Hokkaido Mathematical Journal Vol. 18 (1989), p. 217-222

The average of joint weight enumerators

Tomoyuki YOSHIDA
(Received May 24, 1988)

Abstract. Let C and D be binary linear codes of length n, and let S_n be the symmetric group of degree n. We denote by $W_{C,D}$ the joint weight enumerator of C and D. The purpose of this paper is to represent the average of joint weight enumerators

$$\frac{1}{n!}\sum_{\pi\in S_n} W_{C^\pi,D}(a, b, c, d)$$

by using the ordinary weight distributions of C and D.

1. The statement of the main theorem

Let $F:=\mathrm{GF}(2)$ be the 2-element field and let $V:=F^n$ be the row vector space of n-dimension. Put $N:=\{1, \cdots, n\}$. The *support* and the *weight* of a vector $v\in V$ is defined by

$$\mathrm{supp}(v):=\{i\in N \mid v_i\neq 0\}$$
$$|v|:=\mathrm{wt}(v):=|\mathrm{supp}(v)|.$$

A *code* (or more precisely *binary linear code*) C of length n is a subspace of V. The *minimum weight* d of C is

$$d:=\min\{|u| \mid 0\neq u\in C\}.$$

When a code C of length n is of dimension k and has the minimum distance d, the code is called a $[n, k]$-code or a $[n, k, d]$-code.

The *dual code* of C is defined by

$$C^\perp=\{v\in V \mid \langle u, v\rangle=0 \text{ for all } u\in C\},$$

where $\langle u, v\rangle$ is the ordinary scalar product.

Let π be a permutation on N. For $v\in V$, the vector v^π is the vector of which i-th component is $v_{\pi i}$. Thus the symmetric group S_n acts on V as an automorphism group of the vector space. The code

$$C^\pi:=\{u^\pi \mid u\in C\}$$

is called an *equivalent code* to C. When $C^\pi=C$, the pemutation π is called an *automorphism* of C. The *automorphism group* $Aut(C)$ of the code C is the subgroup of S_n consisting of all automorphisms of C. Under this action of S_n, the weight and the scalar product on V are invariant. Clearly the number of equivalent codes to C is $|S_n : Aut(C)|$.

The *weight enumerator* of a code C is

$$\begin{aligned} W_C(x, y) :&= \sum_{u \in C} x^{n-|u|} y^{|u|} \\ &= \sum_{r} A_r x^{n-r} y^r, \end{aligned}$$

where A_r is the number of te elements of C of weight r.

For any pair of row vectors $u, v \in V$, we define

$$\begin{aligned} I(u, v) &:= \#\{i \in N \mid u_i = 0, v_i = 0\}, \\ J(u, v) &:= \#\{i \in N \mid u_i = 0, v_i = 1\}, \\ K(u, v) &:= \#\{i \in N \mid u_i = 1, v_i = 0\}, \\ L(u, v) &:= \#\{i \in N \mid u_i = 1, v_i = 1\}. \end{aligned}$$

$$\begin{aligned} n &= I(u, v) + J(u, v) + K(u, v) + L(u, v), \\ |v| &= J(u, v) + L(u, v), \\ |u| &= K(u, v) + L(u, v). \end{aligned}$$

Let C and D be codes of length n. Then the *joint weight enumerator* of C and D is

$$\begin{aligned} W_{C,D}(a, b, c, d) :&= \sum_{u \in C} \sum_{v \in D} a^{I(u,v)} b^{J(u,v)} c^{K(u,v)} d^{L(u,v)} \\ &= \sum_{i,j,h,l} A_{i,j,h,l}^{C,D} a^i b^j c^h d^l, \end{aligned}$$

where a, b, c, d are indeterminates and $A_{i,j,h,l}^{C,D}$ is the number of the pairs of $u \in C$ and $v \in D$ such that

$$I(u, v) = i, J(u, v) = j, K(u, v) = k, L(u, v) = l.$$

It is proved in [MMS. 72] that a joint weight enumerator satisfies the following generalized MacWilliams identities:

$$W_{C^\perp,D}(a, b, c, d) = \frac{1}{|C|} W_{C,D}(a+c, b+d, a-c, d-d).$$

$$W_{C,D^\perp}(a, b, c, d) = \frac{1}{|D|} W_{C,D}(a+b, a-b, c+d, c-d).$$

Now, the *average joint weight enumerator* of C and D is defined by

$$W_{C,D}^{av}(a, b, c, d) := \frac{1}{n!} \sum_{\pi \in S_n} W_{C^\pi,D}(a, b, c, d).$$

Clearly if C' is equivalent to C and D' is equivalent to D, then $W_{C',D'}^{av}(a, b, c, d) = W_{C,D}^{av}(a, b, c, d)$.

