# Weight Distribution of Block Codes

郭芳君　徐利君

## *Outline*

I. Introduction

II. Definition and notation

- ◆ The group algebra
- ◆ Generalization of the weight distribution of a code
- ◆ The weight enumerator of a code
- ◆ Characters

III. The statement of main theorem

- ◆ MacWilliams theorems for nonlinear codes
- ◆ MacWilliams theorems for binary linear code (The special case of MacWilliams theorems)
- ◆ Transform of the distance distribution
- ◆ Perfect code

IV. Conclusion

# I. Introduction

- The weight of a codeword is the number of its nonzero coordinates; clearly any given code contains a certain finite number of vector of each weight from zero to n.
- The weight of the code can describe the character of the code. It is also called the spectrum of the code.
- Here, we also propose a definition of weight enumerator $W_{\overline{C}}$. The weight enumerator of the code is a polynomial which presents the weight distribution of the code.
- And we will show that the spectrum of the code determines uniquely the spectrum of the other code. $W_{\overline{C}'}$ is given by a linear transformation of $W_{\overline{C}}$

# II. Definition and notation

◆ The group algebra

✧ The group algebra QG of G over the rational numbers Q consists of all formal sums

$$\sum_{v\in F^n} a_v z^v \quad , a_v \in Q \quad , z^v \in G$$

✧ Addition and multiplication of elements of QG are defined in the natural way by

$$\sum_{v\in F^n} a_v z^v + \sum_{v\in F^n} b_v z^v = \sum_{v\in F^n} (a_v + b_v) z^v ,$$

$$r \sum_{v\in F^n} a_v z^v = \sum_{v\in F^n} r a_v z^v \quad , r \in Q$$

and

$$\sum_{v\in F^n} a_v z^v \sum_{v\in F^n} b_w z^w = \sum_{v,w\in F^n} a_v b_w z^{v+w}$$

✧ QG gives us an algebraic notion for subsets of $F^n$, or codes: corresponding to the code $\overline{C} \subset F^n$ we have the element

$$C = \sum_{u\in c} c_u z^u$$

of QG.

✧ In general it may be helpful to think of the elements of QG as “generalized codes”; the coefficient $c_u$ being the number of times $v$ occurs in the “code”

✧ For example, corresponding to the code {000,011,101,110} we have

$$C = 1 + z_2 z_3 + z_1 z_2 + z_1 z_3$$

◆ Generalization of the weight distribution of a code

An arbitrary element of the group algebra QG

$$C = \sum_{v \in F^n} c_v z^v \quad ,$$

with the property that

$$M = \sum_{v \in F^n} c_v \neq 0$$

Then We call the (n+1)-tuple $\{A_0, \ldots, A_n\}$ the weight distribution of C, where

$$A_i = \sum_{wt(v)=i} c_v$$

This is the natural generalization of the weight distribution of a code.

◆ The weight enumerator of a code

✧ We define the weight enumerator of a code $\overline{C}$ to be

$$W_{\overline{c}}(x, y) = \sum_{v \in F^n} c_v x^{n-wt(v)} y^{wt(v)}$$

$$= \sum_{i=0}^{n} A_i x^{n-i} y^i$$

$A_i$ will denote the number of codewords of weight i in $\overline{C}$. x and y are indeterminates, and $W_{\overline{C}}(x, y)$ is a homogeneous polynomial of degree n in x and y.

✧ **Example.** Consider the even weight code {000,011,101,110}, denoted by $\overline{C}$. The dual $\overline{C}^{\perp}$ is {000,111}, and the weight enumerators are:

$$W_{\overline{C}}(x,y) = x^3 + 3xy^2$$
$$W_{\overline{C}^{\perp}}(x,y) = x^3 + y^3$$

## ◆ Characters

✧ To each $u \in F^n$, $\chi_u$ is called a character of G

$$\chi_u(z^v) = (-1)^{u \cdot v},$$

where $u \cdot v$ is the scalar product of the vectors *u*, *v* over Q.

