Before going over to MacWilliams's result, we have a couple of auxiliary results that we need for its proof.

Lemma 5.1
If $\mathscr{C}$ is a binary linear code of length n and $\mathbf{v} \notin \mathscr{C}^{\perp}$, then

$$\sum_{u \in \mathscr{C}} (-1)^{\mathbf{u} \cdot \mathbf{v}} = 0$$

Proof
$\mathbf{v} \notin \mathscr{C}^{\perp}$ implies that there exists at least one $\mathbf{u} \in \mathscr{C}$ such that $\mathbf{u} \cdot \mathbf{v} \neq 0$. Let $\mathbf{u}^1, \mathbf{u}^2, \ldots, \mathbf{u}^r$ be all the elements of $\mathscr{C}$ such that $\mathbf{u}^i \cdot \mathbf{v} = 1$ for $1 \leq i \leq r$ and $\mathbf{w}^1, \mathbf{w}^2, \ldots, \mathbf{w}^s$ be all the elements of $\mathscr{C}$ such that $\mathbf{w}^j \cdot \mathbf{v} = 0$ for $1 \leq j \leq s$. Then $\mathbf{u}^1 + \mathbf{w}^1, \mathbf{u}^1 + \mathbf{w}^2, \ldots, \mathbf{u}^1 + \mathbf{w}^s$ are distinct elements of $\mathscr{C}$ and

$$(\mathbf{u}^1 + \mathbf{w}^j) \cdot \mathbf{v} = 1 \quad \text{for } 1 \leq j \leq s$$

This shows that $s \leq r$.

Again $\mathbf{u}^1 + \mathbf{u}^1, \mathbf{u}^1 + \mathbf{u}^2, \ldots, \mathbf{u}^1 + \mathbf{u}^r$ are distinct elements in $\mathscr{C}$ and

$$(\mathbf{u}^1 + \mathbf{u}^i) \cdot \mathbf{v} = 0 \quad \forall i, 1 \leq i \leq r$$

Hence $r \leq s$ and we then have $r = s$.

Then,

$$\begin{aligned} \sum_{\mathbf{u} \in \mathscr{C}} (-1)^{\mathbf{u} \cdot \mathbf{v}} &= \sum_{i=1}^{r} (-1)^{\mathbf{u}^i \cdot \mathbf{v}} + \sum_{j=1}^{r} (-1)^{\mathbf{w}^j \cdot \mathbf{v}} \\ &= \sum_{i=1}^{r} (-1) + \sum_{j=1}^{r} (-1)^0 \\ &= 0 \end{aligned}$$

Definition 5.9
Let f be a mapping defined on $V(n, q)$–the space of all vectors of length n over F. Suppose that f takes values in a set in which addition and subtraction are defined so that we can add and subtract the values $f(\mathbf{u})$. Then the **Hadamard transform** $\hat{f}$ of f is defined by

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{v} \in V(n,q)} (-1)^{\mathbf{u} \cdot \mathbf{v}} f(\mathbf{v}) \quad \mathbf{u} \in V(n, q)$$

Lemma 5.2
If $\mathscr{C}$ is an $[n, k, -]$ binary linear code, then

$$\sum_{\mathbf{u} \in \mathscr{C}^{\perp}} f(\mathbf{u}) = \frac{1}{|\mathscr{C}|} \sum_{\mathbf{u} \in \mathscr{C}} \hat{f}(\mathbf{u})$$

where $|\mathscr{C}|$ denotes the order of $\mathscr{C}$.

Proof

$$\begin{aligned}\sum_{\mathbf{u}\in\mathscr{C}} \hat{f}(\mathbf{u}) &= \sum_{\mathbf{u}\in\mathscr{C}} \sum_{\mathbf{v}\in V(n,q)} (-1)^{\mathbf{u}\cdot\mathbf{v}} f(\mathbf{v}) \\ &= \sum_{\mathbf{v}\in V(n,q)} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathscr{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} \\ &= \sum_{\mathbf{v}\in\mathscr{C}^{\perp}} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathscr{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} + \sum_{\mathbf{v}\notin\mathscr{C}^{\perp}} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathscr{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} \\ &= \sum_{\mathbf{v}\in\mathscr{C}^{\perp}} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathscr{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} \qquad \text{(by Lemma 5.1)} \\ &= |\mathscr{C}| \sum_{\mathbf{v}\in\mathscr{C}^{\perp}} f(\mathbf{v})\end{aligned}$$

and the result follows.

