Hokkaido Mathematical Journal Vol. 20 (1991) p. 539-548

The average intersection number of a pair of self-dual codes

Dedicated to Professor Noboru Tanaka's 60-th birthday

Tomoyuki YOSHIDA*
(Received May 25, 1990)

Contents

1. Introduction. 2. The average of intersection numbers. 3. A counter example for Conjecture I. 4. Main theorem. 5. The second moments. 6. The average of dimensions of intersections.

1 Introduction

Let C, $D\subseteq \boldsymbol{F}_2{}^n$ be binary self-dual codes of length n. In the preceding paper, we studied the average of joint weight enumerators of C, D, particularly the average intersection number:

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

and then we show that they can be presented by the weight enumerators of C, D.

After observing the values of average intersection numbers of some typical binary self-dual codes, I stated the following conjecture:

Conjecture I: $\Delta(C, D)\approx 4$ if C, D is of type I but not type II.

Conjecture II: $\Delta(C, D)\approx 6$ if C, D is of type II.

Here, a binary code is called to be type I if it is self-dual, and is called to be type II if it is of type I and the weight of any code word is divisible by 4. For example, let H_8, G_{24}, C_{72} be the extended Hamming code of length 8, the binary Golay code of length 24, an extremal type II code of length 72 which has not yet discovered. Then we have that

$$\Delta(H_8, H_8)=4.8=24/5,$$
$$\Delta(G_{24}, G_{24})=6.02048\cdots=2^8\cdot 5\cdot 79/13\cdot 17\cdot 19,$$
$$\Delta(H_8{}^3, G_{24})=5.91378\cdots=2^8\cdot 97/13\cdot 17\cdot 19,$$

*Partially supported by SFB 7^3 at Fakultät für Mathematik, Universität Bielefeld, FRG, Oct., 1989-Sep., 1990.

$$\Delta C_{72}, G_{24}{}^{3})=6.00000\ 63564\ 39159\ 4056\cdots$$
$$=28\ 56038\ 75129\ 26208/4\ 76005\ 95426\ 49555,$$
$$\Delta(C_{72}, C_{72})=6.00000\ 01969\ 26532\ 39457\cdots$$
$$=2810\ 91045\ 33825\ 53600/468\ 45060\ 18756\ 92031.$$

In this paper, we give a counter-example for Conjecture I. There is no hope that conjecture II is valid, but the author has no counter-example.

However, the above conjectures are valid if we take the average on *all* self-dual codes of type I or II. This idea is very classical and familiar in the theory of error-correcting codes since Shannon. For a binary code C of length n, define

$$\Delta_{\mathrm{I}}(C) :=\frac{1}{|\mathrm{I}_n|}\sum_{D\in \mathrm{I}_n}|C\cap D|, \tag{2}$$

$$\Delta_{\mathrm{II}}(C) :=\frac{1}{|\mathrm{II}_n|}\sum_{D\in \mathrm{II}_n}|C\cap D|, \tag{3}$$

where I_n(resp. II_n) denotes the set of self-dual codes of length n of type I (resp. II). Then the following holds:

THEOREM. *Let C be a binary self-dual code of length n. Then*

$$\Delta_{\mathrm{I}}(C) \approx 4 \quad \textit{if } C \textit{ is of type } \mathrm{I},$$
$$\Delta_{\mathrm{II}}(C) \approx 6 \quad \textit{if } C \textit{ is of type } \mathrm{II}.$$

The roof will be given in Section 4. In Section 5, we give the second moments of intersection numbers of codes of type I or II. In Section 6, we study the average of the dimensions of intersections:

$$\Delta_J^{\dim}(C) :=\frac{1}{|J|}\sum_{D\in J}\dim(C\cap D), \tag{4}$$

where $J=\mathrm{I}_n$ or II_n.

Acknowledgement. The author would like to appreciate to Professor N. J. A. Sloane for his helpful comment for the " six " conjecture in the preceding paper.

