Linear Codes

There is a lack of structure in the block codes we have considered in the first few chapters. Either we chose the code entirely at random, as in the proof of Theorem 1.12, or we built the code using the greedy algorithm, as in the proof of the Gilbert–Varshamov bound, Theorem 3.7. In this chapter, we introduce some algebraic structure to the block codes by restricting our attention to linear codes, codes whose codewords are the vectors of a subspace of a vector space over a finite field. Linear codes have the immediate advantage of being fast to encode. We shall also consider a decoding algorithm for this broad class of block codes. We shall prove the Griesmer bound, a bound which applies only to linear codes and show how certain linear codes can be used to construct combinatorial designs.

4.1 Preliminaries

If $A = \mathbb{F}_q$ and C is a subspace of $\mathbb{F}_q^n$, then we say that C is a **linear code over** $\mathbb{F}_q$ or simply a **linear code**. If the subspace has dimension k, then we say that C is a k-**dimensional linear code over** $\mathbb{F}_q$. Observe that $|C| = q^k$.

As in the case of an n-tuple, we define the **weight** $\mathrm{wt}(v)$ of a vector $v \in \mathbb{F}_q^n$ as the number of non-zero coordinates that v has. Recall that the elements of a code are called codewords.

Lemma 4.1 *The minimum distance d of a linear code C is equal to the minimum weight w of a non-zero codeword of C.*

Proof

Suppose $u \in C$ is a codeword of minimum non-zero weight w. Since C is a subspace, the zero vector 0 is in C. Clearly $d(u, 0) = w$, so $w \geqslant d$.

Suppose u and v are two codewords at minimum distance from each other, so $d(u, v) = d$. Since C is linear, $u - v \in C$, and $d(u - v, 0) = d$. Hence, there is a codeword in C with weight d, which implies that $d \geqslant w$. □

S. Ball, *A Course in Algebraic Error-Correcting Codes*, Compact Textbooks in Mathematics,
https://doi.org/10.1007/978-3-030-41153-4_4

We can describe a linear code C by means of a basis. A matrix G whose rows are a basis for C is called a **generator matrix** for C. Thus,

$$C = \{vG \mid v \in \mathbb{F}_q^k\}.$$

We will often use the short-hand notation $[n, k, d]_q$ code to mean that the code is a k-dimensional linear code of length n and minimum distance d over $\mathbb{F}_q$. For a not necessarily linear code, we use the notation $(n, K, d)_r$ code to mean a code of length n, minimum distance d of size K over an alphabet of size r.

Example 4.2
The minimum weight of the non-zero codewords of the 4-dimensional linear code of length 7 over $\mathbb{F}_2$ generated by the matrix

$$G = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,1 \end{pmatrix}$$

is 3, so it follows from Lemma 4.1 that the code is a $[7, 4, 3]_2$ code. ■

Example 4.3
Consider the $[9, 3, d]_3$ code generated by the matrix

$$G = \begin{pmatrix} 1\,0\,0\,1\,1\,0\,1\,1\,2 \\ 0\,1\,0\,1\,0\,1\,1\,2\,1 \\ 0\,0\,1\,0\,1\,1\,2\,1\,1 \end{pmatrix}.$$

Each row of G has weight 6 and it is immediate to verify that a linear combination of two of the rows also has weight 6. Any linear combination of the first two rows has at most 3 coordinates in common with the third row, so we can conclude that the minimum weight of a non-zero codeword is 6. By Lemma 4.1, G is the generator matrix of a $[9, 3, 6]_3$ code. ■

We can also define a linear code as the solution of a system of linear equations. A **check matrix** for a linear code C is an $m \times n$ matrix H with entries from $\mathbb{F}_q$, with the property that

$$C = \{u \in \mathbb{F}_q^n \mid uH^t = 0\},$$

where H^t denotes the transpose of the matrix H.

Lemma 4.4 *Let C be a linear code with check matrix* H. *If every set of $d - 1$ columns of* H *are linearly independent, and some set of d columns are linearly dependent, then C has minimum distance d.*

Proof

Let u be a codeword of C and let D be the set of non-zero coordinates of u, so $|D| = \mathrm{wt}(u)$. Let h_i be the i-th column of H. Since H is a check matrix for C,

$$\sum_{i \in D} u_i h_i = 0.$$

Thus, there is a linear combination of $|D|$ columns of H which are linearly dependent. Applying Lemma 4.1 concludes the proof. □

Example 4.5

Let C be the linear code over $\mathbb{F}_q$ defined by the $m \times n$ check matrix H, whose columns are vectors which span distinct one-dimensional subspaces of $\mathbb{F}_q^m$. In other words, the columns of H are vector representatives of distinct points of $\mathrm{PG}(m-1, q)$. Since any two columns are H are linearly independent, Lemma 4.4 implies that C has minimum distance at least 3. By Exercise 2.11, the number of points of $\mathrm{PG}(m-1, q)$ is $(q^m - 1)/(q-1)$, so

$$n \leqslant (q^m - 1)/(q-1).$$

If we take

$$n = (q^m - 1)/(q-1),$$

then C is a code of size q^k with parameters, $d = 3$ and

$$k = (q^m - 1)/(q-1) - m.$$

This code C attains the bound in Theorem 3.9, since

$$|C|(1 + n(q-1)) = q^k(1 + q^m - 1) = q^n.$$

Thus, C is a perfect code. ■

Example 4.5 is called the **Hamming code**. Example 4.2 is the Hamming code with $q = 2$ and $m = 3$. A check matrix for this code is

$$\mathrm{H} = \begin{pmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 1\,1\,0\,1\,0\,1\,0 \\ 1\,0\,1\,1\,0\,0\,1 \end{pmatrix}.$$

One can readily check that $\mathrm{GH}^t = 0$, where G is as in Example 4.2, by verifying that the scalar product of any row of G with any row of H is zero.

Lemma 4.6 *Let* G *be a generator matrix for a* k*-dimensional linear code* C*. An* $m \times n$ *matrix* H *is a check matrix for* C *if and only if* $\mathrm{GH}^t = 0$ *and the rank of* H *is* $n - k$*.*

Proof

Suppose that H is an $m \times n$ check matrix for C. All the rows of G are codewords of C, so if u is a row of G, then $u\mathrm{H}^t = 0$, which implies $\mathrm{GH}^t = 0$. The dimension of the code C is $n - \mathrm{rank(H)}$, which implies that the rank of H is $n - k$.

