

## 球の詰め込みと符号理論への入門

北大・理 石川辰義 ( Tatsuyoshi Ishikawa )

北大・理 池田隆一 ( Ryuichi Ikeda )

### § 0 はじめに

表題には "球の詰め込み" とありますが、講演では時間の関係もあって発表できなかつたので、本稿では割愛します。

よって今回は符号理論への入門として Sloane [9] の論文を参考に不変式論の符号理論への応用について紹介します。

### § 1 定義および定理

まず符号理論についてのいくつかの定義と定理を述べる。 ([4], [5])

#### 定義 1.1

$\mathbb{F}_q$  上の  $n$  次元線形空間の  $k$  次元部分空間  $C$  を長さ  $n$  の  $k$  次元線形符号 といい、 $[n, k]$  符号、または  $C[n, k]$  と表わす。符号の元を 符号語 と言う。符号語  $c$  の 重さ  $wt(c)$  を以下のように定義する。

$$wt(c) = \#\{i \mid c_i \neq 0, c = (c_1, c_2, \dots, c_n)\}.$$

符号語の (非 0 の) 最小重さが  $d$  である  $[n, k]$  符号を特に  $[n, k, d]$  符号と表わす。

$u, v \in \mathbb{F}_q^n$  の距離  $d(u, v)$  を以下のように定義する。

$$d(u, v) = \#\{i \mid u_i \neq v_i, u = (u_1, \dots, u_n), v = (v_1, \dots, v_n)\}.$$

$[n, k]$  符号  $C$  の双対符号  $C^\perp$  を以下のように定義する

$$C^\perp = \{u \in \mathbb{F}_q^n \mid u \cdot v = 0 \quad \forall v \in C\}, \text{ ただし } u \cdot v = \sum_{i=1}^n u_i v_i \quad u, v \in C.$$

注  $C$  が  $[n, k]$  符号のとき  $C^\perp$  は  $[n, n-k]$  符号となる。

**定義1.2**  $C = C^\perp$  のとき  $C$  を自己双対符号という。

### 定義1.3

$[n, k]$  符号  $C$  のハミング重み多項式 (或は単に重み多項式)  $W_C(x, y)$  を次のように定義する。

$$W_C(x, y) = \sum_{c \in C} x^{n-\text{wt}(c)} y^{\text{wt}(c)} = \sum_{i=0}^n A_i x^{n-i} y^i,$$

ここで  $A_i = \#\{c \in C \mid \text{wt}(c) = i\}$ .

### 定理1.4 (MacWilliams' identity)

$C$  を  $\mathbb{F}_q$  上の  $[n, k]$  符号、また  $C^\perp$  を  $C$  の双対符号とする。このとき次の等式が成り立つ

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

特に  $C$  が自己双対符号のとき,

$$W_C(x, y) = W_C\left(\frac{1}{\sqrt{q}}(x + (q-1)y), \frac{1}{\sqrt{q}}(x-y)\right).$$

### 定義1.5

$\mathbb{F}_q^n$  のベクトル  $v$  のコンポジション  $s(v) = (s_0(v), s_1(v), \dots, s_{q-1}(v))$  を各  $s_i(v)$  について  $s_i(v) = \#\{j \mid v_j = \omega_i, v = (v_1, \dots, v_n)\}$  で定義する。

但し  $\mathbb{F}_q = \{\omega_0, \dots, \omega_{q-1}\}$  とする。

**定義1.6**

完全重み多項式  $V_c(z_0, \dots, z_{q-1})$  を以下のように定義する,

$$V_c(z_0, \dots, z_{q-1}) = \sum_{c \in C} z_0^{s_0(c)} \cdots z_{q-1}^{s_{q-1}(c)} = \sum_s A(s) z_0^{s_0} \cdots z_{q-1}^{s_{q-1}},$$

$$A(s) = \#\{c \in C \mid s(c) = s\}, \quad s = (s_0, \dots, s_{q-1}) \in Z^q.$$

**定理1.7** (MacWilliams' identity-Complete):

$C$  を  $\mathbb{F}_q$  上の  $[n, k]$  符号、また  $C^\perp$  を  $C$  の双対符号とする。このとき次

の等式が成り立つ

$$V_{c^\perp}(z_0, \dots, z_{q-1}) = \frac{1}{|C|} V_c\left(\sum_{j=0}^{q-1} \chi(\omega_0 \omega_j) z_j, \dots, \sum_{j=0}^{q-1} \chi(\omega_{q-1} \omega_j) z_j\right)$$