2 The average of intersection numbers

2.1 We use the standard notation in the theory of error-correcting codes ([MS 77], [Pl 82]). Let $\boldsymbol{F}_q$ be a q-element field. For a natural number n, $\boldsymbol{F}_q^n$ be a row vector space of dimension n over $\boldsymbol{F}_q$:

$$\boldsymbol{F}_q^n :=\{(v_1, \cdots, v_n) \mid v_i\in \boldsymbol{F}_q\}.$$

The *weight* and the inner product of vectors in $\boldsymbol{F}_q^n$ are defined as follows:

$$\mathrm{wt}(v):=\#\{i \mid v_i \neq 0\}, \tag{1}$$

$$(u, v):=\sum_{i=1}^{n} u_i v_i. \tag{2}$$

A *code* C is a subspace of $\boldsymbol{F}_q^n$. In particular, a code over a 2-element field $\boldsymbol{F}_2$ is called a *binary code*. When $k=\dim C$, such a code C is called a $[n, k]$-code, where n is the *length* of C and k is the *dimension*. The *dual code* $C^\perp$ of C is defiened by

$$C^\perp:=\{v \in \boldsymbol{F}_q^n \mid (u, v)=0 \text{ for all } u \in C\}. \tag{3}$$

A code C is called *self-dual* if $C=C^\perp$. Then $\dim C^\perp = n-\dim C$, and so in particular, the dimension of a self-dual code C is equal to $n/2$ and the length n is even.

2.2 A binary self-dual code C is called to be of *type* I. It is easily proved that for a code C of type I,

$$\boldsymbol{h}:=(1, \cdots, 1) \in C. \tag{4}$$

A binary self-dual code C is called to be of *type* II provided all elements of C have weights divisible by 4. It is well-known that the dimension of a self-dual code of type II is divisible by 8 (cf. [MS 77], [MST 72, Corollary 4.7).

2.3 Let S_n be a symmetric group of degree n. Then S_n acts linearly on the vector space $\boldsymbol{F}_q^n$ by the permutation of coordinates:

$$(v^\pi)_i = y_{\pi(i)}. \tag{5}$$

The *automorphism group* $\mathrm{Aut}(C)$ is defined by

$$\mathrm{Aut}(C):=\{\pi \in S_n \mid C^\pi = C\}. \tag{6}$$

(We do not consider monomial automorphisms.)

2.4 For two code C, D, the *average intersection number* is defined by

$$\Delta(C, D):=\frac{1}{n!}\sum_{\pi \in S_n} |C \cap D^\pi|. \tag{7}$$

Then the following basic result has been proved in the preceding paper [Yo 89, Corollary 1].

2.5 PROPOSITION. *Let C, D be code of length n over $\boldsymbol{F}_q$. Then*

$$\Delta(C, D)=\sum_{r=0}^{n}\frac{a_r b_r}{\binom{n}{r}}, \tag{8}$$

where

$$a_r := \#\{u\in C \mid \mathrm{wt}(u)=r\},$$
$$b_r := \#\{v\in D \mid \mathrm{wt}(v)=r\}.$$

PROOF. There is an easy direct proof for this proposition. Let C_r, D_r be the sets of all elements of C, D of weight r. Then we have that

$$\begin{aligned} n!\Delta(C, D) &= \sum_{\pi\in S_n}|C\cap D^{\pi}| \\ &= \#\{(u, v, \pi)\in C\times D\times S_n \mid u=v^{\pi}\} \\ &= \sum_{r=0}^{n}\sum_{u\in C_r}\sum_{v\in D_r}\#\{\pi\in S_n \mid u=v^{\pi}\} \\ &= \sum_{r=0}^{n} a_r b_r r!(n-r)!. \end{aligned}$$