Suppose that $\mathrm{GH}^t = 0$ and that the rank of H is $n - k$. A codeword u is a linear combination of the rows of G, so $u\mathrm{H}^t = 0$. Hence, the left kernel of H^t contains C. Since the rank of H is $n - k$, the left kernel of H^t has dimension k, so the left kernel of H^t is C. □

Let I_r denote the $r \times r$ identity matrix.
A generator matrix which has the form

$$(\mathrm{I}_k \mid \mathrm{A}),$$

for some $k \times (n - k)$ matrix A, is said to be in **standard form**. The uncoded string v is encoded by vG, whose first k coordinates are precisely the coordinates of v. There are obvious advantages in using a generator matrix in this standard form. Once errors have been corrected, the uncoded string can be recovered from the codeword by simply deleting the last $n - k$ coordinates. Moreover, the following lemma implies that there is a check matrix with a similar simple form.

Lemma 4.7 *Let* C *be the linear code generated by*

$$\mathrm{G} = (\mathrm{I}_k \mid \mathrm{A}),$$

for some $k \times (n - k)$ *matrix* A*. Then the matrix*

$$\mathrm{H} = \left(-\mathrm{A}^t \mid \mathrm{I}_{n-k}\right)$$

is a check matrix for C*.*

Proof

We have to check that the inner product of the i-th row of $\mathrm{G} = (g_{ij})$ with the ℓ-th row of $\mathrm{H} = (h_{\ell j})$ is zero. The entries $g_{ij} = 0$ for $j \leqslant k$ unless $i = j$, in which case $g_{ii} = 1$. The entries $h_{\ell j} = 0$ for $j \geqslant k + 1$ unless $\ell = j - k$, in which case $h_{\ell,\ell+k} = 1$. Hence,

$$\sum_{j=1}^{n} g_{ij}h_{\ell j} = \sum_{j=1}^{k} g_{ij}h_{\ell j} + \sum_{j=k+1}^{n} g_{ij}h_{\ell j} = h_{\ell i} + g_{i,\ell+k} = -a_{i\ell} + a_{i\ell} = 0.$$

□

4.2 Syndrome Decoding

Given a generator matrix G for a linear code C, encoding is fairly simple since we assign the codeword vG to each vector v of $\mathbb{F}_q^k$. Moreover, if the generator matrix is in standard form, as described in the previous section, then we can encode by appending the $n-k$ coordinates of vA to v. Decoding is a far trickier affair. To use nearest neighbour decoding we have to find the codeword of length n which is nearest to the received n-tuple. For a code with no obvious structure, this can only be done by calculating the distance between the received n-tuple and each codeword, something which is laborious and infeasible for large codes. In this section, we consider a decoding algorithm for linear codes which exploits the linearity property.

Let C be a linear code with check matrix H. The **syndrome** of a vector $v \in \mathbb{F}_q^n$ is

$$s(v) = v\mathrm{H}^t.$$

Note that $s(v) = 0$ if and only if $v \in C$, since

$$C = \{v \in \mathbb{F}_q^n \mid vH^t = 0\}.$$

To use **syndrome decoding** we compute a look-up table with entries $s(e)$ for all vectors e of weight at most $t = \lfloor (d-1)/2 \rfloor$. To decode a vector v we compute $s(v)$, use the look-up table to find e such that $s(v) = s(e)$, and decode v as $v - e$. Note that $v - e \in C$ and the distance between v and $v - e$ is at most t.

Example 4.8
The matrix

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

is the generator matrix of a $[8, 4, 4]_3$ code.

Suppose that a codeword u has been sent and we have received the vector

$$v = (1, 0, 1, 0, 0, 1, 0, 2).$$

By Lemma 4.7, the matrix

$$\mathrm{H} = \begin{pmatrix} 0&2&2&2&1&0&0&0 \\ 2&0&2&2&0&1&0&0 \\ 2&2&0&2&0&0&1&0 \\ 2&2&2&0&0&0&0&1 \end{pmatrix}$$

is a check matrix for C.

Note that $-1 = 2$, since we are doing arithmetic with elements of $\mathbb{F}_3$.
To decode using syndrome decoding, we calculate the syndrome of v,

$$s(v) = v\mathrm{H}^t = (2, 2, 2, 0).$$

4

Then we look for the low weight vector e, in this example a vector of weight one, such that $s(v) = s(e)$. If only one error has occurred in the transmission, the syndrome $s(v)$ must be equal to $s(e)$, for some vector e of $\mathbb{F}_q^8$ of weight one. Indeed,

$$s(v) = s((0, 0, 0, 1, 0, 0, 0, 0)).$$

Therefore, we correct v to the codeword

$$v - e = (1, 0, 1, 2, 0, 1, 0, 2),$$

which is $(1, 0, 1, 2)\mathrm{G}$. ■

In general, using a look-up table would involve searching through

$$\sum_{j=1}^{t} \binom{n}{j} (q-1)^j$$

entries, an entry for each non-zero vector of $\mathbb{F}_q^n$ of weight at most t. For n large, this implies that we would have to search through a table with an exponential number of entries, since

$$\binom{n}{\frac{1}{2}\delta n} \sim 2^{h(\frac{1}{2}\delta)n}.$$

This does not imply that there might not be a better method to find the vector e with the property that $s(e) = s(v)$, especially if the linear code has some additional properties we can exploit. However, we will now prove that decoding a linear code using syndrome decoding is an NP problem. Under the assumption that P $\neq$ NP, this implies that there is no polynomial time algorithm that will allow us to decode using syndrome decoding.

Problems in NP are, by definition, decision problems. So what we mean by saying that decoding a linear code using syndrome decoding is an NP problem, is that deciding if we can decode a linear code using syndrome decoding is an NP problem. A decision problem is in P if there exists a polynomial time algorithm which gives a yes/no answer to the problem. A decision problem is in NP, if there exists a polynomial time algorithm which verifies that a "yes" solution to the problem, really is a solution. For example, the Hamiltonian path problem asks if there is a path in a graph which visits all the vertices without repeating any vertex. This is an NP problem since a "yes" solution to the problem is a Hamiltonian path. This solution can be checked in polynomial time by checking that each edge in the path is an edge of the graph.

It is not known if NP is a larger class of problems than P or not. A decision problem D is said to be NP-**complete** if there is a polynomial time algorithm which reduces every problem in NP to D. This implies that if we had a polynomial time algorithm to solve D, then we would have a polynomial time algorithm to solve all problems in NP.

Let T be a subset of $\{1, \ldots, n\}^3$.

A **perfect matching** M is a subset of T of size n,

$$M = \{(a_{j1}, a_{j2}, a_{j3}) \mid j = 1, \ldots, n\} \subseteq T,$$

where for all $i \in \{1, 2, 3\}$,

$$\{a_{ji} \mid j = 1, \ldots, n\} = \{1, \ldots, n\}.$$

Deciding whether T has a perfect matching or not is the **three-dimensional matching problem**. This decision problem is NP-complete.

