Chapter 3

Linear Codes

An important class of codes are linear codes in the vector space $F_q^n$, where $F_q$ is a finite field of order $q$.

**Definition 3.1 (Linear code).** A linear code $C$ is a code in $F_q^n$ for which, whenever $x, y \in C$, then $ax + by \in C$ for all $a, b \in F_q$. That is, $C$ is a linear subspace of $F_q^n$.

**Remark.**
1). The zero vector $0$ automatically belongs to all linear codes.
2). A binary code $C$ is linear if and only if it contains $0$ and the sum of any two codewords in $C$ is also in $C$. Since $F_2 = \{0, 1\}$.
3). A linear code $C$ will always be a $k$-dimensional subspace of $F_q^n$ for some integer $k$ with $1 \leq k \leq n$. So it is the set of all linear combinations of $k$ linearly independent codewords, called basis vectors. We say that these $k$ codewords generate or span the entire code space $C$.

**Definition 3.2 ([n, k] code and [n, k, d] code).** We say that a $k$-dimensional linear code in $F_q^n$ is an $[n, k]$ code, or if we also wish to specify the minimum distance $d$, an $[n, k, d]$ code.

**Remark.** Note that a $q$-ary $[n, k, d]$ code is an $(n, q^k, d)$ code and not every $(n, q^k, d)$ code is a $q$-ary $[n, k, d]$ code (it might not be linear).

**Definition 3.3 (Minimum weight).** The minimum weight of a code to be

$$\text{wt}(C) = \min\{\text{wt}(x) \mid x \in C, x \neq 0\}.$$ 

One of the advantages of linear codes is illustrated by the following lemma.

**Lemma 3.4 (Distance of a Linear Code).** If $C$ is a linear code in $F_q^n$, then $d(C) = \text{wt}(C)$. 


Proof. There exist codewords \( x, y, \) and \( z \) in \( C \) with \( x \neq y, \) and \( z \neq 0 \) such that \( d(x, y) = d(C) \) and \( \text{wt}(z) = \text{wt}(C). \) Then

\[
d(C) \leq d(z, 0) = \text{wt}(z - 0) = \text{wt}(z) = \text{wt}(C) \leq \text{wt}(x - y) = d(x, y) = d(C),
\]

since \( x - y \) is also a codeword in \( C, \) so \( \text{wt}(C) = d(C). \)

\[\square\]

Lecture 8, February 3, 2011

Remark. The above lemma implies, for a linear code, that we only have to examine the weights of the \( M - 1 \) nonzero codewords in order to find the minimum distance. In contrast, for a general nonlinear code, we need to make \( \binom{M}{2} = \frac{M(M-1)}{2} \) comparisons (between all possible pairs of distinct codewords) to determine the minimum distance.

Definition 3.5 (Generator matrix). Let \( C \) be a linear \( [n, k] \) code. A generator matrix of \( C \) is a \( k \times n \) matrix such that the rows are basis vectors of \( C. \)

Examples. A \( q \)-ary repetition code of length \( n \)

\[
C = \begin{pmatrix}
0 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & 0 \\
1 & 1 & \cdots & 1 & 1 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{q-1} & a_{q-1} & \cdots & a_{q-1} & a_{q-1}
\end{pmatrix}
\]

where \( F_q = \{0, a_1, a_2, \ldots, a_{q-1}\}. \)

is an \([n, 1, n]\) linear code with generator matrix

\[
[1, 1, \ldots, 1],
\]

Remark. Linear \( q \)-ary codes are not defined unless \( q \) is a power of a prime (this is simply the requirement for the existence of the field \( F_q \)).

Fact (Not present). However, lower-dimensional codes can always be obtained from linear \( q \)-ary codes by projection onto a lower dimensional subspace of \( F_q^n. \) For example, the ISBN code is a subset of the 9-dimensional subspace of \( F_{11}^{10} \) consisting of all vectors perpendicular to the vector \((1, 2, 3, 4, 5, 6, 7, 8, 9, 10); \) this is the space

\[
\left\{ (x_1, x_2, x_3, \ldots, x_{10}) \in F_{11}^{10} \mid \sum_{k=1}^{10} k x_k \equiv 0 \pmod{11} \right\}
\]

However, not all vectors in this set (for example \( X-00-000000-X \)) are in the ISBN code. That is, the ISBN code is not a linear code.
For linear codes we must slightly restrict our definition of equivalence so that the codes remain linear (e.g., in order that the zero vector remains in the code).

