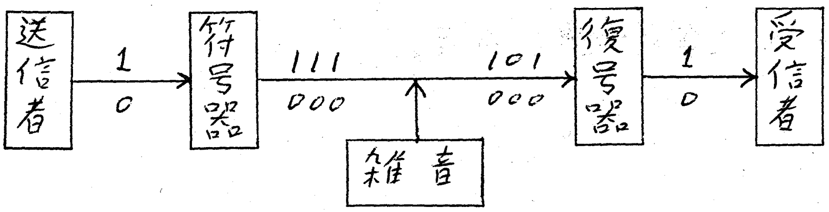
数理解析研究所講究録
第 444 巻 1981 年 180-197

符号理論への不変式論の応用

北大 理学部　　吉田知行

§1. 符号(コード)

符号理論はShannonに始まるといわれている(1948).



今送信者が"0"と"1"から成る情報を受信者に向けて送るとする。しかしこのままの形で送ると雑音のため0と1が入れ換わって、相手方に正しく受け取られないかもしれない。そこで符号器(encoder)によって、"0"を"000"に、"1"を"111"に変換して送信することとする。こうすれば例えば"101"が送られてきた場合は、多数決によって"1"と解釈すればよい。即ち1ビットの情報を送るのに000と111を用い、他の6個のベクトルはエラーを訂正するのに用いるのである。こうすればエラーの確率はずっと小さくなる。この例のコー

ド $\{000, 111\}$ は，実際は3倍もの時間がかかるため，良いコードとは言えない．情報理論的に良いコードを求めるのが符号理論の最大の目標である．最近では通信ばかりでなく，計算機のメモリシステム等でも誤り訂正符号が用いられている．

$\mathbb{F}_q$ を q 元体，$\mathbb{F}_q^n$ を $\mathbb{F}_q$ 上の n 次元ベクトル空間とする．各 $x=(x_1,\cdots,x_n)\in\mathbb{F}_q^n$ と $y=(y_1,\cdots,y_n)\in\mathbb{F}_q^n$ に対し，

$$\partial(x,y):=\#\{i \mid 1\le i\le n,\ x_i\ne y_i\}$$

とおくと，$(\mathbb{F}_q^n,\partial)$ は距離空間になる．∂ を Hamming 距離という．

$$w(x):=\partial(0,x)=\#\{i \mid x_i\ne 0\}$$

を x の重さ(weight)と言う．

定義 ($\mathbb{F}_q$ 上の線型) コードとは，$\mathbb{F}_q^n$ の部分空間のことである．n を C の長さ，$k=\dim C$ をコードの次元という．

$$d:=d(C):=\min\{w(x) \mid 0\ne x\in C\}$$

を C の最小距離という．このような C を $[n,k,d]$-コードという．このコードは $[(d-1)/2]$ 個のエラーを訂正できる．

定義．C を $\mathbb{F}_q$ 上の $[n,k,d]$-コードとする．$A_i:=\#\{u\in C \mid w(u)=i\}$ とおく．このとき，多項式

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

を C の重み分布多項式(weight enumerator) という．さらに

$\mathbb{F}_q$ の元を $\omega_0=0, \omega_1, \cdots, \omega_{q-1}$ とする．$u=(u_1,\cdots,u_n)\in C$ に対し，$s_i:=s_i(u):=\#\{j \mid u_j=\omega_i\}$，$comp(u):=(s_0,\cdots,s_{q-1})$ とおく．さらに $t=(t_0,\cdots,t_{q-1})$ に対し，$A(t):=\#\{u\in C \mid comp(u)=t\}$ とおく．このとき，q 変数多項式

$$V_C(z_0,\cdots,z_{q-1}):=\sum_t A(t)z_0^{t_0}\cdots z_{q-1}^{t_{q-1}}$$
$$=\sum_{u\in C} z_0^{s_0(u)}\cdots z_{q-1}^{s_{q-1}(u)}$$