For example, let T be the set of triples

$$\{(1, 1, 1), (1, 2, 3), (1, 4, 2), (2, 1, 4), (2, 3, 3), (3, 2, 1), (3, 3, 4), (4, 3, 2), (4, 3, 3), (4, 4, 4)\}.$$

The three-dimensional matching problem asks if it is possible to find a subset M of T such that each element of $\{1, 2, 3, 4\}$ appears in each coordinate of an element of M exactly once. In this example the answer is affirmative,

$$M = \{(1, 4, 2), (2, 1, 4), (3, 2, 1), (4, 3, 3)\}.$$

Theorem 4.9

Decoding a linear code using syndrome decoding is NP*-complete.*

Proof

To decode a linear code using syndrome decoding, we have to find a vector e of weight at most t, such that $e\mathrm{H}^t = s$, where $s = s(v)$ and v is the received vector.

We make this a decision problem by asking if there is a vector e of weight at most t such that $e\mathrm{H}^t = s$. We will show that this decision problem is NP-complete by proving that if we had a polynomial time algorithm to solve this decision problem, then we would have a polynomial time algorithm to solve the three-dimensional matching problem.

Let $R_i = \{1, \ldots, n\}$ for $i = 1, 2, 3$. Let T be a subset of $R_1 \times R_2 \times R_3$. Consider the matrix A whose rows are indexed by the triples in T, whose columns are indexed by $R_1 \cup R_2 \cup R_3$, where the $((a_1, a_2, a_3), r_i)$ entry is 1 if $a_i = r_i$ and zero otherwise. Thus, each row has three ones and $3n - 3$ zeros. A perfect matching is given by a vector v of $\{0, 1\}^{|T|}$, necessarily of weight n, such that $v\mathrm{A}$ is equal to the all-one vector j. Therefore, if we have a

polynomial time algorithm which can decide if there is a vector e of weight at most t, such that $eH^t = s$, then we can use this to solve the three-dimensional perfect matching decision problem by asking if there is a vector v of weight n such that $v\mathrm{A} = j$. □

4.3 Dual Code and the MacWilliams Identities

Let C be a k-dimensional linear code over $\mathbb{F}_q$.

The **dual code** of a linear code C is

$$C^{\perp} = \{v \in \mathbb{F}_q^n \mid u \cdot v = u_1 v_1 + \cdots + u_n v_n = 0, \text{ for all } u \in C\}.$$

In other words $C^{\perp}$ is the orthogonal subspace to C, with respect to the standard inner product. The subspace $C^{\perp}$ is the set of solutions of a homogeneous system of linear equations of rank k in n unknowns. Hence, the dual code $C^{\perp}$ is a $(n-k)$-dimensional linear code and length n over $\mathbb{F}_q$.

The following lemma is immediate.

Lemma 4.10 *If* H *is a* $(n-k) \times n$ *check matrix for a* k*-dimensional linear code* C*, then* H *is a generator matrix for* $C^{\perp}$*. Likewise, if* G *is a generator matrix for* C*, then* G *is a check matrix for* $C^{\perp}$*.*

If $C = C^{\perp}$, then we say that C is **self-dual**.

Example 4.11

The extended code of the binary four-dimensional code in Example 4.2 is a self-dual code. It has a generator (and check) matrix

$$\begin{pmatrix} 1\,0\,0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,0\,1\,1 \\ 0\,0\,0\,1\,0\,1\,1\,1 \end{pmatrix}.$$

■

Let A_i denote the number of codewords of weight i of a linear code C of length n.

The **weight enumerator** of C is a polynomial defined as

$$A(X) = \sum_{i=0}^{n} A_i X^i.$$

Let $A^{\perp}(X)$ denote the weight enumerator of the dual code $C^{\perp}$.

There is an important relationship between $A(X)$ and $A^{\perp}(X)$, which implies that one is determined by the other. To be able to prove this relationship, which we shall do in Theorem 4.13, we introduce the trace map and characters.

Let p be the prime such that $q = p^h$. Then the **trace map** from $\mathbb{F}_q$ to $\mathbb{F}_p$ is defined as

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{q/p}.$$

By Lemma 2.6, it is additive, i.e.

$$\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y),$$

and by Lemma 2.4 and Lemma 2.6,

$$\mathrm{Tr}(x)^p = \mathrm{Tr}(x),$$

so, again by Lemma 2.4, $\mathrm{Tr}(x) \in \mathbb{F}_p$.

Observe that if $\mathrm{Tr}(\lambda x) = 0$ for all $\lambda \in \mathbb{F}_q$, then $x = 0$, since as a polynomial (in λ) it has degree q/p. For the same reason, every element of $\mathbb{F}_p$ has exactly q/p pre-images of the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$.

For $u \in \mathbb{F}_q^n$, we define a **character** as a map from $\mathbb{F}_q^n$ to $\mathbb{C}$ by

$$\chi_u(x) = e^{\frac{2\pi i}{p}\mathrm{Tr}(x \cdot u)}.$$

Note that this definition makes sense since $\mathbb{F}_p$ is $\mathbb{Z}/(p\mathbb{Z})$.

Lemma 4.12 *Let C be a linear code over $\mathbb{F}_q$. Then*

$$\sum_{u \in C} \chi_u(x) = \begin{cases} 0 & \text{if } x \notin C^{\perp} \\ |C| & \text{if } x \in C^{\perp} \end{cases}.$$

Proof

If $x \in C^{\perp}$, then $x \cdot u = 0$ for all $u \in C$ which implies $\chi_u(x) = 1$ for all $u \in C$ and we are done.

Suppose $x \notin C^{\perp}$. If $\chi_v(x) = 1$ for all $v \in C$, then $\mathrm{Tr}(v \cdot x) = 0$ for all $v \in C$, so $\mathrm{Tr}(\lambda(v \cdot x)) = 0$ for all $\lambda \in \mathbb{F}_q$ and $v \in C$. This, we observed before, implies $v \cdot x = 0$ for all $v \in C$, so $x \in C^{\perp}$, a contradiction. Thus, there is a $v \in C$ such that $\chi_v(x) \neq 1$. Then,

$$\chi_v(x) \sum_{u \in C} \chi_u(x) = \sum_{u \in C} \chi_{u+v}(x) = \sum_{u \in C} \chi_u(x).$$

which implies

$$\sum_{u \in C} \chi_u(x) = 0.$$

□

The following theorem relates the weight enumerator of a linear code to the weight enumerator of its dual code. It is known as the **MacWilliams identities**.

Theorem 4.13 (MacWilliams)
For a k-dimensional linear code C over $\mathbb{F}_q$ of length n we have

$$q^k A^{\perp}(X) = (1 + (q-1)X)^n A\Big(\frac{1-X}{1+(q-1)X}\Big).$$

Proof
Let $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$.