**Definition 3.6 (Equivalent).** Two linear $q$-ary codes are equivalent if one can be obtained from the other by a combination of

(A). permutation of the positions of the code;

(B). multiplication of the symbols appearing in a fixed column by a nonzero scalar.

**Theorem 3.1.** Two $k \times n$ generator matrices corresponding to equivalent linear $[n, k]$-code in $F_q^n$ if one matrix can be obtained from the other by a sequence of operations.

(R1). Permutation of the rows;

(R2). Multiplication of a row by a non-zero element in $F_q$;

(R3). Addition of a scalar multiple of one row to another;

(C1). Permutation of the columns;

(C2). Multiplication of any column by a nonzero scalar.

**Proof.** The row operations (R1), (R2) and (R3) preserve the linear independence of the rows of a generator matrix and simply replace one basis by another of the same code. Operations of types (C1) and (C2) convert a generator matrix to one for an equivalent code. \hfill \Box

**Theorem 3.2.** Let $G$ be a generator matrix of an $[n, k]$ linear code. Then by performing operations of types (R1), (R2), (R3), (C1) and (C2), $G$ can be transformed to the standard form

$$ [I_k \mid A],$$

where $I_k$ is the $k \times k$ identity matrix, and $A$ is a $k \times (n - k)$ matrix.

**Proof.** Do what we did in Linear algebra. \hfill \Box

**Remark.** If we transform a generator matrix $G$ of $C$ into a standard form matrix $G'$ as the above theorem by row operations only, then $G'$ is also a generator matrix of $C$. But if operations (C1) and (C2) are also used, then $G'$ will generate a code which is equivalent to $C$. (maybe not the same as $C$)
Example 3.1. We have binary linear $[5, 2, 3]$ code

$$C_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

The possible generator matrix for $C_3$ is

$$G_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$G_2 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

or

$$G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

### 3.1 Encoding and Decoding with a linear code

Let us discuss the encoding and decoding with a linear code. First we have the following definition:

**Definition 3.7.** Let $C$ be a linear code in $F_q^n$. Let $u$ be any vector in $F_q^n$. The set $u + C = \{u + x \mid x \in C\}$ is called a coset of $C$.

**Remark.** If $C$ is a linear code in $F_q^n$, then under the vector addition $C$ is an subgroup of the finite abelian group $F_q^n$. The following results follow by $C$ is a finite subgroup of $F_q^n$.

**Lemma 3.8 (Equivalent Cosets).** Let $C$ be a linear code in $F_q^n$ and $u \in F_q^n$. If $v$ is an element of the coset $u + C$, then $v + C = u + C$.

**Proof.** Since $v \in u + C$, then $v = u + x$ for some $x \in C$. Consider any vector $v + y \in v + C$, with $y \in C$. Then

$$v + y = (u + x) + y = u + (x + y) \in u + C,$$

so $v + C \subseteq u + C$. Furthermore $u = v + (-x) \in v + C$, so the same argument implies $u + C \subseteq v + C$. Hence $v + C = u + C$. □
Theorem 3.3 (Lagrange’s Theorem). Suppose $C$ is an $[n, k]$ code in $F_q^n$. Then

1. every vector of $F_q^n$ is in some coset of $C$;
2. every coset contains exactly $q^k$ vectors;
3. any two cosets are either equivalent or disjoint.

Proof. 1). $u = u + 0 \in u + C$ for every $u \in F_q^n$.

2). Since the mapping $\varphi(x) = u + x$ is one-to-one, so $|u + C| = |C| = q^k$. Here $|C|$ denotes the number of elements in $C$.

3). Let $u, v \in F_q^n$. Suppose that the cosets $u + C$ and $v + C$ have a common vector $w = u + x = v + y$, with $x, y \in C$. Then $v = u + (x - y) \in u + C$, so by above lemma $v + C = u + C$.

Definition 3.9 (Coset leader). The vector having minimum weight in a coset is called the coset leader. (If there is more than one vector with the minimum weight, we choose one at random and call it the coset leader)

Remark. The above theorem shows that $F_q^n$ is partitioned into disjoint cosets of $C$:

$$F_q^n = (0 + C) \cup (u_1 + C) \cup \cdots \cup (u_s + C)$$

where $s = \frac{|F_q^n|}{|C|} - 1 = q^{n-k} - 1$, and, by above lemma we may take $0, u_1, \ldots, u_s$ to be the coset leaders.

