Definition 0.1. If C is a linear $[n,k]$-code, its ***weight enumerator*** is defined to be the polynomial

$$\begin{aligned} W_C(z) &= \sum_{i=0}^{n} A_i z^i \\ &= A_0 + A_1 z + \cdots + A_n z^n, \end{aligned}$$

or simply,

$$W_C(z) = \sum_{\mathbf{x} \in C} z^{w(\mathbf{x})}.$$

Example: Let $C = \{000, 011, 101, 110\}$. Its dual code $C^{\perp}$ is $\{000, 111\}$. The weight enumerators of C and $C_{\perp}$ are

$$W_C(z) = 1 + 3z^2, \qquad W_{C^{\perp}}(z) = 1 + z^3$$

The motto behind finding weight enumerator of a code is that it enables us find the probabilty of undetected errors when the code is purely used for error-detection.
Also, the objective of this section will be to find weight enumerator of any binary linear code C to be obtained from the weight enumerator of its dual code $C^{\perp}$, as the enumerator of the latter is much easier to find in cases when n, k are both large, while $n - k$ is relatively small.
In order to reach this result, we will need the following lemmas.

Lemma 0.2. Let C be a binary linear $[n,k]$-code and $\mathbf{y}$ is a fixed vector in $V(n,2)$ and $\mathbf{y} \notin C^{\perp}$. Then $\mathbf{x} \cdot \mathbf{y}$ is equal to 0 and 1 equally often as $\mathbf{x}$ runs over the codewords of C.

Proof. Let $A = \{\mathbf{x} \in C | \mathbf{xy} = 0\}$ and $B = \{\mathbf{x} \in C | \mathbf{xy} = 1\}$.
There exists $\mathbf{u} \in C$ such that $\mathbf{u} \cdot \mathbf{y} = 1$ as $\mathbf{y} \notin C^{\perp}$. Let $\mathbf{u} + A$ denote the set $\{\mathbf{u} + \mathbf{x} | \mathbf{x} \in A\}$. Then it follows that

$$\mathbf{u} + A \subseteq B,$$

Similarly,

$$\mathbf{u} + B \subseteq A.$$

Hence,

$$|A| = |\mathbf{u} + A| \leq |B| = |\mathbf{u} + B| \leq |A|.$$

□

Lemma 0.3. Let C be a binary $[n,k]$-code and let $\mathbf{y}$ be any element of $V(n,2)$. Then

$$\sum_{\mathbf{x} \in C} (-1)^{\mathbf{x} \cdot \mathbf{y}} = \begin{cases} 2^k & \text{if } \mathbf{y} \in C^{\perp} \\ 0 & \text{if } \mathbf{y} \notin C^{\perp} \end{cases}.$$

Proof. If $\mathbf{y} \in C^{\perp}$, then $\mathbf{x} \cdot \mathbf{y} = 0$ for all $\mathbf{x} \in C$, so the result follows.
On the other hand, if $\mathbf{y} \notin C^{\perp}$, then by Lemma 0.2, $(-1)^{\mathbf{x} \cdot \mathbf{y}}$ is equal to 1 and -1 equally often. □

Lemma 0.4. Let $\mathbf{x}$ be a fixed vector in $V(n,2)$ and z be an indeterminate. Then the following polynomial identity holds:

$$\sum_{\mathbf{y} \in V(n,2)} z^{w(\mathbf{y})} (-1)^{\mathbf{x} \cdot \mathbf{y}} = (1 - z)^{w(\mathbf{x})} (1 + z)^{n - w(\mathbf{x})}.$$

Proof.

$$\begin{aligned} \sum_{\mathbf{y} \in V(n,2)} z^{w(\mathbf{y})} (-1)^{\mathbf{x} \cdot \mathbf{y}} &= \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} \left(\prod_{i=1}^{n} z^{y_i} (-1)^{x_i y_i} \right) \\ &= \prod_{i=1}^{n} \left(\sum_{j=0}^{1} z^j (-1)^{j x_i} \right) \\ &= (1 - z)^{w(\mathbf{x})} (1 + z)^{n - w(\mathbf{x})}, \end{aligned}$$

since, $$\sum_{j=0}^{1} z^j(-1)^{jx_i} = \begin{cases} 1+z & \text{if } x_i = 0 \\ 1-z & \text{if } x_i = 1 \end{cases}.$$ □