If $u_i \neq 0$, then

$$\sum_{w_i \in \mathbb{F}_q} \chi_{w_i e_i}(u) = 0,$$

since we sum each p-th root of unity q/p times, and the sum of the p-th roots of unity is zero.

Therefore,

$$\sum_{w_i \in \mathbb{F}_q \setminus \{0\}} \chi_{w_i e_i}(u) = \begin{cases} q-1 & \text{if } u_i = 0 \\ -1 & \text{if } u_i \neq 0 \end{cases}$$

and so

$$\prod_{i=1}^{n} \Big(1 + \sum_{w_i \in \mathbb{F}_q \setminus \{0\}} \chi_{w_i e_i}(u) X\Big) = (1 + (q-1)X)^{n - \mathrm{wt}(u)} (1-X)^{\mathrm{wt}(u)}.$$

Multiplying out the brackets,

$$\prod_{i=1}^{n} \Big(1 + \sum_{w_i \in \mathbb{F}_q \setminus \{0\}} \chi_{w_i e_i}(u) X\Big) = \sum_{w \in \mathbb{F}_q^n} X^{\mathrm{wt}(w)} \prod_{i=1}^{n} \chi_{w_i e_i}(u) = \sum_{w \in \mathbb{F}_q^n} X^{\mathrm{wt}(w)} \chi_u(w).$$

Combining the above two equations,

$$\sum_{w \in \mathbb{F}_q^n} X^{\mathrm{wt}(w)} \chi_u(w) = (1 + (q-1)X)^{n - \mathrm{wt}(u)} (1-X)^{\mathrm{wt}(u)}.$$

Summing over $u \in C$, we have

$$\sum_{u \in C} \sum_{w \in \mathbb{F}_q^n} X^{\mathrm{wt}(w)} \chi_u(w) = (1 + (q-1)X)^n A\Big(\frac{1-X}{1+(q-1)X}\Big),$$

since

$$A(X) = \sum_{u \in C} X^{\mathrm{wt}(u)}.$$

Switching the order of the summations, and applying Lemma 4.12,

$$\sum_{w \in \mathbb{F}_q^n} X^{\mathrm{wt}(w)} \sum_{u \in C} \chi_u(w) = \sum_{w \in C^\perp} X^{\mathrm{wt}(w)} |C| = |C| A^\perp(X).$$

□

Observe that Theorem 4.13 implies that if we know the weights of the codewords of C, then we know the weights of the codewords of $C^\perp$ and in particular the minimum weight of a non-zero codeword and therefore, by Lemma 4.1, the minimum distance of $C^\perp$.

If C is a self-dual code, we can get information about the weights of the codewords of C from Theorem 4.13.

Example 4.14

Let C be a self-dual 4-dimensional binary linear code of length 8, for instance, as in Example 4.11. Then, equating the coefficient of X^j, for $j = 0, \ldots, 8$, in

$$A(X) = 2^{-4}(1 + X)^8 A((1 - X)/(1 + X)),$$

where

$$A(X) = 1 + \sum_{i=1}^{8} a_i X^i,$$

will give a system of nine linear equations and eight unknowns.

This system has the solution

$$A(X) = 1 + 14X^4 + X^8 + \lambda(X^2 - 2X^4 + X^6),$$

for some $\lambda \in \{0, \ldots, 7\}$. Thus, C must contain the all-one vector and if the minimum distance of C is 4, then

$$A(X) = 1 + 14X^4 + X^8.$$

■

We will see an important application of the MacWilliams identities in ▶ Section 4.6 where we will exploit these equations to prove that, under certain hypotheses, we can construct combinatorial designs from a linear code.

4.4 Linear Codes and Sets of Points in Projective Spaces

A linear code C is the row space of a generator matrix G. The multi-set S of columns of G also contains information about the code and its parameters. The length of C is $|S|$, the dimension of C is the length of the vectors in S and, as we shall prove in Lemma 4.15, the weights of the codewords in C can be deduced from the intersection of S with the hyperplanes of $\mathbb{F}_q^k$. Observe that S is a multi-set since columns can be repeated.

Lemma 4.15 *The multi-set S of columns of a generator matrix G of a $[n, k, d]_q$ code C is a multi-set of n vectors of $\mathbb{F}_q^k$ in which every hyperplane of $\mathbb{F}_q^k$ contains at most $n - d$ vectors of S, and some hyperplane of $\mathbb{F}_q^k$ contains exactly $n - d$ vectors of S.*

Proof

There is a bijection between the vectors of $\mathbb{F}_q^k$ and the codewords, given by

$$v \mapsto v\mathrm{G}.$$

For each non-zero vector v of $\mathbb{F}_q^k$, the subspace consisting of the vectors $(x_1, \ldots, x_k) \in \mathbb{F}_q^k$, such that

$$v_1x_1 + \cdots + v_kx_k = 0,$$

is a hyperplane of $\mathbb{F}_q^k$, which we denote by π_v. The non-zero multiplies of v define the same hyperplane, so $\pi_v = \pi_{\lambda v}$, for all non-zero $\lambda \in \mathbb{F}_q$.

We can label the coordinates of vG by the elements of S. The s-coordinate of the codeword vG is the value of the scalar product $v \cdot s$. The scalar product $v \cdot s = 0$ if and only if $s \in \pi_v$. Therefore, the codeword vG has weight w if and only if the hyperplane π_v contains $n - w$ vectors of S. The lemma follows since, by Lemma 4.1, the minimum weight of a non-zero vector of C is equal to the minimum distance. □

Lemma 4.15 is still valid if we replace a vector s of S by a non-zero scalar multiple of s. Thus, we could equivalently state the lemma for a multi-set of points in $\mathrm{PG}(k - 1, q)$, assuming that the vectors in S are non-zero vectors. In the projective space, the hyperplane π_v is a hyperplane of $\mathrm{PG}(k - 1, q)$. The s-coordinate of the codeword vG is zero if and only if the point s is incident with the hyperplane π_v, as we saw in ▶ Section 2.4.

We could also try and construct a multi-set S of points of $\mathrm{PG}(k - 1, q)$ in which we can calculate (or at least bound) the size of the intersections of S with the hyperplanes of $\mathrm{PG}(k-1, q)$. Then Lemma 4.15 implies that we can bound from below the minimum distance of the linear code we obtain from a generator matrix whose columns are vector representatives of the points of S.

