数理解析研究所講究録
第671巻 1988年 81-95

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ったので、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。

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

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。

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

[n,k]符号Cの双対符号 $C^\perp$ を以下のように定義する

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

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。

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

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

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 $s(v) = (s_0(v), s_1(v), \cdots, s_{q-1}(v))$ を各 $s_i(v)$について $s_i(v) = \#\{j \mid v_j = \omega_i, v=(v_1,\cdots,v_n)\}$ で定義する。

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

定義1.6

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

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

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

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

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

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

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

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

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

ただしα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 $2\mid n$, $d\leqq 2[n/8]+2$, $n=2r+8s$,

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

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

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

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

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

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

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

typeⅤ　$W(x,y)=\{x^2+(q-1)y^2\}^{n/2}$

§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。

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

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

としたとき、GはC[x]上に次のように作用する。

$$A\circ f(\mathbf{x})=f(a_1x^t,\cdots,a_nx^t)。$$

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<u>不変式</u>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])

<u>定理2.1</u>

$f(\mathbf{x})\in \mathbb{C}[\mathbf{x}]$ 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

$f_1, \cdots, f_r \in \mathbb{C}[x]$ は $p(f_1, \cdots, f_r) \equiv 0$ となるような $p \in \mathbb{C}[y_1, \cdots, y_r]$ 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 $f_1, \cdots, f_r$ は代数的に独立であると呼ばれる。

定理2.3 $f_1, \cdots, f_{m+1} \in \mathbb{C}[x]$ 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 $f_1, \cdots, f_{m+1}$ の有理関数で表わされるような m+1個の元 $f_1, \cdots, f_{m+1}$ を持つ。

定義2.6

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

定理2.7 I(G)は

$$n \leq \begin{pmatrix} m+g \\ m \end{pmatrix} \quad , \deg f_i \leq g \quad \text{for } i=1, \cdots, n$$

を満たす様な polynomial basis $f_1, \cdots, f_n$ 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 $\Phi_G(\lambda) = \sum_{d=0}^{\infty} a_d \lambda^d$ で定義すると、

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

定義2.9

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

(1)$f_1,\cdots,f_n$ は斉次多項式である。

(2)$f_1,\cdots,f_m$ は代数的に独立である。

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

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

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

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次正方行列の群とする。

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

注 Gの位数は 192 で、Gの元は次の形で表わせる。

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

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

命題3.1

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

$\Longrightarrow$ 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

$$\Phi_G(\lambda)=\frac{1}{192}\left\{\frac{1}{(1-\lambda)^2}+\frac{1}{1-\lambda^2}+\frac{1}{(1-\lambda)(1-i\lambda)}+\cdots\right\}$$

$$=\frac{1}{(1-\lambda^8)(1-\lambda^{24})}$$

$$=(1+\lambda^8+\lambda^{16}+\lambda^{24}+\cdots)(1+\lambda^{24}+\lambda^{48}+\lambda^{72}+\cdots)$$

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∈I(G)）の多項式で表わされる。

と言うことがわかる。

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 typeⅡ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 typeⅡ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

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

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

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、

$f = \theta$　$g = \phi'$　として良い。

実際にはϕ'は係数が大きく扱いにくいため

$\phi = (\theta^3 - \phi')/42 = x^4y^4(x^4 - y^4)^4$ としておくとθ，ϕ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 typeⅡ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 typeⅡ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

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

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

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、

$$W(x,y)=k_1f^6+k_2f^3g+k_3g^2$$

$$=k_1(x^{48}+84x^{44}y^4+2946x^{40}y^8\cdots)+k_2(x^{44}y^4+38x^{40}y^8+\cdots)$$

$$+k_3(x^{40}y^8-\cdots)$$

$$=x^{48}+17296x^{36}y^{12}+535095x^{32}y^{16}+3995376x^{28}y^{20}+7681680x^{24}y^{24}$$

$$+3995376x^{20}y^{28}+535095x^{16}y^{32}+17296x^{12}y^{36}+y^{48}\ .$$

(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

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

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。

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

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

（すなわち，$V(x,y,z)$ は α_{12}，β_6^2，δ_{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。）

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

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

そして $a=x^3+y^3+z^3$，$p=3xyz$，$b=x^3y^3+x^3z^3+y^3z^3$.

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

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

$u \cdot 1 = 0 \Rightarrow 3 \mid (b - c) \Rightarrow 3 \mid b$ 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

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

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

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

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

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

$$M_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$ 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

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

と, 648 個の

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

型の行列を含んでいる。ここで $0 \leqq \upsilon \leqq 11$, $0 \leqq a, b, c, d \leqq 2$, $e=1$ 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 $I(G) \in \mathbb{C}[a, p, b]$ 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 β_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

$$\beta_6 \overset{J_3}{\longleftrightarrow} \beta_6, \quad \beta_6 \overset{M_3}{\longleftrightarrow} -\beta_6 .$$

というように書く。

これより β_6^2 は G-不変である。さらに,

$$a \overset{M_3}{\longleftrightarrow} \frac{1}{\sqrt{3}}(a+2p) \overset{J_3}{\longrightarrow} \frac{1}{\sqrt{3}}(a+2\omega p) \overset{M_3}{\longleftrightarrow} \frac{i}{\sqrt{3}}(a+2\omega^2 p)$$

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,

$$\gamma_{18} \overset{J_3}{\longleftrightarrow} \gamma_{18}, \quad \gamma_{18} \overset{M_3}{\longleftrightarrow} -\gamma_{18}$$

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

$$p \overset{M_3}{\longleftrightarrow} \frac{1}{\sqrt{3}}(a-p) \overset{J_3}{\longrightarrow} \frac{1}{\sqrt{3}}(a-\omega p) \overset{M_3}{\longleftrightarrow} \frac{i}{\sqrt{3}}(a-\omega^2 p)$$

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、

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

ここで、$n = 8j = 24\mu + 8\nu$, $\nu = 0, 1$ or 2 , θ, ϕ 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

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

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<u>極値的重み多項式</u>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]）

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

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

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

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

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

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.Assumus "Coding and Combinatorics." J.Applied Math. Rev.16 (1974) p349-388.

[2] J.H.Conway, N.J.A.Sloane "Sphere packing,lattices and codes." Splinger 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 codes." 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.