Definition 3.10 (Standard array). The standard array (or Slepian) of a linear $[n, k]$ code $C$ in $F_q^n$ is a $q^{n-k} \times q^k$ array listing all the cosets of $F_q^n$ in which the first row consists of the code $C$ with $0$ on the extreme left, and the other rows are the cosets $u_i + C$, each arranged in corresponding order, with the coset leader on the left.

Remark. The standard array may be constructed as follows:

Step 1. List the codewords of $C$, starting with $0$, as the first row.

Step 2. Choose any vector $u_1$, not in the first row, of minimum weight. List the coset $u_1 + C$ as the second row by putting $u_1$ under $0$ and $u_1 + x$ under $x$ for each codeword $x \in C$. 
Step 3. From those vectors not in row 1 and 2, choose $u_2$ of minimum weight and list the coset $u_2 + C$ as in Step 2 to get the third row.

Step 4. Continue in this way until all the cosets are listed and every vector of $F_q^n$ appears exactly once.

Lecture 9, February 8, 2011

Example 3.2. Let us revisit our linear $[5, 2, 3]$ code

$$C_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

with generator matrix

$$G_3 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

The standard array for $C_3$ is a $q^{5-2} \times q^2 = 8 \times 4$ array of cosets listed here in three groups of increasing coset leader weight:

0 0 0 0 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1

0 0 0 1 1 0 1 0 1 1 1 1 1 0 1 1 0 1 0

0 0 1 0 0 0 1 0 0 1 0 1 0 0 1 1 0 0 1

0 0 1 0 0 0 1 0 0 1 0 1 0 0 1 1 1 1 1

0 1 0 0 0 0 1 0 1 1 1 1 1 1 0 1 0 1 1

1 0 0 0 0 1 1 1 0 1 0 0 1 1 0 1 0 1 1

0 0 0 1 1 0 1 1 0 1 0 1 1 0 0 0 0 0 1

0 1 0 1 0 0 0 1 1 1 1 1 1 0 0 1 0 0 0 1

Remark. The last two rows of the standard array for $C_3$ could equally well have been written as

1 1 0 0 0 1 0 1 0 1 0 1 1 1 0 0 0 0 1

1 0 0 0 1 1 1 0 0 0 0 1 1 1 0 1 0 1 0

3.1.1 Encoding with a linear code

Let $C$ be an $[n, k]$ code in $F_q^n$ with generator matrix $G$. We know $C$ contains $q^k$ codewords, corresponding to $q^k$ distinct messages. We identify each message with a $k$-tuple
\( \mathbf{u} = [u_1, u, \ldots, u_k] \), where the components \( u_i \) are elements of \( F_q \). We can encode \( \mathbf{u} \) by multiplying it on the right by \( G \). If the rows of \( G \) are \( \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k \), then

\[
\mathbf{u}G = \sum_{i=1}^{k} u_i \mathbf{x}_i.
\]

This maps \( \mathbf{u} \) to a linear combination of the rows of the generator matrix, i.e., \( \mathbf{u}G \) is indeed a codeword of \( C \). In particular the message with components \( u_i = \delta_{ik} \) gets mapped to the codeword appearing in the \( k \)-th row of \( G \).

**Remark.** The encoding rule is even simpler if \( G \) is in standard form. Suppose \( G = [I_k \mid A] \), where \( A = (a_{ij}) \) is a \( k \times (n - k) \) matrix. Then the message vector \( \mathbf{u} \) is encoded as

\[
\mathbf{x} = \mathbf{u}G = x_1 x_2 \cdots x_k x_{k+1} \cdots x_n,
\]

where \( x_i = u_i \), for \( 1 \leq i \leq k \), are the **message digits** and

\[
x_{k+i} = \sum_{j=1}^{k} a_{ji} u_j, \quad 1 \leq i \leq n - k,
\]

are the **check digits**. The check digits represent redundancy which has been added to the message to give protection against noise.