ここで  $\chi: \mathbb{F}_q \rightarrow \mathbb{C}$  は以下のように定義される

$$\chi(\lambda) = \xi^\lambda, \quad q = p^f, \quad \xi = e^{2i\pi/p},$$

$$\mathbb{F}_q = \{\omega_0, \dots, \omega_{q-1}\} \quad (\omega_0 = 0 \text{ とする}),$$

$$\lambda = \lambda_0 + \lambda_1 \alpha + \dots + \lambda_{f-1} \alpha^{f-1}, \quad \lambda_i \in \mathbb{F}_p$$

ただし  $\alpha$  は  $\mathbb{F}_p$  上の  $f$  次の原始既約多項式の根の1つ。

**定理1.8** (Gleason-Pierce) ([1])

$C$  を自己双対  $[n, k, d]$  符号で任意の符号語についてその重さを割り切

るような自然数の定数  $c$  が存在するものとし、 $W_c(x, y)$  を  $C$  の重み多項

式とする。このとき以下の I-V のいずれかが成り立ち、I から IV のいずれ

の場合においても重み多項式は次のような形で表わされる。

$$W(x, y) = \sum_{r, s} k_{rs} f(x, y)^r g(x, y)^s.$$

ここで  $k_{rs} \in \mathbb{C}$ , また  $f, g$  は各タイプごとに定義される。

type I  $q=2, c=2$ , このとき  $2 \mid n, d \leq 2[n/8]+2, n=2r+8s$ ,

$$f(x, y) = x^2 + y^2 \quad g(x, y) = x^2 y^2 (x^2 - y^2)^2,$$

type II  $q=2$ ,  $c=4$ , このとき  $8|n$ ,  $d \leq 4[n/24]+4$ ,  $n=8r+24s$ ,

$$f(x, y) = x^8 + 14x^4 y^4 + y^8 \quad g(x, y) = x^4 y^4 (x^4 - y^4)^4,$$

type III  $q=3$ ,  $c=3$ , このとき  $4|n$ ,  $d \leq [n/12]+3$ ,  $n=4r+12s$

$$f(x, y) = x^4 + 8xy^3 \quad g(x, y) = y^3 (x^3 - y^3)^3,$$

type IV  $q=4$ ,  $c=2$ , このとき  $2|n$ ,  $d \leq [n/6]+2$ ,  $n=2r+6s$

$$f(x, y) = x^2 + 3y^2 \quad g(x, y) = y^2 (x^2 - y^2)^2,$$

type V  $W(x, y) = \{x^2 + (q-1)y^2\}^{n/2}$

## § 2 不変式論からの準備

$G$  を位数  $g$  の複素  $m$  次正方行列の群とする。

$$A = (a_1, \dots, a_m)^t \in G \quad (a_i: \text{行ベクトル}), \quad \mathbf{x} = (x_1, \dots, x_m),$$

$$f(\mathbf{x}) = f(x_1, \dots, x_m) \in \mathbb{C}[x_1, \dots, x_m] (= \mathbb{C}[\mathbf{x}])$$

としたとき、 $G$  は  $\mathbb{C}[\mathbf{x}]$  上に次のように作用する。

$$A \circ f(\mathbf{x}) = f(a_1 x^t, \dots, a_n x^t)。$$

任意の  $A \in G$  に対して  $A \circ f(\mathbf{x}) = f(\mathbf{x})$  となるとき  $f(\mathbf{x})$  は  $G$  の 不変式 と呼ばれる。

以下、 $I(G)$  を群  $G$  の不変式全体からなる環とする。

以下の定理は証明なしに述べる。( [9] )