Note that

$$\chi_u(z^v) = \begin{cases} 1 & \text{if } u, v \text{ are orthogonal,} \\ -1 & \text{if not} \end{cases}$$

✧ $\chi_u$ is extended to act on QG by linearity:

$$\chi_u\left(\sum_{v \in F^n} a_v z^v\right) = \sum_{v \in F^n} a_v \chi_u(z^v) = \sum_{v \in F^n} (-1)^{u \cdot v} a_v$$

# III. The statement of main theorem

◆ MacWilliams theorems for nonlinear codes

✧ Define a code $\overline{C}$

$$C = \sum_{u \in \overline{c}} c_u z^u ,$$

$\{A_0, \ldots, A_n\}$ is the weight distribution of $\overline{C}$, where

$$A_i = \sum_{wt(v)=i} c_v ,$$

and the weight enumerator of a code $\overline{C}$ to be

$$W_c(x, y) = \sum_{v \in F^n} c_v x^{n-wt(v)} y^{wt(v)}$$

$$= \sum_{i=0}^{n} A_i x^{n-i} y^i$$

✧ The transform of $\overline{C}$ is the element $\overline{C}'$ of QG given by

$$C' = \frac{1}{M} \sum_{u \in F^n} \chi_u(C) z^u$$

and $$C' = \sum_{u \in F^n} c_u' z^u ,$$

so that

$$c_u' = \frac{1}{M} \chi_u(C)$$

$$= \frac{1}{M} \chi_u\left( \sum_{v \in F^n} c_v z^v \right)$$

$$= \frac{1}{M} \sum_{v \in F^n} (-1)^{u \cdot v} c_v \qquad , u \in F^n$$

Then the weight distribution of $\overline{C}^{'}$ is

$\{A_1^{'},...,A_n^{'}\}$,where

$$A_i^{'} = \sum_{wt(u)=i} c_u^{'} = \frac{1}{M} \sum_{wt(u)=i} \chi_u(C)$$

and the weight enumerator of $\overline{C}^{'}$ is

$$W_{\overline{C}^{'}}(x,y) = \sum_{i=0}^{n} A_i^{'} x^{n-i} y^i$$

$W_{\overline{C}^{'}}$ is given by a linear transformation of $W_{\overline{C}}$

✧ MacWilliams theorems for nonlinear codes

$$W_{\overline{C}^{'}}(x,y) = \frac{1}{M} W_{\overline{C}}(x+y, x-y)$$

or equivalently

$$A_k^{'} = \frac{1}{M} \sum_{i=0}^{n} A_i P_k(i), \qquad k = 0,...,n$$

$P_k(i)$ is Krawtchouk polynomial which

$$(1+z)^{n-i}(1-z)^i = \sum_{k=0}^{i} P_k(i) z^k$$

✧ MacWilliams theorems for binary linear code

If C is an [n,k] binary linear cod with dual code $\overline{C}^{\perp}$

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

where $|C|=2^{k}$ is the number of codeword in $\overline{C}$.

Equivalently,

$$\sum_{k=0}^{n}A_{k}^{'}x^{n-k}y^{k}=\frac{1}{|C|}\sum_{i=0}^{n}A_{i}(x+y)^{n-i}(x-y)^{i},$$

or

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

.

✧ The relationship between the $A_{i}^{'}$'s and $A_{i}$'s

$$A_{k}^{'}=\frac{1}{|C|}\sum_{i=0}^{n}A_{i}P_{k}(i)$$

$$(x+y)^{n-i}(x-y)^{i}=\sum_{k=0}^{n}P_{k}(i)x^{n-k}y^{k}$$

✧ **Example.** Consider the even weight code {000,011,101,110}, denoted by $\overline{C}$. The dual $\overline{C}^{\perp}$ is {000,111}, and the weight enumerators are:

$W_{\overline{C}}(x,y) = x^3 + 3xy^2$ and $W_{\overline{C}^{\perp}}(x,y) = x^3 + y^3$

$$\frac{1}{4}W_{\overline{C}}(x+y,x-y) = \frac{1}{4}[(x+y)^3 + 3(x+y)(x-y)^2]$$
$$= x^3 + y^3$$
$$= W_{\overline{C}^{\perp}}(x,y)$$

◆ Transform of the distance distribution

Now let $\overline{C}$ be linear or nonlinear. Let D=(1/M)$C^2$ . IF we expand

D= $\sum_{w\in F^n} d_w z^w$ ，

The weight distribution of D is

{$B_0$……$B_n$}，where

$$B_i = \sum_{wt(w)=i} d_w$$

{$B_0$……$B_n$} is the distance distribution of $\overline{C}$

By applying MacWilliams Theorem to the

element D=(1/M)$C^2$ of QG we obtain：

The transform of the distance distribution is

$$B_s' = \frac{1}{M}\sum_{wt(u)=s}\chi_u(D)$$

$$= \frac{1}{M}\sum_{i=0}^{n} B_i P_s(i) \text{ ， s=0,……,n.}$$

✧Properties of the $B_i'$s

1. $B_i' \geq 0$ ， i=0,……..,n.
2. If $0 \in \overline{C}$ ，$B_i = 0 \Rightarrow A_i=0$.
3. $B_i' = 0 \Rightarrow \chi_u(C) = 0$ for all $u$ of weight $i \Rightarrow A_i' = 0$.
4. $B_i' \neq 0 \Rightarrow \chi_u(C) \neq 0$ for some $u$ of weight $i$.