を完備重み分布関数という．これは n 次の斉次多項式である．

定義．C を $\mathbb{F}_q$ 上の $[n,k,d]$-コードとする．C の k 個の基底を $x_1=(x_{11},\cdots,x_{1n}),\cdots,x_k=(x_{k1},\cdots,x_{kn})$ とする．$k\times n$ 行列 $G:=(x_{ij})$ を C の生成行列という．$(n-k)\times n$ 行列 H で，階数 $n-k$ で $GH^t=0$ なるものをパリティ検査行列（parity check matrix）という．$C=\{u\in\mathbb{F}_q^n \mid xH^t=0\}$ である．

生成行列 G として $(I_k \mid G')$ の形のものがとれ，パリティ検査行列 H として，$(-G'^t \mid I_{n-k})$ をとれる．このような G と H を選んだ時，送信者は $(u_1,\cdots,u_k)$ を，$(x_1,\cdots,x_n)=(u_1,\cdots,u_k)G$（ここで，$x_1=u_1,\cdots,x_k=u_k$）の形に符号化して送信する．$(x_1',\cdots,x_n')$ を受信した受信者は (i) $(x_1',\cdots,x_n')H^t=0$ ならエラーは起こらず（このとき $(x_1',\cdots)\in C$），$(x_1',\cdots,x_k')$ がもとのデータだと判断する．また (ii) $(x_1',\cdots,x_n')H^t\neq 0$ ならエラーが起こっているので，訂正可能な場合は訂正してもとのデータを復する．

コードに関する工学的な要求として次があげられる.

(1) nが小 (符号化が速い),

(2) kが大 (多くのデータを送れる),

(3) dが大 (誤まり訂正能力が大きい).

これらの条件は数学的に見ても興味深い.

§2. コードの例.

(1) $\{(a, \cdots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$. これは $\mathbb{F}_q$ 上の $[n, 1, n]$-コードで,「くり返しによるコード」とか「多数決によるコード」と呼ばれる. 重さ分布関数は,

$$V_C(z_0, \cdots, z_{q-1}) = \sum_{i=0}^{q-1} z_i^n$$

$$W_C(x, y) = x^n + (q-1)y^n.$$

(2) Hamming コード H_n. $n = 2^r - 1$, $k = n - r$. パリティ検査行列 H は, 長さ r の $(0,1)$-列ベクトル $(\neq 0)$ $2^r - 1$ 個からなる $r \times n$-行列である. $r = 3$ なら

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

H_n は $[2^r - 1, n - r, 3]$-コードである.

(3) 拡大コード. C を $\mathbb{F}_2$ 上の $[n, k, d]$-コードとする. $\exists c \in C$ s.t. $w(c)$ が奇数, と仮定する. C のパリティ検査行列を H とする. 次の $(n-k+1) \times (n+1)$ 行列をパリティ検査行列と

するコード$\hat{C}$をCの拡大という；

$$\hat{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ & H & & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{pmatrix}.$$

例えばHammingコードH_7から拡大HammingコードH_8が得られるが，これは[8,4,4]-コードである．一般に[n,k,d]-コードの拡大は[$n+1$,k,$d+1$]-コードであり，

$$\hat{C} = \{(x_1,\cdots,x_{n+1}) \in \mathbb{F}_2^{n+1} \mid (x_1,\cdots,x_n) \in C,\ x_1+\cdots+x_{n+1}=0\}.$$

(4) <u>Binary Golay codes</u> これは$\mathbb{F}_2$上の[23,12,7]-コードG_{23}である．その拡大コードG_{24}もGolayコードという．G_{24}の生成行列は次である．