### 定理 2.1

$$f(\mathbf{x}) \in \mathbb{C}[\mathbf{x}] \text{ ならば } \bar{f}(\mathbf{x}) = \frac{1}{g} \sum_{A \in G} A \circ f(\mathbf{x}) \in I(G)。$$

この定理は不変式を実際に計算するときに役立つ。

次に不変式環  $I(G)$  の生成元について考察する。

**定義 2.2**

$f_1, \dots, f_r \in \mathbb{C}[x]$  は  $p(f_1, \dots, f_r) \equiv 0$  となるような  $p \in \mathbb{C}[y_1, \dots, y_r]$  が存在するときは 代数的に従属 であると呼ばれる。

そうでないとき  $f_1, \dots, f_r$  は 代数的に独立 であると呼ばれる。

**定理 2.3**  $f_1, \dots, f_{m+1} \in \mathbb{C}[x]$  は代数的に従属である。

**定理 2.4**  $I(G)$  は  $m$  個の代数的に独立な元を持つ。

**定理 2.5**

$I(G)$  はその任意の元が  $f_1, \dots, f_{m+1}$  の有理関数で表わされるような  $m+1$  個の元  $f_1, \dots, f_{m+1}$  を持つ。

**定義 2.6**

任意の不変元が  $f_1, \dots, f_r$  ( $\in I(G)$ ) の多項式で表わされるとき  $f_1, \dots, f_r$  を  $I(G)$  の polynomial basis と呼ぶ。

**定理 2.7**  $I(G)$  は

$$n \leq \binom{m+g}{m}, \quad \deg f_i \leq g \quad \text{for } i=1, \dots, n$$

を満たす様な polynomial basis  $f_1, \dots, f_n$  を持つ。

**定理 2.8 (Molien)**

$a_d$  を  $G$  の斉次  $d$  次一次独立な不変元の数とする。 $G$  の Molien 級数を

$$\Phi_G(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d \quad \text{で定義すると、}$$

$$\Phi_G(\lambda) = \frac{1}{g} \sum_{A \in G} \frac{1}{\det(I - \lambda A)} \quad \text{となる。 ( } I \text{ は単位行列 )}$$

**定義 2.9**

$I(G)$  の polynomial basis  $f_1, \dots, f_n$  ( $n \geq m$ ) は次の条件を満たすとき good であるという。

(1)  $f_1, \dots, f_n$  は斉次多項式である。

(2)  $f_1, \dots, f_m$  は代数的に独立である。

(3)  $I(G) = \begin{cases} B & \text{if } n=m \\ B \oplus f_{m+1}B \oplus \dots \oplus f_nB & \text{if } n \geq m \text{ (} B = \mathbb{C}[f_1, \dots, f_m] \text{)} \end{cases}$

$d_i = \deg f_i$  ( $1 \leq i \leq n$ ) とする。このとき Molien 級数は

$$\Phi_G(\lambda) = \begin{cases} \frac{1}{\prod_{i=1}^m (1 - \lambda^{d_i})} & \text{(if } n=m) \\ \frac{1 + \sum_{j=m+1}^n \lambda^{d_j}}{\prod_{i=1}^m (1 - \lambda^{d_i})} & \text{(if } n > m) \end{cases} \quad \dots \text{ (#)}$$

の形に書ける。

$I(G)$  は必ずしも good polynomial basis をもつとは限らないようだが、幸いにも次のことが成り立っている。

**定理 2.10** ([3, Prop. 13])

$I(G)$  は常に good polynomial basis をもつ。

注 このことから Molien 級数はいつでも (#) の形に書けることが保証される。しかしこの逆は成り立つとは限らない。すなわち、Molien 級数が (#) の形に書けたからといって、それに対応する good polynomial basis が存在するとは限らない。

$$\frac{1}{1 - \lambda}$$

は

$$\frac{1 + \lambda}{1 - \lambda^2}$$

ともかける。そしてこの2つの式はともに (#) の形になっていることに注意されたい。実際、逆の成り立たない例が ([9, p.101]) にある。

### § 3 不変式論の符号理論への応用

$G$  を次の  $M, J$  で生成される複素 2 次正方形行列の群とする。

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad J = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