Example 4.16

Let $\phi(X) = \phi(X_1, X_2, X_3)$ be an irreducible homogeneous polynomial over $\mathbb{F}_q$ in three variables of degree m. Let S be the set of points of $\mathrm{PG}(2, q)$ which are zeros of this

polynomial. Since ϕ is irreducible, each line of PG$(2, q)$ contains at most m points of S. By Lemma 4.15, the matrix whose columns are a vector representative of the points of S is a $3 \times |S|$ matrix which generates a code with minimum distance at least $n - \deg \phi$. This can give an easy way to make codes with surprisingly good parameters. For example, suppose q is a square and we take the Hermitian curve, defined as the zeros of the polynomial

$$\phi(X) = X_1^{\sqrt{q}+1} + X_2^{\sqrt{q}+1} + X_3^{\sqrt{q}+1}.$$

This curve has $q\sqrt{q}+1$ points and is irreducible. Thus we obtain a $[q\sqrt{q}+1, 3, q\sqrt{q}-\sqrt{q}]_q$ code. ■

We say that two codes are **equivalent** if one can be obtained from the other by a permutation of the coordinates and permutations of the symbols in each coordinate. Note that non-linear codes can be equivalent to linear codes. Indeed, one can obtain a non-linear code (of the same size, length and minimum distance) from a linear code by simply permuting the symbols of $\mathbb{F}_q$ in a fixed coordinate.

We can use S to obtain a model for all codes that are equivalent to a linear code C, this is called the **Alderson–Bruen–Silverman** model. Let S be the multi-set of n points of $\Sigma = \text{PG}(k-1, q)$, obtained from the columns of a generator matrix G of the k-dimensional linear code C of length n. For each point $(s_1 : \ldots : s_k)$ of S, we define a hyperplane π_s of $\Sigma = \text{PG}(k-1, q)$ as the kernel of the linear form

$$\alpha_s(X) = s_1 X_1 + \cdots + s_k X_k.$$

We embed Σ in a PG(k, q) and consider PG$(k, q) \setminus \Sigma$ which, by Exercise 2.12, is isomorphic to AG(k, q). Within PG(k, q), we label each hyperplane $(\neq \Sigma)$ containing π_s with an element of $\mathbb{F}_q$. For each point v of the affine space PG$(k, q) \setminus \Sigma$ we obtain a codeword u of C', a code equivalent to the code C. The coordinates of u are indexed by the elements of S, and the s-coordinate of u is the label given to the unique hyperplane of PG(k, q) spanned by π_s and v. Observe that two codewords u and u' of C' (obtained from the points v and v', respectively) agree in an s-coordinate if and only if $\alpha_s(v) = \alpha_s(v')$. The vectors $v\text{G}$ and $v'\text{G}$ are codewords of C, so agree in at most $n - d$ coordinates, which implies that there are at most $n - d$ elements $s \in S$ such that $\alpha_s(v) = \alpha_s(v')$. Thus, u and u' agree in at most $n - d$ coordinates. Furthermore, there are two codewords which agree in exactly $n - d$ coordinates. Therefore, the code C' is of length n and minimum distance d. It is Exercise 4.10, to prove that the code C' is equivalent to the linear code C. This model is used in Exercise 4.11 to prove that if a linear code has a non-linear extension, then it has a linear extension.

4.5 Griesmer Bound

In ▶ Chapter 3 we proved various bounds involving the length, the minimum distance and the size of a block code. In this section, we shall prove another bound involving these

parameters, the Griesmer bound, which is specifically for linear codes. The Griesmer bound follows almost directly from the following lemma.

Lemma 4.17 *If there is a* $[n, k, d]_q$ *code, then there is a* $[n - d, k - 1, \geqslant \left\lceil \frac{d}{q} \right\rceil]_q$ *code.*

4

Proof

Let S be the multi-set of columns of a generator matrix G of a k-dimensional linear code C of length n and minimum distance d over $\mathbb{F}_q$.

By Lemma 4.15, there is a non-zero vector $v \in \mathbb{F}_q^k$ such that the hyperplane π_v of $\mathbb{F}_q^k$ contains $n - d$ vectors of S. Let S' be this multi-set of $n - d$ vectors. Let G′ be the $k \times (n - d)$ matrix whose columns are the vectors of S'. The matrix G′ generates a linear code C', obtained from G′ by left multiplication by a vector of $\mathbb{F}_q^k$. The matrix G′ is not, strictly speaking, a generator matrix of C', since its rows are not linearly independent. The vector v is in the left nucleus of G′. The code C' is the subspace spanned by the rows of the matrix G′.

We want to prove that C' is a $(k - 1)$-dimensional linear code. The rank of G′ is at most $k - 1$, since $v\mathrm{G}' = 0$. If the rank is less than $k - 1$, then there is another vector $v' \in \mathbb{F}_q^k$, not in the subspace spanned by v, for which $v'\mathrm{G}' = 0$. But then we can find a $\lambda \in \mathbb{F}_q$ such that $(v + \lambda v')\mathrm{G}$ has zeros in more than $n - d$ coordinates, which implies that C has non-zero codewords of weight less than d, which contradicts Lemma 4.1. Hence, C' is a $(k - 1)$-dimensional linear code.

Let d' be the minimum distance of the code C' . By Lemma 4.15, there is a hyperplane π' of π_v which contains $n - d - d'$ vectors of S'. By Exercise 2.12, there are precisely $q + 1$ hyperplanes of $\mathbb{F}_q^k$ containing the co-dimensional two subspace π'. Each one of these hyperplanes contains at most $n - d$ vectors of S and so at most d' vectors of $S \setminus \pi'$. Hence,

$$n \leqslant (q + 1)d' + n - d - d',$$

which gives

$$d' \geqslant \left\lceil \frac{d}{q} \right\rceil.$$

□

Theorem 4.18 (Griesmer bound)
If there is a $[n, k, d]_q$ *code, then*

$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Proof

By induction on k.

For $k = 1$ the bound gives $n \geqslant d$, which is clear.

By Lemma 4.17, there is a $[n - d, k - 1, d']_q$ code, where

$$d' \geqslant \left\lceil \frac{d}{q} \right\rceil.$$

By induction,

$$n - d \geqslant \sum_{i=0}^{k-2} \left\lceil \frac{d'}{q^i} \right\rceil \geqslant \sum_{i=0}^{k-2} \left\lceil \frac{d}{q^{i+1}} \right\rceil = \sum_{i=1}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

□

Example 4.19

Consider the problem of determining the largest ternary code C of length 10 and minimum distance 4. The Plotkin bound from Lemma 3.10 does not apply, since $d + n/r - n$ is negative. The sphere packing bound, Theorem 3.9, implies

$$|C| \leqslant 3^{10}/21.$$

The Griesmer bound tells us that if there is a linear code with these parameters, then

$$10 \geqslant 4 + 2 + k - 2.$$

and so

$$|C| \leqslant 3^6.$$

To construct such a code, according to Lemma 4.15, we need to find a set S of 10 points in PG(5, 3) with the property that any hyperplane is incident with at most 6 points of S. Let G be the 6×10 matrix whose columns are vector representatives of the 10 points of S. The matrix G is the generator matrix of a $[10, 6, 4]_3$ code. Such a matrix G can be found directly, see Exercise 4.14. However, we can construct such a code geometrically in the following way.