$$G = \begin{array}{c}
\begin{array}{cccccccccccccccccccccccc} \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty' & 0' & 1' & 2' & 3' & 4' & 5' & 6' & 7' & 8' & 9' & 10' \end{array} \\
\left[\begin{array}{c|ccccccccccc|c|ccccccccccc}
1 & 1 & & & & & & & & & & & & 1 & 1 & & 1 & 1 & 1 & & & & 1 & \\
1 & & 1 & & & & & & & & & & & & 1 & 1 & & 1 & 1 & 1 & & & & 1 \\
1 & & & 1 & & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & & \\
1 & & & & 1 & & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & & \\
1 & & & & & 1 & & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 & \\
1 & & & & & & 1 & & & & & & & & & & 1 & & 1 & 1 & & 1 & 1 & 1 \\
1 & & & & & & & 1 & & & & & & 1 & & & & 1 & & 1 & 1 & & 1 & 1 \\
1 & & & & & & & & 1 & & & & & 1 & 1 & & & & 1 & & 1 & 1 & & 1 \\
1 & & & & & & & & & 1 & & & & 1 & 1 & 1 & & & & 1 & & 1 & 1 & \\
1 & & & & & & & & & & 1 & & & & 1 & 1 & 1 & & & & 1 & & 1 & 1 \\
1 & & & & & & & & & & & 1 & & 1 & & 1 & 1 & 1 & & & & 1 & & 1 \\
\hline
 & & & & & & & & & & & & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right]
\end{array}$$

(5) <u>Ternary Golay codes</u> G_{11}, G_{12}. これらは$\mathbb{F}_3$上の[12,6,5]-コードと[12,6,6]-コードである

<u>重み分布関数について</u>．

HammingコードH_n ($n=2^r-1$)の重み分布関数

$$W_C(x,y) = \frac{1}{n+1}\{(x+y)^n + n(x+y)^{(n-1)/2}(x-y)^{(n+1)/2}\}.$$

拡大Hamming コード H_8 について，

$$W_C(x,y) = x^8 + 14x^4y^4 + y^8.$$

Golay コード G_{23}，G_{24} について，

$$W_{G_{23}}(x,y) = x^{23} + 253x^{16}y^7 + 506x^{15}y^8 + 1288x^{12}y^{11} + 1288x^{11}y^{12} + 506x^8y^{15} + 253x^7y^{16} + y^{23}.$$

$$W_{G_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

Golay コード G_{12} について（完備）重み分布関数

$$V_{G_{12}}(x,y,z) = x^{12} + y^{12} + z^{12} + 22(x^6y^6 + x^6z^6 + y^6z^6) + 220(x^6y^3z^3 + x^3y^6z^3 + x^3y^3z^6)$$

$$W_{G_{12}}(x,y) = x^{12} + 3y^{12} + 204x^6y^6 + 440x^3y^9.$$

自己同型群について．C を $[n,k,d]$-コードとする．対称群 S_n の元 σ は自然に $\mathbb{F}_2^n$ に作用している．σ が $C \subseteq \mathbb{F}_2^n$ を動かさない時 σ を C の自己同型という．C の自己同型全体のなす群を $Aut(C)$ と書く．

$$Aut(H_7) \cong GL(3, \mathbb{F}_2)$$

$$Aut(G_{23}) \cong M_{23},\quad Aut(G_{24}) \cong M_{24},$$

$$Aut(G_{11}) \cong M_{11},\quad Aut(G_{12}) \cong M_{12}.$$

ここで M_n は Mathieu 群．

なお重み分布関数を実際に求めるのは大変である．自己双対コード（G_{24}, G_{12} など）については次節の方法が有力である．

6.

§3. Macwilliams の定理.

<u>定義</u> C を $[n,k,d]$-コードとする.

$$C^{\perp} := \{(x_1,\cdots,x_n)\in \mathbb{F}_q^n \mid \textstyle\sum_i x_i y_i = 0 \ \text{for}\ {}^{\forall}(y_1,\cdots)\in C\}.$$

このとき $C^{\perp}$ を C の<u>双対コード</u>という. これは $[n, n-k, d']$-コードである(ある d' に対して). $C=C^{\perp}$ のとき C を<u>自己双対コード</u>という. 自己双対コードについて $k=n/2$.

拡大 Hamming コード H_8, Golay コード G_{12}, G_{24} は自己双対コードである. 変わったものとしては有限射影平面から得られるコードがある. $(P,\mathcal{L})$ を位数 n の有限射影平面とする. A をその結合行列とすると, A は $\mathbb{F}_2$ 上の $v\times v$ 行列とみなせる($v=n^2+n+1$ = 点の個数). C を A の行ベクトルで生成された $\mathbb{F}_2^v$ の部分空間とする. 組合せ論の大問題として, n が素数巾であることが予想されており, 実際 $n\leq 6$ は証明されている. $n=10$ が次の問題となるが, この場合は C の拡大コード $\hat{C}$ が $[112, 56, 12]$-自己双対コードになる(E.F. Assmus, J.G. Thompson). しかしその重み分布関数は完全には決まっていない.