注  $G$  の位数は 192 で、 $G$  の元は次の形で表わせる。

$$\eta^v \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \cdot \eta^v \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix} \cdot \frac{\eta^v}{\sqrt{2}} \begin{pmatrix} 1 & \beta \\ \alpha & -\alpha \beta \end{pmatrix}$$

$$\alpha, \beta \in \{1, -1, i, -i\}, \eta = (1+i)/\sqrt{2}, 0 \leq v \leq 7.$$

#### 命題 3.1

$C$  を type II (定理 1.8) の  $[n, k]$  符号、 $W_C$  を  $C$  の重み多項式とする。

$\Rightarrow W_C$  は  $G$ -不変。

( $\because$ ) MacWilliams の恒等式より  $W_C$  は  $M$  で不変。又  $C$  は重偶符号である

から  $J$  でも不変。□

$G$  の Molien 級数は

$$\begin{aligned} \Phi_G(\lambda) &= \frac{1}{192} \left\{ \frac{1}{(1-\lambda)^2} + \frac{1}{1-\lambda^2} + \frac{1}{(1-\lambda)(1-i\lambda)} + \dots \right\} \\ &= \frac{1}{(1-\lambda^8)(1-\lambda^{24})} \\ &= (1+\lambda^8+\lambda^{16}+\lambda^{24}+\dots)(1+\lambda^{24}+\lambda^{48}+\lambda^{72}+\dots) \end{aligned}$$

この事から、

①  $I(G)$  の 1 でない元の最小次数は 8。

②  $I(G)$  の任意の元が 8 次の式  $f$  と 24 次の式  $g$  ( $f, g \in I(G)$ ) の多項式で表わされる。

とすることがわかる。

deg d	invariants	ad
0	1	1
8	f	1
16	$f^2$	1
24	$f^3, g$	2
32	$f^4, fg$	2
40	$f^5, f^2g$	2
48	$f^6, f^3g, g^2$	3
⋮	⋮	⋮

長さ 8, 24 の type II の符号でその重み多項式が代数的に独立ならばそれらを  $f, g$  とすることができる。

ところで type II の符号として次の 2 つの有名な符号がある。

$H_8$  ( Humming[8, 4, 4] 符号),  $G_{24}$  ( Golay[24, 12, 8] 符号)。

それぞれの重み多項式は

$$\theta = W_H = x^8 + 14x^4y^4 + y^8,$$

$$\phi' = W_G = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

これらは  $I(G)$  の元で、なおかつ代数的に独立であることがわかるので、

$$f = \theta \quad g = \phi' \quad \text{として良い。}$$

実際には  $\phi'$  は係数が大きく扱いにくいいため

$$\phi = (\theta^3 - \phi')/42 = x^4y^4(x^4 - y^4)^4 \quad \text{としておくと } \theta, \phi \text{ はそれぞれ 8 次と}$$

