k]$ code then $C^\perp$ is a linear $[n, n-k]$ code.

Definition 2.6 Any generator matrix of $C^\perp$ is called a *parity check matrix* of C.

If H is a parity check matrix, the code C consists of all vectors $x = (x_1, \ldots, x_n)$ which are solutions of the homogeneous system of linear equations with coefficient matrix H:

$$C = \{x \in F_q^n \mid Hx^T = 0.\} \tag{3}$$

Definition 2.7 The Hamming *weight* $w(x)$ of a vector $x \in F_q^n$ is defined as the number of its nonzero components:

$$w(x) = |\{i \mid x_i \neq 0\}|.$$

Clearly, $d(x, y) = w(x - y)$, where d is the Hamming distance. In particular, $w(x) = d(x, \bar{0})$, where $\bar{0}$ is the all-zero vector.

Definition 2.8 The *minimum weight* of a code C is defined as the smallest among the weights of all nonzero vectors in C.

An important property of the Hamming distance is that it is invariant under translation:

$$d(x, y) = d(x + z, y + z)$$

for arbitrary vectors x, y, z. This property implies the following result.

Theorem 2.9 *The minimum distance of a linear code is equal to its minimum weight.*

We use the notation $[n, k, d]$ for a linear $[n, k]$ code with minimum distance, or equivalently, minimum weight d. For example, the whole space F_q^n is an $[n, n, 1]$ code.

In the binary case ($q = 2$), the weight function satisfies the following identity:

$$w(x + y) = w(x) + w(y) - 2w(x * y) \tag{4}$$

for arbitrary vectors $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n)$, $x, y \in F_2^n$, where $x * y$ is defined as

$$x * y = (x_1 y_1, \ldots, x_n y_n).$$

Exercise 2.10 Prove the identity (4).

Exercise 2.11 (i) Show that the set C of all binary vectors of length $n \geq 2$ of even weight form an $[n, n - 1, 2]$ code.
(ii) Find a parity check matrix of C.
(iii) Find a generator matrix of C.

The minimum weight of a linear code can be determined by linear dependencies of columns of its parity check matrix. Assume that C is a linear code of length n with a parity check matrix $H = [h_1, \ldots, h_n]$, where h_i is the ith

column of H, $1 \leq i \leq n$. Let x be a nonzero vector from C of weight w, and let $x_{i_1}, \ldots, x_{i_w}$ be the nonzero components of x. We have

$$Hx^T = h_{i_1} x_{i_1} + \cdots + h_{i_w} x_{i_w} = 0,$$

hence, the columns $h_{i_1}, \ldots, h_{i_w}$ are linearly dependent. This implies the following simple, but very useful result.

Theorem 2.12 *The minimum weight of a linear code with a parity check matrix H is equal to the largest integer d such that every $d-1$ columns of H are linearly independent.*

Corollary 2.13 *A linear code with a parity check matrix H can correct single errors if every two columns of H are linearly independent. In particular, a binary linear code can correct single errors if all columns of its parity check matrix are nonzero and distinct.*

Example 2.14 All columns of the following matrix

$$H = \begin{pmatrix} 11110 \\ 01101 \\ 00111 \end{pmatrix}$$

are nonzero and distinct. Thus, H is a parity check matrix of a binary code with minimum weight $d \geq 3$.

Exercise 2.15 Determine the minimum distance of the code from Example 2.14.

Another immediate corollary of Theorem 2.12 is the following inequality known in coding theory as the *Singleton Bound* .

Theorem 2.16 *(The Singleton Bound). If C is an $[n, k, d]$ code then*

$$d \leq n - k + 1. \tag{5}$$

Proof. Let H be an $(n-k) \times n$ parity check matrix of C. The rank of H does not exceed the number of rows $n-k$. Consequently, the largest number of linearly independent columns of H is $n-k$, while every $n-k+1$ columns of H are linearly dependent. □

Definition 2.17 An $[n, k, d]$ code with $d = n - k + 1$ is called *maximum distance separable* code, or an *MDS* code.

Exercise 2.18 Give a generator matrix of a binary $[5, 4, 2]$ MDS code.

Definition 2.19 A generator matrix of the form $G = (I_k|B)$, where I_k is the identity matrix of order k, is called a *standard* generator matrix.

Exercise 2.20 If $G = (I_k|B)$ is a generator matrix of an $[n, k]$ code C then $H = (-B^T|I_{n-k})$ is a parity check matrix of C.

For the next definition, it is convenient to think of a code C of length n as an array with n columns having as rows the words of C.

Definition 2.21 Two codes C' $C'' \subseteq F_q^n$ are *permutation equivalent*, if C'' can be obtained by permuting the columns of C'. If F_q is a finite field of order q, two codes C', $C'' \in F_q^n$ are *monomially equivalent* if C'' can be obtained by permuting the columns of C' and multiplying some columns of C' by nonzero elements from F_q.

Definition 2.22 An *automorphism* of a code is any any equivalence of the code to itself. The set of ll automorphisms of a code forms a group under composition, called the *automorphism group* of the code.

Exercise 2.23 Find the automorphism group of the binary $[6, 3]$ code with generator matrix $G = (I_3|J_3 - I_3)$.

Exercise 2.24 (1) Show that every linear $[n, k]$ code is equivalent to a code which has a standard generator matrix.
(2) Give an example of a code which does not have a standard generator matrix.

Definition 2.25 A set of k coordinate positions $i_1, i_2, \ldots i_k$ of a linear $[n, k]$ code $C \subseteq F_q^n$ is called an *information set* if the k columns of G with indices $i_1, i_2, \ldots i_k$ are linearly independent over F_q.

Clearly, an $[n, k]$ code admits a standard generator matrix if and only if the first k coordinate positions form an information set.

The meaning of an information set is the following: any codeword is obtained by recording in the k information positions any of the possible q^k words of length k over F_q, and the remaining $n - k$ coordinates are calculated as linear combinations of the k information symbols. The exact linear combinations are determined by using a parity check matrix of the code.

Exercise 2.26 List all information sets of the binary $[5, 2]$ code with generator matrix

$$G = \begin{pmatrix} 11010 \\ 10111 \end{pmatrix}.$$

3 Syndrome decoding of linear codes

The decoding algorithm implied by Theorem 1.2 requires computing the Hamming distances between the received message and all codewords. This algorithm is inefficient for codes containing a large number of words. There is a more efficient decoding algorithm for linear codes known as *syndrome decoding* .

Suppose that $C \subseteq F_q^n$ is a linear $[n, k]$ code over a finite field F_q, and let $b \in F_q^n$ be a vector. The *coset* of C with *representative* b is defined as the set of vectors

$$C + b = \{c + b \mid c \in C\}. \tag{6}$$

The main properties of cosets are summarized in the following lemma.

Lemma 3.1 *Assume that $C \subseteq F_q^n$ is a linear $[n, k]$ code.*
(i) Any coset of C contains the same number of vectors as C.
(ii) $C + b_1 = C + b_2$ if and only if $b_2 - b_1 \in C$.
(iii) Two cosest of C are either disjoint or identical (as sets of vectors).
(iv) The whole space F_q^n is a union of q^{n-k} disjoint cosets of C:

$$F_q^n = C \cup (C + b_1) \cup \cdots \cup (C + b_{q^{n-k}-1}).$$

Exercise 3.2 Prove Lemma 3.1.

A vector of minimum weight in a given coset is called a coset *leader*. A coset may have more than one leader. The leader of the code itself is the zero vector.

Example 3.3 The cosets of the binary $[4, 2]$ code C with generator matrix

$$G = \begin{pmatrix} 1011 \\ 0101 \end{pmatrix}$$

are given in Table 3.4. For each coset, a leader is chosen as a representative and listed in the first column. Note that the coset with a leader 0001 contains a second vector of weight one, 0100, which also is a leader.

Table 3.4 *The cosets of a binary $[4, 2]$ code*

Leader	Coset			
0000	0000	1011	0101	1110
0001	0001	1010	0100	1111
0010	0010	1001	0111	1100
1000	1000	0011	1101	0110

Suppose that $C \subseteq F_q^n$ is an $[n, k]$ code with a parity check matrix H. The *syndrome* $s(b)$ of a vector $b \in F_q^n$ is defined as the $(n-k) \times 1$ column vector equal to

$$s(b) = Hb^T.$$

Lemma 3.5 *All vectors in a given coset have the same syndrome.*

Proof. If x, y are two vectors belonging to a coset $C + b$, we have

$$x = x' + b,\ y = y' + b$$

for some $x', y' \in C$, and

$$s(x) = H(x' + b)^T = H(x')^T + Hb^T = Hb^T,$$
$$s(y) = H(y' + b)^T = H(y')^T + Hb^T = Hb^T,$$

thus $s(x) = s(y)$. □

Example 3.6 The following is a parity check matrix of the binary $[4, 2]$ code from Example 3.3:

$$H = \begin{pmatrix} 1010 \\ 1101 \end{pmatrix}.$$

The syndromes of the coset leaders are listed in Table 3.7.

Table 3.7 *Coset leaders and their syndromes*

Leader	Syndrome
0000	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
0001	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
0010	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
1000	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Suppose now that a vector $x \in F_q^n$ belonging to a linear code C with a parity check matrix H has been sent over a noisy channel, and a vector $y \in F_q^n$ has been accepted at the receiving end. The vector

$$e = y - x,$$

called the *error vector*, determines whether any errors have occurred in the process of transmitting x. If $e = \mathbf{0}$ no errors have occurred, hence $y = x$. Otherwise, the weight of e is equal to the number of errors, i.e., the number of coordinates of x which have been altered during the transmission. Note that

$$Hy^T = He^T.$$

This observation is the base of the following decoding algorithm, known as Syndrome Decoding.

1. Compute the syndrome $s(y) = Hy^T$ of the received vector y.
2. Find a coset leader e having the same syndrome as y.
3. If e is the only leader in the coset with syndrome $s(y)$, decode y as $x = y - e$. Otherwise, conclude that an error pattern has been detected that cannot be corrected.

Theorem 3.8 *The syndrome decoding algorithm determines correctly the initial codeword x provided that the number of errors t does not exceed $[(d-1)/2]$, where d is the minimum distance of the code.*

Proof. Note that any two distinct vectors of weight $t \leq [(d-1)/2]$ belong to distinct cosets. Thus, the error vector e is equal to the unique coset leader having the same syndrome as y. □

An implementation of the syndrome decoding algorithm requires finding the coset leaders and computing their syndromes, which is done only once and recorder in a table similar to Table 3.7.

Example 3.9 The $[4, 2]$ binary code from Example 3.3 has minimum distance $d = 2$. Thus, $[(d-1)/2] = [(2-1)/2] = 0$ and the code cannot correct arbitrary single errors. However, the vectors 0010 and 1000 are unique leaders in their cosets, thus represent error patterns which can be corrected by syndrome decoding. In other words, the code can correct a single error affecting the first or the third coordinate of any codeword.

Example 3.10 The binary Hamming code of length 7 is a linear $[7, 4]$ code with parity check matrix H having as columns all distinct nonzero $(0, 1)$-vectors with three components, ordered lexicographically. Since the columns of H are nonzero and distinct, the minimum distance d of the code is at least 3. On the other hand, there are triples of linearly dependent columns, hence $d = 3$ and the code can correct any single error. There are $2^{7-4} = 2^3 = 8$ cosets, with coset leaders the zero vector (for the code itself), and the seven vectors in F_2^7 of weight 1. The syndrome of a leader of weight one having ith nonzero coordinate ($1 \leq i \leq 7$), is equal to the ith column of H. Thus, the syndrome decoding algorithm for correcting single errors with the Hamming code reads as follows:

1. Given a vector $y \in F_2^7$, compute its syndrome $s(y)$.
2. If $s(y) = \mathbf{0}$, no errors have occurred, thus $x = y$. Otherwise, if $s(y)$ is equal to the ith column of H, decode y as the vector x obtained from y by replacing the ith coordinate y_i of y with $1 - y_i$.