Theorem 5.3
(MacWilliams's Identity for binary linear codes.) If $\mathscr{C}$ is an $[n, k, -]$ binary linear code with dual code $\mathscr{C}^{\perp}$, then

$$W_{\mathscr{C}^{\perp}}(x, y) = \frac{1}{|\mathscr{C}|} W_{\mathscr{C}}(x + y, x - y)$$

where $|\mathscr{C}| = 2^k$ is the number of code words in $\mathscr{C}$. Equivalently,

$$\sum_{j=0}^{n} A'_j x^{n-j} y^j = \frac{1}{|\mathscr{C}|} \sum_{i=0}^{n} A_i (x + y)^{n-i} (x - y)^i$$

or

$$\sum_{\mathbf{u}\in\mathscr{C}^{\perp}} x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})} = \frac{1}{|\mathscr{C}|} \sum_{\mathbf{u}\in\mathscr{C}} (x + y)^{n-\mathrm{wt}(\mathbf{u})} (x - y)^{\mathrm{wt}(\mathbf{u})}$$

Proof
Define a map $f: V(n, q) \to \mathbb{B}[x, y]$, where $\mathbb{B}[x, y]$ is the polynomial ring in the two commuting variables x and y, by

$$f(\mathbf{u}) = x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})} \quad \mathbf{u} \in V(n, q)$$

Of course, here $q = 2$. Let $\hat{f}$ denote the Hadamard transform of f. Then, we have

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{v}\in V(n,q)} (-1)^{\mathbf{u}\cdot\mathbf{v}} x^{n-\mathrm{wt}(\mathbf{v})} y^{\mathrm{wt}(\mathbf{v})}$$

Let

$$\mathbf{u} = (u_1 \quad u_2 \quad \cdots \quad u_n)$$

and

$$\mathbf{v} = (v_1 \quad v_2 \quad \cdots \quad v_n)$$

Then

$$\begin{aligned}\hat{f}(\mathbf{u}) &= \sum_{\mathbf{v}\in V(n,q)} (-1)^{u_1v_1+\cdots+u_nv_n} \prod_{i=1}^{n} x^{1-v_i}y^{v_i} \\ &= \sum_{v_1=0}^{1}\sum_{v_2=0}^{1} \cdots \sum_{v_n=0}^{1}\prod_{i=1}^{n}(-1)^{u_iv_i}x^{1-v_i}y^{v_i} \\ &= \prod_{i=1}^{n}\sum_{w=0}^{1}(-1)^{u_iw}x^{1-w}y^{w}\end{aligned}$$

If $u_i = 0$, then

$$\sum_{w=0}^{1}(-1)^{u_iw}x^{1-w}y^{w} = x + y$$

while if $u_i = 1$, then

$$\sum_{w=0}^{1}(-1)^{u_iw}x^{1-w}y^{w} = x - y$$

Therefore,

$$\hat{f}(\mathbf{u}) = (x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})}$$

From Lemma 5.2, it follows that

$$\begin{aligned}\sum_{\mathbf{u}\in\mathscr{C}^\perp} f(\mathbf{u}) &= \frac{1}{|\mathscr{C}|}\sum_{\mathbf{u}\in\mathscr{C}}\hat{f}(\mathbf{u}) \\ &= \frac{1}{|\mathscr{C}|}\sum_{\mathbf{u}\in\mathscr{C}}(x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})}\end{aligned}$$

or

$$\sum_{\mathbf{u}\in\mathscr{C}^\perp} x^{n-\mathrm{wt}(\mathbf{u})}y^{\mathrm{wt}(\mathbf{u})} = \frac{1}{|\mathscr{C}|}\sum_{\mathbf{u}\in\mathscr{C}}(x+y)^{n-\mathrm{wt}(\mathbf{u})}(x-y)^{\mathrm{wt}(\mathbf{u})}$$

or

$$W_{\mathscr{C}^\perp}(x,y) = \frac{1}{|\mathscr{C}|}W_{\mathscr{C}}(x+y, x-y)$$

Exercises 5.5

1. Determine the code words of the (4, 7) binary polynomial code generated by $1 + X^2 + X^3$. Also find the weight enumerator of its dual.
2. Determine the code words of the (3, 6) binary polynomial code generated by $1 + X + X^2$. Also find the weight enumerator of its dual.

3. Determine the code words of the (i) (2, 4); (ii) (2, 5) ternary code generated by the polynomial (a) $X^2 + X - 1$; (b) $X^3 + 2X + 1$. Also find their duals. Write down the weight enumerators of the two codes and their duals.
4. Determine the (3, 5) ternary code generated by $X^2 + X - 1$. Also find its dual. Write down the weight enumerators of the code and its dual.
5. Find the weight enumerators of the duals of the codes of Case (iv) in Example 5.1 and question 3 of Exercise 5.3.