さて双対コードの(完備)重み分布関数を元のコードの重み分布関数から計算するのが Macwilliams の定理である.

<u>定理</u>(Macwilliams). C が $\mathbb{F}_q$ 上の $[n,k,d]$-コードなら,

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

$q=2$ の場合の証明を述べておく.

補題. $F:=\mathbb{F}_2$, A: アーベル群, $f: F^n \longrightarrow A$ を写像, C を F 上の $[n,k,d]$-コードとする. f の Hadamard 変換を次で定義する:

$$\hat{f}(u) := \sum_{v\in F^n} (-1)^{u\cdot v} f(v) \qquad \forall u \in F^n.$$

このとき Poisson の和公式が成立する:

$$\frac{1}{2^k}\sum_{u\in C}\hat{f}(u) = \sum_{u\in C^\perp} f(u).$$

(証明)
$$\sum_{u\in C}\hat{f}(u) = \sum_{u\in C}\sum_{v\in F^n}(-1)^{u\cdot v} f(v)$$
$$= \sum_{v\in F^n}\Big(\sum_{u\in C}(-1)^{u\cdot v}\Big) f(v).$$

各 $v\in F^n$ に対し, $\chi_v : C \longrightarrow \{\pm 1\} : u \longmapsto (-1)^{u\cdot v}$ は C の指標だから, 直交関係により

$$\chi_v = 1_C \Rightarrow \sum_{u\in C}(-1)^{u\cdot v} = |C| = 2^k$$

$$\chi_v \neq 1_C \Rightarrow \sum_{u\in C}(-1)^{u\cdot v} = 0.$$

ところが, $\chi_v = 1_C \Leftrightarrow (-1)^{u\cdot v} = \quad \forall u\in C \Leftrightarrow uv = 0 \quad \forall u \in C$

$\Leftrightarrow v \in C^\perp$

$$\therefore \sum_{u\in C}\hat{f}(u) = \sum_{v\in C^\perp} 2^k f(v) = 2^k \sum_{v\in C^\perp} f(v). \quad \text{QED.}$$

(定理の証明) $f(u) := x^{n-w(u)} y^{w(u)}$ とおくと,

$$\sum_{v\in C^\perp} f(v) = W_{C^\perp}(x,y).$$

一方ベクトルを成分ごとに計算すると,

$$\hat{f}(u) = \sum_{v\in F^n}(-1)^{u\cdot v} f(v) = \sum_{v\in F^n}(-1)^{u\cdot v} x^{n-w(v)} y^{w(v)}$$

$$= \sum_{(v_1,\cdots)\in F^n} (-1)^{u_1v_1+\cdots+u_nv_n} \prod_{i=1}^{n} x^{1-v_i} y^{v_i}$$
$$= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_iv_i} x^{1-v_i} y^{v_i}$$
$$= \prod_{i=1}^{n} \sum_{w=0}^{1} (-1)^{u_iw} x^{1-w} y^{w}$$
$$= (x+y)^{n-w(u)} (x-y)^{w(u)}.$$

補題より定理が得られる．　　　　　　　　　　　　QED.

系．C が $[n, n/2, d]$-自己双対コードなら，
$$W_C(x,y) = W_C\left(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right).$$

さて不変式論の簡単な結果を使うと自己双対コードの重み分布関数がきわめて特殊な形をしていることがわかる．

定理（Gleason）．C を $\mathbb{F}_q$ 上の自己双対 $[n, k, d]$ コードとすると，重み分布関数 $W_C(x,y)$ は，$g := x^2+(q-1)y^2$ と $h := xy-y^2$ の多項式として表わせる：
$$W_C(x,y) \in \mathbb{C}[g, h].$$

（証明）　$A := \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$，$B := \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$．　$(A^2 = I)$

