COMPSCI 690T Coding Theory and Applications	April 26, 2017
Lecture 23	
Instructor: Arya Mazumdar	*Scribe: Names Redacted*

1 MacWilliam's Identity and Fourier Transform over Boolean Algebras

1.1 Background

We are interested in the weight distribution of codes. With respect to some code C, we define A_w to be the number of codewords of weight w.

1.2 Weight distribution of Hamming codes

Remember, Hamming codes have parameters $[2^m - 1, 2^m - 1 - m, 3]$.
For such a code, we have:

$$A_0 = 1, A_1 = 0, A_2 = 0$$

We know that Hamming codes achieve the sphere packing bound. Therefore, every binary vector is distance at most 1 from a Hamming codeword.
Consider a Hamming codeword of weight 3. There are 3 weight 2 vectors that are distance 1 away from it, and there are $\binom{n}{2}$ weight 2 vectors in total. It follows that $A_3 = \binom{n}{2}/3$ since 3 weight 2 vectors are distance 1 away from a weight 3 codeword.

We can make a similar argument for A_4. There are $\binom{n}{3} - A_3$ weight 3 vectors that are not codewords. Therefore, $A_4 = (\binom{n}{3} - A_3)/4$.
This inductive procedure can be done for arbitrary w, but there is an easier way to compute the weight distribution of Hamming code.

1.3 MacWilliam's identity

We define the weight enumerator polynomial

$$A(x, y) = \sum_{w=0}^{n} A_w x^{n-w} y^w.$$

If C is a linear code, MacWilliam's identity states

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

The dual code of a hamming code is called a Simplex code. It has parameters $[2^m - 1, m, 2^{m-1}]$. The simplex code achieves the Plotkin bound, which means that all codewords other than 0 have weight $\frac{n+1}{2}$.

So for a Simplex code we have

$$A_0 = 1, A_{\frac{n+1}{2}} = n.$$

It follows that for the Simplex code,

$$A(x, y) = x^n + nx^{n-(n+1)/2} y^{(n+1)/2} = x^n + nx^{(n-1)/2} y^{(n+1)/2}.$$

From the MacWilliam's Identity, we get that for the Hamming code

$$A^{\perp}(x, y) = ((x + y)^n + n(x + y)^{(n-1)/2} (x - y)^{(n+1)/2})/(n + 1).$$

The proof of the identity comes from Fourier transform.

1.4 Fourier transform over boolean algebras

Let $f : \{0,1\}^n \to \mathbb{R}$ be a Boolean function. For any $u, v \in \{0,1\}^n$ let $\langle u, v\rangle$ be the Inner product of u and v.

We define

$$\hat{f}(u) = \sum_{v\in\{0,1\}^n} (-1)^{\langle u,v\rangle} f(v)$$

Lemma:

$$\sum_{v\in C^{\perp}} f(v) = \frac{1}{|C|} \sum_{v\in C} \hat{f}(v).$$

Proof

$$\sum_{v\in C} \hat{f}(v) = \sum_{v\in C} \sum_{u\in\{0,1\}^n} (-1)^{\langle u,v\rangle} f(u) = \sum_{u\in\{0,1\}^n} f(u) \sum_{v\in C} (-1)^{\langle u,v\rangle}.$$

If $u \in C^{\perp}$, then for any $v \in C$, $\langle u, v\rangle = 0$. Therefore,

$$\sum_{v\in C} (-1)^{\langle u,v\rangle} = |C|.$$

Suppose $u \notin C^{\perp}$. Let W be the subspace generated by $C^{\perp}$ and u. By construction , W has dimension 1 higher than that of $C^{\perp}$. It follows that $W^{\perp}$, which is a subspace of C, has dimension 1 smaller than that of C. Therefore $|W^{\perp}| = |C|/2$. This means that for exactly half the elements $v \in C$, $\langle u, v\rangle = 0$. This means that in this case

$$\sum_{v\in C} (-1)^{\langle u,v\rangle} = 0.$$

It follows that

$$\sum_{v\in C} \hat{f}(v) = |C| \sum_{u\in C^{\perp}} f(u).$$

■

1.5 Proof of MacWilliam's identity

Choose

$$f(v) = x^{n-wt(v)} y^{wt(v)}.$$

Then

$$\hat{f}(v) = \sum_{u\in\{0,1\}^n} (-1)^{<u,v>} x^{n-wt(u)} y^{wt(u)} = \sum_{u_1=0}^{1} ... \sum_{u_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_i v_i} x^{1-u_i} y^{u_i} =$$

$$\prod_{i=1}^{n} \sum_{z=0}^{1} (-1)^{z v_i} x^{1-z} y^{z} = (x+y)^{n-wt(v)} (x-y)^{wt(v)}.$$

Substituting $\hat{f}(v) = (x+y)^{n-wt(v)}(x-y)^{wt(v)}$ into the lemma, we get

$$\sum_{v\in C^{\perp}} x^{n-wt(v)} y^{wt(v)} = 1/|C| \sum_{v\in C} (x+y)^{n-wt(v)} (x-y)^{wt(v)}.$$

This implies

$$\sum_{w=0}^{n} A_w^{\perp} x^{n-w} y^{w} = 1/|C| \sum_{w=0}^{n} A_w (x+y)^{n-w} (x-y)^{w}$$

giving the result.