◆ Dual distance and orthogonal arrays

Definition. The dual distance $d'$ of a code $\overline{C}$ is defined by $B_i' = 0$ for $1 \leq i \leq d'-1$ ，$B_{d'}' \neq 0$. If $\overline{C}$ is linear，$d'$ is the minimum distance of $\overline{C}^{\perp}$.

Note that with this definition of $d'$，Equation hold for the distance distributions of nonlinear

codes.

- Let $\overline{C}$ be the M×n array of all code words of $\overline{C}$. If $\overline{C}$ is linear，any set of $r \le d' - 1$ columns of $\overline{C}$ must be linearly independent，otherwise $\overline{C}^{\perp}$ would contain a vector of weight $r < d'$.This statement is also true for nonlinear codes.
- Any set of $r \le d' - 1$ columns of $\overline{C}$ contains each r-tuple exactly M/$2^{r}$ times，and $d'$ is the largest number with this property.
- **Remark.** An array with this property is called an orthogonal array of n constraints，2 levels，strength $d' - 1$ and index M/$2^{d'-1}$.

➢ Example

The (11,12,6) Hadamard code $A_{12}$. Since this is a simplex code and contains 0，the weight and distance distribution are equal：

$i$ ：0 6

$A_i = B_i$：1 11， $W_{A_{12}}(x, y) = x^{11} + 11x^5 y^6.$

The transformed distribution is obtained from

$$\frac{1}{12}W_{A_{12}}(x+y,x-y)=\frac{1}{12}((x+y)^{11}+11(x+y)^{5}(x-y)^{6})$$

$$=\sum_{i=0}^{11}B_i'x^{11-i}y^{i}\ ,$$

and is equal to

| $i$ : | 0 | 3 | 4 | 5 | 6 | 7 | 8 | 11 |
|---|---|---|---|---|---|---|---|---|
| $B_i'$ : | 1 | $18\frac{1}{3}$ | $36\frac{2}{3}$ | $29\frac{1}{3}$ | $29\frac{1}{3}$ | $36\frac{2}{3}$ | $18\frac{1}{3}$ | 1 |

Note that $\sum B_i' = 170\frac{2}{3} = 2^{11}/12$ , Also $B_i' \geq 0$ , as required. This table shows that $d'$=3.

◆ Perfect code

The sphere of radius $e$ around $v$ is then describe by

$$z^{v}(Y_0+Y_1+\cdots Y_e)$$

If $\overline{C}$ is a perfect (n,M,2e+1) code，this fact is expand by the identity

$$C\cdot(Y_0+Y_1+\cdots Y_e)=\sum_{u\in F^n}z^{u}\ ,$$

where $C = \sum_{v \in C} z^v$

- Example

For the perfect single-error-correcting code

{000,111}， C=1+$z_1z_2z_3$，

$Y_0+Y_1=1+z_1+z_2+z_3$，and indeed

$$C \cdot (Y_0 + Y_1) = 1 + z_1 + z_2 + z_3 + z_1z_2 + z_1z_3 + z_2z_3 + z_1z_2z_3$$

# IV. Conclusion

✧ The weight enumerator of the code $\overline{C}$ is denoted by

$$W_{\overline{C}}(x,y)=\sum_{i=0}^{n}A_i x^{n-i}y^i \quad =\sum_{u\in C}c_v x^{n-wt(u)}y^{wt(u)}$$

✧ MacWilliwams theorem for nonlinear code

$$W_{\overline{C}'}(x,y)=\frac{1}{M}W_{\overline{C}}(x+y,x-y)=\sum_{i=0}^{n}A_i' x^{n-i}y^i$$

$$A_K'=\frac{1}{M}\sum_{i=0}^{n}A_i P_K(i)\ ,\ \text{k=0,……..,n}$$

$$P_K(x)=P_K(x;n)=\sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}\ ,$$

k=0,1,2,…

✧ MacWilliwams theorem for binary linear codes $\quad W_{\overline{C}^{\perp}}(x,y)=\frac{1}{2^K}W_{\overline{C}}(x+y,x-y)$

✧ The transform of the distance distribution is $B_S'=\frac{1}{M}\sum_{i=0}^{n}B_i P_s(i)$ ，s=0,……..,n

$$B_i=\sum_{wt(u)=i}d_w$$

- Reference

1. Reed，p88-89
2. F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, Amsterdam North-Holland,1977.
3. F.J. MacWilliams, “A theorem on the distribution of weights in a systematic code”, Bell System Tech.J. , vol.42, pp.79-94.