Let $C^\perp$ be the linear code over $\mathbb{F}_q$ generated by the $4 \times (q^2+1)$ matrix H, whose columns are the points of an elliptic quadric. For example, we could take the elliptic quadric defined as the zeros of the homogeneous quadratic form

$$X_1X_2 - f(X_3, X_4),$$

where $f(X_3, X_4)$ is an irreducible homogeneous polynomial of degree two. Explicitly the points of the quadric are

$$\{(1, f(x, y), x, y) \mid x, y \in \mathbb{F}_q\} \cup \{(0, 1, 0, 0)\}.$$

As in the real projective space, the elliptic quadric has no more than two points incident with any line. To verify this algebraically, consider the line which is the intersection of the planes defined by $X_1 = a_3X_3 + a_4X_4$ and $X_2 = b_3X_3 + b_4X_4$. The x_3 and x_4 coordinates in the intersection with the quadric satisfy

$$(a_3x_3 + a_4x_4)(b_3x_3 + b_4x_4) - f(x_3, x_4) = 0,$$

which is a homogeneous polynomial equation of degree two in two variables. It is not identically zero, since f is irreducible, so there are at most two (projectively distinct or homogeneous) solutions for (x_3, x_4); the x_1 and x_2 coordinates are then determined by $x_1 = a_3x_3 + a_4x_4$ and $x_2 = b_3x_3 + b_4x_4$. This checks the intersection with q^4 lines, the intersection with the remaining lines can be checked similarly.

Therefore, any three columns of the matrix H are linearly independent, since three linearly dependent columns would imply three collinear points on the elliptic quadric. The elliptic quadric has four co-planar points, so H has four linearly dependent columns. By Lemma 4.4, C has a minimum distance 4 and is therefore a $[q^2 + 1, q^2 - 3, 4]_q$ code. Substituting $q = 3$, we obtain a ternary linear code C meeting the Griesmer bound.

The geometry also allows us to calculate the weight enumerator of $C^\perp$ and hence the weight enumerator of C. Since any three points span a plane which intersects the elliptic quadric in a conic, and a conic contains $q + 1$ points, there are

$$\frac{(q^2 + 1)q^2(q^2 - 1)}{(q + 1)q(q - 1)} = (q^2 + 1)q$$

planes incident with $q + 1$ points of the elliptic quadric and the remaining $q^2 + 1$ planes are incident with exactly one point. This implies that $C^\perp$ has $(q^2 + 1)q(q - 1)$ codewords of weight $q^2 - q$, $(q^2 + 1)(q - 1)$ codewords of weight q^2 and one codeword of weight zero.

For $q = 3$, the weight enumerator of $C^\perp$ is

$$A^\perp(X) = 1 + 60X^6 + 20X^9.$$

The MacWilliams identities, Theorem 4.13, imply that C has weight enumerator,

$$A(X) = 1 + 60X^4 + 144X^5 + 60X^6 + 240X^7 + 180X^8 + 20X^9 + 24X^{10}.$$

Even if we do not restrict ourselves to linear codes, there is no larger code known with these parameters. The best known upper bound is $|C| \leqslant 891$.

■

Example 4.20

Consider the problem of determining if there is a $(16, 256, 6)_2$ code C, that is a binary code of length 16 with minimum distance 6 and size 256. The sphere packing bound, Theorem 3.9, implies

$$|C|(1+16+\binom{16}{2}) \leqslant 2^{16},$$

which is satisfied. The Plotkin bound, Theorem 3.12, does not give a contradiction since

$$|C| \leqslant d2^{n-2d+2} = 384.$$

Now, suppose that the code is linear, so C is a $[16, 8, 6]_2$ code. The Griesmer bound is also satisfied since,

$$n \geqslant 6 + \left\lceil \frac{6}{2} \right\rceil + \left\lceil \frac{6}{4} \right\rceil + \sum_{i=3}^{7} \left\lceil \frac{6}{2^i} \right\rceil = 16.$$

However, Lemma 4.17 implies the existence of a $[10, 7, \geqslant 3]_2$ code. This code is a 1-error correcting binary code of length 10, so the sphere packing bound, Theorem 3.9, implies that

$$(1+10)2^7 \leqslant 2^{10},$$

which is a contradiction. Therefore, there is no $[10, 7, \geqslant 3]_2$ code. Hence, there is no $[16, 8, 6]_2$ code. However, there is a non-linear $(16, 256, 6)_2$ code and we shall construct one both in ▶ Chapter 9 and in ▶ Chapter 10. ■

4.6 Constructing Designs from Linear Codes

A τ-design is a collection $\mathcal{D}$ of κ-subsets of $\{1, \ldots, n\}$ with the property that every τ-subset of $\{1, \ldots, n\}$ is contained in precisely λ subsets of D, for some fixed positive integer λ. If we want to specify the parameters, then we say that D is a τ-(n, κ, λ) design.

Let $u \in \mathbb{F}_q^n$. The **support** of $u = (u_1, \ldots, u_n)$ is a subset of $\{1, \ldots, n\}$ defined as

$$\{i \in \{1, \ldots, n\} \mid u_i \neq 0\}.$$

In this section we shall prove that if the codewords of the dual of a linear code C have few distinct weights, then one can construct τ-designs from the supports of codewords of C of a fixed weight. Before proving the main theorem, we will prove by counting that we can construct a 3-design from the extended Hamming code, Example 4.11.

Example 4.21

In Example 4.14, we calculated the weight distribution for the extended Hamming code in Example 4.11 and deduced that there are 14 codewords of weight 4. Two codewords u and v of weight 4 have at most two 1's in common, since otherwise $u + v$ would be a codeword of weight 2. Therefore, every 3-subset of $\{1, \ldots, 8\}$ is contained in the support of at most one codeword of weight 4. There are $14\binom{4}{3} = 56$ subsets of size 3 of the 14 supports of the 14 codewords of weight 4 and $\binom{8}{3} = 56$ subsets of size 3 of $\{1, \ldots, 8\}$. Hence, each 3-subset is

contained in a unique support of a codeword of weight 4 and we have deduced that the set of these supports is a 3-(8, 4, 1) design. ■

In the following theorem, κ can be any number in the set $\{d, \ldots, n\}$ in the case that $q = 2$, since the condition is vacuous. If $q \neq 2$, then, by Exercise 4.15, the condition is surely satisfied if

$$\kappa \in \{d, \ldots, d-1+\left\lfloor \frac{d-1}{q-2} \right\rfloor\}.$$

In order to simplify the statement of the following theorem, we say that C has a weight w if there is a codeword of C of weight w.