**Example 3.3.** Let \( C \) be a binary \([7, 4, 3]\) linear code with generator matrix

\[
G = \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{bmatrix}
\]

It is clear that \( C \) is equivalent to the binary \((7, 16, 3)\) perfect code developed in Chapter 1. Given the message \([0, 1, 0, 1]\) (4-tuples), the encoded codeword

\[
[0, 1, 0, 1] \cdot \begin{bmatrix}
1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1
\end{bmatrix} = [0, 1, 0, 1, 1, 0, 0]
\]

is just the sum of the second and fourth rows of \( G \).

For a general linear code, we summarize the encoding part of the communication scheme in the following diagram:
3.1.2 Decoding with a linear code

Definition 3.11 (Error vector). If the codeword \( x \) is sent, but the received vector is \( y \), we define the error vector \( e = y - x \).

The decoder must decide from \( y \) which codeword \( x \) was transmitted, or equivalently which error vector \( e \) has occurred. First, let’s look at a simpler example of standard array:

Example 3.4 (Simpler example). Let \( C \) be the binary \([4, 2]\) code

\[
C = \begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0
\end{pmatrix}
\]

with generator matrix

\[
G_3 = \begin{bmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1
\end{bmatrix}
\]

The standard array for \( C \) is a \( q^{4-2} \times q^2 = 4 \times 4 \) array of cosets listed here in two groups of increasing coset leader weight:

\[
\begin{align*}
0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{align*}
\]

Remark. The third row of the standard array for \( C \) could equally well be written as

\[
0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1
\]

We now describe how the decoder uses the given standard array. When \( y \) is received (e.g., 1111 in the above example), its position in the array is found. Then the decoder decides that the error vector \( e \) is the coset leader (0100) found at the extreme left of \( y \) and \( y \) is decoded as the codeword \( x = y - e(1011) \) at the top of the column containing \( y \).

Briefly, a received vector is decoded as the codeword at the top of its column in the standard array.

The error vector which will be corrected are precisely the coset leaders, irrespective of which codeword is transmitted. By choosing a minimum weight vector in each coset
as coset leader, we ensure that standard array decoding is a nearest neighbour decoding scheme.

**Remark.** 1). In above example, with given array, a single error will be corrected if it occurs in any of the first 3 positions. (a) below but not if it occurs in the 4th position (b) below.

<table>
<thead>
<tr>
<th>Message</th>
<th>Codeword</th>
<th>Noisy Channel</th>
<th>Received vector</th>
<th>Decoded word</th>
<th>Received message</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) 01</td>
<td>0101</td>
<td>0101</td>
<td>0001</td>
<td>0101</td>
<td>01</td>
</tr>
<tr>
<td>(b) 01</td>
<td>0101</td>
<td>0101</td>
<td>0100</td>
<td>0000</td>
<td>00</td>
</tr>
</tbody>
</table>

2). For the standard array of the linear binary [5, 2, 3] code, any single error will be corrected. Since any vector or weight 1 is a coset leader.

**Lecture 10, February 10, 2011**

**Remark.** Let $C$ be a linear code. Then all of the words of weight $t$ could be a coset leader and they are the unique coset leaders in the corresponding cosets if and only if $C$ can correct $t$ errors.

**Proof.** “⇒” Indeed, $x$ is sent and $y$ is received with $t$ errors, i.e., the error vector $e$ has weight $t$. Then $y$ lies in the coset $e+C$ (since $y = x + e \in e+C$), by the assumption and the definition of coset leader we know $e$ is the only possibility of the coset leader of coset $e+C$. So we should decode $y$ as the top codeword of the column containing $y$, i.e., decoding $y$ as $y-e = x$. So $C$ can correct this $t$ errors.

“⇐” We prove this direction by contradiction. First case, assume a word $u$ of weight $t$ could not be a coset leader. Let $v$ be the coset leader of the coset $u+C$ in a standard array of $C$, then we know $\text{wt}(v) < \text{wt}(u) = t$. In particular, $u \neq v$. For a codeword $x$ is sent and $y = u + x$ is received with $t$ errors (since $\text{wt}(u) = t$). Then we should decode $y$ as $y-v = x + (u-v) \neq x$, i.e., this linear code $C$ can not correct $t$ errors. It is a contradiction. Second case, in a coset we have two choices of coset leaders having weight $t$. Assume $u$ is a coset leader having weight $t$ in a given standard array of $C$ and $v$ is another word having weight $t$ in $u+C$, i.e., $v = u + z$ with $0 \neq z \in C$. Suppose codeword $x$ is sent and $y = x + v$ is received. Then we have $y = x+u+z = u+(x+z) \in u+C$, i.e., $y$ is in the coset of $u$ as a coset leader. By the decoding rule of linear code, we should decode $y$ as $y-u = x + z \neq x$. We have the linear code can not correct $t$ errors.