□

2.6 EXAMPLE. Let H_8, G_{24} and C_{72} be the extended Hamming code of length 8 and the binary Golay code of length 24, the supposed extremal code of type II of length 72. Then the weight enumerators of H_8 and G_{24} are given by $a_0=a_8=1$, $a_4=14$ for H_8 and $a_0=a_{24}=1$, $a_8=a_{16}=759$, $a_{12}=2576$ for G_{24}. Futhermore, the one of C_{72} is given in [CP 82]. Using these values, we have that

$$\Delta(H_8, H_8)=4.8\text{-}24/5,$$
$$\Delta(G_{24}, G_{24})=6.02048\cdots=2^8\cdot5\cdot7\cdot79/13\cdot17\cdot19.$$
$$\Delta(C_{72}, C_{72})=6.000000\,01969\,26532\,39457\cdots$$
$$=2810\,91045\,33825\,53600/468\,45060\,18756\,92031.$$

See also Introduction.

3 A counter-example for Conjecture I

3.1 Counterexample: In this section, we give a counter-example for conjecture I. Let $C_2=\{00, 11\}$ be a trivial binary self-dual code of length 2. Then the direct sum C_2^m of m copies of C_2 is a type I code of length 2 $m=n$ and the number of elements of C_2^m of weight $2r$ equals $\binom{m}{r}$. Thus by Proposition 2.5, we have that

$$\begin{aligned}\Delta(C_2^m, C_2^m) &= \sum_{r=0}^{m} \frac{\binom{m}{r}^2}{\binom{2m}{2r}} \\ &= \frac{1}{\binom{2m}{m}} \sum_{r=0}^{m} \binom{2r}{r}\binom{2m-2r}{m-r}.\end{aligned}$$

In order to find this summation, we consider the following power series:

$$\begin{aligned}&\sum_{m=0}^{\infty} \binom{2m}{m} \Delta(C_2^m, C_2^m) t^m \\ &= \sum_{m=0}^{\infty} \sum_{r=0}^{m} \binom{2r}{r}\binom{2m-2r}{m-r} t^m \\ &= \sum_{r,s} \binom{2r}{r}\binom{2s}{s} t^{r+s} \\ &= \left(\sum_{r=0}^{\infty} \binom{2r}{r} t^r\right)^2 = \left(\frac{1}{\sqrt{1-4t}}\right)^2 = \frac{1}{1-4t} \\ &= \sum_{m=0}^{\infty} 4^m t^m.\end{aligned}$$

Thus we have that

$$\Delta(C_2^m, C_2^m) = 4^m / \binom{2m}{m}.$$

Using Stirling's formula $n! \approx n^n e^{-n} \sqrt{2n\pi}$, we conclude that

$$\Delta(C_2^m, C_2^m) \approx \sqrt{m\pi} \to \infty \quad (m \to \infty).$$

Hence the codes C_2^m, $m \geq 1$ do not satisfy Conjecture I.

3.2 Let H_8 be the extended Hamming code of length 8. Then it follows from Proposition 2.5 that

$$\Delta(H_8^n, H_8^n) = \sum_{r=0}^{2m} \frac{a_r^2}{\binom{8m}{4r}},$$

where a_r, $r \geq 0$ are defined as coefficient of the following polynomial:

$$(1+14t+t^2)^m = \sum_{r=0}^{2m} a_r t^r.$$

It seems to be still true that $\Delta(H_8^n, H_8^n) \approx 6$.

4 Main theorem

In this section, we state the main theorem of this paper and prove it.