4 The sphere-packing bound

The length n, the minimum distance d, and the total number of codewords (or *size*) $M = |C|$ are the main parameters of a code C. Increasing d is generally possible at the expense of decreasing M or increasing n. If d and M are fixed, the most interesting codes are those of shortest length n. If d and n are fixed, one looks for a code of largest possible size M. Thus, there are three fundamental optimization problems imposed by fixing two of the parameters n, d, M and optimizing with respect to the third. Explicit solutions of any of these optimization problems are rarely known in general. However, there are estimates, or *bounds* for the optimal values in terms of inequalities.

The following theorem gives an upper bound on the size of a q-ary code of given length and minimum distance.

Theorem 4.1 *(The Sphere-packing, or Hamming bound) .*
Suppose that C is a q-ary code of length n and minimum Hamming distance d. Then

$$|C| \leq \frac{q^n}{\sum_{i=0}^{[(d-1)/2]} \binom{n}{i}(q-1)^i} \tag{7}$$

Proof. The spheres of radius $r = [(d-1)/2]$ around the codewords of C are pairwise disjoint. Every word of length n belongs to at most one such sphere. Thus, using the formula (1) for the volume of a sphere, we have

$$|C|(\sum_{i=0}^{[(d-1)/2]} \binom{n}{i}(q-1)^i) \leq q^n,$$

and (7) follows. □

A code that satisfies the equality in (7) is called *perfect*.

A trivial example of a perfect code with $d = 1$ is the set F_q^n of all words of length n.

Another example is the binary *repetition* code of odd length $n = 2m+1$, consisting of the all-one vector $\bar{1} = 111\ldots1$, and the zero vector. In this case, $d = n = 2m+1$, and the size of a sphere of radius $m = (n-1)/2$ is

$$\sum_{i=0}^{(n-1)/2} \binom{n}{i} = \frac{1}{2}2^n = 2^{n-1}.$$

Nontrivial examples of perfect codes with $d = 3$ are discussed in the next section.

Exercise 4.2 Is it possible to find 16 binary vectors of length 7 such that any two are at Hamming distance at least 4?

5 The Hamming codes

In this section, we describe a class of linear perfect single error-correcting codes ($d = 3$) known as *Hamming codes*.

We know from 2.13 that a linear binary code has minimum distance at least 3 if and only if all columns in the parity check matrix are nonzero and distinct.

The binary Hamming code $H_m(2)$ of length $n = 2^m - 1$, $(m \geq 2)$ and dimension $k = n - m$ is defined as a linear code with a parity check matrix H having as columns all distinct nonzero vectors with m components. By Definition 2.21, all binary Hamming codes of given length $n = 2^m - 1$ are equivalent. It is convenient to assume that the columns of H are ordered lexicographically, that is, the ith column of H is the binary presentation of the number i, $1 \leq i \leq 2^m - 1$. Clearly, the first three columns of H are linearly dependent over the field of order 2, $F_2 = GF(2)$. By 2.13, the minimum distance of $H_m(2)$ is equal to 3. A sphere of radius 1 in F_2^n is of size n_+1. Since

$$\frac{2^n}{n+1} = 2^{2^m-1-m} = 2^{n-m},$$

the Hamming code $H_m(2)$ is perfect.

Clearly, any binary linear code of length $n = 2^m-1$, dimension $k = n-m$, and minimum distance $d = 3$, is equivalent to $H_m(2)$.

The binary Hamming codes were introduced by Richard Hamming [6] in 1950, who proposed also a simple decoding algorithm for such codes. Suppose that $y \in F_2^n$ $(n = 2^m - 1)$ is a vector obtained from some codeword $x \in F_2^n$ by changing at most one coordinate of x (from 0 to 1 or vice versa). Then x can be recovered from y as fallows. We compute the column-vector S, called the *syndrome* of y, as

$$S = Hy^T, \tag{8}$$

where H is the parity check matrix of $H_m(2)$.

If S is the zero vector then $y \in H_m(2)$ and we assume that no errors have occurred, i.e., $x = y$. Otherwise, S is identical with one of the columns of H. If S is equal to the ith column of H then x is obtained from y by replacing the ith component y_i of y by $1 - y_i$.

The decoding algorithm of the Hamming code is a special case of the *syndrome decoding*.

Nonbinary Hamming Codes.

For every prime power q and every length $n = (q^m - 1)/(q - 1)$, $(m \geq 2)$, there are linear perfect single-error-correcting codes over the finite field of order q, $GF(q)$, being analogues of the binary Hamming codes.

The q-ary Hamming code $H_m(q)$ is defined as a linear code over $GF(q)$ with parity check matrix H having as columns representatives of all 1-dimensional vector spaces of the m-dimensional vector space $GF(q)^m$.

Exercise 5.1 Verify that $H_m(q)$ is perfect.

Exercise 5.2 Describe a decoding procedure for correcting single errors using $H_m(q)$.

6 Vasil'ev codes

All examples of nontrivial perfect codes discussed so far are linear codes.

Exercise 6.1 If C is a perfect code, any coset $C + y$, where $y \notin C$, is a perfect nonlinear code.

Vasil'ev [29] described the following "doubling" construction that starts from a binary single-error-correcting perfect code of length n and produces a perfect code of length $2n + 1$ which is often nonlinear and not a coset of any linear code.

Let E be a perfect binary code of minimum distance 3 and length $n = 2^m - 1$ containing the zero vector (for example, E could be the Hamming code $H_m(2)$). Let f be a function that assigns value 0 or 1 to every vector from E, such that $f(\bar{0}) = 0$, where $\bar{0}$ denotes the zero vector. Let π be the function defined on F_2^n that assigns 0 to all vectors of even weight, and 1 to all vectors of odd weight. Equivalently, if $x = (x_1, \ldots, x_n) \in F_2^n$ then

$$\pi(x) = (x_1 + \cdots + x_n) \ mod \ 2.$$

Theorem 6.2 *Let C be a binary code of length $2n + 1$ defined as follows:*

$$C = \{(v, (v + a) \ mod \ 2, (\pi(v) + f(a)) \ mod \ 2) \mid a \in E, \ v \in F_2^n\}. \qquad (9)$$

Then
(i) C is a perfect binary single error-correcting code.
(ii) If f is nonlinear then the code C is nonlinear, and is not a coset of a linear code.

Proof. Let $x, y \in C$, where

$$x = (v, v+a, \pi(v)+f(a)), y = (u, u+b, \pi(u)+f(b) : a, b \in E; u, v \in F_2^n. \quad (10)$$

The Hamming distance $d(x, y)$ between x and y is equal to

$$d(x, y) = d(v, u) + d(v + a, u + b) + d(\pi(v) + f(a), \pi(u) + f(b)).$$

If $u = v$ then $x \neq y$ only if $a \neq b$, in which case

$$d(x, y) \geq d(a, b) \geq 3.$$

If $u \neq v$, but $a = b$, we have

$$d(x, y) = 2d(v, u) + d(\pi(v), \pi(u)),$$

hence $d(x, y) \geq 4$ whenever $d(u, v) \geq 2$.

If $d(v, u) = 1$ then the Hamming weights of v and u are of different parity modulo 2, hence $d(\pi(v), \pi(u)) = 1$ and $d(x, y) = 3$.

If $a \neq b$ then $d(a, b) = w(a - b) \geq 3$, and

$$d(x, y) \geq w(v-u)+w(v-u+a-b) \geq w(v-u)+w(a-b)-w(v-u) = w(a-b) \geq 3.$$

Thus, the minimum distance of C is 3. The size of C is

$$2^n \cdot 2^{n-m} = 2^{2n-m} = 2^{2^{m+1}-m-2},$$

hence C is a perfect code.

To prove (ii), we note that choosing $v = a = 0$ in (9) gives the zero vector, thus C is either linear, or a nonlinear code that is not a coset of a linear code.

Let $x, y \in C$ be defined as in (10). We have

$$x + y = (v + u, v + u + a + b, \pi(v) + \pi(u) + f(a) + f(b)),$$

where all additions are modulo 2. Since

$$\pi(v) + \pi(u) = \pi(v + u),$$

the vector $x + y$ belongs to C if and only if $a + b \in E$ and

$$f(a) + f(b) = f(a + b).$$

Thus, the code C is linear if E is linear and f is a linear function, and nonlinear if f is nonlinear. □

A code obtained via the construction of Theorem 6.2 is called a *Vasil'ev code*.

Exercise 6.3 Let C be a binary linear code of dimension k and $f: C \to \{0,1\}$ be a function such that $f(\bar{0}) = 0$ and

$$f(a+b) = f(a) + f(b)$$

for all $a, b \in C$, where all additions are modulo 2. Prove that either f is constant or f takes value 1 at exactly 2^{k-1} vectors from C.

Exercise 6.4 Show that a Vasil'ev code of length 7 is necessarily linear.

Exercise 6.5 Find an explicit example of a nonlinear Vasil'ev code of length 15.

Note 6.6 There are exactly nineteen equivalence classes of Vasi'ev codes of length 15 (F. Hergert [8]).

Note 6.7 All perfect binary single-error-correcting codes of length 15 have been enumerated recently by Östergard and Pottonen [19].

Note 6.8 Nonlinear perfect single-error-correcting q-ary codes exist for arbitrary prime power q (Schönheim [27], Lindström [9]).

7 The binary Golay codes

In this section, we describe a perfect binary 3-error-correcting code, namely, a $[23, 12, 7]$ code, discovered by Golay in 1949 [5].

Definition 7.1 A code C is *self-orthogonal* if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$.

Note 7.2 Any generator matrix of a self-dual code is also a parity check matrix of the same code, and vice versa.

Since the dual code $C^{\perp}$ of a linear $[n, k]$ code C is an $[n, n-k]$ code, it follows that if C is self-orthogonal then $k \leq n/2$. If C is self-dual then $k = n/2$, hence n is even.

In what follows, we assume that any dual code is defined with respect to the ordinary inner product (2). Any vector $x = (x_1, \ldots, x_n)$ which belongs to a self-orthogonal code is orthogonal to itself:

$$x \cdot x = x_1^2 + \cdots + x_n^2 = 0, \tag{11}$$

where all operations are evaluated in the corresponding finite field.

Note 7.3 Equation (11) implies that all vectors in a binary self-orthogonal code are of even weight, and all vectors in a ternary self-orthogonal code have weights divisible by 3.

Exercise 7.4 Prove that in a binary linear code either all codewords are of even weight or exactly half of the codewords are of even weight.

Exercise 7.5 Prove that if C is a binary linear self-orthogonal code then either all vectors in C have weights divisible by 4, or exactly half of the vectors have weights divisible by 4.

Definition 7.6 A code C is called *even* if all vectors in C have even weights, and *doubly-even* if all vectors in C have weights divisible by 4.

Exercise 7.7 A binary linear code with a generator matrix G is self-orthogonal if and only if the rows of G are pairwise orthogonal and all rows have even weights.

Exercise 7.8 A binary linear self-orthogonal code with a generator matrix G is doubly-even if and only if all rows of G have weights divisible by 4.

The *extended* binary Golay code $\mathcal{G}_{24}$ is a linear $[24, 12]$ code with a generator matrix

$$G = \begin{pmatrix} & 1 & & \\ I_{12} & \vdots & A & \\ & 1 & & \\ & 0 \;\; 1 & \dots & 1 \end{pmatrix}, \tag{12}$$

where A is an 11 by 11 circulant matrix with six nonzero entries (equal to 1) in the first row located positions 2, 6, 7, 8, 10, 11.

Theorem 7.9 *The extended Golay code is a doubly-even self-dual code with minimum distance 8.*

Proof. The last row of G is of weight 12, while all other rows are of weight 8. The inner product of the last row of G with any other row is 6. The product of any two distinct rows of A is 3, hence the product of the corresponding rows of G is 4. It follows from 7.7 and 7.8 that G generates a doubly-even

self-orthogonal code, and since the rank of G is $12 = 24/2$, this code is self-dual. Consequently, the matrix

$$H = \begin{pmatrix} 1 & \dots & 1 & 0 & \\ & & & 1 & \\ & A^T & & \vdots & I_{12} \\ & & & 1 & \end{pmatrix} \tag{13}$$

is both a parity check matrix and another generator matrix of $\mathcal{G}_{24}$. Since $\mathcal{G}_{24}$ is doubly-even and G has rows of weight 8, the minimum weight of $\mathcal{G}_{24}$ is either 4 or 8.