24 次の代数的に独立な  $I(G)$  の元となり  $f = \theta, g = \phi$  とできる。

以上のことにより次の定理が示される。

**定理3.2** 任意の  $G$ -不変な多項式は  $f, g$  の多項式で表わされる。

**定理3.3** Gleasonの定理(1.8)の type II での主張が得られる。

この定理を利用して実際にいくつかの符号の重み多項式を計算してみよう。

☆ 拡張 QR[48, 24, 12] 符号は type II の符号なので、その重み多項式

は  $G$ -不変。よって前定理より重み多項式  $W$  は

$$W(x, y) = \sum k_{rs} f^r(x, y) g^s(x, y), \quad 8r + 24s = 48$$

$$f(x, y) = x^8 + 14x^4y^4 + y^8, \quad g(x, y) = x^4y^4(x^4 - y^4)^4$$

と、表わされる。更に  $8r + 24s = 48$  を満たす  $r, s$  の組は

$(r, s) = (6, 0), (3, 1), (0, 2)$  のみなので、

$k_{60} = k_1, k_{31} = k_2, k_{02} = k_3$  とすると、

$$\begin{aligned} W(x, y) &= k_1 f^6 + k_2 f^3 g + k_3 g^2 \\ &= k_1 (x^{48} + 84x^{44}y^4 + 2946x^{40}y^8 \dots) + k_2 (x^{44}y^4 + 38x^{40}y^8 + \dots) \\ &\quad + k_3 (x^{40}y^8 - \dots) \\ &= x^{48} + 17296x^{36}y^{12} + 535095x^{32}y^{16} + 3995376x^{28}y^{20} + 7681680x^{24}y^{24} \\ &\quad + 3995376x^{20}y^{28} + 535095x^{16}y^{32} + 17296x^{12}y^{36} + y^{48} \end{aligned}$$

(最小重さ  $d=12$  より  $k_1=1, k_2=-84, k_3=246$ )

☆ 次に [72, 36, 16] 符号の重み多項式を計算してみる。但しこの符号が存

在するかどうかについてはまだわかっていない。前の例と同様の方法で

$(r, s) = (9, 0), (6, 1), (3, 2), (0, 3)$

と計算できる。そうすると

$$\begin{aligned}
W(x, y) = & x^{72} + 249849x^{56}y^{16} + 18106704x^{52}y^{20} + 462962955x^{48}y^{24} \\
& + 4397342400x^{44}y^{28} + 16602715899x^{40}y^{32} + 25756721120x^{36}y^{36} \\
& + 16602715899x^{32}y^{40} + 4397342400x^{28}y^{44} + 462962955x^{24}y^{48} \\
& + 18106704x^{20}y^{52} + 249849x^{16}y^{56} + y^{72}
\end{aligned}$$

となることがコンピューターを使うことによりすぐに求められる。

( PC9801VX21上で Reduce3.3を使用。 )

typeⅢの符号で特別な場合については次の事がわかっている。

$C$  を自己双対3元  $[n, \frac{1}{2}n, d]$  符号とする。

$1 = (1, 1, \dots, 1) \in C$  と仮定する。 $V(x, y, z)$  を  $C$  の完全重み多項式とすると、

$$V(x, y, z) \in C[\alpha_{12}, \beta_6^2, \delta_{36}] \oplus \beta_6 \gamma_{18} C[\alpha_{12}, \beta_6^2, \delta_{36}]$$

(すなわち、 $V(x, y, z)$  は  $\alpha_{12}$ ,  $\beta_6^2$ ,  $\delta_{36}$  の多項式と、別のそのような多項式を  $\beta_6 \gamma_{18}$  倍した多項式との和として一意的に表わされる。)

$$\text{ここで,} \quad \alpha_{12} = a(a^3 + 8p^3) \quad , \quad \beta_6 = a^2 - 12b,$$

$$\gamma_{18} = a^6 - 20a^3p^3 - 8p^6, \quad \delta_{36} = p^3(a^3 - p^3)^3$$

$$\text{そして} \quad a = x^3 + y^3 + z^3, \quad p = 3xyz, \quad b = x^3y^3 + x^3z^3 + y^3z^3.$$

ここで  $\gamma_{18}^2 = \alpha_{12}^3 - 64\delta_{36}$  である。(多項式の添字は次数を表わす。)

(証明の概略)

$u \in C$  の成分が  $a$  個の  $0$ ,  $b$  個の  $1$ ,  $c$  個の  $2$  をもつとする。 $C$  は自己双対符号で  $1$  を含むから

$$u \cdot u = 0 \Rightarrow 3 \mid (b + c),$$

$$u \cdot 1 = 0 \Rightarrow 3 \mid (b - c) \Rightarrow 3 \mid b \text{ and } 3 \mid c,$$

$$1 \cdot 1 = 0 \Rightarrow 3 \mid (a + b + c) \Rightarrow 3 \mid a,$$

従って  $V(x, y, z)$  は

$$\begin{pmatrix} \omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, J_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}$$

$$\omega = e^{2\pi i / 3}$$

で不変である。また  $-u$  は  $a$  個の 0,  $c$  個の 1,  $b$  個の 2 をもち,  $1+u$  は

$a$  個の 0,  $c$  個の 1,  $b$  個の 2 をもつので  $V(x, y, z)$  は

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

で不変である。(すなわち 3 次の対称群  $S_3$  の作用で不変である。)