□
3.2 Syndrome Decoding

First we introduce the definition of inner product.

**Definition 3.12 (Inner product and orthogonal).** The inner product $u \cdot v$ of vectors $u, v \in F_q^n$ is the scalar defined by

$$ u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n = \sum_{i=1}^{n} u_i v_i. $$

If $u \cdot v = 0$, then $u$ and $v$ are called **orthogonal**.

**Example 3.5.** In $F_2^4$, we have

$$(1001) \cdot (1101) = 1 + 0 + 0 + 1 = 0, \quad (1111) \cdot (1110) = 1 + 1 + 1 + 0 = 1,$$

in $F_3^4$,

$$(2011) \cdot (1210) = 2 + 0 + 1 + 0 = 0, \quad (1212) \cdot (2121) = 2 + 2 + 2 + 2 = 2.$$ 

The proof of the following lemma is left as a straightforward exercise for the reader.

**Lemma 3.13.** For any $u, v$ and $w$ in $F_q^n$ and $a, b \in F_q$, then we have

1). $u \cdot v = v \cdot u,$

2). $(au + bv) \cdot w = a(u \cdot w) + b(v \cdot w).$

**Definition 3.14 (Dual code).** Let $C$ be a $[n,k]$ linear code in $F_q^n$. The dual code $C^\perp$ of $C$ in $F_q^n$ is the set of all vectors that are orthogonal to every codeword of $C$:

$$ C^\perp = \{ v \in F_q^n \mid v \cdot u = 0 \text{ for all codewords } u \in C \}. $$

By the above lemma, we know $C^\perp$ is a subspace of $F_q^n$, i.e., a linear code. Later, we will show $C^\perp$ is a linear code of dimension $n - k$.

**Lemma 3.15.** Suppose $C$ is an $[n,k]$ code with generator matrix $G$. Then a vector $v \in F_q^n$ belongs to $C^\perp$ if and only if $v$ is orthogonal to every row of $G$; i.e., $v \in C^\perp \iff Gv^t = 0$. That is the dual code $C^\perp$ is just the null space of $G$:

$$ C^\perp = \{ u \in F_q^n \mid Gu^t = 0 \}. $$

Here $v^t$ denotes the transpose of $v$. 
Proof. The only if part is obvious since the rows of $G$ are codewords. For the if part, suppose that the rows of $G$ are $r_1, r_2, \ldots, r_k$ and that $v \cdot r_i = 0$ for each $i$. If $x$ is any codeword of $C$, then $x = \sum_{i=1}^{k} a_i x_i$ for some scalars $a_i \in F_q$ since the rows of $G$ form a basis of $C$. Hence we have

$$v \cdot x = \sum_{i=1}^{k} a_i (v \cdot r_i) = \sum_{i=1}^{k} a_i \cdot 0 = 0.$$ 

Thus $v$ is orthogonal to every codeword of $C$ and so is in $C^\perp$. 

Theorem 3.4. Suppose $C$ is an $[n,k]$ code in $F_q^n$. Then the dual code $C^\perp$ of $C$ is a linear $[n, n-k]$ code.

First proof. From linear algebra, we know that the space spanned by the $k$ linearly independent rows of $G$ is a $k$ dimensional subspace and the null space of $G$, which is just $C^\perp$, is an $n-k$ dimensional subspace. 

Second proof. It is clear that $C^\perp$ is a linear code. It is also clear that if codes $C_1$ and $C_2$ are equivalent, then so also are $C_1^\perp$ and $C_2^\perp$. Hence it is enough to show that $\dim(C^\perp) = n-k$ in the case where $C$ has a standard form generator matrix $G = [I_k \mid A]$ where $A = (a_{ij})$ is a $k \times (n-k)$ matrix. Then

$$C^\perp = \{(v_1, v_2, \ldots, v_n) \in F_q^n \mid v_i + \sum_{j=1}^{n-k} a_{ij} v_{k+j} = 0, \quad i = 1, 2, \ldots, k\}.$$ 

Clearly for each of the $q^{n-k}$ choices of $(v_{k+1}, v_{k+2}, \ldots, v_n)$, there is a unique vector $(v_1, v_2, \ldots, v_n)$ in $C^\perp$. Hence $|C^\perp| = q^{n-k}$ and so $\dim(C^\perp) = n-k$. 

