TWO PROOF FOR THE MACWILLIAMS IDENTITY: BINARY CASE

Student: Emre KARADUMAN
Advisor: Assist. Prof. Mehmet Emin KÖROĞLU

Abstract

In this thesis, the aim is to understand two proofs of the MacWilliams Identity in binary case. Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, linguistics, and computer science for the purpose of designing efficient and reliable data transmission methods.

Firstly, we recall some mathematical concepts. Then we introduce the basics of coding theory such as a code, the dual of a code and the weight enumerator etc. Finally, we proposed two proof of MacWilliams Identity in binary cases.

Need to Know

Linear Code

A linear code $\mathscr{C}$ of length n, dimension k and minimum distance d over the alphabet $\mathbb{F}_q$ is denoted by the triple $[n,k,d]_q$ and is a subspace of the n-dimensional vector space $\mathbb{F}_q^n$ [4].

The Dual of The Code $\mathscr{C}$

If $\mathscr{C}$ is an $[n,k]$ linear code over $\mathbb{F}_q$, its dual or orthogonal code $\mathscr{C}^\perp$ is the set of vectors which are orthogonal to all codewords of $\mathscr{C}$:

$$\mathscr{C}^\perp = \{\mathbf{u} | \mathbf{u}\cdot\mathbf{v} = \langle \mathbf{u},\mathbf{v}\rangle = \mathbf{0} \text{ for all } \mathbf{v}\in\mathscr{C}\},$$

where for the vectors $\mathbf{u} = (u_1,u_2,\dots,u_n)$ and $\mathbf{v} = (v_1,v_2,\dots,v_n) \in \mathbb{F}_q^n$

$$\mathbf{u}\cdot\mathbf{v} = \langle \mathbf{u},\mathbf{v}\rangle = u_1v_1 + u_2v_2 + \ldots + u_nv_n = \sum_{i=1}^{n} u_iv_i.$$

Hamming Weight Enumerator

Let $\mathscr{C}$ be a linear code of length n and let A_i be the number of codewords of weight i. Then

$$A(z) := \sum_{i=0}^{n} A_iz^i$$

is called the weight enumerator of $\mathscr{C}$ [3].

Proofs

First Proof of MacWilliams Identity in Binary Case

Let $\mathbb{F}_2^n$ be the binary vector space of dimension n, $d_H(.,.)$ and $w_H(.)$ denote the Hamming distance and weight respectively, and $<.,.>$ be the scalar product of two binary vectors. For any set E, $|E|$ denote the number of the elements in E. Suppose $\mathscr{C}$ is a binary code of length n with M codewords and

$$D_i = \frac{1}{M^2}|(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b}\in\mathscr{C}, d_H(\mathbf{a},\mathbf{b}) = i|,\ i = 0,1,...,n \quad (1)$$

where $\{D_i\}_0^n$ is the weight distribution of the code $\mathscr{C}$ and $f(z) = \sum_{i=0}^n D_iz^i$ be weight enumerator of the code $\mathscr{C}$.

$$\bar{D}_i = \frac{1}{M^2}\sum_{\mathbf{u}\in\mathbb{F}_2^n w_H(\mathbf{u})=i}[\sum_{\mathbf{a}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{a}>}]^2,\ i = 0,1,...,n,$$

length n with M codeword. Obviously, $\bar{D}_i \geq 0$. Set $g(z) = \sum\limits_{i=0}^{n} \bar{D}_iz^i$.

Let $f(z)$ and $g(z)$ be weight enumerators of the binary linear code $\mathscr{C}$ and its dual $\mathscr{C}^\perp$, respectively. Then we have,

$$g(z) = (1+z)^n f(\frac{1-z}{1+z}) \quad (2)$$

$$f(z) = \frac{1}{2^n}(1+z)^n g(\frac{1-z}{1+z}) \quad (3)$$

Obviously, substitute $\frac{1-z}{1+z}$ as z to get the other one
$\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n$, let $\mathbf{u} = (u_1,u_2,\dots,u_n)$ and $\mathbf{v} = (v_1,v_2,\dots,v_n)$.
Scalar product defined by:

$$<\mathbf{u},\mathbf{v}> = |\{i : u_i = v_i = 1\}| = \sum_{i=1}^{n} u_iv_i,$$

$$<1-\mathbf{u},1-\mathbf{v}> = |\{i : \mathbf{u}_i = \mathbf{v}_i = 0\}|. \quad (4)$$

$$<1-\mathbf{u},1-\mathbf{v}> = <1,1> - <1,\mathbf{v}> - <\mathbf{u},1> - <\mathbf{u},\mathbf{v}>$$

$$<1-\mathbf{u},1-\mathbf{v}> = n - \frac{w_H(\mathbf{u})}{2} - \frac{w_H(\mathbf{v})}{2} - \frac{d_H(\mathbf{u},\mathbf{v})}{2}$$

$$<\mathbf{u},\mathbf{v}> = \frac{w_H(\mathbf{u}) + w_H(\mathbf{v}) - d_H(\mathbf{u},\mathbf{v})}{2} \quad (5)$$