Assume that $x = (x_1, \dots, x_{12}, x_{13}, \dots, x_{24}) \in \mathcal{G}_{24}$ is a codeword of weight 4. Let i be the weight of the first 12 positions of x, $(x_1, \dots, x_{12})$. Then x is the sum of i of rows of G and $4 - i$ rows of H. Since neither G nor H has any rows of weight 4, it follows that $i = 2$. Using formula (4), one verifies that the weight of the sum of any two rows of G is 8, a contradiction. Thus, the minimum weight of $\mathcal{G}_{24}$ is 8. □

The Golay code $\mathcal{G}_{23}$ of length 23 is a $[23, 12, 7]$ code having a generator matrix obtained by deleting one of the columns of G (12). Since

$$\frac{2^{23}}{\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}} = \frac{2^{23}}{2^{11}} = 2^{12},$$

the code $\mathcal{G}_{23}$ is perfect.

Definition 7.10 The *weight distribution* of a code of length n is the sequence $a_0, a_1, \dots, a_n$, where a_i is the number of codewords of weight i $(0 \le i \le n)$.

Exercise 7.11 Prove that if C is a binary linear code of length n with weight distribution $\{a_i\}_{i=0}^n$ containing the the all-one vector $\bar{1}$=$(1, \dots, 1)$, then $a_i = a_{n-i}$ for all $0 \le i \le n$.

Exercise 7.12 Prove that if C is a binary linear $[n, k]$ code with a generator matrix having a nonzero ith column $(1 \le i \le n)$, there are exactly 2^{k-1} vectors in C with ith coordinate equal to zero.

Exercise 7.13 Find the weight distribution of the extended Golay code $\mathcal{G}_{24}$.

Exercise 7.14 Find the weight distribution of the perfect Golay code $\mathcal{G}_{23}$.

Definition 7.15 The *support* $sup(x)$ of a vector $x = (x_1, \ldots, x_n)$ is the set of indices of its nonzero coordinates:

$$sup(x) = \{i \mid x_i \neq 0\}.$$

Definition 7.16 Given integers t, v, k, λ with $v \geq k \geq t \geq 0$, $\lambda \geq 0$, a t-(v, k, λ) design D is a pair $(X, \mathcal{B})$, where X is a finite set of v *points*, and $\mathcal{B}$ is a collection of k-subsets of X called *blocks* such that every t-subset of X is contained n exactly λ blocks.

A design is *simple* if there are no repeated blocks.

A t-design with $\lambda = 1$, i.e., a t-$(v, k, 1)$ design, is also called a *Steiner system*, and often denoted by $S(t, k, v)$.

Exercise 7.17 Prove that if D is a t-(v, k, λ) design with point set X and s is an integer in the range $0 \leq s \leq t$, any s-subset of X is contained in

$$\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}$$

blocks of D. In particular, the total number of blocks is

$$b = \lambda_0 = \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Exercise 7.18 Show that the collection of the supports of vectors of weight 8 in $\mathcal{G}_{24}$ is a 5-$(24, 8, 1)$ design.

Exercise 7.19 Show that the collection of the supports of vectors of weight 7 in $\mathcal{G}_{23}$ is a 4-$(23, 7, 1)$ design.

Note 7.20 The full automorphism group of $\mathcal{G}_{24}$ is the 5-transitive Mathieu group M_{24} [18], while the full automorphism group of $\mathcal{G}_{23}$ is the 4-transitive Mathieu group M_{23} [18].

8 The ternary Golay codes

In [5], Golay described also a ternary perfect double-error-correcting code, namely an $[11, 6, 5]$ code, widely known in the literature as the *ternary Golay code*.

The *extended ternary Golay code* $\mathcal{G}_{12}$ is a linear ternary $[12, 6]$ code with a generator matrix

$$G = \begin{pmatrix} & 1 & & \\ I_6 & \vdots & & A \\ & 1 & & \\ & 0 & 1 \ \ \ldots & 1 \end{pmatrix}, \tag{14}$$

where A is the 5 by 5 circulant matrix with first row 012210.

Theorem 8.1 *The extended ternary Golay code is a self-dual code with minimum distance 6.*

Proof. Since all rows of G are of weight 6 (a multiple of 3), and the inner product of every two rows of G is a multiple of 3, $\mathcal{G}_{12}$ is self-dual, with minimum weight D equal to 3 or 6. A codeword of weight 3 has to be either a row of G (14), or a row of the parity check matrix H given by (15).

$$H = \begin{pmatrix} 2 & \ldots & 2 & 0 & \\ & & & 2 & \\ & -A^T & & \vdots & I_6 \\ & & & 2 & \end{pmatrix} \tag{15}$$

Since neither G nor H has any rows of weight 3, it follows that $d = 6$. □

Puncturing one of the twelve coordinates of $\mathcal{G}_{12}$ yields an $[11, 6, 5]$ code $\mathcal{G}_{11}$. Since

$$\frac{3^{11}}{1 + 2 \cdot 11 + 2^2 \binom{11}{2}} = 3^6,$$

the code $\mathcal{G}_{11}$ is perfect.

Exercise 8.2 Let A be the 11 by 11 circulant from (12). Prove that the matrix

$$\begin{pmatrix} & 1 \\ J - A & \vdots \\ & 1 \end{pmatrix}$$

is a generator matrix of a ternary self-dual $[12, 6, 6]$ code.

Exercise 8.3 Let H_{12} be an Hadamard matrix of order 12. Show that H_{12} is a generator matrix of a ternary self-dual $[12, 6, 6]$ code.

Exercise 8.4 Find the weight distribution of the extended Golay code $\mathcal{G}_{12}$.

Exercise 8.5 Find the weight distribution of $\mathcal{G}_{11}$.

Exercise 8.6 Prove that the supports of all vectors of weight 5 in $\mathcal{G}_{11}$ are the blocks of a 4-$(11, 5, 1)$ design.

Exercise 8.7 Prove that the supports of all vectors of weight 6 in $\mathcal{G}_{12}$ are the blocks of a 5-$(12, 6, 1)$ design.

Note 8.8 Any automorphism of a ternary code is a signed permutation being a composition of a permutation of the coordinates followed by a negation of coordinates. The set of all permutations obtained by neglecting the negations in automorphisms of $\mathcal{G}_{11}$ is a permutation group isomorphic to the 4-transitive Mathieu group M_{11} [17] of order $7920 = 11 \cdot 10 \cdot 9 \cdot 8$. Similarly, the permutations obtained by neglecting the negations in automorphisms of $\mathcal{G}_{12}$ is a permutation group isomorphic to the 5-transitive Mathieu group M_{12} [17] of order $95040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

Note 8.9 In [5], Golay introduced not only the perfect binary $[23, 12, 7]$ and ternary $[11, 6, 5]$ codes, but also all linear binary and q-ary perfect single-error-correcting codes, widely known in the literature as Hamming codes.

Note 8.10 The parameters of all perfect codes over a finite filed were determined in a series of papers by van Lint [10], [11], [12], Tietäväinen [28], and Zinoviev and Leontiev [30]. The main result is that a nontrivial linear perfect code is either a Hamming code or a Golay code. In addition, any nonlinear perfect code with minimum distance greater than 3 is a coset of a Golay code, and any perfect single-eerror-correcting codes has the parameters of a Hamming code. For a proof of the uniqueness (up to equivalence) of the Golay codes see Pless [22], [23, Chapter 10], and Delsarte and Goethals [4]. A more recent survey on perfect codes is the paper by Heden [7].

9 The Assmus-Mattson characterization of perfect codes

Suppose that q is a prime power, and let $C \subseteq GF(q)^n$ be a linear q-ary code of length n. Let w be an integer, $0 < w < n$. If $q > 2$ and $x \in C$ is a vector of weight w, all $q-1$ nonzero multiples αx of x, where $\alpha \in GF(q),\ \alpha \neq 0$, share the same support. We associate with x and its multiples the support $sup(x)$, and define a collection of w-subsets $\mathcal{D}$ of the set of coordinate indices $\{1, 2, \ldots, n\}$, consisting of the supports of all codewords in C of weight w.

The next theorem, due to Assmus and Mattson [2], describes a relationship between perfect codes and t-designs supported by their codewords of minimum weight.

Theorem 9.1 *A linear code C over $GF(q)$ of length n and minimum distance $d = 2e + 1$ is perfect if and only if the collection of supports of all codewords of weight d is a simple $(e+1) - (n, 2e+1, (q-1)^e)$ design.*

Proof. Assume that C is a perfect code with minimum distance $d = 2e + 1$. Let T be an arbitrary $(e+1)$-subset of $\{1, 2, \ldots, n\}$. Any vector $x \in GF(q)^n$ of weight $e + 1$ with support $sup(x) = T$ is at distance e from exactly one codeword $y \in C$, and the weight of y is equal to $d = 2e + 1$. The number of all vectors in $GF(q)^n$ having T as a support is equal to $(q-1)^{e+1}$, and each two such vectors are at distance e from distinct codewords. Therefore, not counting scalar multiples, T is contained in exactly $(q-1)^e$ supports of codewords of weight $d = 2e + 1$. Consequently, the collection of supports of codewords of minimum weight is an $(e+1) - (n, 2e+1, (q-1)^e)$ design.

Let us assume now that the supports of all codewords of minimum weight $d = 2e + 1$ in a linear code $C \subseteq GF(q)^n$ form a simple $(e+1) - (n, 2e+1, (q-1)^e)$ design. Any vector $u \in GF(q)^n$ of weight not exceeding e is at distance at most e from the zero codeword. Suppose that the spheres of radius e around all codewords of C do not contain all vectors of $GF(q)^n$, and let y be a vector of smallest weight among all vectors which are at distance greater than or equal to $e + 1$ from every codeword. It follows that y is of weight at least $e + 1$. Let $y_{i_1}, \ldots, y_{i_{e+1}}$ be a set of $e + 1$ nonzero coordinates of y. The set of indices $T = \{i_1, \ldots, i_{e+1}\}$ is contained in $(q-1)^e$ supports of codewords of minimum weight. The number of codewords of minimum weight whose supports contain T is equal to $(q-1)^{e+1}$, and any two such codewords differ in at least one position from T. Thus, there is a codeword

z of minimum weight which coincides with y in all positions from T:

$$z_{i_1} = y_{i_1}, \ldots, z_{i_{e+1}} = y_{i_{e+1}}.$$

Consequently, the vector $y' = z - y$ is of weight smaller than the weight of y, and is at distance at least $e+1$ from all codewords, which contradicts to the choice of y. □

Corollary 9.2 *The number of codewords of minimum weight $2e+1$ in a linear perfect q-ary code of length n is equal to*

$$\frac{n(n-1)\cdots(n-e)}{(2e+1)(2e)\cdots(e+1)}(q-1)^e.$$

Corollary 9.3 *The supports of minimum weight vectors of the binary Golay code $\mathcal{G}_{23}$ form a 4-$(23, 7, 1)$ design.*

Corollary 9.4 *The supports of minimum weight vectors of the ternary Golay code $\mathcal{G}_{11}$ form a 3-$(11, 5, 4)$ design.*

Note 9.5 The 3-$(11, 5, 4)$ design from 9.4 is actually a 4-$(11, 5, 1)$ design.

We note that if $q = 2$, the only nonzero multiple of a vector $x \neq \bar{0}$ is x itself. Thus, the proof of Theorem 9.1 implies the following result.

Theorem 9.6 *A binary code of length $n = 2^m - 1$ ($m \geq 2$) and minimum distance 3 which contains the zero vector is perfect if and only if the collection of the supports of all codewords of weight 3 is a 2-$(2^m - 1, 3, 1)$ design.*

Corollary 9.7 *The supports of minimum weight vectors of any Vasil'ev code of length $2^m - 1$ form a 2-$(2^m - 1, 3, 1)$ design.*

Note 9.8 A 2-design with block size 3 and $\lambda = 1$, i.e., a 2-$(v, 3, 1)$ design is also called a *Steiner triple system*, and is often denoted by $STS(v)$.