4.1 Let $J=\mathrm{I}$ or II and let J_n be the set of binary self-dual codes of length n of type J. We put

$$\varepsilon(J):=\begin{cases}1 & \text{if } J=\mathrm{I},\\ 2 & \text{if } J=\mathrm{II}.\end{cases}$$

4.2 Let E be a subspace of $\boldsymbol{F}_q^n$ with $\boldsymbol{h}=(1,\cdots,1)\in E\subseteq E^{\perp}$ and dim $E=k$. When $J=\mathrm{II}$, we further assume that

$$\mathrm{wt}(e)\equiv 0 \pmod 4 \quad \text{for all } e\in E.$$

Put

$$M:=2^{n/2}.$$

For $J=\mathrm{I}$ or II and integer $k\geq 1$, we define an integer $N_{n,k}^J$ by

$$N_{n,k}^J:=\#\{C\in J_n \mid E\subseteq C\}, \tag{1}$$

so that [MST 72] yields that

$$N_{n,k}^J=\prod_{i=2-\varepsilon(J)}^{\frac{n}{2}-k+1-\varepsilon(J)}(2^i+1). \tag{2}$$

The right hand side does not depend on E. In particular, applying this formula to $k=1$, we have that

$$|J_n|=\prod_{i=2-\varepsilon(J)}^{\frac{n}{2}-\varepsilon(J)}(2^i+1). \tag{3}$$

(Remember that $\boldsymbol{h}\in C$ for any binary self-dual code C.)Thus

$$N_{n,k}^J/|J_n|=\prod_{i=0}^{k-2}\frac{1}{M\cdot 2^{-i-\varepsilon(J)}+1}. \tag{4}$$

In particular, when $k=1,2,3$, we have that

$$N_{n,1}^J/|J_n|=1, \tag{5}$$

$$N_{n,2}^J/|J_n|=\frac{1}{M\cdot 2^{-\varepsilon(J)}+1}, \tag{6}$$

$$N_{n,3}^J/|J_n|=\frac{1}{(M\cdot 2^{-\varepsilon(J)}+1)\cdot(M\cdot 2^{-\varepsilon(J)-1}+1)}. \tag{7}$$

4.3 THEOREM (MAIN THEOREM). *Let C be a binary self-dual code of length n. Then the following hold:*

(1) *If C is of type* I, *then*

$$\Delta_{\mathrm{I}}(C)=4-\frac{4}{2^{n/2-1}+1}\approx 4.$$

(2) *If* C *is of type* II, *then*

$$\Delta_{\mathrm{II}}(C)=6-\frac{6}{2^{n/2-2}+1}\approx 6.$$

PROOF. Let $J=\mathrm{I}$ or II and let $C\in J_n$. Then we have that

$$\begin{aligned}\sum_{D\in J_n}|C\cap D|&=\#\{(u,D)\in C\times J_n \mid u\in D\}\\ &=\sum_{u\in C}\#\{D\in J_n \mid u\in D\}.\end{aligned}$$

We divide this summation into three parts, that is, $u=0$, $u=\boldsymbol{h}$ and $u\in C-\{0,\boldsymbol{h}\}$, so that

$$\begin{aligned}\sum_{D\in J_n}|C\cap D|&=\Big(\sum_{a=0,\boldsymbol{h}}+\sum_{u\in C-\{0,\boldsymbol{h}\}}\Big)\#\{D\in J_n|\langle\boldsymbol{h},u\rangle\subseteq D\}\\ &=2\times N_{n,1}+(|C|-2)\times N_{n,2}.\end{aligned}$$

Here, $\langle u,\boldsymbol{h}\rangle$ is the subspace generated by u and $\boldsymbol{h}$ of $\boldsymbol{F}_2^n$. Thus by (5) and (6),

$$\begin{aligned}\Delta_J(C)&=2+(2^{n/2}-2)\cdot\frac{N_{n,2}}{|J_n|}\\ &=2+(2^{n/2}-2)\cdot\frac{1}{2^{n/2-\varepsilon(J)}+1}\\ &=(2+2^{\varepsilon(J)})\times\Big(1-\frac{1}{2^{n/2-\varepsilon(J)}+1}\Big).\end{aligned}$$

This complete the proof of the theorem. □

5 The second moments

In this section, we calculate the second moments of intersection numbers.