Theorem 0.5 (**MacWilliams identity**). If C is a binary $[n,k]$-code with dual code $C^\perp$, then

$$W_{C^\perp}(z) = \frac{1}{2^k}(1+z)^n W_C\left(\frac{1-z}{1+z}\right).$$

Proof. We will express

$$f(z) = \sum_{\mathbf{x}\in C}\left(\sum_{\mathbf{y}\in V(n,2)} z^{w(\mathbf{y})}(-1)^{\mathbf{x}\cdot\mathbf{y}}\right)$$

in two ways.
Firstly, by Lemma 0.4,

$$\begin{aligned} f(z) &= \sum_{\mathbf{x}\in C}(1-z)^{w(\mathbf{x})}(1+z)^{(n-w(\mathbf{x}))} \\ &= (1+z)^n \sum_{\mathbf{x}\in C}\left(\frac{1-z}{1+z}\right)^{w(\mathbf{x})} \\ &= (1+z)^n W_C\left(\frac{1-z}{1+z}\right) \end{aligned}$$

Secondly, reversing the order of summation gives

$$\begin{aligned} f(z) &= \sum_{\mathbf{y}\in V(n,2)} z^{w(\mathbf{y})}\left(\sum_{\mathbf{x}\in C}(-1)^{\mathbf{x}\cdot\mathbf{y}}\right) \\ &= \sum_{\mathbf{y}\in C^\perp} z^{w(\mathbf{y})}2^k && \text{(by Lemma 0.3)} \\ &= 2^k W_{C^\perp}(z) \end{aligned}$$

Equating these two results gives the expression in theorem. □

More useful form of Theorem 0.5 is when the C and the $C^\perp$ are interchanged, (corresponding change in k also).

Example: If we have $C = \{000, 011, 101, 110\}$ and $C^\perp = \{000, 111\}$ as in earlier example, we have $W_{C^\perp}(z) = 1 + z^3$.
By theorem 0.5, we get

$$\begin{aligned} W_C = \frac{1}{2}(1+z)^3 W_{C^\perp}\left(\frac{1-z}{1+z}\right) &= \frac{1}{2}[(1+z)^3 + (1-z)^3] \\ &= 1 + 3z^2, \end{aligned}$$

The idea of finding W_C with the help of $W_{C^\perp}$ using Theorem 0.5 works really well in the case of binary Hamming code $\mathrm{Ham}(r,2)$ because hamming codes have large number of codewords even for small values of r, so directly calculating W_C is not feasible. Now, we will see why finding $W_{C^\perp}$ first is much more easier in this case.

Theorem 0.6. Let C be the binary Hamming code $\mathrm{Ham}(r,2)$. Then every non-zero codeword of $C^\perp$ has weight 2^{r-1}.

Proof. Let

$$H = \begin{bmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \vdots \\ \mathbf{h}_2 \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{r1} & h_{r2} & \cdots & h_{rn} \end{bmatrix}$$

be the parity-check matrix of C where $\mathbf{h}_i$ are the rows. Let a non-zero codeword $\mathbf{c} = \sum_{i=1}^{r} \lambda_i \mathbf{h}_i$ of $C^{\perp}$. Since C is a Hamming code, columns of H are precisely the non-zero vectors of $V(r,2)$, so number of zero coordinates ($n_0(\mathbf{c})$) are equal to non-zero elements of the set

$$X = \left\{ x_1 x_2 \cdots x_r \in V(r,2) \;\middle|\; \sum_{i=1} r\lambda_i x_i = 0 \right\}$$

i.e. $n_0(\mathbf{c}) = |X| - 1$. Now X is a $r-1$-dimensional subspace of $V(r,2)$ (we can view it as a dual code of a code of 1-dimension).
So, $n_0(\mathbf{c}) = 2^{r-1} - 1$, which is independent of $\mathbf{c}$. Therfore,

$$\begin{aligned} w(\mathbf{c}) = n - n_0(\mathbf{c}) &= 2^r - 1 - (2^{r-1} - 1) \\ &= 2^{r-1} \end{aligned}$$

□

The combined result of theorems 0.5 and 0.6 gives the weight enumerator of binary Ham$(r,2)$, of length $n = 2^r - 1$, as

$$\frac{1}{2^r}[(1+z)^n + n(1-z^2)^{(n-1)/2}(1-z)].$$

Also, the probability of undetected errors in a binary $[n,k]$-code C given by Theorem **??**, becomes

$$P_{\text{undetec}}(C) = (1-p)^n \left[W_C\left(\frac{p}{1-p}\right) - 1 \right]$$

or by using Theorem 0.5

$$P_{\text{undetec}}(C) = \frac{1}{2^{n-k}}[W_{C^{\perp}}(1-2p) - (1-p)^n].$$