ECE 6606 - Coding Theory and Applications

MacWilliams Identity

The MacWilliams identity relates the weight enumerator $A(z)$ of a linear code to the weight enumerator $B(z)$ of it dual code. We restrict our attention to binary linear code, although everything generalizes easily to non-binary linear codes.

Theorem 1. *Let $\mathcal{C}$ be a (n,k) binary linear block code over $GF(2)$ with weight enumerator $A(z)$ and let $B(z)$ be the weight enumerator of $\mathcal{C}^\perp$. Then,*

$$B(z) = 2^{-k}(1+z)^n A\left(\frac{1-z}{1+z}\right),$$

or equivalently

$$A(z) = 2^{-(n-k)}(1+z)^n B\left(\frac{1-z}{1+z}\right).$$

The proof of this result relies on a property of the *Hadamard transform.* For a a function f defined on GF(2), the Hadamard transform of $\hat{f}$ of f is

$$\hat{f}(\mathbf{u}) \triangleq \sum_{\mathbf{v}\in \mathrm{GF}(2)^n} (-1)^{\mathbf{u}\cdot\mathbf{v}} f(\mathbf{v}),$$

where $\mathbf{u}\cdot\mathbf{v}$ is the scalar product of $\mathbf{u}$ and $\mathbf{v}$.

Lemma 1. *Let $\mathcal{C}$ be a k-dimensional subspace of $GF(2)^n$ and let f be a function defined on $GF(2)^n$. Then,*

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

where $|\mathcal{C}|$ denotes the number of elements in $\mathcal{C}$.

Proof. We expand $\sum_{\mathbf{u}\in\mathcal{C}} \hat{f}(\mathbf{u})$ as follows.

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathcal{C}} \hat{f}(\mathbf{u}) &= \sum_{\mathbf{u}\in\mathcal{C}} \sum_{\mathbf{v}\in \mathrm{GF}(2)^n} (-1)^{\mathbf{u}\cdot\mathbf{v}} f(\mathbf{v}) \\
&= \sum_{\mathbf{v}\in \mathrm{GF}(2)^n} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathcal{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} \\
&= \sum_{\mathbf{v}\in\mathcal{C}^\perp} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathcal{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} + \sum_{\mathbf{v}\notin\mathcal{C}^\perp} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathcal{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}}
\end{aligned}$$

If $\mathbf{v}\in\mathcal{C}^\perp$ and $\mathbf{u}\in\mathcal{C}$ then $\mathbf{u}\cdot\mathbf{v} = 0$. Hence,

$$\sum_{\mathbf{v}\in\mathcal{C}^\perp} f(\mathbf{v}) \sum_{\mathbf{u}\in\mathcal{C}} (-1)^{\mathbf{u}\cdot\mathbf{v}} = |\mathcal{C}| \sum_{\mathbf{v}\in\mathcal{C}^\perp} f(\mathbf{v})$$

If $\mathbf{v} \notin \mathcal{C}^\perp$ and $\mathbf{u}$ spans $\mathcal{C}$, we can show that $\mathbf{u} \cdot \mathbf{v}$ takes values zero and one the same number of times. Define the set $\mathcal{S}(\mathbf{v}) \triangleq \{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 0\}$, which forms a subgroup of $\mathcal{C}$. Now, let $\mathbf{u}^* \in \mathcal{C}$ be such that $\mathbf{u} \cdot \mathbf{v} = 1$. The set $\mathbf{u}^* + \mathcal{S}(\mathbf{v})$ is a coset of $\mathcal{S}(\mathbf{v})$ in $\mathcal{C}$, and by Lagrange's theorem $|\mathcal{S}(\mathbf{v})| = |\mathbf{u}^* + \mathcal{S}(\mathbf{v})|$. For any $\mathbf{w} \in \mathbf{u}^* + \mathcal{S}(\mathbf{v})$, $\mathbf{w} \cdot \mathbf{v} = 1$, hence $\mathbf{u}^* + \mathcal{S}(\mathbf{v}) \subset \{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 1\}$. Conversely, if $\mathbf{w} \in \{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 1\}$, we can write

$$\mathbf{w} = \mathbf{u}^* + \underbrace{\mathbf{u}^* + \mathbf{w}}_{\in \mathcal{S}(\mathbf{v})} \quad \in \mathbf{u}^* + \mathcal{S}(\mathbf{v}).$$

Therefore, $\{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 1\} \subset \mathbf{u}^* + \mathcal{S}(\mathbf{v})$ and

$$|\{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 1\}| = |\{\mathbf{u} \in \mathcal{C} : \mathbf{u} \cdot \mathbf{v} = 0\}|.$$

Consequently,

$$\sum_{\mathbf{v} \notin \mathcal{C}^\perp} f(\mathbf{v}) \sum_{\mathbf{u} \in \mathcal{C}} (-1)^{\mathbf{u} \cdot \mathbf{v}} = 0.$$

□

Going back to the proof of the main theorem, notice that we can write $A(z)$ as

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

Define $f(\mathbf{u}) \triangleq z^{\mathrm{wt}(\mathbf{u})}$, whose Hadamard transform is

$$\begin{aligned}
\hat{f}(\mathbf{u}) &= \sum_{\mathbf{v} \in \mathrm{GF}(2)} (-1)^{\mathbf{u} \cdot \mathbf{v}} z^{\mathrm{wt}(\mathbf{v})} \\
&= \sum_{\mathbf{v} \in \mathrm{GF}(2)} (-1)^{\sum_{i=0}^{n-1} u_i v_i} \prod_{i=0}^{n-1} z^{v_i} \\
&= \sum_{\mathbf{v} \in \mathrm{GF}(2)} \prod_{i=0}^{n-1} (-1)^{u_i v_i} z^{v_i} \\
&= \sum_{v_0 \in \{0,1\}} \sum_{v_1 \in \{0,1\}} \cdots \sum_{v_{n-1} \in \{0,1\}} \prod_{i=0}^{n-1} (-1)^{u_i v_i} z^{v_i} \\
&= \prod_{i=0}^{n-1} \sum_{v_i \in \{0,1\}} (-1)^{u_i v_i} z^{v_i}
\end{aligned}$$

If $u_i = 0$ then $\sum_{v_i \in \{0,1\}} (-1)^{u_i v_i} z^{v_i} = 1 + z$, else $\sum_{v_i \in \{0,1\}} (-1)^{u_i v_i} z^{v_i} = 1 - z$. Therefore,

$$\hat{f}(u) = (1+z)^{n - \mathrm{wt}(\mathbf{u})} (1-z)^{\mathrm{wt}(\mathbf{u})} = \left(\frac{1-z}{1+z}\right)^{\mathrm{wt}(\mathbf{u})} (1+z)^n$$

Applying the previous lemma, we obtain

$$\begin{aligned}
B(z) = \sum_{\mathbf{u} \in \mathcal{C}^\perp} z^{\mathrm{wt}(\mathbf{u})} &= \frac{1}{|\mathcal{C}|} (1 + z^n) \sum_{\mathbf{u} \in \mathcal{C}} \left(\frac{1-z}{1+z}\right)^{\mathrm{wt}(\mathbf{u})} \\
&= 2^{-k} (1 + z^n) A\left(\frac{1-z}{1+z}\right)
\end{aligned}$$