Theorem 4.22

Let C be an $[n, k, d]_q$ code such that $C^\perp$ has at most $d - \tau$ non-zero weights of weight at most $n - \tau$, for some $\tau \leqslant d - 1$. If κ has the property that two codewords of C of weight κ have the same support if and only if they are multiples of each other, then the set of supports of the codewords of C of weight κ is a τ-(n, κ, λ) design, for some λ.

Proof

Let T be a τ-subset of $\{1, \ldots, n\}$. Let $C \setminus T$ be the code obtained from C by deleting the coordinates indicated by the elements of T. If after deleting τ coordinates the codewords u and v are the same, then u and v differ in at most τ coordinates. Since $\tau \leqslant d - 1$, this cannot occur, so deleting the coordinates does not reduce the number of codewords. Hence, $C \setminus T$ is a k-dimensional linear code of length $n - \tau$.

Let $C_T^\perp$ be the subset of codewords of $C^\perp$ which have zeros in all the coordinates indicated by the elements of T. Then $C_T^\perp \setminus T$ is a linear code and

$$C_T^\perp \setminus T \subseteq (C \setminus T)^\perp,$$

since a vector in $C_T^\perp$ is orthogonal to all the vectors of C and has zeros in the coordinates indicated by the elements of T. Furthermore,

$$\dim(C_T^\perp \setminus T) = \dim C_T^\perp$$

since the codewords of $C_T^\perp$ have zeros in the coordinates indexed by T, so deleting these coordinates does not reduce the number of codewords.

Let H be a generator matrix for $C^\perp$. Let L be the set of τ vectors of $\mathbb{F}_q^{n-k}$ which are the columns of H indicated by the elements of T. Then

$$C_T^\perp = \{v\mathrm{H} \mid v \in \mathbb{F}_q^{n-k},\ v \cdot s = 0,\ \text{for all } s \in L\},$$

since $v\mathrm{H}$ is a codeword of $C^{\perp}$ and has zeros in the coordinates indexed by T precisely when $v \cdot s = 0$, for all $s \in L$.

Hence,

$$\dim C_T^{\perp} \geqslant n - k - \tau.$$

Now,

$$\dim(C \setminus T) = k$$

implies

$$\dim(C \setminus T)^{\perp} = n - \tau - k$$

and we just proved that

$$\dim(C_T^{\perp} \setminus T) \geqslant n - \tau - k,$$

so we have that

$$C_T^{\perp} \setminus T = (C \setminus T)^{\perp}.$$

The weight of a codeword of $C_T^{\perp} \setminus T$ is the weight of the corresponding codeword of $C^{\perp}$. By hypothesis, $C^{\perp}$ has at most $d - \tau$ non-zero weights of weight at most $n - \tau$. Since at least τ of the coordinates of a codeword of $C_T^{\perp}$ are zero, $C_T^{\perp}$ has weights at most $n - \tau$. Therefore, $(C \setminus T)^{\perp}$ has at most $d - \tau$ non-zero weights.

Since $C \setminus T$ has minimum distance at least $d - \tau$, Exercise 4.16 implies that the weight enumerator of $C \setminus T$ is determined.

If u is a non-zero codeword, then μu is another codeword with the same support as u, for all non-zero $\mu \in \mathbb{F}_q$. The number $\lambda(q-1)$, of codewords of $C \setminus T$ of weight $\kappa - \tau$, is determined by the weight enumerator of $C \setminus T$. The number λ does not depend on which subset T we choose, only the size of the subset T. By induction on κ, for all τ-subsets T of $\{1, \ldots, n\}$, there are a fixed number of supports of the codewords of weight κ containing T. Therefore, the set of the supports of the codewords of C of weight κ is a τ-(n, κ, λ) design. □

Example 4.23

Consider the $[10, 6, 4]_3$ code from Example 4.19. The dual code $C^{\perp}$ has codewords of weight 0,6 and 9 so, according to Theorem 4.22, the set of supports of the codewords of weight κ is a 3-design, provided that no two codewords of C of weight κ have the same support. By Exercise 4.15, we can be assured of this for $\kappa \in \{4, 5, 6, 7\}$.

To calculate λ, we count in two ways the number of 3-subsets. Each 3-subset of $\{1, \ldots, 10\}$ is contained in λ 3-subsets of the design, so

$$\binom{10}{3}\lambda = \binom{\kappa}{3}\alpha,$$

where α is the number of supports of codewords of C of weight κ. The number of supports of codewords of weight κ is the number of codewords of weight κ divided by $q-1$.

Therefore, from the code C we can construct a 3-$(10, 4, 1)$-design, a 3-$(10, 5, 6)$-design and a 3-$(10, 6, 5)$-design. ■

4

In Example 4.23, we could have constructed the designs directly from the elliptic quadric. For example, the 3-$(10, 4, 1)$ design is obtained by taking subsets of 4 co-planar points and the 3-$(10, 5, 6)$ design is obtained by taking subsets of 5 points, no 4 co-planar. In ▶ Chapter 5 we shall construct codes from polynomial divisors of $X^n - 1$ which will often satisfy the hypothesis of Theorem 4.22 and allow us to construct designs. In many cases, these designs cannot be constructed directly from any geometrical object.

4.7 Comments

The MacWilliams identities from ▶ Chapter 4 appear in MacWilliams' thesis "Combinatorial Problems of Elementary Group Theory", although the standard reference is [50]. The MacWilliams identities lead to a set of constraints on the existence of an $[n, k, d]_q$ code. We have that $A_0 = 1$ and $A_1 = \cdots = A_{d-1} = 0$ and that

$$1 + A_d + \cdots + A_n = q^k.$$

Since

$$A_i^{\perp} \geqslant 0,$$

Theorem 4.13 implies, for a fixed n and q, the linear constraint

$$\sum_{j=0}^{n} A_j K_i(j) \geqslant 0.$$

The coefficients

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

are called the **Krawtchouk polynomials**. Delsarte [21] proved that from the distance distribution between the codewords of an arbitrary code (not necessarily a linear code) one can deduce similar inequalities, called the **linear programming bound**. This can be a powerful tool, not only in ruling out certain parameter sets, but also for the construction of codes, since it can give significant information about the distance distribution.

The Griesmer bound is from [31] and the Hamming code was first considered by Hamming in [34]. The upper bound on the size of the code in Example 4.19 is from [55].

The Alderson–Bruen–Silverman model for codes equivalent to linear codes in ▶ Section 4.4 is from [2]. The fact that a linear code with a non-linear extension has a linear extension, Exercise 4.11, is due to Alderson and Gács, see [1].

Theorem 4.22 is the Assmus–Mattson theorem from [4].

The bound in Exercise 4.3 is due to Varshamov [75] and is known as the linear Gilbert–Varshamov bound.