We have proved MacWilliams's Identity for binary linear codes. MacWilliams's Identity giving weight enumerator of the dual code $\mathscr{C}^{\perp}$ once the weight enumerator of $\mathscr{C}$ is known is available for linear codes over any finite field of q elements:

Theorem 5.4
If $\mathscr{C}$ is a linear code over a field F of q elements, then

$$W_{\mathscr{C}^{\perp}}(x, y) = \frac{1}{|\mathscr{C}|} W_{\mathscr{C}}(x + (q-1)y, x - y)$$

We do not go into the proof of this theorem.

5.4 NEW CODES OBTAINED FROM GIVEN CODES

Let $\mathscr{C}$ be a linear $[n, k, d]$ code over GF(q) with generator matrix **G** and parity check matrix **H**. There are several ways in which $\mathscr{C}$ can be modified to yield new codes. However, we here discuss only three such modifications.

5.4.1 Extending a code

Let $\hat{\mathscr{C}}$ be the set of words of length $n + 1$ obtained from the words of $\mathscr{C}$ such that the first n symbols form a word in $\mathscr{C}$ and the $(n + 1)$th symbol is the negative of the sum of the first n symbols. Then the sum of all the symbols of any word in $\hat{\mathscr{C}}$ is always zero. Clearly $\hat{\mathscr{C}}$ is again a linear code over GF(q) and is of length $n + 1$. Given a basis $c(1), c(2), \ldots, c(k)$ of $\mathscr{C}$, we extend every word in the basis by adding an overall parity check. The resulting set of words is again linearly independent over GF(q). On the other hand, if

$$c' = c_1 c_2 \cdots c_n c_{n+1} \in \hat{\mathscr{C}}$$

then $c = c_1 c_2 \cdots c_n$ is in $\mathscr{C}$ and so is a linear combination of $c^{(1)}, c^{(2)}, \ldots, c^{(k)}$. Let

$$c = \alpha_1 c^{(1)} + \alpha_2 c^{(2)} + \cdots + \alpha_k c^{(k)} \quad \alpha_i \in \mathrm{GF}(q) \tag{5.3}$$

Then

$$c_i = \alpha_1 c_i^{(1)} + \alpha_2 c_i^{(2)} + \cdots + \alpha_k c_i^{(k)} \quad 1 \leq i \leq n$$

Therefore

$$\sum_{i=1}^{n} c_i = \alpha_1 \sum_{i=1}^{n} c_i^{(1)} + \alpha_2 \sum_{i=1}^{n} c_i^{(2)} + \cdots + \alpha_k \sum_{i=1}^{n} c_i^{(k)}$$
$$= -\alpha_1 c_{n+1}^{(1)} - \alpha_2 c_{n+1}^{(2)} - \cdots - \alpha_k c_{n+1}^{(k)}$$

or

$$c_{n+1} = \alpha_1 c_{n+1}^{(1)} + \alpha_2 c_{n+2}^{(2)} + \cdots + \alpha_k c_{n+1}^{(k)} \tag{5.4}$$

Equations (5.3) and (5.4) together show that c' is a linear combination of the words obtained from $c^{(1)}, \ldots, c^{(k)}$ by adding an overall parity check. This proves that $\hat{\mathscr{C}}$ is of dimension k. It is clear that the minimum distance $\hat{d}$ of the code $\hat{\mathscr{C}}$ is d or $d+1$.

If $\mathscr{C}$ is a binary linear code, observe that the weight of every non-zero code word in $\hat{\mathscr{C}}$ is even. Moreover, if d is odd, then $\hat{d} = d+1$. However, in the non-binary case $\hat{d}$ may be d again.

For example, let $\mathscr{C}$ be the linear code over GF(3) generated by the matrix

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

The code words of $\mathscr{C}(\hat{\mathscr{C}})$ are:

Message words		Code words of $\mathscr{C}$				Code words of $\hat{\mathscr{C}}$				
0	0	0	0	0	0	0	0	0	0	0
1	0	1	−1	0	1	1	−1	0	1	−1
−1	0	−1	1	0	−1	−1	1	0	−1	1
0	1	0	1	−1	1	0	1	−1	1	−1
1	1	1	0	−1	−1	1	0	−1	−1	1
−1	1	−1	−1	−1	0	−1	−1	−1	0	0
0	−1	0	−1	1	−1	0	−1	1	−1	1
1	−1	1	1	1	0	1	1	1	0	0
−1	−1	−1	0	1	1	−1	0	1	1	−1

Thus $d = 3 = \hat{d}$.

