Exercises 5.1

1. Prove that the inverse of a permutation matrix is a permutation matrix.
2. Find a code equivalent to the code of Case (iv)(a) above such that, in the generating matrix of the equivalent code, the first three columns form the identity matrix.
3. Prove that the relation of two codes being equivalent is an equivalence relation.
4. Give a proof of the corollary to Proposition 5.3.
5. Find the permutation matrix which corresponds to
   (i) the permutation $\sigma = (1, 3, 2)$ of the set $\{1, 2, 3\}$.
   (ii) the permutation $\sigma = (1, 3, 2, 5)$ of the set $\{1, 2, 3, 4, 5\}$.
6. Find the permutation of the appropriate set corresponding to these permutation matrices.

(i)

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

(ii)

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

(iii)

$$\mathbf{P} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

(iv)

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

5.2 DUAL CODE OF A LINEAR CODE

Definition 5.3

Let $\mathbf{x} = (x_1 \quad x_2 \quad \cdots \quad x_n)$, $\mathbf{y} = (y_1 \quad y_2 \quad \cdots \quad y_n)$ be two vectors of length n over a field F. Then, by the intersection $\mathbf{x} * \mathbf{y}$ of $\mathbf{x}$ and $\mathbf{y}$, we mean the vector

$$\mathbf{x} * \mathbf{y} = (x_1 y_1 \quad x_2 y_2 \quad \cdots \quad x_n y_n)$$

while by their scalar product $\mathbf{x}\cdot\mathbf{y}$ we mean the element

$$\mathbf{x}\cdot\mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n \text{ of } F$$

Thus

$$\mathbf{x}\cdot\mathbf{y} = \mathbf{x}\mathbf{y}^t = {}^{\mathbf{y}\cdot\mathbf{x}} = \mathbf{y}\mathbf{x}^t$$

For example, if $F = \mathbb{B}$ and

$$\mathbf{x} = (1 \quad 1 \quad 0 \quad 1) \qquad \mathbf{y} = (1 \quad 1 \quad 1 \quad 1)$$
$$\mathbf{z} = (1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1) \qquad \mathbf{t} = (1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1)$$

then

$$\mathbf{x}*\mathbf{y} = (1 \quad 1 \quad 0 \quad 1)$$
$$\mathbf{x}\cdot\mathbf{y} = 1 + 1 + 0 + 1 = 1$$

and

$$\mathbf{z}*\mathbf{t} = (1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1)$$
$$\mathbf{z}\cdot\mathbf{t} = 1 + 0 + 0 + 0 + 0 + 1 = 0$$

Definition 5.4
Two vectors $\mathbf{x}$ and $\mathbf{y}$ of the same length n over F are called **orthogonal** if $\mathbf{x}\cdot\mathbf{y} = 0$ or equivalently

$$\mathbf{x}\mathbf{y}^t = \mathbf{y}\cdot\mathbf{x} = \mathbf{y}\mathbf{x}^t = 0$$

Exercises 5.2

1. For binary vectors $\mathbf{x}$ and $\mathbf{y}$ of the same length, prove that $\mathbf{x}\cdot\mathbf{y} = 0$ iff $\mathrm{wt}(\mathbf{x}*\mathbf{y})$ is even and $\mathbf{x}\cdot\mathbf{y} = 1$ iff $\mathrm{wt}(\mathbf{x}*\mathbf{y})$ is odd.
2. Prove that a ternary vector $\mathbf{x}$ is orthogonal to itself iff its weight is divisible by 3.

We have defined dual of a code $\mathscr{C}$ as the code generated by a parity check matrix of the code $\mathscr{C}$. We now define the dual in a more general way – but finally it amounts to the same thing.