とすれば，(1) $W_C(x,y)$ は A によって不変（Macwilliams），(2) $W_C(x,y)$ は B によって不変（W_C が $n=2k$ 次の斉次多項式だから）．$R = \mathbb{C}[x,y] = \bigoplus_{m=0}^{\infty} R_m$，$R_m$ は m 次の斉次多項式全体，$G := \langle A, B\rangle \leq GL(2,\mathbb{C})$ とすれば，$W_C(x,y) \in R^G$．

そこで Molien (Poincare) 級数を計算すると,

$$P(R^G, t) := \sum_{m=0}^{\infty} (\dim R_m^G)\, t^m$$

$$= \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(I - t\sigma)} \qquad \text{(Molien の定理)}$$

$$= \frac{1}{(1-t^2)^2} = (1+t^2+t^4+\cdots)(1+t^2+t^4+\cdots)$$

不変式論より $R^G = \mathbb{C}[g, h]$, $g = x^2+(q-1)y^2$, $h = 2xy - y^2$ となるから定理が示された. Q.E.D.

以上のことは完備重み分布関数についていえる.

<u>定理.</u> C を $\mathbb{F}_q$ 上の $[n,k,d]$-コードとする. $\mathbb{F}_q$ の元を $\{\omega_0 = 0, \omega_1, \cdots, \omega_{q-1}\}$ と並べておく. $\chi : \mathbb{F}_q \longrightarrow \mathbb{C}$ を加法群 $\mathbb{F}_q^+$ の自明でない指標とする. このとき完備重み分布関数について次が成立する.

$$V_{C^\perp}(z_0, \cdots, z_{q-1}) = \frac{1}{q^k} V_C\left(\sum_{i=0}^{q-1} \chi(\omega_0 \omega_i) z_i, \cdots, \sum_{i=0}^{q-1} \chi(\omega_{q-1}\omega_i) z_i\right),$$

この定理の応用として, Gleason の定理を $\mathbb{F}_3$ に拡張した Sloane の定理がある.

<u>定理.</u> $V(x, y, z)$ を, $\mathbb{1} = (1, \cdots, 1)$ を含む $\mathbb{F}_3$ 上の自己双対 $[n, n/2, d]$-コードの完備重み分布関数とすると,

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

ここで, $\alpha_{12} = a(a^3 + 8p^3)$, $\beta_6 = a^2 - 12b$, $\gamma_{18} = a^6 - 20a^3p^3 - 8p^6$, $\delta_{36} = p^3(a^3 - p^3)^3$, さらに $a = x^3+y^3+z^3$,

$p=3xyz$，$b=x^3y^3+x^3z^3+y^3z^3$ である．($\gamma_{18}^2=\alpha_{12}^3-64\delta_{36}$).

（証明の概略）まず $\mathbf{1}\in C=C^{\perp}$ より $V\in\mathbb{C}[x^3,y^3,z^3]$ となる．よって $V(x,y,z)$ は $\mathrm{diag}(\omega^i,\omega^j,\omega^k)$ によって不変．ここで $\omega=e^{2\pi\sqrt{-1}/3}$．次に $u\in C$ なら $-u\in C$，$\mathbf{1}+u\in C$ 等によって $V(x,y,z)$ は任意の3次の置換行列によって不変．最後に，定理より $V(x,y,z)$ は

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

によって不変．したがってこれら3種類の行列の生成する群 G によって，$V(x,y,z)$ は不変である．なお $|G|=2^5\cdot3^4$．第2段として，$G\subseteq GL(3,\mathbb{C})$ の Molien 級数を計算すると，

$$P(R^G,t)=\frac{1+t^{24}}{(1-t^{12})^2(1-t^{36})}$$

あとは不変式論の知識を使って，不変式環の多項式基底を求める．

§4．不変式論から．

符号理論で使われる不変式論の結果は古典的なものであるが，一応よく使われる結果を述べておこう．

G を $GL(n,\mathbb{C})$ の有限部分群，$R=\mathbb{C}[x_1,\cdots,x_n]$ とすると，G は R に（多元環準同型として）作用する：

$$f^{\sigma}(X_1,\cdots,X_n) := f\left(\sum_i a_{1i}X_i,\cdots,\sum_i a_{ni}X_i\right),$$