Example 3.6. It is easily checked that

1). if

$$C = \begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1
\end{pmatrix},$$

then $C^\perp = C$. 

Lecture 11, February 15, 2011
2). if 
\[ C = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \] then \( C^\perp = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \).

**Proposition 3.16.** For any \([n, k]\) code \( C \), \( (C^\perp)^\perp = C \).

*Proof.* Clearly \( C \subseteq (C^\perp)^\perp \) since every vector in \( C \) is orthogonal to every vector in \( C^\perp \) by definition. But \( \dim((C^\perp)^\perp) = n - \dim(C^\perp) = n - (n - k) = k \), so we have \( C = (C^\perp)^\perp \). \( \square \)

**Definition 3.17 (Parity-check matrix).** Let \( C \) be an \([n, k]\) linear code. An \((n - k) \times n\) generator matrix \( H \) of \( C^\perp \) is called a parity-check matrix of \( C \).

**Remark.** The parity check matrix of linear \([n, k]\) code is an \((n - k) \times k\) matrix satisfying \( GH^t = 0 \), where \( H^t \) denotes the transpose of \( H \) and \( 0 \) is an all zero matrix. It follows the lemma and theorem that if \( H \) is a parity check matrix of \( C \), then

\[ C = \{v \in F_n^q \mid Hv^t = 0\}. \]

In this way any linear code is completely specified by a parity-check matrix.

In above example, (1)
\[ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \]
is both a generator matrix and a parity-check matrix, while in (2), \([111]\) is a parity-check matrix.

**Theorem 3.5 (Minimum distance).** A linear code has minimum distance \( d \) if and only if \( d \) is the maximum number such that any \( d - 1 \) columns of its parity check matrix are linearly independent.

*Proof.* Let \( C \) be a linear code, then we have \( \text{wt}(C) = d(C) = d \). Suppose \( u \) is a codeword in \( C \) such that \( \text{wt}(u) = d(C) = d \). Since

\[ u \in C \implies Hu^t = 0 \]

and \( u \) has \( d \) nonzero components, we see that some \( d \) columns of \( H \) are linearly dependent. However, any \( d - 1 \) columns of \( H \) must be linearly independent, or else there would exist a nonzero codeword in \( C \) with weight \( d - 1 \). \( \square \)
Remark.  
1). Equivalently, a linear code has minimum distance \(d\) if \(d\) is the smallest number for which some \(d\) columns of its parity-check matrix are linearly dependent.

2). For a linear code with minimum weight 3, Theorem tells us that any two columns of its parity-check matrix must be linearly independent, but that some 3 columns are linearly dependent.

**Definition 3.18 (Syndrome).** Suppose \(H\) is a parity-check matrix of an \([n, k]\) linear code \(C\). Then for any vector \(u \in F_q^n\), the column vector \(Hu^t\) is called the syndrome of \(u\), denoted \(S(u)\).

Remark.  
1). if the rows of \(H\) are \(r_1, r_2, \ldots, r_{n-k}\), then \(S(u) = (u \cdot r_1, u \cdot r_2, \ldots, u \cdot r_{n-k})^t\).

2). \(S(u) = 0 \iff u \in C\).

3). Some authors define the syndrome of \(u\) to be the row vector \(uH^t\) (i.e., the transpose of \(S(u)\) as defined above).

**Lemma 3.19.** Two vectors \(u\) and \(v\) are in the same coset of a linear code \(C\) if and only if they have the same syndrome.

*Proof.* \(u\) and \(v\) are in the same coset \(\iff u - v \in C \iff H(u - v)^t = 0 \iff Hu^t = Hv^t\). \(\square\)

**Corollary 3.20.** There is a one-to-one correspondence between cosets and syndromes.

Remark. In standard array decoding, if \(n\) is small there is no difficulty in locating the received vector \(y\) in the array. But if \(n\) is large, we can save a lot of time by using the syndrome to find out which coset (i.e., which row of the standard array) contains \(y\). This leads to an alternative decoding scheme known as syndrome decoding. When a vector \(y\) is received, one computes the syndrome \(Hy^t\) and compares it to the syndromes of the coset leaders. If the coset leader having the same syndrome is of minimal weight within its coset, it is the error vector for decoding \(y\).