Let $b = b_1 b_2 \cdots b_n$ be a code word in $\mathscr{C}$ and $c = c_1 \cdots c_n c_{n+1}$ be the corresponding code word in $\hat{\mathscr{C}}$. Then $c_1 + c_2 + \cdots + c_{n+1} = 0$ and, therefore, parity check matrix $\hat{\mathbf{H}}$ of $\hat{\mathscr{C}}$ must contain an all one word of length $n+1$. It is then clear that

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

which is an $(n-k+1) \times (n+1)$ matrix.

Definition 5.10
The above process of obtaining the code $\hat{\mathscr{C}}$ from the given code $\mathscr{C}$ is called **extending a code** and also $\hat{\mathscr{C}}$ is called the **extended code of** $\mathscr{C}$.

Example 5.5
The (4, 7) binary Hamming code has a parity check matrix

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

and, therefore, a parity check matrix of extended Hamming code is

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

The code words of the extended Hamming code are:

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

Exercise 5.6
Find the extended code $\hat{\mathscr{C}}$ by adding an overall parity check where $\mathscr{C}$ is the code generated by

(a) $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ over $\mathbb{B}$

(b) $\begin{pmatrix} 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix}$ over GF(3)

5.4.2 Expurgating a code

Let $\mathscr{C}$ be a binary linear code of length n having code words of both even and odd weights. Then it is easy to see that exactly half the code words in $\mathscr{C}$ are of even weight and the other half are of odd weight. This follows from the observation that sum of two words both of odd weight or both of even weight is of even weight while the sum of two words one of which is of odd weight and

the other of even weight is always of odd weight. Also it follows from this that $\mathscr{C}'$ the set of all even weight words is a subspace of $\mathscr{C}$ of dimension $k-1$ if $\mathscr{C}$ is of dimension k. The process of omitting code words is called **expurgation** or expurgating a code. The minimum distance d' of $\mathscr{C}'$ is always at least d while if d is odd strict inequality holds: $d' > d$.

Example 5.6

The $[7, 4, 3]$ binary Hamming code has code words of odd as well as even weights. Expurgating this code by throwing away odd weight code words gives a $[7, 3, 4]$ code. As Hamming code has minimum distance 3, the expurgated code has minimum distance 4.

Expurgation of codes is not available just for binary codes but may be defined for non-binary codes as well. If $\mathscr{C}$ is a linear $[n, k, d]$ code over GF(q) with parity check matrix $\mathbf{H}$, we may expurgate $\mathscr{C}$ by changing $\mathbf{H}$ to $\mathbf{H}_1$ by adding a row of all ones. If the row of all ones is linearly dependent on the rows of $\mathbf{H}$, then no code words are thrown away in this process. However, if the all ones row is linearly independent of the rows of $\mathbf{H}$, then precisely those code words of $\mathscr{C}$ will belong to the expurgated code $\mathscr{C}'$ the sum of all the entries of which is zero.

Exercises 5.7

1. Obtain the expurgated codes of the codes of Case (iv) of Examples 5.1 and Case (iii) of Examples 5.2 and also of their duals. Find also their extended codes.
2. Obtain the extended and the expurgated codes of the ternary self dual code of length 4 generated by 1201 and 1012.

5.4.3 Augmenting a code by adding new code words

The reverse process of expurgating is called **augmenting** a code. While by adding a row of all ones to parity check matrix removed certain words from $\mathscr{C}$, adding a row of all ones to the generator matrix $\mathbf{G}$ of $\mathscr{C}$ may result in adding new code words. If the row of all ones is a linear combination of the rows of $\mathbf{G}$, the augmented code of $\mathscr{C}$ is $\mathscr{C}$ itself. However, if the row of all ones is not a linear combination of the rows of $\mathbf{G}$, then the augmented code is the linear space generated by $\mathscr{C}$ and the all ones word. In this case, dimension of the augmented code becomes $k+1$ when k is the dimension of $\mathscr{C}$.

Exercises 5.8

1. What effect the addition of row of all ones to the parity check matrix of the $[7, 4, 3]$ binary Hamming code have on the given code $\mathscr{C}$?
2. Obtain the augmented codes of the codes of Case (iv) of Examples 5.1, and Case (iii) of Examples 5.2 and their duals.