$$\sigma = (a_{ij}) \in G \subseteq GL(n,\mathbb{C}).$$

Gによる不変式環を $R^G=\{f\in R \mid f^{\sigma}=f\ \forall\sigma\in G\}$ とし，d次の斉次多項式のなすRの部分加群を R_d，$R_d^G = R_d \cap R^G$ とすれば，$R=\bigoplus_{d=0}^{\infty} R_d$，$R^G=\bigoplus_{d=0}^{\infty} R_d^G$ となる．Molien (Poincaré) 級数を次で定義する：

$$P_G(t) := \sum_{n=0}^{\infty} (\dim R_n^G)\, t^n \in \mathbb{C}[[t]].$$

<u>定理</u>（Molien, 1897）

$$P_G(t) = \frac{1}{|G|}\sum_{\sigma\in G}\frac{1}{\det(I-t\sigma)}.$$

<u>定理</u>（Hochster-Eagon, 1971）. R^G は Cohen-Macaulay 環．したがって斉次多項式 $\theta_1,\cdots,\theta_m$, $\eta_1,\cdots,\eta_t$ が存在して，

(i) $\theta_1,\cdots,\theta_m$ は代数的に独立，

(ii) $R^G = \bigoplus_{i=1}^{t} \mathbb{C}[\theta_1,\cdots,\theta_m]\eta_i$.

（注意）上の定理で，$d_i=\deg\theta_i$，$e_i=\deg\eta_i$ のときは，

$$P_G(t) = \left(\sum_{i=1}^{t} t^{e_i}\right)\Big/\prod_{j=1}^{m}(1-t^{d_j}).$$

<u>定理</u>．$R^G=\mathbb{C}[\theta_1,\cdots,\theta_m]$ で $\theta_1,\cdots,\theta_m$ が代数的に独立斉次式 $\Longleftrightarrow$ Gがユニタリ reflection で生成される．

しかも $d_i=\deg\theta_i$ なら，$|G|=d_1\cdots d_m$，$\sum(d_i-1)=\#\{u.\ \text{refl. in}\ G\}$.

§5、応用.

以下Cは$\mathbb{F}_q$上の長さnの自己双対コードとし、次の問題を考える.

問題. nとqを与えたとき、$\mathbb{F}_q$上の長さnの自己双対コードは最大いくつまでのエラーを訂正(または検出)できるか? 即ち次の量を求めよ.

$$d^* := \mathrm{Max}\left\{ d(C) \;\middle|\; \begin{array}{l} C\text{は}\mathbb{F}_q\text{上の長さ}n\text{の} \\ \text{自己双対コード} \end{array} \right\}.$$

一般に$d = d(C)$のとき、Cの重み分布関数について、

$$W_C(x, y) = x^n + A_d x^{n-d} y^d + A_{d+1} x^{n-d-1} y^{d+1} + \cdots,$$

$$A_1 = \cdots = A_{d-1} = 0,\quad A_d \neq 0,\quad A_i \geqq 0\ (\forall i).$$

定理(Gleason, Pierce, Turyn). $t > 1$を自然数とする. 任意の$u \in C$に対し$wt(u)$がtの倍数で、Cはnontrivialと仮定する. このときCは次の4つの型のどれかになる.

Type	q	t	d(C)
I*	2	2	$\leqq 2[n/8]+2$
II	2	4	$\leqq 4[n/24]+4$
III	3	3	$\leqq 3[n/12]+3$
IV	4	2	$\leqq 2[n/6]+2$.