Definition 5.5
If $\mathscr{C}$ is an $[n, k, d]$ linear code over F, its **dual code** or **orthogonal code** $\mathscr{C}^\perp$ is the set of all vectors of length n that are orthogonal to all code words of $\mathscr{C}$, i.e.

$$\mathscr{C}^\perp = \{\mathbf{u} \in \mathbf{V}(n, q) \mid \mathbf{u}\cdot\mathbf{v} = 0 \ \forall \mathbf{v} \in \mathscr{C}\}$$

Examples 5.2

Case (i)
Consider the linear code as in Case (iv)(a) of Examples 5.1. Let $(x_1 \quad x_2 \quad x_3 \quad x_4)$ be a vector orthogonal to all (those vectors isomorphic to) the code words. In particular $(x_1 \quad x_2 \quad x_3 \quad x_4)$ is orthogonal to code words 1100, 0111 and 1010.

Therefore,

$$x_1 + x_2 = 0 = x_2 + x_3 + x_4 = x_1 + x_3$$

These relations then show that

$$x_1 = x_2 = x_3 \quad \text{and} \quad x_4 = 0$$

Therefore

$$\mathscr{C}^{\perp} = \{0000, 1110\}$$

Observe that $\mathscr{C}^{\perp}$ is also a linear code and $\dim \mathscr{C}^{\perp} + \dim \mathscr{C} = 4$.

Case (ii)

Consider the (4, 7) binary Hamming code $\mathscr{C}$:

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

It is a [7, 4, 3] linear code with 1110100, 0111010, 0011101 and 0001011 as a basis. As a consequence of this, it follows that the code words of the (4, 7) Hamming code are in one-to-one correspondence with the code words of the code generated by the matrix

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

A vector $(x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7)$ is orthogonal to $\mathscr{C}$ iff it is orthogonal to the basis vectors. For this, we have

$$x_1 + x_2 + x_3 + x_5 = 0$$

$$x_2 + x_3 + x_4 + x_6 = 0$$

$$x_3 + x_4 + x_5 + x_7 = 0$$

$$x_4 + x_6 + x_7 = 0$$

These imply

$$x_5 = x_1 + x_2 + x_3$$

$$x_7 = x_2 + x_3$$

$$x_4 = x_1 + x_3$$

$$x_6 = x_1 + x_2$$

In matrix form, these equations can be rewritten as

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_7 \end{pmatrix} = 0$$

Thus the generator matrix of the dual code $\mathscr{C}^{\perp}$ is

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

In view of this, it follows that $\mathscr{C}^{\perp}$ is a linear code of dimension 3. All the code words of $\mathscr{C}^{\perp}$ are:

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

Case (iii)

Consider the (4, 7) polynomial code $\mathscr{C}$ generated by the polynomial $1 + X + X^3$. A generator matrix of this code is

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

A word $x = (x_1x_2x_3x_4x_5x_6x_7)$ is orthogonal to every code word in $\mathscr{C}$ iff $\mathbf{G}\mathbf{x}^t = 0$, i.e. iff

$$x_1 + x_2 + x_4 = 0$$

$$x_2 + x_3 + x_5 = 0$$

$$x_3 + x_4 + x_6 = 0$$

$$x_4 + x_5 + x_7 = 0$$

These relations give

$$x_4 = x_1 + x_2$$

$$x_5 = x_2 + x_3$$
$$x_6 = x_1 + x_2 + x_3$$
$$x_7 = x_1 + x_3$$

In matrix notation, it follows that

$$\mathbf{x} = (x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7)$$
$$= (x_1 \quad x_2 \quad x_3) \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Thus the dual code is generated by the matrix

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

and hence is a (3, 7) code. All the code words of this code are:

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

If the dual code were a polynomial code generated by

$$f(X) = 1 + bX + cX^2 + dX^3 + eX^4$$

then it follows from the above that

$$(a_0 + a_1X + a_2X^2)f(X) = a_0 + a_1X + a_2X^2 + (a_0 + a_1)X^3 + (a_1 + a_2)X^4 + (a_0 + a_1 + a_2)X^5 + (a_0 + a_2)X^6 \; \forall a_0, a_1, a_2 \in \mathbb{B}$$