Exercise 9.9 (i) Use the construction from [9] or [27] to find a nonlinear perfect single-error-correcting ternary code of length 13 that contains the zero vector.
(ii) Find the weight distribution of the code.
(iii) Verify whether the supports of codewords of weight 3 support a 2-design.

Definition 9.10 Given a binary code C of length n, the *extended code* $\hat{C}$ is defined as a code of length $n+1$ obtained by adding to each codeword $x = (x_1, \ldots, x_n) \in C$ a new coordinate x_{n+1} equal to the *overall parity check*, that is, $x_{n+1} = 0$ if the weight of x is even, and $x_{n+1} = 1$ if the weight of x is odd.

Clearly, all vectors of the extended code are of even weight. If C is a linear $[n, k]$ code with minimum distance d, the extended code $\hat{C}$ is a linear $[n+1, k]$ code with minimum distance $\hat{d}$, with $\hat{d}$=d if d is even, and $\hat{d} = d + 1$ if d is odd.

If C is a binary perfect code, the extended code $\hat{C}$ also yields a design.

Theorem 9.11 *(Assmus and Mattson [2]). If C is a perfect binary code of length n and minimum weight $d = 2e + 1$ containing the zero vector, the supports of the codewords of weight $2e + 2$ in the extended code $\hat{C}$ form an $(e + 2)$-$(n + 1, 2e + 2, 1)$ design.*

Proof. Let $\hat{u}$ be a binary vector of length $n + 1$ and weight $e + 2$. We will show that the support of $\hat{u}$ is contained in the support of exactly one codeword of $\hat{C}$ of weight $2e+2$. The supports of any two distinct codewords $x, y \in \hat{C}$ of weight $2e + 2$ can share at most $e + 1$ coordinates. Thus, the support of $\hat{u}$ can be covered by the support of at most one codeword of weight $2e+2$. We denote by u the vector of length n obtained by removing the last coordinate $\hat{u}_{n+1}$ of $\hat{u}$. Assume that $\hat{u}_{n+1}$=0. Let $c \in C$ be a vector which is at distance at most e from u. The weight of x is equal to $w(c) = 2e + i$ for some integer $i \geq 1$. We have

$$d(c, u) = w(c + u) = 3e + i + 2 - 2w(c * u) \leq e,$$

and

$$w(c * u) \leq e + 2,$$

hence

$$e + 1 + \frac{i}{2} \leq w(c * u) \leq e + 2.$$

Thus, $i = 2$, $w(c) = 2e+2$, and the support of $\hat{u}$ is covered by the support of $\hat{c} \in C$, where $w(\hat{c}) = 2e + 2$ and $\hat{c}$ is obtained by extending c with an overall parity check equal to zero.

Assume now that $\hat{u}_{n+1}$=1. The shortened vector u is of weight $e+1$, and according to Theorem 9.1, the support of u is covered by the support of a

codeword $c \in C$ of weight $2e+1$. The extended word $\hat{c}$ is of weight $2e+2$ and has $(n+1)$st coordinate equal to 1, and the support of $\bar{u}$ is contained in the support of $\bar{c}$. □

Corollary 9.12 *The minimum weight vectors of the extended code of a binary perfect single-error-correcting code of length* $2^m - 1$ *containing the zero vector support a* 3-$(2^m, 4, 1)$ *design.*

Definition 9.13 A 3-$(v, 4, 1)$ designs is also called a *Steiner quadruple system*, and is often denoted by $SQS(v)$.

Corollary 9.14 *The minimum weight vectors in the extended Golay code* $\mathcal{G}_{24}$ *support a* 5-$(24, 8, 1)$ *design.*

Exercise 9.15 Find the number of codewords of weight 4 in the binary Hamming code of length $2^m - 1$.

Exercise 9.16 Find the number of codewords of weight 4 in the extended code of a prefect binary single-error-correcting code of length $2^m - 1$ containing the zero vector.

Exercise 9.17 Find the weight distribution of the dual code of the binary Hamming code of length $2^m - 1$.

10 Perfect codes and data compression

The major use of error-correcting codes is, as their name suggests, for detection and correction of random errors that may occur in the encoded data during transmission or while the data is being stored on some memory device. However, codes can also be used for data compression, a process that allows for adding some noise to the data with the purpose of achieving a higher transmission rate or saving memory space. In this application, perfect codes have some advantages, as noted by Shannon in 1959 [26].

Suppose that some data of nature that can tolerate up to a certain degree of noise is to be stored or transmitted, and the purpose is to save memory space or increase the transmission speed, hence reduce the cost of storage or transmission. A typical example is data being transmitted over a telephone line, or other type of audio or visual data.

Let us assume that data is recorded in messages of length n over a finite field $GF(q)$ of order q. Assume further that C is a perfect $[n, k, d = 2e + 1]$ code over $GF(q)$. Let $y \in GF(q)^n$ be an arbitrary data string of length n. There exist a unique codeword $x \in C$ such that x differs from y in at most e positions. The message y is compressed to a string $\bar{x}=(x_{i_1}, \ldots, x_{i_k})$ of k information symbols of x, where $i_1, \ldots, i_k$ are k linearly independent columns of a generator matrix of C, and $\bar{x}$ is then transmitted over a noiseless channel or stored instead of y. At the receiving end, $\bar{x}$ is decompressed to the whole codeword x of length n, and x is being tilized instead of y. Assuming that no errors have occurred during transmission or while $\bar{x}$ was being stored, this procedure can alter up to e components of the original data y. For many applications, such a loss of precision may be tolerable.

Example 10.1 If C is a binary linear Hamming code of length $n = 2^m - 1$, a compressed message consists of $n - m$ bits only, and a decompressed message differs from the original data in at most one of the n bits.

Example 10.2 Using the binary perfect Golay code $\mathcal{G}_{23}$, any message of 23 bits is compressed to a shorter message of 12 bits only, and the decompressed message differs from the original data in at most 3 out of 23 bits.

Exercise 10.3 Use the binary Hamming code of length 7 to compress and decompress the data message $(1, 1, 0, 0, 0, 1, 1)$.

11 MacWillimas identities

In this section, we discuss a relation between the weight distribution of a linear code and that of its dual code, discovered by F. J. MacWilliams [13], [14].

The *weight enumerator* of a code C of length n is a polynomial

$$A(x) = \sum_{i=0}^{n} a_i x^i,$$

where a_i is the number of codewords of C of weight i.

Theorem 11.1 *(MacWillimas). Suppose that C is a linear $[n, k]$ code over $GF(q)$ with weight distribution $\{a_i\}_{i=0}^n$, and let $\{b_i\}_{i=0}^n$ be the weight distribution of the dual code $C^\perp$. The weight enumerators of C and $C^\perp$ are related by the equation*

$$q^k \sum_{i=0}^{n} b_i x^i = \sum_{j=0}^{n} a_j (1-x)^j (1+(q-1)x)^{n-j}. \tag{16}$$

Proof. There are several identities equivalent to (16), all known as *MacWilliams identities*. We will prove one such identity, from which (16) will follow.

Comparing the coefficients of x^i in the left and right-hand sides of equation (16), we can find a formula expressing $b_0, \ldots, b_n$ in terms of $a_0, \ldots, a_n$. For this purpose, we expand (16) as follows:

$$\sum_{i=0}^{n} b_i x^i = q^{-k} \sum_{j=0}^{n} a_j (1-x)^j (1+(q-1)x)^{n-j} =$$
$$q^{-k} \sum_{j=0}^{n} \sum_{s=0}^{j} \sum_{t=0}^{n-j} a_j \binom{j}{s} (-1)^s x^s \binom{n-j}{t} (q-1)^t x^t.$$

Let $s + t = i$. Then

$$\sum_{i=0}^{n} b_i x^i = q^{-k} \sum_{j=0}^{n} \sum_{s=0}^{n} \sum_{i=s}^{n-j+s} a_j \binom{j}{s} \binom{n-j}{i-s} (-1)^s (q-1)^{i-s} x^i =$$
$$q^{-k} \sum_{j=0}^{n} \sum_{s=0}^{n} \sum_{i=0}^{n} a_j \binom{j}{s} \binom{n-j}{i-s} (-1)^s (q-1)^{i-s} x^i =$$
$$q^{-k} \sum_{i=0}^{n} x^i \sum_{j=0}^{n} a_j \sum_{s=0}^{n} \binom{j}{s} \binom{n-j}{i-s} (-1)^s (q-1)^{i-s}.$$

Note that extending the summation from $i = s$ to $n - j + s$, to $i = 0$ to n is possible because all additional terms are equal to 0. After this, we can change the order of summation. Comparing the coefficients of x^i, we have

$$b_i = q^{-k} \sum_{j=0}^{n} a_j \sum_{s=0}^{n} \binom{j}{s} \binom{n-j}{i-s} (-1)^s (q-1)^{i-s}.$$

Substituting $x = 1 + y$ in (16) gives

$$q^k \sum_{i=0}^{n} b_i (1+y)^i = \sum_{j=0}^{n} a_j (-y)^j (q + (q-1)y)^{n-j}.$$

Extending the limits of summation and comparing the coefficients of y^m, we have

$$\sum_{i=m}^{n} b_i \binom{i}{m} = q^{n-k-m} \sum_{j=0}^{m} a_j \binom{n-j}{n-m} (-1)^j (q-1)^{m-j}.$$

Similarly, substituting $x = 1/(1+y)$ in (16) gives

$$q^k \sum_{i=0}^{n} b_i (1+y)^{n-i} = \sum_{j=0}^{n} a_j y^j (y+q)^{n-j},$$

which implies

$$\sum_{i=0}^{n-m} b_i \binom{n-i}{m} = q^{n-k-m} \sum_{j=0}^{m} a_j \binom{n-j}{n-m}. \tag{17}$$

Now we will prove equation (17). Let $s = \{s_1, \ldots, s_m\}$ be a set of m distinct integer numbers in the range $1 \le s_i \le n$, and let $t = \{t_1, \ldots, t_{n-m}\}$ be the complementary set of s in the set of integers between 1 and n. Let F_s be the subspace of $GF(q)^n$ consisting of all vectors having zeros in positions $t_1, \ldots, t_{n-m}$. The subspace F_t is defined similarly with respect to the set of indices s. Note that $F_t = {F_s}^{\perp}$.

The subspace of $C^{\perp}$ consisting of all codewords having zeros in positions $s_1, \ldots, s_m$ coincides with $C^{\perp} \cap F_t$. Note that

$$(C \cap F_s)^{\perp} = C^{\perp} \oplus {F_s}^{\perp} = C^{\perp} \oplus F_t,$$

where $\oplus$ denotes the sum of the corresponding subspaces, that is,

$$U \oplus V = \{\alpha u + \beta v \mid u \in U,\ v \in V;\ \alpha, \beta \in GF(q).\}$$

Let d_s denote the dimension of $C \cap F_s$, and let d_t be the dimension of $C^\perp \cap F_t$. Since $(C^\perp \oplus F_t)^\perp = C \cap F_s$, the dimension of $C^\perp \oplus F_t$ is equal to $n - d_s$. On the other hand,

$$\dim(C^\perp \oplus F_t) = \dim C^\perp + \dim F_t - \dim(C^\perp \cap F_t) = (n-k) + (n-m) - d_t,$$

thus

$$n - d_s = (n-k) + (n-m) - d_t,$$

or

$$d_t = d_s + n - k - m.$$

Let us count in two was the ordered pairs (s, v), where s is an m-subset of $N = \{1, \ldots, n\}$, and $v \in C \cap F_s$. For any given s, there are q^{d_s} such pairs. The total number of pairs is

$$\sum_{s \subset N} q^{d_s}.$$

Each vector $v \in C$ of weight j contains $n - j$ nonzero coordinates, and each set t, which is an $(n-m)$-subset of these coordinates defines a set s that forms a pair with v. For any given m, we can choose s in $\binom{n-j}{n-m}$ ways. Thus, we have

$$\sum_{s \subset N} q^{d_s} = \sum_{j=0}^{n} a_j \binom{n-j}{n-m}.$$

Similarly, counting the pairs (t, v), where t is an $(n-m)$-subset of N, and $v \in C^\perp \cap F_t$, we have

$$\sum_{t \subset N} q^{d_t} = \sum_{i=0}^{n} b_i \binom{n-i}{m}.$$

Since $d_t = d_s + n - k - m$ and every subset t defines a unique s, we have

$$\sum_{t \subset N} q^{d_t} = \sum_{s \subset N} q^{d_s + n - k - m} = q^{n-k-m} \sum_{s \subset N} q^{d_s},$$

which implies (17), and consequently (16). □

Corollary 11.2 *(Pless power moment identities [20]).*

$$\sum_{i=0}^{n} (n-i)^r a_i = \sum_{i=0}^{r} b_i \Big(\sum_{v=i}^{r} v! S(r, v) q^{k-v} \binom{n-i}{n-v} \Big), \ r = 0, 1, \ldots, n, \qquad (18)$$

where $S(r, v)$ is a Stirling number of the second kind,

$$S(r, v) = \frac{1}{v!} \sum_{i=1}^{v} (-1)^{v-i} \binom{v}{i} i^r.$$

Note 11.3 The equation (16) can be rewritten more compactly as

$$q^k B(x) = (1 + (q-1)x)^n A(\frac{1-x}{1+(q-1)x}).$$

Exercise 11.4 Find the weight enumerators of the binary Hamming codes of length 3 and 7 and their dual codes, and then use (16) to verify your results.