*) Type IIに属さないもの. [ ]はGauss記号

以下 Type II のコード C について $d := d(C) \leqq 4[n/24]+4$ を示そう，$w(x) \equiv 0\ (4)\ (^\forall x \in C)$ だから，

$$i \not\equiv 0\ (4) \Rightarrow A_i := \#\{u \in C \mid w(u) = i\} = 0.$$

$$\therefore W_C(x,y) = \sum_{i=0}^{[n/4]} A_{4i}\, x^{n-4i} y^{4i}.$$

$$\therefore W_C(x,y) = W_C(x, \sqrt{-1}\, y).$$

したがって $W_C(x,y)$ は $\begin{pmatrix} 1 & \\ & \sqrt{-1} \end{pmatrix}$ で不変．Macwilliams の定理によって，$W_C(x,y)$ は

$$G = \left\langle \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \right\rangle \subseteq GL(2, \mathbb{C})$$

で不変となる．$|G| = 64 \times 3$ である．Molien 級数は

$$P_G(t) = \frac{1}{(1-t^4)(1-t^8)}.$$

不変式論により，$W_C(x,y) \in R^G = \mathbb{C}[\theta_8, \varphi_{24}]$, $\deg \theta_8 = 8$, $\deg \varphi_{24} = 24$ となる．ここで

$$\theta_8(x,y) := W_{H_8}(x,y) = x^8 + 14x^4y^4 + y^8,$$

$$\varphi'_{24}(x,y) := W_{G_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24},$$

$$\varphi_{24}(x,y) := \frac{\theta_8^3 - \varphi'_{24}}{42} = x^4y^4(x^4-y^4)^4.$$

θ_8 と φ_{24} は代数的に独立である．以上により次が示された．

<u>定理.</u> C が Type II なら $W_C(x,y) \in \mathbb{C}[\theta_8, \varphi_{24}]$.

系. $n \equiv 0 \pmod 8$.

$W^*(x,y) = \sum_{i=0}^{\mu} a_i \theta_8^{j-3i} \varphi_{24}^i \in \mathbb{C}[\theta_8, \varphi_{24}]$, ここで, $n = 8j = 24\mu + 8\nu$, $\nu = 0,1,2$ としたとき, $\mu+1$ 個の $a_0, a_1, \cdots \in \mathbb{C}$ をうまく選んで,

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

の形にできる. しかも $A^*_{4\mu+4} > 0$. 例えば,

$$n = 24\mu \Rightarrow A^*_{4\mu+4} = \binom{n}{5}\binom{5\mu-2}{\mu-1} \Big/ \binom{4\mu+4}{5} > 0.$$

したがって, 重み分布関数の係数について, $A_1 = \cdots = A_{4\mu+3} = 0$ とはできるが, $A_1 = \cdots = A_{4\mu+4} = 0$ とはできない.

$$\therefore d(C) = \min_{0 \neq u \in C} w(u) \leq 4\mu + 4 = 4[n/24] + 4.$$

以上によって

定理. C が Type II なら, $d(C) \leq 4\left[\frac{n}{24}\right] + 4$.

定義. 上の不等式で等号が成立するとき, extremal という. (C が他の Type のときも定義できる).

定理. Type II の extremal コードは有限個しかない.

実際十分大きな n (≥ 3712) に対して $A_{4\mu+8} < 0$ だから.

$n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 136$ に対しては Type II のコードの存在が知られている. $n = 8$ のときは, 拡大 Hamming コード H_8, $n = 16$ のときは $H_8 \oplus H_8$, $n = 24$ のときは拡大 Golay コード G_{24} である. $n = 72$ の場合が重要な未解決問題となっている.

§∞. あとがき.

(1) 有限群 G が可換環 R に作用しているとする. 写像

$$\overline{N}_H^G : R^H[\epsilon] \longrightarrow R^G[\epsilon] : f \longmapsto \prod_{\sigma\in H\backslash G} f^\sigma$$

$(H \leq G)$ を考える. 各 $r \in R^H$ に対し,

$$\overline{N}_H^G(r\epsilon+1) = \sum_{i=0}^{|G:H|} \mu_i(r)\,\epsilon^i \quad , \mu_i(r) \in R^G$$

となるから, $1+|G:H|$ 個の写像

$$\mu_i : R^H \longrightarrow R^G \qquad i=0,1,\cdots,|G:H|.$$

が得られた. 明らかに $\mu_0(r)=1$ であり,

$$\mu_1 = T_H^G : R^H \longrightarrow R^G : r \longmapsto \sum_{\sigma\in H\backslash G} r^\sigma = T_H^G(r).$$

$$\mu_{|G:H|} = N_H^G : R^H \longrightarrow R^G : r \longmapsto \prod_{\sigma\in H\backslash G} r^\sigma = N_H^G(r).$$

T_H^G は *trace* と呼ばれる加法的写像であり, N_H^G は *norm* とか乗法的 *induction* と呼ばれる乗法的写像である. R が $\mathbb{C}$ 多元環の場合は T_H^G は全射であり, $R^H = R^G \oplus \mathrm{Ker}\,T_H^G$ である. これらの写像は具体的な不変式を作るのによく使われる.