To compute the syndrome for a code, we need only first determine the parity check matrix. The following lemma describes an easy way to construct a parity-check matrix from a standard-form generator matrix.

**Lemma 3.21.** If \(G = [I_k | A]\) is a standard form generator matrix of an \([n, k]\) code \(C\), then a parity-check matrix \(H\) for \(C\) is given by \(H = [-A^t | I_{n-k}]\).
Proof. It is clear that \( H \) has the size required of a parity-check matrix and its rows are linearly independent. Hence it is enough to show that every row of \( H \) is orthogonal to every row of \( G \), i.e., to show \( GH^t = 0 \). Indeed, we have

\[
GH^t = [I_k | A] \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix} = -I_k \cdot A + A \cdot I_{n-k} = -A + A = 0.
\]

\[ \square \]

Example 3.7. Our \((5, 4, 3)\) code \( C_3 \) is

\[
C_3 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1
\end{pmatrix}
\]

The possible generator matrix for \( C_3 \) is

\[
G_3 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [I_2 | A]
\]

of standard form. Then a parity-check matrix \( H_3 \) for \( C_3 \) is

\[
H_3 = [-A^t | I_{5-2}] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}
\]

Remark. The syndrome \( He^t \) of a binary error vector \( e \) is just the sum of those columns of \( H \) for which the corresponding entry in \( e \) is nonzero.

The following theorem makes it particularly easy to correct errors of unit weight. It will play a particularly important role for the Hamming codes discussed in the next chapter.

Theorem 3.6. The syndrome of a vector that has a single error of \( m \) in the \( i \)th position is \( m \) times the \( i \)th column of \( H \).

Proof. Let \( e_i \) be the vector with the value \( m \) in the \( i \)th position and zero in all other positions. If the codeword \( x \) is sent and the vector \( y = x + e_i \) is received, then the syndrome \( Hy^t = Hx^t + He_i^t = 0 + He_i^t = He_i^t \) is just \( m \) times the \( i \)th column of \( H \). \[ \square \]
Example 3.8. For our $(5, 4, 3)$ code, if $y = 10111$ is received, we compute $Hy^t = 001$, which matches the fifth column of $H$. Thus, the fifth digit is in error (assuming that only a single error has occurred), and we decode $y$ to the codeword 10110, just as we deduced earlier using the standard array.

Remark. If the syndrome does not match any of the columns of $H$, we know that more than one error has occurred. We can still determine which coset the syndrome belongs to by comparing the computed syndrome with a table of syndromes of all coset leaders. If the corresponding coset leader has minimal weight within its coset, we are able to correct the error. To decode errors of weight greater than one we will need to construct a syndrome table, but this table, having only $q^{n-k}$ entries, is smaller than the standard array, which has $q^n$ entries.

Lecture 12, February 17, 2011

3.3 Problems

These problems is the problems in Chapter 2 of Professor Bowman’s online lecture notes.

Problem 3.1. Show that the $(7, 16, 3)$ code developed in Chapter 1 is linear.

Problem 3.2. Show that the $(7, 16, 3)$ perfect binary code in Chapter 1 is a $[7, 4, 3]$ linear code (note that $2^4 = 16$) with generator matrix

$$
\begin{bmatrix}
1 \\
1 \times_1 \\
1 \times_2 \\
1 \times_3 \\
\end{bmatrix} =
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1
\end{bmatrix}
$$

Problem 3.3. Show that the generator matrix for the $(7, 16, 3)$ perfect code in Chapter 1 can be written in standard form as

$$
G =
\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1
\end{bmatrix}
$$

Problem 3.4. If a generator for a linear $[n, k]$ code is in standard form, show that the message vector is just the first $k$ bits of the codeword.
Problem 3.5. Show that dual code $C^\perp$ to a linear code $C$ is itself linear.

Problem 3.6. Show that the null space of a matrix is invariant to standard row reduction operations (permutation of rows, multiplication of a row by a non-zero scalar, and addition of one row to another) and that these operations may be used to put a matrix $H$ of full rank into standard form.

Problem 3.7. Using the binary linear code with parity check matrix

\[
H = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}
\]

decode the received vector 1011.