Exercise 11.5 Find the weight distribution of the dual code of the binary Hamming code $H_4(2)$ of length 15 by a direct computation, and then use (16) to find the weight distribution of $H_4(2)$.

Exercise 11.6 Use the results from 11.4 and 11.5 to make a conjecture for the weight enumerator of the dual code of the binary Hamming code of length $n = 2^m - 1$, for any $m \geq 2$.

12 The Assmus-Mattson Theorem

In this section we discuss a theorem proved by Assmus and Mattson [3] in 1969, which gives a sufficient condition for the codewords of given weight in a linear code to support a t-design. We start with two lemmas.

Lemma 12.1 *Suppose that G is a $k \times n$ generator matrix of a linear $[n, k, d]$ code. Any $k \times (n - d + 1)$ matrix G' obtained by removing $d - 1$ columns of G is of rank k.*

Proof. Suppose the contrary, that is, the rank of G' is smaller than k. Then there exists a nonzero linear combination of the rows of G' which is equal to the zero vector of length $n - d + 1$. The linear combination with the same coefficients of the corresponding rows of G is a nonzero vector of weight at most $d - 1$, a contradiction. □

Lemma 12.2 *Let C be a q-ary $[n, k, d]$ code. Let u_0 be the largest integer such that*

$$u_0 - \lceil \frac{u_0}{q-1} \rceil < d,$$

where $\lceil x \rceil$ denotes the smallest integer number greater than or equal to x. If $a, b \in C$ are codewords having the same weight $u \leq u_0$ and share the same support, then $a = \beta b$ for some $\beta \in GF(q)$, $\beta \neq 0$.

Proof. Let $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$, and let $i_1, \ldots, i_u$ be the nonzero positions of a and b. We consider the set

$$M = \{\frac{a_{i_j}}{b_{i_j}} \mid j = 1, \ldots, u.\}$$

There exists a nonzero element $\beta \in GF(q)$ which occurs at least $\lceil u/(q-1) \rceil$ times in M. It follows that the weight of $a - \beta b$ is at most $u - \lceil u/(q-1) \rceil$. Since $u \leq u_0$, we have

$$u - \lceil \frac{u}{q-1} \rceil < d.$$

Thus, $u - \lceil u/(q-1) \rceil = 0$, and $a = \beta b$. □

Theorem 12.3 *(Assmus and Mattson [3]). Let C be a linear $[n, k, d]$ code, and let $\bar{d}$ be the minimum distance of the dual code $C^\perp$. Denote by u_0 the largest integer such that $u_0 - \lceil u_0/(q-1) \rceil < d$, and let w_0 be the largest integer satisfying $w_0 - \lceil w_0/(q-1) \rceil < \bar{d}$. If $q = 2$, we set $u_0 = w_0 = n$. Suppose that the number s of distinct nonzero weights in $C^\perp$ which are smaller than or equal to $n - t$, satisfies $s \leq d - t$. Then, for each weight u, such that $d \leq u \leq u_0$ the supports of codewords of weight u in C, yield a t-design. Furthermore, for each weight w such that $\bar{d} \leq w \leq \min\{n - t, w_0\}$, the supports of codewords of weight w in the dual code $C^\perp$, also yield a t-design.*

Proof. Let T be a fixed t-subset of the set of coordinates $X = \{1, 2, \ldots, n\}$. We denote by C' the code of length $n-t$ obtained by removing the coordinates contained in T from all codewords of C. Let C_0 denote the subcode of C consisting of all codewords having zeros in all t coordinates from T. Assume now that $t < d$. It follows from Lemma 12.1 that C' is an $[n - t, k]$ code. Clearly,

$$(C_0^\perp)' \subseteq (C')^\perp.$$

Since the dimension of $(C_0^{\perp})'$ is greater than or equal to $n-k-t$, we have $(C_0^{\perp})' = (C')^{\perp}$.

Let w_i, $1 \leq i \leq r$ be all distinct nonzero weights in $C^{\perp}$ which are smaller than or equal to $n-t$. These are also the only possible nonzero weights of $(C_0^{\perp})'$. Since the minimum weight of C' is greater than or equal to $d-t$, we know the first $d-t$ coefficients of the weight enumerator of C'. The number $d-t$ is greater than or equal to the number of nonzero coefficients of the weight enumerator of $(C_0^{\perp})'$. The MacWilliams identities (17) give a system of independent linear equations with a unique solution which does not depend on the choice of T, but only on its size t. Thus, the weight distribution of $(C_0^{\perp})'$ is independent of the choice of T. Since $C' = ((C_0^{\perp})')^{\perp}$, the same holds for the weight distribution of C'. In particular, the number of codewords of weight $d-t$ in C' does not depend on the choice of T, hence every t-subset of the set of coordinate indices is contained in the supports of a constant number of codewords of minimum weight d. Thus, the supports of minimum weight vectors in C form a t-design.

Suppose now that w is an integer in the range $\bar{d} \leq w \leq \min\{n-t, w_0\}$, and let D be the collection of supports of all codewords of weight w in $C^{\perp}$. We consider the family D' consisting of the complements of the sets in D. If T is a t-subset of $X = \{1, \ldots, n\}$, the number of bocks of D' containing T is equal to the number of codewords of weight w in $(C_0^{\perp})'$ divided by $q-1$ according to Lemma 12.2, and this number does not depend on the choice of T. Thus, D' is a t-design, and consequently, D is also a t-design.

We now prove that the supports of codewords of C of any weight u, $d \leq u \leq u_0$, form a t-design. We already know that this is true for $u = d$. We prove the statement by induction. Suppose that the supports of all codewords of C of any weight u' such that $d \leq u' < u$ form a t-design, and let D be the collection of supports of all codewords of C of weight u. By Lemma 12.2, the number of blocks of D containing a given t-subset $T \subset \{1, \ldots, n\}$ is equal to the number of codewords of weight $u-t$ in C' divided by $q-1$. The total number of words of weight $u-t$ in C' is independent of the choice of T. Thus D is a t-design. □

Example 12.4 The extended binary Golay code $\mathcal{G}_{24}$ is a self-dual $[24, 12, 8]$ code with nonzero weights 8, 12, 16, and 24. There are three nonzero weights smaller than $n = 24$, and $d - 5 = 8 - 5 = 3$. Hence, the supports of any

given weight form a 5-design. The weight distribution of the code is

$$a_0 = a_{24} = 1,\ a_8 = a_{16} = 759,\ a_{12} = 2576.$$

It follows from Theorem 12.3 that the codewords of weight 8 form a 5-$(24, 8, 1)$ design (or a Steiner system $S(5, 8, 24)$), while the codewords of weight 12 form a 5-$(24, 12, 48)$ design. The design supported by codewords of weight 16 is a 5-$(24, 16, 78)$ design having as blocks the complements of blocks of the design supported by codewords of weight 8.

Example 12.5 The extended ternary Golay code $\mathcal{G}_{12}$ is a self-dual $[12, 6, 6]$ code. The nonzero weights are 6, 9, and 12, hence the Assmus-Mattson Theorem 12.3 applies for $t = 5$. The weight distribution is

$$a_0 = 1,\ a_6 = 264,\ a_9 = 440,\ a_{12} = 24.$$

The codewords of minimum weight support a 5-$(16, 6, 1)$ design, while the vectors of weight 9 support a 5-$(12, 9, 70)$ design. Note that

$$\binom{12}{9} = \binom{12}{3} = 220.$$

Thus, the 5-$(12, 9, 70)$ design supported by codewords of weight 9 is a complete, or trivial design, having all possible 9-subsets as blocks.

Exercise 12.6 Prove that the supports of codewords of weight 4 of the binary code with generator matrix

$$G = \begin{pmatrix} & 0 & 1 & & 1 & & 1 \\ & 1 & & & & & \\ I_4 & 1 & & & J_3 - I_3 & & \\ & 1 & & & & & \end{pmatrix}$$

support a 3-$(8, 4, 1)$ design.

Exercise 12.7 Prove that the code from Exercise 12.6 is equivalent to the extended code of the binary Hamming code of length 7.

Exercise 12.8 Prove that the codewords of any nonzero weight smaller than $2^m - 1$ of the binary Hamming code of length $2^m - 1$ form a 2-design. In particular, the minimum weight codewords support a Steiner system $S(2, 3, 2^m - 1)$.

Exercise 12.9 Prove that the codewords of any nonzero weight smaller than 2^m of the extended binary Hamming code of length 2^m form a 3-design. In particular, the minimum weight codewords support a Steiner system $S(3, 4, 2^m)$.

Exercise 12.10 Prove that for any prime power $q \geq 2$, and any $m \geq 2$, the codewords of any nonzero weight smaller than $(q^m - 1)/(q - 1)$ of the q-ary Hamming code of length $(q^m - 1)/(q - 1)$ form a 2-design.

13 Self-dual codes and t-designs

The Assmus-Mattson Theorem 12.3 applies to codes with relatively high minimum distance and few distinct nonzero weights in their dual codes.

The extended Golay codes and the $[8, 4, 4]$ code from Exercise 12.6 all yield designs via Assmus-Mattson's Theorem, and are all self-dual. Self-dual codes, and more generally, self-orthogonal codes over a field of order 2 or 3 have regular gaps in their weight distribution. In the binary case, all weights are even, and it is possible also that all weights are divisible by 4 (in the latter case the code is called *doubly-even*; otherwise, a binary self-orthogonal code containing words of weight not divisible by 4 is called *singly-even*.) In a ternary self-orthogonal code, all weights are divisible by 3. If $q = 4$ and the dual code is defined with respect to the Hermitian inner product

$$x \cdot y = x_1 y_1^2 + \cdots + x_n y_n^2, \tag{19}$$

for $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in GF(4)^n$, all weights in a quaternary Hermitian self-orthogonal code are even.

The following upper bounds on the minimum distance of a self-dual code were proved by Mallow and Sloane [16], and MacWilliams, Odlyzko, Sloane and Ward [15].

Theorem 13.1 *Let C be a self-dual $[n, n/2, d]$ code over $GF(q)$, where $q = 2,\ 3,$ or 4.*
(i) If $q = 2$ and C is singly-even, then $d \leq 2\lfloor n/8 \rfloor + 2$.
(ii) If $q = 2$ and C is doubly-even, then $d \leq 4\lfloor n/24 \rfloor + 4$.
(iii) If $q = 3$, then $d \leq 3\lfloor n/12 \rfloor + 3$.
(iv) If $q = 4$ and C is Hermitian self-dual, then $d \leq 2\lfloor n/6 \rfloor + 2$.

A self-dual code whose minimum distance meets the corresponding upper bound in 13.1 is called *extremal*.

The extended binary and ternary Golay codes, as well as the extended $[8, 4, 4]$ Hamming code, are all extremal.