Comparing the coefficients of X, X^2, X^3 gives

$$a_1 + a_0b = a_1$$
$$a_2 + a_1b + a_0c = a_2$$
$$a_0d + a_1c + a_2b = a_0 + a_1$$

for all $a_0, a_1, a_2 \in \mathbb{B}$. These relations then imply that

$$b = c = 0 \quad \text{and} \quad a_0d = a_0 + a_1 \; \forall a_0, a_1$$

But whatever the value of d in $\mathbb{B}$, the relation

$$a_0d = a_0 + a_1 \; \forall a_0, a_1 \in \mathbb{B}$$

is not possible. This proves that the dual code $\mathscr{C}^\perp$ is not a polynomial code. We thus have the following observation: The dual of a polynomial code need not be a polynomial code.

Theorem 5.2
Let $\mathscr{C}$ be a linear $[n, k, d]$ code with generator matrix $\mathbf{G}$ and parity check matrix $\mathbf{H}$. Then $\mathscr{C}^{\perp}$ is a linear $[n, n-k, -]$ code with generator matrix $\mathbf{H}$ and parity check matrix $\mathbf{G}$.

Proof
By definition

$$\mathscr{C}^{\perp} = \{\mathbf{u} \in V(n, q) | \mathbf{u}\mathbf{v}^{t} = 0 \ \forall \mathbf{v} \in \mathscr{C}\}$$

Let $\mathbf{u}, \mathbf{w} \in \mathscr{C}^{\perp}$ and $\alpha, \beta \in \mathrm{GF}(q) = F$. For any $\mathbf{v} \in \mathscr{C}$,

$$\begin{aligned}(\alpha\mathbf{u} + \beta\mathbf{w})\mathbf{v}^{t} &= (\alpha\mathbf{u})\mathbf{v}^{t} + (\beta\mathbf{w})\mathbf{v}^{t} \\ &= \alpha(\mathbf{u}\mathbf{v}^{t}) + \beta(\mathbf{w}\mathbf{v}^{t}) = 0\end{aligned}$$

Therefore $\mathscr{C}^{\perp}$ is a linear code.

Suppose that $\mathbf{G}$ is an $r \times n$ matrix. Then

$$\mathscr{C} = \{\mathbf{a}\mathbf{G} | \mathbf{a} \in V(r, q)\}$$

But the map $\phi: V(r, q) \to \mathscr{C}$ given by

$$\phi(\mathbf{a}) = \mathbf{a}\mathbf{G}, \quad \mathbf{a} \in V(r, q)$$

is a vector space homomorphism which is clearly onto. Let $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_n$ denote the columns of $\mathbf{G}$. We may suppose that the columns $\mathbf{G}_1, \mathbf{G}_2, \ldots, \mathbf{G}_r$ are linearly independent. Then $\mathbf{B} = (\mathbf{G}_1 \quad \mathbf{G}_2 \quad \cdots \quad \mathbf{G}_r)$ is a non-singular square matrix of order r.

Let $\mathbf{a} \in V(r, q)$ such that $\phi(\mathbf{a}) = 0$, i.e. $\mathbf{a}\mathbf{G} = 0$. Then also $\mathbf{a}\mathbf{B} = 0$ which implies that $\mathbf{a} = (\mathbf{a}\mathbf{B})\mathbf{B}^{-1} = 0\mathbf{B}^{-1} = 0$. Hence ϕ is an isomorphism. Therefore

$$k = \dim \mathscr{C} = \dim V(r, q) = r$$

Hence $\mathbf{G}$ is a $k \times n$ matrix.

Let $\mathbf{u} \in \mathscr{C}^{\perp}$. Then

$$\mathbf{v}\mathbf{u}^{t} = 0 \forall \mathbf{v} \in \mathscr{C}$$

i.e.

$$\mathbf{a}(\mathbf{G}\mathbf{u}^{t}) = (\mathbf{a}\mathbf{G})\mathbf{u}^{t} = 0 \forall \mathbf{a} \in V(k, q)$$

This easily implies that $\mathbf{G}\mathbf{u}^{t} = 0$.