(2) §5 の問題や結果は格子や保型関数を連想させる. 実際 *Sloane* 等がこのことを指摘している. 対応するものとしては次のものがあげられる:

コード ⟷ 格子, 重さ分布関数 ⟷ *theta* 関数,

不変式 ⟷ 保形関数, θ_8 ⟷ E_2 (*Eisenstein* 級数),

φ_{24} ⟷ Δ, H_8 ⟷ E_8, G_{24} ⟷ Λ_{24} (*Leech lattice*).

この他, "24" がどちらの理論でも重要な役をはたすし, §5

の問題は空間に球をできるだけ密に埋めこむ問題に対応している。C が $\mathbb{F}_2$ 上のコードなら、$L(C)=\{x \in \mathbb{R}^n \mid \sqrt{2}\,x \bmod 2 \in C\}$ とすることによって格子が得られる。

（3）この講演の内容は Monthly (vol 84, 1977) にのった N.J.A. Sloane の解説をもとにしたもので新らしいことは含まれていない。

参考文献

(1) F.J.Macwilliams-N.J.A.Sloane: The Theory of Error-Correcting Codes, North-Holland ,1978.

(2) J.H.van Lint: Coding Theory, LN 201, Springer, 1971.

(3) 特集「符号理論」，数理科学 1980年12月号

[1] J.H.Conway-A.M.Odlyzko-N.J.A.Sloane: Extremal self dual lattices exist only in dimensions 1 to 8, 12, 14, 15, 23,and 24, Mathematika 25 (1978), 36-43.

[2] A.M.Gleason, Weight polynomials of self-dual codes and the Macwilliams identities, in Actes Congres Intern. de Mathematique, 3 (1970), 211-215.

[3] J.Leech-N.J.A.Sloane: Sphere packings and error-corecting codes, Canad. J. Math., 23 (1971), 718-745.

[4] F.J.Macwilliams-N.J.A.Sloane-J.G.Thompson: Good self-dual codes exist, Discrete Math., 3 (1972),153-162.

[5] F.J.Macwilliams-N.J.A.Sloane-J.G.Thompson: On the existence of a projective plane of order 10, J. Combi. Theory, 14A (1973),66-78.

[6] C.L.Mallows-V.Pless-N.J.A.Sloane: Self-dual codes over GF(3), SIAM J. Applied Math., 31(1976),649-666.

[7] V.Pless : Symmetry codes over GF(3) and new five designs, J. Combi. Theory, 12 (1972), 209-246.

[8] V.Pless-N.J.A.Sloane: On the classification and enumeration of self-dual codes, J. Combi. Theory, 18A (1975),315-335.

[9] N.J.A.Sloane : Error-correcting codes and invariant theory: New applications of a nineteenth-century technique, Amer. Math. Monthly, 84 (1977), 82- 107.

[10] N.J.A.Sloane : Codes over GF(4) and complex lattices, J. of Algebra, 52 (1978), 168-181.

[11] R.Stanley : Invariants of finite groups and their applications to combinatorics, Bull. A.M.S., 1 (1979),475-511.

[12] C.L.Mallows-A.M.Odlyzko-N.J.A.Sloane: Upper bounds for modular forms, lattices, and codes, J. of Algebra, 36 (1975), 68-75.

[13] F.J.Macwilliams-A.M.Odlyzko-N.J.A.Sloane-H.N.Ward, Self-dual codes over GF(4), J. Combi. Theory, A25 (1978),288-318.

[14] N.J.A.Sloane, Binary codes, lattices and sphere-packings, Combinatorial surveys :Proc. of the sixth British combinatorial conference, 117-164, Academic Press, 1977.