5.1 THEOREM. *Let* C *be a binary self-dual code of length* n. *Put* $M:=|C|=2^{n/2}$. *Then the following hold*:

(1) *If* C *is of type* I, *then*

$$\frac{1}{|\mathrm{I}_n|}\sum_{D\in \mathrm{I}_n}|C\cap D|^2=\frac{24M^2}{(M+2)(M+4)}\approx 24.$$

(2) *If* C *is of type* II, *then*

$$\frac{1}{|\mathrm{II}_n|}\sum_{D\in \mathrm{II}_n}|C\cap D|^2=\frac{60M^2}{(M+4)(M+8)}\approx 60.$$

PROOF. Let $J=\mathrm{I}_n$ or II_n and let $\varepsilon:=\varepsilon(J)$. Then similarly as in the proof of the theorem of the preceding section, we have that

$$\begin{aligned}\sum_{D\in J}|C\cap D|^2&=\#\{(u,v,D)\in C\times C\times J\,|\,u,v\in D\}\\&=\sum_{u,v\in C}\#\{D\in J\,|\,\langle u,v,\boldsymbol{h}\rangle\subseteq D\}\\&=\sum_{\dim\langle u,v,\boldsymbol{h}\rangle=1}+\sum_{\dim\langle u,v,\boldsymbol{h}\rangle=2}+\sum_{\dim\langle u,v,\boldsymbol{h}\rangle=3}\\&=4N_{n,1}^J+6(|C|-2)\cdot N_{n,2}^J+(|C|-2)\cdot(|C|-4)\cdot N_{n,3}^J.\end{aligned}$$

Thus by (5), (6), (7) of the preceding section,

$$\begin{aligned}\frac{1}{|J|}\sum_{D\in J}|C\cap D|^2&=4+\frac{4(M-2)}{M\cdot 2^{-\varepsilon}+1}+\frac{(M-2)(M-4)}{(M\cdot 2^{-\varepsilon}+1)\cdot(M\cdot 2^{-\varepsilon-1}+1)}\\&=\frac{M^2\cdot 2^{-2\varepsilon}(2^{\varepsilon}+1)(2^{\varepsilon}+2)}{(M\cdot 2^{-\varepsilon}+1)\cdot(M\cdot 2^{-\varepsilon-1}+1)}.\end{aligned}$$

The theorem follows immediately from this formula. □

6 The average of dimensions of intersection

In this section, we study the average of the dimensions of intersections.

6.1 The *Gaussian binomial coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k-dimensional subspaces in $\boldsymbol{F}_q^n$. Then we have that

$$\begin{bmatrix} n \\ k \end{bmatrix}_q=\frac{(q)_n}{(q)_k\cdot(q)_{n-k}},\tag{1}$$

where

$$(q)_r:=\prod_{i=1}^{k}(q^i-1).\tag{2}$$

6.2 THEOREM. *Let $J=\mathrm{I}_n$ or II_n and let C be a binary self-dual code of length n. Let $N_{n,k}^J$ be the number given in* (2) *of Section* 4. *Define $T_1, T_2, \cdots$ by*

$$T_1:=T_2:=1,\quad T_k:=(-1)^k(2)_{k-2}\quad(k\geq 2).$$

Then

$$\frac{1}{|J|}\sum_{D\in J}\dim(C\cap D)=\sum_{k=1}^{n/2}T_k\cdot\begin{bmatrix} n/2-1 \\ k-1 \end{bmatrix}_2\cdot\prod_{i=0}^{k-2}\frac{1}{M\cdot 2^{-i-\varepsilon(J)}+1}.$$

PROOF. For $C\in J$, we have that

$$\sum_{D\in J}\dim(C\cap D)=\sum_{\substack{\boldsymbol{h}\in U\subseteq C\\ D\cap C=U}}\sum_{D\in J}\dim(U)$$
$$=\sum_{\boldsymbol{h}\in U\subseteq C}\dim(U)\times\#\{D\in J|C\cap D=U\}.$$