Exercise 13.2 Verify that the $[6, 3]$ code over $GF(4) = \{0, 1, \alpha, \alpha^2\}$ with a generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha \end{pmatrix}$$

is Hermitian self-dual and extremal.

Theorem 13.3 *An extremal self-dual $[n, n/2]$ code yields t-designs, where:*
(a) if $q = 2$ and C is singly-even, then $t = 3$ if $n \equiv 0 \pmod 8$, $t = 2$ if $n \equiv 2 \pmod 8$, and $t = 1$ if $n \equiv 4 \pmod 8$;
(b) if $q = 2$ and C is doubly-even, then $t = 5,\ 3,$ or 1 according to $n \equiv 0,\ 8,$ or $16 \pmod{24}$;
(c) $t = 5$ if $q = 3$ and $n \equiv 0 \pmod{12}$;
(d) $t = 5$ if $q = 4$ and $n > 6$ and $n \equiv 0 \pmod 6$.

Exercise 13.4 Prove Theorem 13.3.

Table 13.5 *Some 5-Designs derived from self-dual codes*

Design	Code	Comments
5-(12,6,1)	$[12, 6, 6],\ q = 3$	Extended ternary Golay code
Golay code 5-(18,8,6) 5-(18,10,180)	$[18, 9, 8], q = 4$	Extended cyclic code
5-(24,8,1) 5-(24,12,48)	$[24, 12, 8],\ q = 2$	Extended binary Golay code
5-(24,9,6) 5-(24,12,576) 5-(24,15,8580)	$[24, 12, 9],\ q = 3$	Extended QR code; Pless symmetry code [21]
5-(30,12,220) 5-(30,14,5390) 5-(30,16,123000)	$[30, 15, 12],\ q = 4$	Extended QR code
5-(36,12,45) 5-(36,15,5577) 5-(36,18,209685) 5-(36,21,2438973)	$[36, 18, 12],\ q = 3$	Pless symmetry code
5-(48,12,8) 5-(48,16,1365) 5-(48,20,36176) 5-(48,24,190680)	$[48, 24, 12],\ q = 2$	Extended QR code
5-(48,15,364) 5-(48,18,50456) 5-(48,21,2957388) 5-(48,24,71307600) 5-(48,27,749999640)	$[48, 24, 15],\ q = 3$	Extended QR code Pless symmetry code
5-(60,18,3060) 5-(60,21,449820) 5-(60,24,34337160) 5-(60,27,1271766600) 5-(60,30,24140500956) 5-(60,33,239329029060)	$[60, 30, 18],\ q = 3$	Pless symmetry code Extended QR code

14 Pless symmetry codes

The symmetry codes are a class of ternary self-dual codes introduced by Pless [21]. The smallest symmetry code is the extended ternary Golay code, and a few more symmetry codes of larger length also yield 5-designs.

Let $p > 2$ be a prime, and let χ be the *Legendre symbol*, defined as follows:

$$\chi(i) = \begin{cases} 0 & \text{if} \quad i = 0, \\ 1 & \text{if} \quad i \text{ is a quadratic residue} \pmod p, \\ -1 & \text{if} \quad i \text{ is not a quadratic residue} \pmod p. \end{cases} \tag{20}$$

Since half of the integers between 1 and $p-1$ are quadratic residues, and the other half are non-residues, we have

$$\sum_{i=0}^{p-1} \chi(i) = 0.$$

If $1 \le a, b \le p-1$, then $\chi(ab) = 1$ if a and b are both quadratic residues or non-residues, and $\chi(ab) = -1$ if one of a, b is a quadratic residue and the other is a non-residue. Thus

$$\chi(ab) = \chi(a)\chi(b) \tag{21}$$

for any $a, b \in GF(p)$.

Lemma 14.1 *For every integer i in the range $1 \le i \le p-1$, we have*

$$\sum_{a=0}^{p-1} \chi(a)\chi(a+i) = -1. \tag{22}$$

Proof. If $1 \le a \le p-1$, the equation $a + i = ax$ has a unique solution $x = (a+i)/a$ in $GF(p)$. In addition, if $a \ne b$, $1 \le a, b \le p-1$, then $(a+i)/a \ne (b+i)/b$. Note also that $(a+i)/a \ne 1$ for $i \ne 0$. Thus,

$$\sum_{a=0}^{p-1} \chi(a)\chi(a+i) = \sum_{a=1}^{p-1} \chi(a)\chi(a+i) = \sum_{a=1}^{p-1} \chi(a)\chi(ax).$$

Using (21), we have

$$\sum_{a=1}^{p-1} \chi(a)\chi(ax) = \sum_{a=1}^{p-1} \chi(a^2x) = \sum_{a=1}^{p-1} \chi(a^2)\chi(x) = \sum_{x=0,\ x\ne 1}^{p-1} \chi(x) = -\chi(1) + \sum_{x=0}^{p-1} \chi(x) = -1.$$

□

Let $Q = (q_{ij})$ be the $p \times p$ matrix $q_{i,j} = \chi(j-i)$ for $0 \le i, j \le p-1$. Using Lemma 22, it is easy to prove the following.

Lemma 14.2 *(i)* $QJ = JQ = 0$.
(ii) $QQ^T = pI - J$.

Exercise 14.3 Prove Lemma 14.2.

Given an odd prime $p \equiv 2 \pmod 3$, the *symmetry code* $C(p)$ [21] is defined as the ternary code with generator matrix

$$G = \begin{pmatrix} & 0 & 1 & \cdots & 1 \\ & \chi(-1) & & & \\ I_{p+1} & \vdots & & Q & \\ & \chi(-1) & & & \end{pmatrix}.$$

Theorem 14.4 *The symmetry code $C(p)$ is a self-dual $[2p+2, p+1]$ code.*

Exercise 14.5 Prove Theorem 14.4.

Exercise 14.6 Show that the symmetry code $C(5)$ is equivalent to the extended ternary Golay code.

The minimum distances of $C(11)$, $C(17)$, $C(23)$, and $C(29)$ are 9, 12, 15, and 18, respectively. Thus, all these codes are extremal and yield 5-designs.

15 Quadratic-residue codes

Let $p > 2$ be a prime, and let χ be the Legendre symbol (22). Let $Q = (q_{ij})_{p \times p}$, where $q_{ij} = \chi(j-i)$.

Lemma 15.1

$$Q^T = \begin{cases} Q & \text{if } p \equiv 1 \pmod 4, \\ -Q & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{23}$$

Proof. We have

$$q_{ij} = \chi(j-i) = \chi(-1)\chi(i-j) = \chi(-1)q_{ji}.$$

Let β be a primitive element of $GF(p) = Z_p$. Then $\beta^{p-1} = 1$ and

$$\beta^{p-1} - 1 = (\beta^{\frac{p-1}{2}} - 1)(\beta^{\frac{p-1}{2}} + 1) = 0.$$

Since $\beta^{\frac{p-1}{2}} - 1 \neq 0$, it follows that

$$\beta^{\frac{p-1}{2}} = -1.$$

If $p \equiv 1 \pmod 4$, $p = 4m+1$, then

$$\beta^{\frac{p-1}{2}} = \beta^{2m} = -1$$

and -1 is a quadratic residue modulo p, hence $\chi(-1) = 1$ and $q_{ij} = q_{ji}$.

If $p \equiv 3 \pmod 4$, $p = 4m+3$, then

$$\beta^{\frac{p-1}{2}} = \beta^{2m+1} = -1$$

and -1 is a quadratic nonresidue modulo p, hence $\chi(-1) = -1$ and $q_{ij} = -q_{ji}$. □

The matrix $M = (Q + J - I)/2$ is a square $(0,1)$-matrix with constant row and column sum equal to $(p-1)/2$. Alternatively, $M = (m_{ij})_{p\times p}$, where

$$m_{i,j} = \begin{cases} 1 & \text{if } i \neq j \text{ and } j-i \text{ is a quadratic residue} \pmod p, \\ 0 & \text{otherwise.} \end{cases} \tag{24}$$

Lemma 15.2

$$MM^T = \begin{cases} \frac{p-1}{4}I + \frac{p-1}{4}J - M & \text{if } p \equiv 1 \pmod 4, \\ \frac{p+1}{4}I + \frac{p-3}{4}J & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{25}$$

Proof. Use Lemma 23. □

Corollary 15.3 *The matrix M is the incidence matrix of a $2-(p,(p-1)/2,(p-3)/4)$ design if $p \equiv 3 \pmod 4$, and the adjacency matrix of a strongly regular graph with parameters $n = p$, $k = (p-1)/2$, $\lambda = (p-5)/4$, $\mu = (p-1)/4$ if $p \equiv 1 \pmod 4$.*

A 2-(v, k, λ) design having equal number of points and blocks, $v = b$, is called *symmetric*. If D is a symmetric design, every point is contained in k blocks, every two blocks share exactly λ points, and $k(k-1) = \lambda(v-1)$. Thus, the incidence matrix A of a symmetric 2-(v, k, λ) design satisfies the equations

$$AJ = JA = kJ,\ AA^T = A^TA = (k-\lambda)I + \lambda J. \tag{26}$$

Lemma 15.4 *Let p be a prime and let A be the incidence matrix of a symmetric 2-(v, k, λ) design such that $p \mid k-\lambda$, but $p^2 \not| k-\lambda$ and $p \not| k$. Then the rank of A over $GF(q)$, $\mathrm{rank}_q(A)$, where $q = p^s$, $s \geq 1$, is equal to $(v+1)/2$.*

Proof. The determinant of AA^T can be found easily by using (26) and applying elementary row operations (adding multiples of rows to other rows):

$$\det(AA^T) = k^2(k-\lambda)^{v-1}. \tag{27}$$

Consequently, $\det(A^2) = (k-\lambda)k^2$, and

$$\det(A) = \pm k(k-\lambda)^{\frac{v-1}{2}}.$$

Applying elementary operations of adding a multiple of a row (or column) to another row (or column) and permuting rows and columns, we can put A into diagonal form. These operations are equivalent to multiplying A from the left and from the right by integral matrices with determinant 1 (unimodular matrices) B, C so that

$$BAC = \mathrm{diag}(d_1, d_2, \ldots, d_v)$$

for some integer $d_1, \ldots, d_v$. Hence,

$$\det(BAC) = d_1d_2\cdots d_v = \det(A) = \pm k(k-\lambda)^{\frac{v-1}{2}}.$$

The largest power of p that divides $\det(A)$ is $(v-1)/2$. Consequently, p can divide at most $(v-1)/2$ of the numbers $d_1, \ldots, d_v$, and the p-rank of BAC, and consequently,

$$\mathrm{rank}_p(A) \geq \frac{v+1}{2}.$$

On the other hand, we have

$$(J-A)(J-A)^T = (k-\lambda)I + (v-2k+\lambda)J.$$

Note that $k(k-1) = \lambda(v-1)$ implies

$$\lambda(v-k) = (k-\lambda)(k-1),$$

and since $p \not| k$, we have $p \not| \lambda$, hence $p|(v-k)$, and $p|(v-2k+\lambda = (v-k) - (k-\lambda))$. Thus, the weight of every row of $J-A$, as well as the product of every two rows of $J-A$, is divisible by p, hence the row space of $J-A$ over $GF(p)$ is a self-orthogonal code, hence $\text{rank}_p(J-A) \leq v/2$. Equation (27) implies that $k-\lambda$ is a square if v is even. Thus, by the assumptions of the theorem, v is odd and

$$\text{rank}_p(J-A) \leq \frac{v-1}{2}.$$

Since $p \not| k$, the all-one vector $\bar{1}$ is contained in the row (and column) space of A over $GF(q)$, and since $p \not| v$, the vector $\bar{1}$ is not contained in the row (or column) space of $J-A$ over $GF(q)$. Thus

$$\text{rank}_p(A) = \text{rank}_p(J-A) + 1 \leq \frac{v+1}{2},$$

which completes the proof. □

Corollary 15.5 *(Assmus and Maher [1]). Let A be the incidence matrix of a symmetric 2-(v,k,λ) design and let p be a prime such that $p \mid k-\lambda$, $p^2 \not| k-\lambda$, $p \not| k$, and $-\lambda$ is a square in $GF(p)$. The code C over $GF(q)$ of length $(v+1)/2$ with a generator matrix obtained by adding to A a constant column with entries equal to $\sqrt{-\lambda}$, is a self-dual $(v+1, \frac{v+1}{2})$ code.*

Exercise 15.6 Prove Corollary 15.5.