最後に, 定理 1.4 で  $q=3$  のとき  $V(x, y, z)$  は

$$M_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \quad \text{で不変である。}$$

これら 6 個の行列で生成される群  $G$  は, 位数 2592 で, 1944 個の

$$s^v \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^a & 0 \\ 0 & 0 & \omega^b \end{pmatrix} M_3^e \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^c & 0 \\ 0 & 0 & \omega^d \end{pmatrix}, \quad s = e^{2\pi i / 12}$$

と, 648 個の

$$s^v \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^a & 0 \\ 0 & 0 & \omega^b \end{pmatrix} P,$$

型の行列を含んでいる。ここで  $0 \leq v \leq 11$ ,  $0 \leq a, b, c, d \leq 2$ ,  $e=1$  or  $3$  で

$P \in S_3$  である。

そこで  $G$  の Molien 級数を計算すると,

$$\Phi_G(\lambda) = \frac{1 + \lambda^{24}}{(1 - \lambda^{12})^2 (1 - \lambda^{36})}$$

となることがわかる。また  $G = \langle J_3, M_3, S_3 \rangle$  であることもわかる。

$S_3$  で不変ということと、 $C$  の任意の元の重さは 3 で割り切れることから  $I(G) \in C[a, p, b]$  である。そこで  $a, p, b$  の多項式で  $J_3, M_3$  で不変なものを探そう。例えば  $\beta_6$  は  $J_3$  で不変だが、 $M_3$  によって  $-\beta_6$  に移される。このことを

$$\beta_6 \xleftrightarrow{J_3} \beta_6, \quad \beta_6 \xleftrightarrow{M_3} -\beta_6.$$

というように書く。

これより  $\beta_6^2$  は  $G$ -不変である。さらに,

$$a \xleftrightarrow{M_3} \frac{1}{\sqrt{3}}(a+2p) \xrightarrow{J_3} \frac{1}{\sqrt{3}}(a+2\omega p) \xleftrightarrow{M_3} \frac{i}{\sqrt{3}}(a+2\omega^2 p)$$

であるから  $a(a+2p)(a+2\omega p)(a+2\omega^2 p) = a(a^3 + 8p^3) = \alpha_{12}$

も  $G$  の不変式である。また,

$$\gamma_{18} \xleftrightarrow{J_3} \gamma_{18}, \quad \gamma_{18} \xleftrightarrow{M_3} -\gamma_{18}$$

より  $\beta_6 \gamma_{18}$  も  $G$  の不変式である。最後に,

$$p \xleftrightarrow{M_3} \frac{1}{\sqrt{3}}(a-p) \xrightarrow{J_3} \frac{1}{\sqrt{3}}(a-\omega p) \xleftrightarrow{M_3} \frac{i}{\sqrt{3}}(a-\omega^2 p)$$

は不変式  $p^3(a-p)^3(a-\omega p)^3(a-\omega^2 p)^3 = p^3(a^3 - p^3)^3 = \delta_{36}$  を与える。

$\alpha_{12}, \beta_6^2, \delta_{36}, \beta_6 \gamma_{18}$  が good polynomial basis になることは簡単に示すことができる。□

## § 4 終わりに

不変式の理論を使うといくつかのよい符号が存在しないことを示すことができる。

C を 2 元自己双対重偶  $[n, \frac{1}{2}n, d]$  符号とする。このとき、

$$W(x, y) = \sum_{i=0}^{\mu} a_i \theta^{j-3i} \phi^i \dots (*)$$

ここで、 $n = 8j = 24\mu + 8\nu$ ,  $\nu = 0, 1 \text{ or } 2$ ,  $\theta, \phi$  は § 3 で定義された多項式とする。