$$\begin{aligned}\bar{D}_i &= \frac{1}{M^2}\sum_{\mathbf{u}\in\mathbb{F}_2^n w_H(\mathbf{u})=i}[\sum_{\mathbf{a}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{a}>}]^2\\ &= \frac{1}{M^2}\sum_{\mathbf{u}\in V(n,2) w_H(\mathbf{u})=i}(\sum_{\mathbf{a}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{a}>}\sum_{\mathbf{b}\in\mathscr{C}}(-1)^{-<\mathbf{u},\mathbf{b}>})\\ &= \frac{1}{M^2}\sum_{\mathbf{u}\in\mathbb{F}_2^n w_H(\mathbf{u})=i}\sum_{\mathbf{a}\in\mathscr{C}}\sum_{\mathbf{b}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{a}-\mathbf{b}>}\\ &= \frac{1}{M^2}\sum_{\mathbf{u}\in\mathbb{F}_2^n w_H(\mathbf{u})=i}\sum_{\mathbf{a}\in\mathscr{C}}\sum_{\mathbf{b}\in\mathscr{C}}(-1)^{\frac{w_H(\mathbf{u})+w_H(\mathbf{a}-\mathbf{b})-d_H(\mathbf{u},\mathbf{a}-\mathbf{b})}{2}}\\ &= \frac{1}{M^2}\sum_{\mathbf{u}\in V(n,2) w_H(\mathbf{u})=i}\sum_{j=0}^{n}\sum_{\mathbf{a}\in\mathscr{C}}\sum_{\mathbf{b}\in\mathscr{C} d_H(\mathbf{a},\mathbf{b})=j}(-1)^{\frac{i+j-d_H(\mathbf{u},\mathbf{a}-\mathbf{b})}{2}}\end{aligned}$$

Since $d_H(\mathbf{a},\mathbf{b}) = j$ there are j nonzero positions in the binary vector $\mathbf{a}-\mathbf{b}$. First, we suppose that there are s nonzero positions in $\mathbf{a}-\mathbf{b}$ and $\mathbf{u}$. In this case, $\frac{i+j-d_H(\mathbf{u},\mathbf{a}-\mathbf{b})}{2} = s$ and the number s ranges from 0 to j. For every such fixed pair $(\mathbf{a},\mathbf{b})$ of binary vectors there are $\binom{j}{s}\binom{n-j}{i-s}$ binary vectors $\mathbf{u}$, because $w_H(\mathbf{u}) = i$. Thus, we have

$$\bar{D}_i = \sum_{j=0}^{n}\sum_{s=0}^{j} D_j(-1)^s\binom{j}{s}\binom{n-j}{i-s}.$$

Now, we have

$$\begin{aligned}(1+z)^n f(\frac{1-z}{1+z}) &= \sum_{j=0}^{n} D_j(1+z)^{n-j}(1-z)^j\\ &= \sum_{j=0}^{n} D_j\sum_{s=0}^{j}\binom{j}{s}(-1)^s z^s\sum_{t=0}^{n-j}\binom{n-j}{t}z^t\\ &= \sum_{j=0}^{n}\sum_{s=0}^{j}\sum_{t=0}^{n-j}(-1)^s\binom{j}{s}\binom{n-j}{t}z^{s+t}D_j = g(z)\ [6].\end{aligned}$$

Second Proof of MacWilliams Identity in Binary Case

Let $A(z)$ and $B(z)$ denote the weight enumerators for (n,k) binary linear code $\mathscr{C}$ and its dual code $\mathscr{C}^\perp$, i.e.,

$$A(z) = \sum_{i=0}^{n} A_iz^i \quad (6)$$

is weight enumerator for $\mathscr{C}$.

$$B(z) = \sum_{j=0}^{n} B_jz^j \quad (7)$$

is weight enumerator for $\mathscr{C}^\perp$.
Then $A(z)$ and $B(z)$ are related by the formula

$$B(z) = \frac{1}{2^k}\sum_{i=0}^{n} A_i(1-z)^i(1+z)^{n-i}. \quad (8)$$

Alternatively, equating coefficients of z^j on both sides of up side of the equation, we have

$$B_j = \frac{1}{2^k}\sum_{i=0}^{n} A_iK_{i,j}^{(n)} \text{ for } j = 0,...,n, \quad (9)$$

where $K_{i,j}^n$ is the coefficient of z^j in $(1-z)^i(1+z)^{n-i}$, i.e.,

$$K_{i,j}^{(n)} = \sum_h (-1)^h\binom{i}{h}\binom{n-i}{j-h}. \quad (10)$$

What (8) says is that the weight enumerator vector $\mathbf{a} = (A_0,A_1,...,A_n)$ and $\mathbf{b} = (B_0,B_1,...,B_n)$ are related by the formula,

$$\mathbf{b} = \frac{1}{2^k}\mathbf{a}K^{(n)}. \quad (11)$$

If $\mathbf{x} = (x_1,...,x_m)$ is a binary vector of any length, $|\mathbf{x}|$ denotes its Hamming weight, i.e., the number of nonzero components of $\mathbf{x}$. In particular, if $\mathbf{x}$ is a scalar, i.e., $m = 1$, then

$$|\mathbf{x}| = \begin{cases} 0, \text{ if } x_i = 0\\ 1, \text{ if } x_i = 1\end{cases}. \quad (12)$$