Given a prime $p > 2$ and a prime power q, the q-ary *quadratic-residue code* $QR = QR(p,q)$ is defined as a linear code of length $n = p$ over $GF(q)$ with generator matrix M defined by (24). A *extended quadratic-residue code* QR^* is a code over $GF(q)$ of length $p+1$ having as generator matrix the matrix M bordered by the all-one column.

Theorem 15.7 *Let $n \equiv 3 \pmod 4$ be a prime.*
(i) If p_1 is a prime such that $n \equiv -1 \pmod{p_1}$, the code $QR^*(n,q)$, where $q = p_1^s$, $s \geq 1$, is self-orthogonal.
(ii) If, in addition, $p_1 \not| n-1$ and $p_1^2 \not| n+1$, the code $QR*(n,q)$ is self-dual.

Exercise 15.8 Prove Theorem 15.7.

Exercise 15.9 If $n \equiv -1 \pmod 8$ is prime, the binary extended code QR^* of length $n+1$ is self-orthogonal and doubly-even.

Example 15.10 The binary extended quadratic-residue codes of length 8, 24, 32, 48, 72 are doubly-even self-orthogonal codes. In addition, the codes of length 8, 24 and 72 are self-dual by Theorem 15.7. The codes of length 32 and 48 are also self-dual, although their self-duality does not follow from Theorem 15.7. The codes of length 8, 24, 32, and 48 are extremal. The codes of length 8 and 32 yield 3-designs, while the codes of length 24 and 48 yield 5-designs by the Assmus-Mattson Theorem 12.3. The code $QR(23, 2)$ is equivalent to the binary Golay code, while $QR(7, 2)$ is equivalent to the Hamming code.

Example 15.11 The ternary extended quadratic-residue codes of length 12, 24, 48, and 60 are self-dual and extremal, hence yield 5-designs by the Assmus-Mattson Theorem. The code $QR(11, 3)$ is equivalent to the perfect ternary Golay code, while the extended code $QR(11, 3)^*$ is equivalen to the extended ternary Golay code.

Exercise 15.12 Give an example of a symmetric 2-$(15, 8, 4)$ design of 2-rank 4.

Exercise 15.13 Give an example of a symmetric 2-$(15, 7, 3)$ design of 2-rank 5.

Exercise 15.14 Give an example of a 3-$(16, 8, 3)$ design of 2-rank 5.

Exercise 15.15 (i) Prove that if A is the incidence matrix of a symmetric 2-$(31, 15, 7)$ design then

$$6 \leq \text{rank}_2(A) \leq 16.$$

(ii) Give an example of a symmetric 2-$(31, 15, 7)$ design with incidence matrix of 2-rank 6.
(iii) Give an example of a symmetric 2-$(31, 15, 7)$ design with incidence matrix of 2-rank 16.

16 Cyclic codes

A code $C \subseteq GF(q)^n$ is *cyclic* if the permutation $(1, 2, \ldots, n)$ is an automorphism of the code. Thus, for every vector $(a_0, a_1, \ldots, a_{n-1}) \in C$, we have also $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$. Consequently, along with every codeword, the code contains all of its cyclic shifts.

A cyclic code does not have to be linear, but an elegant algebraic theory has been developed for linear cyclic codes. If $a = (a_0, \ldots, a_{n-1})$ is a vector of a cyclic code $C \subseteq GF(q)^n$, we can associate with a the polynomial

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$

where x is a variable. With this in mind, we can think of C as a set of polynomials in x of degree at most $n-1$. The cyclic property of C implies that if $a(x) \in C$ then $x^m a(x) \pmod{(x^n - 1)} \in C$ for all $m = 0, 1, \ldots, n-1$. If C is a linear cyclic code and $a(x) \in C$ then $a(x) \sum_{i=0}^{n-1} b_i x^i \pmod{(x^n - 1)}$ belongs to C for arbitrary $b_0, \ldots, b_{n-1} \in GF(q)$. Thus, C is closed under multiplication with polynomials in x modulo $x^n - 1$. In algebraic terms, a linear cyclic code is an *ideal* in the ring of polynomials $R_n = F[x]/(x^n - 1)$, where $F[x]$ is the ring of all polynomials in x over the field $GF(q)$. Thus, we have the following.

Theorem 16.1 *A subset $C \subseteq R_n$ is a linear cyclic code if and only if C is an ideal in R_n.*

A polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is *monic* if $a_{n-1} = 1$. The next theorem shows that cyclic codes are principal ideals in R_n.

Theorem 16.2 *Assume that $C \subseteq R_n$ is a linear cyclic $[n, k]$ code with $k \geq 1$, and let $g(x)$ be a monic polynomial of minimum degree in C. Then*

$$C = < g(x) > = \{b(x)g(x) \pmod{(x^n - 1)} \mid b(x) \in R_n\}.$$

Proof. Since $k \geq 1$, C contains nonzero polynomials. Let $g(x)$ be a monic polynomial of minimum degree in C. If $a(x)$ is an arbitrary nonzero polynomial in C, we can divide $a(x)$ by $g(x)$ in R_n: there are $b(x) \in R_n$ and $r(x) \in R_n$, where the degree of $r(x)$ is smaller than the degree of $g(x)$, such that

$$a(x) = b(x)g(x) + r(x) \pmod{x^n - 1},$$

hence $r(x) = a(x) - b(x)g(x) \in C$. The choice of $g(x)$ now implies that $r(x) = 0$.

Note that if $g_1(x)$ is another monic polynomial of minimum degree in C then $g_1(x) = b(x)g(x)$ implies $\deg(b(x)) = 0$ and $b(x) = 1$, thus, $g_1(x) = g(x)$, and the polynomial $g(x)$ is the unique monic polynomial of minimum degree in C. □

The polynomial $g(x)$ from Theorem 16.2 is called the *generator polynomial* of the cyclic code C. By definition, the zero polynomial is the generator polynomial of the cyclic $(n, 0]$ code consisting of the zero vector only. The constant 1 is the generator polynomial of the whole space, the $[n, n]$ code $R_n = GF(q)^n$.

Theorem 16.3 *If $g(x)$ is the generator polynomial of a cyclic $[n, k]$ code $C \subseteq R_n$ with $k \geq 1$, then*
(i) The degree of $g(x)$ is equal to $n-k$, and if $g(x) = g_0+g_1x+\ldots g_{n-k-1}x^{n-k-1}+x^{n-k}$, the following circulant $k \times n$ matrix G is a generator matrix of C:

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k-1} & 1 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & 0 & g_{n-k-1} & 1 & \ldots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \ldots & g_0 & \ldots & \ldots & & 1 \end{pmatrix}. \tag{28}$$

(ii) $g(x)$ divides $x^n - 1$.

Proof. (i) Since $|C| = q^k$, it follows from Theorem 16.2 that the degree of $g(x)$ is equal to $n - k$. Thus, a generator matrix must have k linearly independent rows, all being vectors from C, and the matrix (28) has these properties.
(ii) We can divide $x^n - 1$ by $g(x)$ in the ring $F[x]$:

$$x^n - 1 = h(x)g(x) + r(x), \tag{29}$$

where $\deg(r(x)) < \deg(g(x))$. Equation (29) implies that in the ring R_n we have

$$r(x) = -b(x)g(x) \in C,$$

hence $r(x)$ must be the zero polynomial and $x^n - 1 = h(x)g(x)$. □

If $g(x)$ is a generator polynomial of a cyclic code $C \subseteq R_n$, the polynomial $h(x) = (x^n - 1)/g(x)$ is called the *check polynomial* of C.

Theorem 16.4 *If* $h(x) = h_0 + h_1 x + \ldots h_{k-1}x^{k-1} + x^k$ *is the check polynomial of a cyclic* $[n, k]$ *code then the following* $(n-k) \times n$ *circulant matrix* H*,*

$$H = \begin{pmatrix} 1 & h_{k-1} & \ldots & h_0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & h_1 & h_0 & \ldots & 0 \\ \vdots & & & & & & \\ 0 & 0 & \ldots & 1 & \ldots & & h_0 \end{pmatrix}, \tag{30}$$

is a parity check matrix of C*.*

Exercise 16.5 Prove Theorem 16.4.

If $a(x)$ is a polynomial of degree m, the polynomial $x^m a(\frac{1}{x})$ is called the *reciprocal* of $a(x)$.

Exercise 16.6 Prove that if $h(x)$ is the check polynomial of a cyclic code C then the reciprocal polynomial of $h(x)$ is a generator polynomial of the dual code $C^{\perp}$.

Exercise 16.7 Find generator polynomials for all binary cyclic codes of length 7.

Exercise 16.8 Find generator polynomials for all ternary cyclic codes of length 11.

17 Factoring $x^n - 1$

Finding cyclic codes of length n over a finite field $GF(q)$ requires factoring $x^n - 1$ in the ring of polynomials $F_q[x]$ over $GF(q)$.

Lemma 17.1 *If* $f(x) \in F_{p^s}[x]$ *then*

$$f(x^{p^s}) = (f(x))^{p^s}.$$

Exercise 17.2 Prove Lemma 17.1.

If $\beta \in GF(q)$, where $q = p^s$, $s \geq 1$, and p is a prime, then

$$\beta^q = \beta,$$

hence β is a root of the polynomial $x^q - x \in F_p[x]$.

The *minimal polynomial* $m(x) = m_\beta(x)$ over $GF(p)$ of an element $\beta \in GF(p^s)$ is defined as a monic polynomial of smallest degree with coefficients in $GF(p)$ having β as a root.

Lemma 17.3 *The minimal polynomial $m(x) = m_\beta(x)$ of an element $\beta \in GF(p^s)$ has the following properties.*
(a) $m(x)$ is irreducible over $F_p[x]$.
(b) $m(x)$ divides every polynomial in $F_p[x]$ having β as a root.
(c) $m(x)$ is unique.
(d) $m(x)$ divides $x^{p^s} - x$.
(e) The degree of $m(x)$ does not exceed s.

Exercise 17.4 Prove Lemma 17.3.

Corollary 17.5

$$x^{p^s} - x = \prod_{\beta \in GF(p^s)} m_\beta(x). \tag{31}$$

Exercise 17.6 Let q be a prime power. How many distinct cyclic codes of length $n = q - 1$ over $GF(q)$ are there?

Exercise 17.7 How many distinct cyclic codes of length 40 over $GF(41)$ of dimension 35 are there?

The multiplicative group of $GF(q)$ is a cyclic group. Any generator of this group is called a *primitive* element of $GF(q)$. Thus, $\beta \in GF(q)$ is primitive if $\beta^i \neq 1$ for $0 < i < q - 1$, and

$$GF(q) = \{0, \beta, \beta^2, \ldots, \beta^{q-2}, \beta^{q-1} = 1\}.$$

Exercise 17.8 List the primitive elements of $GF(17)$.

An element $\beta \in GF(q)$ is a *primitive* nth root of unity if $\beta^n = 1$ and $\beta^i \neq 1$ for $0 < i < n$. It follows that n divides $q - 1$, and $n = q - 1$ if and only if β is a primitive element of $GF(q)$. If β is a primitive element of $GF(q)$ then $\gamma = \beta^d$ is a primitive nth root of unity with $n = (q - 1)/d$.

Given a prime power q and a positive integer n relatively prime to q, the *order* of q modulo n is defined as the smallest positive integer d such that $q^d \equiv 1 \pmod{n}$.

Let s be an integer with $0 \leq s < n$. The *q-cyclotomic coset* of s modulo n is the set

$$C_s = \{s, sq, \ldots, sq^{d-1} \pmod{n}\},$$

where d is the smallest positive integer such that $sq^d \equiv s \pmod{n}$. Note that the order of q modulo n is equal to the size of the q-cylotomic coset of 1.