MAIN THEOREM. *Let C and D be binary linear codes of length n. Let A_r(resp. B_r) be the number of elements of C (resp. D) of weight r. Then*

$$W_{C,D}^{av}(a, b, c, d)=\sum_{r,s} A_r B_s a^{n-r-s} b^s c^r F_{n,r,s}(ad/bc),$$

where

$$F_{n,r,s}(z):=\sum_i \frac{\binom{s}{i}\binom{n-s}{r-i}}{\binom{n}{r}} z^i$$

is the probability generating function of the hypergeometric distribution $H(r, s, n)$.

Clearly, $J(u, v)=K(u, v)=0$ if and only if $u=v$. Thus

$$W_{C,D}^{av}(1, 0, 0, 1)=\frac{1}{n!}\sum_{\pi\in S_n}|C^\pi \cap D|(=:\Delta(C, D)).$$

We call $\Delta(C, D)$ the *average intersection number* of C and D. The following corollary follows directly from the main theorem.

COROLLARY 1. *Under the same assumption,*

$$\Delta(C, D)=\sum_r A_r B_r \Big/ \binom{n}{r}.$$

2. Proof of the theorem

In this section we give the proof of the main theorem. For two codes C and D of length n, define

$$B_{r,s,i}^{CD}:=\#\{(u, v)\in C\times D \,|\, |u|=r, |v|=s, L(u, v)=i\}.$$

Then we have that

$$A_{i,j,k,l}^{C,D}=B_{k+l,j+l,l}^{C,D} \text{ for } i+j+k+l=n,$$

and so

$$W_{C,D}(a, b, c, d)=\sum_{r,s,l} B_{r,s,l}^{C,D} a^{n-r-s+l} b^{r-e} c^{s-l} d^l. \tag{2-1}$$

Let C_r(resp. D_r) be the set of elements of C(resp. D) of weight r. In order to calculate the sum of $B_{r,s,l}^{C^\pi,D}$ for all $\pi\in S_n$, we count the following number in two ways:

$$\#\{(u, v, \pi)\in C_r\times D_s\times S_n \,|\, L(u^\pi, v)=l\}$$

for $r, s, l \in N$. First of all, this number is equal to

$$\text{(2-2)} \qquad \sum_{\pi \in S_n} B^{C^\pi, D}_{r,s,l}.$$

Next this number is also equal to

$$\text{(2-3)} \qquad \sum_{u \in C_r} \sum_{v \in D_s} \#\{\pi \in S_n | L(u^\pi, v) = l\}.$$

In order to calculate (2-3), let $u \in C_r$, $v \in D_s$ and let $A := \mathrm{supp}(u)$, $B := \mathrm{supp}(v)$. Then

$$\begin{aligned} \#\{\pi \in S_n | L(u^\pi, v) = l\} &= \#\{\pi \in S_n || A^\pi \cap B| = l\} \\ &= r!(n-r)! \#\{A' \subseteq N || A'| = r, |A' \cap B| = l\} \\ &= r!(n-r)! \binom{s}{l} \binom{n-s}{r-l} \\ &= n! \binom{s}{l} \binom{n-s}{r-l} \Big/ \binom{n}{r}. \end{aligned}$$

Remember that the subgroup of S_n which stabilizes a subset A with $|A| = r$ has the order $r!(n-r)!$. Since (2-2) and (2-3) are equal, we have that

$$\text{(2-4)} \qquad \sum_{\pi \in S_n} B^{C^\pi, D}_{r,s,l} = A_r B_n n! \binom{s}{l} \binom{n-s}{r-l} \Big/ \binom{n}{r}.$$

By (2-1) and the definition of the average weight enumerator, we have that

$$\begin{aligned} W^{av}_{C,D}(a, b, c, d) &= \sum_{r,s,l} A_r B_s \frac{\binom{s}{l}\binom{n-s}{r-l}}{\binom{n}{r}} a^{n-r-s+l} b^{s-l} c^{r-1} d^l \\ &= \sum_{r,s,l} A_r B_s a^{n-r-s} b^s c^r F_{n,r,s}(ad/bc). \end{aligned}$$

The theorem in proved.

3. Numerical examples

In this section, we give some examples of the average joint weight enumerators for some well-known self-dual codes.