Lemma 1. Look the inner sum $\sum\limits_{\mathbf{u}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{v}>}$. Consider the map

$$\phi_\mathbf{v} : \mathscr{C} \to \mathbb{F}_2$$

$$\mathbf{u} \longmapsto <\mathbf{u},\mathbf{v}>$$

$\phi_\mathbf{v}$ is an additive group homomorphism. $Ker(\phi_\mathbf{v}) = \mathscr{C} \iff \mathbf{v}\in\mathscr{C}^\perp$. If $\mathbf{v}\notin\mathscr{C}^\perp$, then $Ker(\phi_\mathbf{v}) \neq \mathscr{C}$, $\phi_\mathbf{v}$ is onto by the first isomorphism theorem.

$$\mathscr{C}/Ker(\phi_\mathbf{v}) \cong \mathbb{F}_2 \iff |Ker(\phi_\mathbf{v})| = \frac{|\mathscr{C}|}{2}$$

that means $\phi_\mathbf{v}(\mathbf{u}) = 0$ for $\frac{|\mathscr{C}|}{2}$ values of $\mathbf{u}$ and $\phi_\mathbf{v}(\mathbf{u}) = 1$ for $\frac{|\mathscr{C}|}{2}$ values of $\mathbf{u}$.

$$\sum_{\mathbf{u}\in\mathscr{C}}(-1)^{<\mathbf{u},\mathbf{v}>} = \begin{cases} |\mathscr{C}|, \text{ if } \mathbf{v}\in\mathscr{C}^\perp\\ 0, \text{ if } \mathbf{v}\notin\mathscr{C}^\perp\end{cases}.$$

Similarly, we can say that if $\mathscr{C}$ is an $[n,k]$ linear code over $\mathbb{F}_2$, and if $\mathbf{y}$ is an arbitrary n-vector over $\mathbb{F}_2$, then

$$\sum_{\mathbf{x}\in\mathscr{C}} <\mathbf{x},\mathbf{y}> = \begin{cases} 2^k, \text{ if } \mathbf{y}\in\mathscr{C}^\perp\\ 0, \text{ if } \mathbf{y}\notin\mathscr{C}^\perp\end{cases}. \quad (13)$$

Lemma 2. Let $\mathbf{x}$ be a fixed vector of length n over $\mathbb{F}_2$, with $|\mathbf{x}| = i$, and let V_j denote the set of all binary vectors of length n and weight j. Then,

$$\sum_{\mathbf{y}\in V_j} <\mathbf{x},\mathbf{y}> = K_{i,j}^{(n)}. \quad (14)$$

Our proof of the MacWilliams Identity is now simply a matter noting that

$$\sum_{\mathbf{y}\in V_j}\sum_{\mathbf{x}\in\mathscr{C}} <\mathbf{x},\mathbf{y}> = \sum_{\mathbf{x}\in\mathscr{C}}\sum_{\mathbf{y}\in V_j} <\mathbf{x},\mathbf{y}>,$$

and that by Lemma 1,

$$\sum_{\mathbf{y}\in V_j}\sum_{\mathbf{x}\in\mathscr{C}} <\mathbf{x},\mathbf{y}> = \sum_{\mathbf{y}\in V_j\cap\mathscr{C}^\perp} 2^k = 2^kB_j,$$

while by Lemma 2,

$$\sum_{\mathbf{x}\in\mathscr{C}}\sum_{\mathbf{y}\in V_j} <\mathbf{x},\mathbf{y}> = \sum_{\mathbf{x}\in\mathscr{C}} K_{|\mathbf{x}|,j}^{(n)} = \sum_{i=0}^{n} A_iK_{i,j}^{(n)}.$$

$$\sum_{\mathbf{x}\in\mathscr{C}}\sum_{\mathbf{y}\in V_j} <\mathbf{x},\mathbf{y}> = \sum_{i=0}^{n} A_iK_{i,j}^{(n)}.$$

Thus $2^kB_j = \sum_{i=0}^n A_iK_{i,j}^{(n)}$ [5].

Conclusion

In this thesis, two proofs of the MacWilliams Identity for binary case are examined and explained in details. MacWilliams Identity gives a strong relation between the weight enumerator of a code and its dual. In many cases, it allow us to significantly reduce the computational complexity of the computation weight enumerator of a given code.

References

[1] Roman, Steven and Axler, S and Gehring, FW, Advanced linear algebra,

[2] Van Lint, Jacobus Hendricus, Introduction to coding theory

[3] Ling, San and Xing, Chaoping, Coding theory: a first course

[4] MacWilliams, Florence Jessie and Sloane, Neil James Alexander, The theory of error correcting codes

[5] McEliece, Robert J, The generalized distributive law

[6] Jiao, Rongzheng and Lu, Hongwen, An elementary proof of MacWilliams-Delsarte identity

[7] Strang, Gilbert, Introduction to linear algebra