Problem 3.8. Consider the linear $[6, M, d]$ binary code $C$ generated by

\[
G = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}
\]

1). Find a parity check matrix $H$ for $C$.

2). Determine the number of codewords $M$ and minimum distance $d$ of $C$. Justify your answers.

3). How many errors can this code correct?


5). Suppose the vector 011011 is received. Can this vector be decoded, assuming that only one error has occurred? If so, what was the transmitted vector?

6). Suppose the vector 011010 is received. Can this vector be decoded, assuming that only one error has occurred? If so, what was the transmitted vector?

Problem 3.9. 1). Let $C$ be a linear code. If $C = C^\perp$, prove that $n$ is even and $C$ must be an $[n, n/2]$ code.

2). Prove that exactly $2^{n-1}$ vectors in $F_2^n$ have even weight.

3). If $C^\perp$ is the binary repetition code of length $n$, prove that $C$ is a binary code consisting of all even weight vectors. Hint: find a generator matrix for $C^\perp$. 
Problem 3.10. Let \( C \) be the code consisting of all vectors in \( F_q^n \) with checksum 0 mod \( q \). Let \( C' \) be the \( q \)-ary repetition code of length \( n \).

1). Find a generator matrix \( G \) and parity-check matrix \( H \) for \( C \). What are the sizes of these matrices?

2). Find a generator matrix \( G' \) and parity-check matrix \( H' \) for \( C' \).

3). Which of the following statements are correct? Circle all correct statements.
   \[
   \begin{align*}
   &\bullet \ C' \subset C^\perp, \\
   &\bullet \ C' = C^\perp, \\
   &\bullet \ C' \supset C^\perp, \\
   &\bullet \text{Neither } C' \supset C^\perp \text{ nor } C' \subset C^\perp \text{ holds.} \\
   &\bullet \ C' \cap C^\perp = \emptyset.
   \end{align*}
   \]

4). Find \( d(C) \). Justify your answer.

5). Find \( d(C') \). Justify your answer.

6). How many codewords are there in \( C' \)?

7). How many codewords are there in \( C'' \)?

8). Suppose \( q = 2 \) and \( n \) is odd. Use part (7) to prove that \( \sum_{k=0}^{n-1} \binom{n}{k} = 2^{n-1} \).

Problem 3.11. Consider the linear \([7, M, d]\) binary code \( C \) generated by

\[
G = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}
\]

1). Find a parity check matrix \( H \) for \( C \).

2). Determine the number of codewords \( M \) in \( C \). Justify your answer.

3). Find the maximum number \( N \) such that any set of \( N \) columns of \( H \) are linearly independent. Justify your answer.

4). Determine the minimum distance \( d \) of \( C \).

5). How many errors can \( C \) correct?
6). By examining the inner (dot) products of the rows of $G$ with each other, determine which of the following statements are correct (circle all correct statements and explain):

- $C' \subset C^\perp$,
- $C' = C^\perp$,
- $C' \supset C^\perp$,
- Neither $C' \supset C^\perp$ nor $C' \subset C^\perp$ holds.
- $C' \cap C^\perp = \emptyset$.

7). Suppose the vector 110011 is received. Can this vector be decoded, assuming that no more than one error has occurred? If so, what was the transmitted codeword?

8). Suppose the vector 1010100 is received. Can this vector be decoded, assuming that no more than one error has occurred? If so, what was the transmitted codeword?

9). Suppose the vector 1111111 is received. Show that at least 3 errors have occurred. Can this vector be unambiguously decoded by $C$? If so what was the transmitted codeword? If not, and if only 3 errors have occurred, what are the possible codewords that could have been transmitted?

**Problem 3.12.** Consider a single error-correcting ternary code $C$ with parity-check matrix

$$G = \begin{bmatrix}
2 & 1 & 1 & 1 & 0 & 0 \\
1 & 2 & 0 & 0 & 1 & 0 \\
0 & 2 & 2 & 0 & 0 & 1
\end{bmatrix}$$

1). Find a generator matrix $G$ of $C$.

2). Use $G$ to encode the information messages 100, 010, 001, 200, 201, and 221.

3). What is the minimum distance of this code?

4). Decode the received word 122112, if possible. If you can decode it, determine the corresponding message vector.

5).Decode the received word 102201, if possible. If you can decode it, determine the corresponding message vector.