(1) Let $C = \{\mathbf{0}, \mathbf{1}\}$ be the repetition code of length n and let D be any code of length n. Then

$$W^{av}_{C,D}(a, b, c, d) = W_D(a, c) + W_D(b, d),$$

where $W_D(x, y)$ is the weight enumerator of D.

(2) Let H_8 be the extended Hamming code of length 8. Then

$$W^{av}_{H_8,H_8}(a, b, c, d)=a^8+b^8+c^8+d^8+14(a^4+d^4)(b^4+c^4) +\frac{14}{5}(a^4d^4+b^4c^4+16ab^3c^3d +16a^3bcd^3+36a^2b^2c^2d^2)$$

Furthermore by the corollary, we have that

$$\Delta(H_8, H_8)=1+14/5+1=4.8.$$

(3) Let G_{24} be the binary Golay code of length 24. The weight distributions of this code are $A_0=A_{24}=1$, $A_8=A_{16}=759$, $A_{12}=2576$. Thus

$$\begin{aligned}\Delta(G_{24}, G_{24})&=2+\frac{759^2}{\binom{24}{8}}\times 2+\frac{2576^2}{\binom{24}{12}}\\&=2^8\cdot 5\cdot 79/13\cdot 17\cdot 19\\&=6.02048\ldots.\end{aligned}$$

(4) Let H_8^3 be the direct sum of three copies of the extended Hamming code H_8. Then

$$\begin{aligned}\Delta(H_8^3, G_{24})&=2+\frac{759\cdot 591}{\binom{24}{8}}\times 2+\frac{2576\cdot 2828}{\binom{24}{12}}\\&=2^8\cdot 97/13\cdot 17\cdot 19.\\&=5.91378\ldots.\end{aligned}$$

(5) Let C_{72} be a self-dual [72, 36, 16]-code in which the weight of each codeword is a multiple of 4. It is unknown whether such a code exists or not. The weight distribution of this code is found, for example, in **[CP. 82]**. Then we have that

$$\begin{aligned}\Delta(C_{72}, G_{24}^3)&=28560387512926208/4760059542649555\\&=6.000006356439159 40561\ldots,\\ \Delta(C_{72}, C_{72})&=28109104533825536 00/4684850601875692031\\&=6.00000196926532 39457\ldots.\end{aligned}$$

4. Some remarks

(1) As is stated in Section 1, joint weight enumerators satisfy generalized MacWilliams identities. Thus average joint weight enumerators also satisfy such identities. However they follow from the ordinary MacWilliams identity for weight enumerators, and hence we can not obtain any new restrictions to weight distribution. This disappointing fact is shown as follows: Let C and D be (binary linear) codes of length n. Let

$$W_C(x, y)=\sum_{r=0}^{n} A_r x^{n-r} y^r,\ W_D(x, y)=\sum_{r=0}^{n} B_r x^{n-r} y^r,$$

be the weight enumerators of C, D, respectively. Then by the main theorem, we have that

$$W_{C,D}^{av}(a, b, c, d)=\sum_s B_s \frac{(n-s)!}{n!}\left(b\frac{\partial}{\partial a}+d\frac{\partial}{\partial c}\right)^s W_C(a, b).$$

From the MacWilliams identity

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

we have the generalized MacWilliams identity

$$W_{C^\perp,D}^{av}(a, b, c, d)=\frac{1}{|C|} W_{C,D}^{av}(a+c, b+d, a-c, b-d).$$

(2) If we use the general linear group $\Gamma := GL(n, 2)$ instead of the symmetric group S_n, then the average intersection number of D, D is given by the following:

$$\frac{1}{|\Gamma|}\sum_{\sigma\in\Gamma}|C^\sigma \cap D|=1+\frac{(|C|-1)\cdot(|D|-1)}{|V|-1}.$$

This is easily proved by counting in two ways. For example, if C and D are self-dual of dimension k, then this value is equal to $2(2^k-1)/(2^k+1)\approx 2$.

(3) It seems provable that the average intersection numbers of doubly-even self dual binary codes are asymptotically equal to 6.

References

[CP. 82] J. H. CONWAY and V. PLESS, *On primes dividing the group order of a doubly-even* (72, 36, 16) *code and the group order of a quaternary* (24, 12, 10) *code*, Discrete Math **38** (1982), 143-156.

[MMS. 72] F. J. MACWILLIAMS, C. L. MALLOWS, and N. J. A. SLOANE, *Generalizations of Gleason's theorem on weight enumerators of self-dual codes*, IEEE Trans. Information Theory **IT-18** (1972), 794-805.

Department of Mathematics
Hokkaido University