Conversely, if $\mathbf{u} \in V(n, q)$ such that $\mathbf{G}\mathbf{u}^{t} = 0$, then

$$(\mathbf{a}\mathbf{G})\mathbf{u}^{t} = 0 \forall \mathbf{a} \in V(k, q)$$

Hence

$$\mathscr{C}^{\perp} = \{\mathbf{u} \in V(n, q) | \mathbf{G}\mathbf{u}^{t} = 0\}$$

which proves that $\mathbf{G}$ is a parity check matrix for $\mathscr{C}^{\perp}$.

Next define a map θ: $V(n,q) \to V(n,q)$ by

$$\theta(\mathbf{x}) = \mathbf{G}\mathbf{x}^t, \quad \mathbf{x} \in V(n,q)$$

θ is clearly a linear transformation. Therefore

$$\text{rank}(\theta) + \text{nullity of } \theta = n - \text{the dimension of } V(n,q)$$

But

$$\text{rank}(\theta) = \text{rank } \mathbf{G} = k$$

Therefore

$$\text{nullity of } \theta = n - k$$

Also, the nullity of θ is the dimension of $\ker\theta$ and $\ker\theta = \mathscr{C}^\perp$. Hence, $\dim \mathscr{C}^\perp = n - k$.

It is clear from the definition of $\mathscr{C}^\perp$ that $\mathscr{C} \subseteq (\mathscr{C}^\perp)^\perp$. Also

$$\dim(\mathscr{C}^\perp)^\perp = n - \dim \mathscr{C}^\perp = n - (n-k) = k = \dim \mathscr{C}$$

Hence $\mathscr{C} = (\mathscr{C}^\perp)^\perp$.

Let $\mathscr{C}'$ be the code generated by $\mathbf{H}$. Every code word in $\mathscr{C}$ is orthogonal to every row of $\mathbf{H}$ and hence is orthogonal to every code word in $\mathscr{C}'$. Therefore $\mathscr{C}' \subseteq \mathscr{C}^\perp$.

The matrix $\mathbf{H}$ being an $(n-k) \times n$ matrix with $n-k$ columns linearly independent, $\mathscr{C}'$ is a vector space of dimension $n-k$. But $\mathscr{C}^\perp$ is already proved to be of dimension $n-k$. Hence $\mathscr{C}' = \mathscr{C}^\perp$ and so $\mathbf{H}$ is a generator matrix of $\mathscr{C}^\perp$.

Remarks 5.1

1. The above reasoning has also proved that $(\mathscr{C}^\perp)^\perp = \mathscr{C}$.
2. We have defined dual only of a linear code. However, we may define the dual of a fixed length code which is not necessarily linear or matrix code: If $\mathscr{C}$ is a code of length n (not necessarily linear) over F, then
$$\mathscr{C}^\perp = \{\mathbf{u} \in V(n,q) \mid \mathbf{u} \cdot \mathbf{v} = 0 \ \forall \mathbf{v} \in \mathscr{C}\}.$$
3. Every code word in $\mathscr{C}^\perp$ when $\mathscr{C}$ is linear is of the form $\mathbf{aH}$, where $\mathbf{a}$ is the vector related to a message sequence of length $n-k$.

Definition 5.6

A linear code $\mathscr{C}$ over F is called **self dual** if $\mathscr{C}^\perp = \mathscr{C}$.

Observe that the length of a self dual code is always even and the weight of every code word of a binary self dual code is also even.

Examples 5.3

Let $\mathscr{C}$ be a binary self dual code of length 4. Then its dimension is clearly 2. The vectors (1 1 0 0) and (1 0 1 0) are linearly independent over $\mathbb{B}$ and so generate a space of dimension 2. But

$$(1\ 1\ 0\ 0)(1\ 0\ 1\ 0)^t \neq 0$$