Define two functions f, g on subspaces of $C\cong \boldsymbol{F}_2^{n/2}$ by

$$f(U):=\#\{D\in J \mid C\cap D=U\},$$
$$g(W):=\#\{D\in J \mid W\subseteq D\},$$

so that

$$g(W)=\sum_{W\subseteq U\subseteq C}f(U),$$

and

$$g(W)=N^J_{n,\dim W}\quad \text{if } \boldsymbol{h}\in W\subseteq V.$$

Let μ be the Möbius function of the lattice of subspaces of C. Then it is known that

$$\mu(U,W)=\begin{cases}(-1)^r 2^{\binom{r}{2}} & \text{if } U\subseteq W \text{ and } \dim(W/U)=r,\\ 0 & \text{otherwise.}\end{cases}$$

See, for example, Aigner's book [Ai 79], Proposition 4.20 (iii). It follows from the Möbius inversion formula that for $\boldsymbol{h}\in U\subseteq V$,

$$f(U)=\sum_{U\subseteq W\subseteq C}\mu(U,W)\,g(W)$$
$$=\sum_{U\subseteq W\subseteq C}(-1)^{\dim(W/U)}\,2^{\binom{\dim(W/U)}{2}}\,N^J_{n,\dim W}.$$

Thus

$$\frac{1}{|J|}\sum_{D\in J}\dim(C\cap D)$$
$$=\frac{1}{|J|}\sum_{k=1}^{n/2}\begin{bmatrix}n/2-1\\ m-1\end{bmatrix}_2\sum_{r=0}^{k-1}(-1)^r2^{\binom{r}{2}}(m-r)\begin{bmatrix}k-1\\ r\end{bmatrix}_2 N^J_{n/2,k}$$
$$=\frac{1}{|J|}\sum_{k=1}^{n/2}T_k\cdot\begin{bmatrix}n/2-1\\ m-1\end{bmatrix}_2\cdot N^J_{n/2,k},$$

where

$$T_k:=\sum_{r=0}^{k-1}(-1)^r(k-r)2^{\binom{r}{2}}\begin{bmatrix}k-1\\ r\end{bmatrix}_2.$$

Clearly, $T_1=T_2=1$. By the q-binomial theorem, we have that

$$F_n(\lambda):=\sum_{r=0}^{n}\begin{bmatrix} n \\ r \end{bmatrix}_q q^{\binom{r}{2}}\lambda^r=\prod_{i=1}^{n}(1+q^{i-1}\lambda).$$

For $q=2$ and $k\geq 2$,

$$\begin{aligned} T_k &= \sum_{r=0}^{k-1}(-1)^r(k-r)2^{\binom{r}{2}}\begin{bmatrix} k-1 \\ r \end{bmatrix}_2 \\ &= k\,F_{k-1}(-1)+F'_{k-1}(-1) \\ &= k\delta_{k,1}+(-1)^k\prod_{j=1}^{k-2}(2^j-1) \\ &= (-1)^k\prod_{j=1}^{k-2}(2^j-1). \end{aligned}$$

The theorem is proved. □

References

[Ai 79] M. AIGNER, "Combinatorics", Springer-Verlag, Berlin, 1979.

[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 qaternay (24, 12, 10) code, *Discrete Math,* **38** (1982), 143-156

[MST 72] F. J. MACWILLIAMS, N. J. A. Sloane and J. G. Thompson, Good self dual codes exist, *Discrete Math.,* **3** (1972), 153-162.

[MS 77] F. J. MACWILLIAMS and N. J. A. SLOANE, "The Theory of Frror-Correcting Codes", North Holland, New York, 1977.

[Pl 82] V. PLESS, "Introduction to the Theory of Error-Correcting Codes", Wiley-Interscience Series in Discrete Math., New York, 1982.

[Yo 89] T. YOSHIDA, The average of joint weight enumerators, *Hokkaido Math. J.,* **18** (1989), 217-222.

Department of Mathematics
Hokkaido University
Kita 10 Nishi 8
Sapporo 060
JAPAN