Lemma 17.9 *Let n be a positive integer such that $gcd(n, q) = 1$. Let t be the order of q modulo n, and let β be a primitive nth root of unity in $GF(q^t)$. For every integer s with $0 \leq s < n$, the minimal polynomial of β^s over $GF(q)$ is given by*

$$m_{\beta^s}(x) = \prod_{j \in C_s} (x - \beta^j).$$

Exercise 17.10 Prove Lemma 17.9.

Theorem 17.11 *Let n be a positive integer such that $gcd(n, q) = 1$. Let t be the order of q modulo n, and let β be a primitive nth root of unity in $GF(q^t)$. The factorization of $x^n - 1$ into irreducible factors over $GF(q)$ is given by*

$$x^n - 1 = \prod_s m_{\beta^s}(x),$$

where $m_{\beta^s}(x)$ is the minimal polynomial of β^s over $GF(q)$.

Corollary 17.12 *If q is a prime power and n is a positive integer such that $gcd(n, q)$=1 then $x^n - 1$ has n distinct roots in $GF(q^t)$, where t is the order of q modulo n.*

Proof. Since n divides $q^t - 1$, the polynomial $x^n - 1$ divides $x^{q^t-1} - 1$. Thus, every root of $x^n - 1$ is also a root of $x^{q^t-1} - 1$. The polynomial $x^{q^t-1} - 1$ has $q^t - 1$ distinct roots in $GF(q^t)$ being the nonzero elements of $GF(q^t)$. □

Exercise 17.13 Prove Theorem 17.11.

Exercise 17.14 Factor $x^{15} - 1$ over $GF(2)$.

Exercise 17.15 Factor $x^{23} - 1$ over $GF(2)$.

Exercise 17.16 How many distinct cyclic binary linear codes of length 17 are there? List the dimensions of these codes.

Exercise 17.17 Give the generator polynomial $g(x)$, check polynomial $h(x)$, and the parity check-matrix matrix associated with $h(x)$, of a linear binary cyclic code length 15 which is equivalent to the Hamming code of length 15.

Exercise 17.18 (i) Find a generator polynomial for a cyclic ternary $[11, 6]$ code.
(ii) Show that a cyclic ternary $[11, 6]$ code has minimum distance 5 (consequently, it is equivalent to the perfect ternary Golay code).

Exercise 17.19 Find the minimal polynomials of the elements of $GF(16)$ over $GF(2)$.

Exercise 17.20 Find the minimal polynomials of the elements of $GF(3^5)$ over $GF(3)$.

Exercise 17.21 Determine the smallest field of characteristic 3, $GF(3^t)$, that contains all roots of $x^{23} - 1$.

Exercise 17.22 Determine the number of cyclic ternary codes of length 13.

Exercise 17.23 Give the generator polynomial of a cyclic ternary $[13, 10]$ code.

18 Idempotent generators of cyclic codes

An element e of the ring R_n is called an *idempotent* if $e^2 = e$. Trivial examples are $e = 0$ and $e = 1$.

Theorem 18.1 *Let q be a prime power and n be a positive integer such that $gcd(n, q) = 1$, and let C be a linear cyclic code of length n over $GF(q)$. There exists an idempotent $e(x) \in C$ such that*

$$C =< e(x) >= \{a(x)e(x) \mid a(x) \in R_n\}.$$

Proof. If C is the code of dimension zero then $e(x)$ is the zero polynomial. If $C = R_n$ is the whole space, we can take $e(x) = 1$. Suppose that C is a code of dimension k, $1 < k < n$. The generator polynomial $g(x)$ and check polynomial $h(x)$ of C are both nonzero polynomials such that $g(x)h(x) = x^n - 1$. Since all roots of $x^n - 1$ in R_n are distinct (by Corollary 17.12), it follows that $gcd(g(x), h(x)) = 1$. By the Euclidean algorithm, there exist polynomials $a(x), b(x) \in F_q[x]$ such that

$$a(x)g(x) + b(x)h(x) = 1 \tag{32}$$

in $F_q[x]$. Consider the polynomial $e(x) = a(x)g(x) \in C$. Multiplying both sides of (32) by $e(x)$ gives

$$e^2(x) = a^2(x)g^2(x) + a(x)g(x)b(x)h(x) = a(x)g(x) = e(x). \qquad (33)$$

Since

$$a(x)g(x)b(x)h(x) = (a(x)b(x))(g(x)h(x)) = 0$$

in R_n, $e(x) = a(x)g(x)$ is an idempotent in R_n. Since $e(x)$ is a multiple of $g(x)$ in R_n, it follows that $e(x) \in C$ and $< e(x) > \subseteq C$.

If $c(x) \in C$ then $c(x) = f(x)g(x)$ for some $f(x) \in R_n$. Multiplying both sides of (32) by $c(x) = f(x)g(x)$ gives

$$f(x)g(x)a(x)g(x) + f(x)g(x)b(x)h(x) = c(x),$$

and since $f(x)g(x)b(x)h(x) = 0$ in R_n, we have

$$c(x) = (f(x)g(x))e(x) \in < e(x) > .$$

Thus, $C \subseteq < e(x) >$, and consequently, $C = < e(x) >$. □

An idempotent $e(x)$ of a cyclic code C such that $C = < e(x) >$ is called an *idempotent generator* of C.

Exercise 18.2 Prove that a cyclic code has only one idempotent generator.

Exercise 18.3 Find an idempotent generator for the ternary Golay code of length 11.

Idempotents are very easy to find in the binary case. If $q = 2$ and n is an odd integer, a polynomial $e(x) \in R_n$, $e(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_s}$ is an idempotent if and only if

$$x^{i_1} + x^{i_2} + \cdots + x^{i_s} = x^{2i_1} + x^{2i_2} + \cdots + x^{2i_s}$$

in R_n. Thus, the set of exponents $\{i_1, \ldots, i_s\}$ is a union of 2-cyclotomic cosets modulo n.

Example 18.4 If $n = 7$, the 2-cyclotomic cosets are

$$\{0\},\ \{1, 2, 4\},\ \{3, 6, 5\},$$

and the idempotents in R_7 are $0, 1 = x^0, x+x^2+x^4,\ x^3+x^6+x^5,\ 1+x+x^2+x^4,$ $1+x^3+x^6+x^5,\ x+x^2+x^4+x^3+x^6+x^5$, and $1+x+x^2+x^4+x^3+x^6+x^5$.

Theorem 18.5 *If C is a cyclic code with an idempotent generator $e(x)$, the generator polynomial of C is $g(x) = gcd(e(x), x^n - 1)$.*

Exercise 18.6 Prove Theorem 18.5.

Example 18.7 The generator polynomial of the binary cyclic code of length 7 with idempotent generator $x^3 + x^6 + x^5$ is

$$gcd(x^3+x^6+x^5, x^7-1) = gcd(x^3(1+x^2+x^3), (x-1)(x^3+x+1)(x^3+x^2+1) = x^3+x^2+1.$$

Idempotent generators are used in the traditional definition of binary quadratic residue (QR) codes. Let $n \equiv \pm 1 \pmod 8$ be a prime. Then 2 is a quadratic residue modulo n. We denote by Q the set of quadratic residues, and by N the set of quadratic nonresidue modulo n:

$$Q = \{\, i \mid 1 \le i \le n-1,\ i \equiv a^2 \pmod n,\ a \in Z\},\ N = \{\, j \mid 1 < j \le n-1,\ j \notin Q\}.$$

The binary cyclic codes C_Q, C_N having as idempotent generators the polynomials

$$e_Q = \sum_{i \in Q} x^i,\ e_N = \sum_{j \in N} x^j$$

respectively, are known as *quadratic residue codes.*

Theorem 18.8 *Let $n \equiv -1 \pmod 8$ be a prime.*
(a) C_Q and C_N are equivalent.
(b) $C_Q \cap C_N =< \bar{1} >$.
(c) $\dim(C_q) = \dim(C_N) = (n+1)/2$.
(d) The extended quadratic residue codes are self-dual and doubly-even.
(e) (The square root bound) The minimum distance d of C_Q satisfies the inequality $d^2 - d + 1 \ge n$.

Exercise 18.9 Prove Theorem 18.8.

Example 18.10 If $n = 31$ or $n = 47$, the extended binary quadratic-residue codes are self-dual. In these cases, Theorem 15.7 only implies that the extended quadratic residue codes are self-orthogonal. See also Exercise 15.9 and Example 15.10.

Exercise 18.11 Give the idempotent generator of C_Q for $n = 23$.

Exercise 18.12 Prove that the minimum distance of the binary quadratic-residue code C_Q of length 23 is 7, thus, the code is perfect.

References

[1] E.F. Assmus, Jr., and D. P. Maher, Nonexistence proofs for projective designs, *Amer. Math. Monthly*, **85** (1978), 110-12.

[2] E.F. Assmus, Jr., H.F. Mattson, Jr., Coding and Combinatorics, *SIAM Review*, **16** (1974), 349-388.

[3] E. F. Assmus, Jr., and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory*, **6**, (1969), 122-151.

[4] P. Delsarte and J. -M. Goethals, Unrestricted codes with the Golay parameters are unique, *Discrete Math.*, **12** (1975), 211-224.

[5] M. J. E. Golay, Notes on digital coding, *Proc. IEEE*, **37** (1949), 657.

[6] R. W. Hamming, Error detecting and error correcting codes, *Bell Syst. Tech. J.*, **29** (1950), 147-160.

[7] O. Heden, A survey of perfect codes, *Advances in Mathematics of Communications*, **2** (2008), 223-247.

[8] F. Hergert, The equivalence classes of the Vasil'ev codes of length 15, *Lecture Notes in Math.*, **969** (1982), 176-186.

[9] B. Lindström, On group and nongroup perfect codes in q symbols, *Math. Scand.*, **25** (1969), 149-158.

[10] J.H. van Lint, On the nonexistence of perfect 2- and 3-Hamming-error-correcting codes over $GF(q)$, *Information and Control*, **16** (1970), 396-401.

[11] J.H. van Lint, A survey of perfect codes, *Rocky Mountain J. Math.* **5** (1975), 199-224.

[12] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, 1982.

[13] F. J. MacWilliams, Combinatorial problems of elementary group theory, PhD Thesis, Department of Math., Harvard University, May 1962.

[14] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.*, **42** (1963), 79-94.

[15] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, and H.N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory* A **25** (1978), 288-318.

[16] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Information and Control* **22** (1973), 188-200.

[17] E. Mathieu, Memoire sur létude des fonctions de plusiers quantités, *J. Math. p. et a.*, **6** (1861), 241-323.

[18] E. Mathieu, Sur la fonction cinq fois transitive de 24 quantités, *J. Math. p. et a.*, **18** (1873), 25-46.

[19] Patric R.J. Östergard, Olli Pottonen, The perfect binary one-error-correcting codes of length 15: Part I - classification, arXiv:0806.2513v1 [cs.IT], 16 June 2008.

[20] V. Pless, Power moment identities on weight distributions in error correcting codes, *Information and Control* **6** (1963), 147-152.

[21] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory* **5** (1968), 215-228.

[22] V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory*, **5** (1968), 215-228.

[23] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, 3d Ed., Wiley, 1998.

[24] C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. Royal Statist. Soc.*, Supplement, **9** (1947), 128-139.

[25] C. Shannon, A mathematical theory of communication, *Bell System J.*, **27** (1948), 623-656.

[26] C. Shannon, Coding theorems for a discrete source with a fidelity criterion, *IRE Nat. Conv. Rec.*, Part 4, (1959), 142-163.

[27] J. Schönheim, On linear and nonlinear single-error-correcting q-ary perfect codes, *Information and Control*, **12** (1968), 23-26.

[28] A. Tietäväinen, On the nonexistence of perfect codes over finite fields, *SIAM J. Appl. Math.* **24** (1973), 88-96.

[29] J. L. Vasil'ev On nongroup close-packed codes (*in Russian*), *Probl. Kibernet.*, **8** (1962), 337-339, translated in *Probleme der Kibernetik* **8** (1965), 375-378.

[30] V.A. Zinoviev, V.K. Leontiev, The nonexistence of perfect codes over Galois fields, *Problems of Control and Information* **2** (1973), 123-132.

Index