4.8 Exercises

4.1 *Prove that if C is linear, then the extended code $\overline{C}$ is linear.*

4.2 *Prove that the code in Example 4.2 is a perfect code.*

4.3 *Prove that if*

$$\sum_{j=0}^{d-2} \binom{n-1}{j} (q-1)^j < q^{n-k},$$

then there exists an $[n, k, d]_q$ code.

4.4 *Prove that the system of equations in Example 4.14 has the solution*

$$A(X) = 1 + 14X^4 + X^8 + \lambda(X^2 - 2X^4 + X^6).$$

4.5 *Prove that the code in Example 4.8 has minimum distance 4 and decode the received vector $(0, 1, 1, 0, 2, 2, 2, 0)$ using syndrome decoding.*

4.6 *Prove that the code C in Example 3.4 is linear but not self-dual although for the weight enumerator $A(X)$ of C, we have $A(X) = A^{\perp}(X)$. Prove that C is equivalent to $C^{\perp}$.*

4.7 *Let C be the linear code over $\mathbb{F}_5$ generated by the matrix*

$$\mathrm{G} = \begin{pmatrix} 1\,0\,0\,1\,1\,2 \\ 0\,1\,0\,1\,2\,1 \\ 0\,0\,1\,2\,1\,1 \end{pmatrix}.$$

Calculate the minimum distance of C and decode the received vector $(0, 2, 3, 4, 3, 2)$ using syndrome decoding.

4.8 *Let C be the linear code over $\mathbb{F}_7$ defined by the check matrix*

$$\mathrm{H} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,2\,3\,4\,5\,6 \\ 0\,1\,4\,2\,2\,4\,1 \\ 0\,1\,1\,6\,1\,6\,6 \end{pmatrix}.$$

i. Prove that C is a $[7, 3, 5]_7$ code.
ii. Decode the received vector $(2, 2, 3, 6, 1, 2, 2)$ using syndrome decoding.

4.9 *Let C be the 3-dimensional linear code over $\mathbb{F}_3$ generated by the matrix*

$$\begin{pmatrix} 1\,0\,0\,1\,1\,2\,0\,1\,1 \\ 0\,1\,0\,1\,2\,1\,1\,0\,1 \\ 0\,0\,1\,2\,1\,1\,1\,1\,0 \end{pmatrix}.$$

Prove that C has minimum distance 6 and use syndrome decoding to decode the received vector

$$(1, 2, 0, 2, 0, 2, 0, 0, 0).$$

4.10 *Prove that the code C' obtained from the Alderson–Bruen–Silverman model is equivalent to the linear code C from which the model is set up.*

4.11 *Let S be the set of n vectors obtained from the set of columns of a generator matrix of a linear code C and suppose that C has an extension to a code of length $n + 1$ and minimum distance $d + 1$.*

i. Prove that there is a function

$$f : \mathbb{F}_q^k \to \mathbb{F}_q$$

with the property that if $f(u) = f(v)$, then $u - v$ is orthogonal (with respect to the standard inner product) to less than $n - d$ points of S.

ii. Let T be the set of vectors of $\mathbb{F}_q^k$ which are orthogonal to $n - d$ vectors of S. Let $v \in T$ and let $u_1, \ldots, u_{k-2}$ be a set of $k - 2$ vectors extending v to a set of $k - 1$ linearly independent vectors. Prove that for all $\lambda_1, \ldots, \lambda_{k-2}, \lambda, \mu \in \mathbb{F}_q$, $\lambda \neq \mu$,

$$f(\lambda_1 u_1 + \cdots + \lambda_{k-2} u_{k-2} + \lambda v) \neq f(\lambda_1 u_1 + \cdots + \lambda_{k-2} u_{k-2} + \mu v).$$

iii. Prove that if every hyperplane of $\mathbb{F}_q^k$ contains a vector of T, then every hyperplane of $\mathbb{F}_q^k$ contains q^{k-2} vectors u such that $f(u) = 0$.
iv. Prove that there is a hyperplane of $\mathbb{F}_q^k$ not containing a vector of T.
v. Prove that C has a linear extension. In other words, it can be extended to a $[n+1, k, d+1]_q$ code.

4.12 *Prove that for fixed $r = n - d$, the Griesmer bound implies $n \leqslant (r - k + 2)q + r$.*

4.13 *Let $r = n - d$ and let S be the set of columns of a generator matrix of a 3-dimensional linear code C of length $(r - 1)q + r$, so we have equality in the bound of Exercise 4.12. Prove that S is a set of vectors of $\mathbb{F}_q^k$ in which every hyperplane contains 0 or r vectors of S. Equivalently show that the non-zero codewords of C have weight n or d.*

4.14

i. *Verify that equality in the Griesmer bound occurs for the parameters of the code C in Example 4.19 if and only if $q = 3$.*

ii. *Let G be a 6×10 matrix*

$$\mathrm{G} = \left(\mathrm{I}_6 \middle| \mathrm{A}\right).$$

Let S be the set of rows of the 6×4 matrix A, considered as 6 points of $\mathrm{PG}(3, 3)$. Prove that G is a generator matrix of a $[10, 6, 4]_3$ code if and only if S has the property all points of S have weight at least three (i.e. the points of S have at most one zero coordinate), no two points of S are collinear with a point of weight one and that no three points of S are collinear.

iii. *Find a matrix A so that G is a generator matrix for a $[10, 6, 4]_3$ code.*

4.15 *Let C be a linear code over $\mathbb{F}_q$, where $q \neq 2$.*

i. *Prove that if $w - \lceil w/(q - 1) \rceil < d$, where d is the minimum distance of a linear code C, then two codewords of C of weight w have the same support if and only if they are multiples of each other.*

ii. *Prove that if $w \leqslant (d - 1)(q - 1)/(q - 2)$, then $w - \lceil w/(q - 1) \rceil < d$.*

4.16 *Let C be a linear code of length n and minimum distance d with the property that $C^\perp$ has at most d distinct weights, $w_1, \ldots, w_d$.*

i. *Let A_j denote the number of codewords of C of weight j and let $A_j^\perp$ denote the number of codewords of $C^\perp$ of weight j. Prove that*

$$q^k \sum_{j=0}^{n} A_j^\perp (1-X)^j = (1+(q-1)(1-X))^n + \sum_{j=d}^{n} A_j X^j (1+(q-1)(1-X)^{n-j}).$$

ii. *Prove that the $n + 1$ polynomials $X^{n-r}(1 + (q - 1)(1 - X)^r)$ $(r = 0, \ldots, n - d)$, $(1 - X)^{w_j}$ $(j = 1, \ldots, d)$ are linearly independent.*

iii. *Prove that the weight enumerator of $C^\perp$ is determined.*

iv. *Prove that the weight enumerator of C is determined.*