今 (\*) の  $\mu + 1 = [n/24] + 1$  個の係数  $a_i$  を

$$W(x, y) = x^n + A_{4\mu+4} x^{n-4\mu-4} y^{4\mu+4} + \dots$$

となるように選ぶ。すなわち  $a_i$  は  $W(x, y)$  の先頭の係数をできるだけ多く 0 にするように選ぶ。このとき  $a_i$  達は一意的に決まる ([8], [9])。この重み多項式 ( $W^*$  とおく) は自己双対符号の中で最小重さが最大となるものである。 $W^*$  を 極值的重み多項式 と呼ぶ。

もし  $W^*$  を重み多項式として持つ符号が存在すればその最小重さは  $A_{4\mu+4}$  が 0 でない限り  $4\mu + 4$  である。

$A_{4\mu+4}$  は次のようになることがわかっている。 ([7])

$$\frac{\binom{n}{5} \binom{5\mu-2}{\mu-1}}{\binom{4\mu+4}{5}}, \quad \text{if } n = 24\mu,$$

$$\frac{1}{4} n(n-1)(n-2)(n-4) \frac{(5\mu)!}{\mu!(4\mu+4)!}, \quad \text{if } n = 24\mu + 8$$

$$\frac{3}{2}n(n-2) \frac{(5\mu+2)!}{\mu!(4\mu+4)!}, \quad \text{if } n = 24\mu + 16$$

これらは決して0にならない。よって次の定理が成り立つ。

**定理4.1**

長さ  $n$  の 2元自己双対重偶符号の最小重さは高々  $4[n/24]+4$  である。

最小重さが  $4[n/24]+4$  である 2元自己双対重偶符号の存在性についてはあまりわかっていない。 $n \leq 48$  ともう少し大きい値でいくつか存在することが知られている。

未だその存在が知られていない最小の長さが  $n = 72$  である。また、このような符号が有限個しかないことが次の定理からわかる。

**定理4.2** ([6])

$b$  を任意の定数とする。(\*) の  $a_i$  を

$$W(x, y) = x^n + A_{4d} x^{n-4d} y^{4d} + \dots \quad (d \geq n/6 - b)$$

となるように選ぶ。すると十分大きい  $n$  に対して、ある係数  $A_i$  が負になる。よって長さ  $n$  の 2元自己双対重偶符号は十分大きな  $n$  に対しては存在しない。

似たようなことが 3元符号についても成り立つ。

**定理4.3** ([6])

$b$  を任意の定数とする。最小重さが  $3[n/12]+3-3b$  以上である長さ  $n$  の 3元自己双対符号は十分大きな  $n$  に対しては存在しない。

## 参考文献

- [1] E.F. Assmus "Coding and Combinatorics." J. Applied Math.  
Rev. 16 (1974) p349-388.
- [2] J.H. Conway, N. J. A. Sloane "Sphere packing, lattices and codes."  
Springer Verlag.
- [3] M. Hochster, J. A. Eagon "Cohen-Macaulay rings, invariant theory,  
and the generic perfection of determinantal loci." Amer. J. Math.  
93 (1971)p1020-1058.
- [4] F. J. MacWilliams, C. L. Mallows, N. J. A. Sloane "Generalization of  
Gleason's Theorem on Weight Enumerators of self-dual codes."  
IEEE IT-18 (1972) p794-805.
- [5] F. J. MacWilliams, N. J. A. Sloane "The theory of error correcting  
codes." North-Holland.
- [6] C. L. Mallows, A. M. Odlyzko, N. J. A. Sloane "Upper bounds for  
modular forms, lattices, and codes." J. Alg. 36 (1975) p68-76.
- [7] C. L. Mallows, N. J. A. Sloane "An upper bound for self-dual cod-  
es." Information and Control 22 (1973) p188-200.
- [8] V. Pless "An introduction to the theory of error correcting  
codes." Wiley Interscience.
- [9] N. J. A. Sloane "Error correcting codes and invariant theory."  
Ame. Math. Monthly 84 (1977) p82-107.