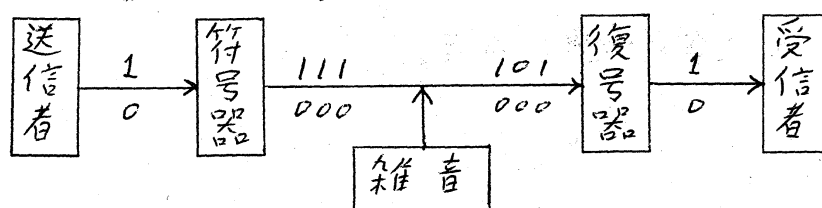


符号理論への不変式論の応用

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白けて送るとする、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、て、相手方に正しく受け取られなれりかもしれなれり。そこで符号器 (encoder) によ、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、また場合は、多数決によ、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

に $\{000, 111\}$ 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。

$\mathbb{F}_2$ を2元体, $\mathbb{F}_2^n$ を $\mathbb{F}_2$ 上の n 次元ベクトル空間とする。各 $x = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ と $y = (y_1, \dots, y_n) \in \mathbb{F}_2^n$ に対し,

$$\varrho(x, y) := \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\}$$

とくと, $(\mathbb{F}_2^n, \varrho)$ は距離空間になる。 ϱ を Hamming 距離 と言う。

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

を x の 重さ (weight) と言う。

定義 $(\mathbb{F}_2$ 上の 線型) コード とは, $\mathbb{F}_2^n$ 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 と言う。

$$\alpha := \alpha(C) := \min\{w(x) \mid 0 \neq x \in C\}$$

を C の 最小距離 と言う。このような C を $[n, k, \alpha]$ -コード と言う。このコードは $[(\alpha-1)/2]$ 個のエラーを訂正できる。

定義 C を $\mathbb{F}_2$ 上の $[n, k, \alpha]$ -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) と言う。さらに

$\mathbb{F}_q$ の元を $\omega_0=0, \omega_1, \dots, \omega_{q-1}$ とする. $u=(u_1, \dots, u_n) \in C$ に対し, $\delta_i := \delta_i(u) := \#\{j \mid u_j = \omega_i\}$, $\text{comp}(u) := (\delta_0, \dots, \delta_{q-1})$ とおく. さらに $t=(t_0, \dots, t_{q-1})$ に対し, $A(t) := \#\{u \in C \mid \text{comp}(u)=t\}$ とおく. このとき, q 変数多項式

$$\begin{aligned} V_C(z_0, \dots, z_{q-1}) &:= \sum_t A(t) z_0^{t_0} \dots z_{q-1}^{t_{q-1}} \\ &= \sum_{u \in C} z_0^{\delta_0(u)} \dots z_{q-1}^{\delta_{q-1}(u)} \end{aligned}$$

を 完備重み分布関数 という. これは n 次の齊次多項式である.

定義. C を $\mathbb{F}_q$ 上の $[n, k, \alpha]$ -コードとする. C の k 個の基底を $x_1=(x_{11}, \dots, x_{1n}), \dots, x_k=(x_{k1}, \dots, x_{kn})$ 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 $(I_k \mid G')$ の形のものがとれ, パリティ検査行列 H とし $(-G'^t \mid I_{n-k})$ をとれる. このような G と H を選んだ時, 送信者は $(u_1, \dots, u_k)$ を, $(x_1, \dots, x_n) = (u_1, \dots, u_k)G$ (ここで, $x_1=u_1, \dots, x_k=u_k$) の形に符号化して送信する. $(x'_1, \dots, x'_n)$ を受信した受信者は (i) $(x'_1, \dots, x'_n)H^t = 0$ ならエラーは起こらず (このとき $(x'_1, \dots, x'_n) \in C$), $(x'_1, \dots, x'_k)$ が元のデータだと判断する. また (ii) $(x'_1, \dots, x'_n)H^t \neq 0$ 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元のデータを改復する.

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) α が大 (誤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) $\{(a_1, \dots, a_n) \mid a_i \in \mathbb{F}_2\} \subseteq \mathbb{F}_2^n$. これは $\mathbb{F}_2$ 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. 重み分布関数は,

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

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

(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 $[n, k, \alpha]$ -コードとする.

$\exists c \in C$ せ. $w(c)$ 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 $\hat{C}$ を次の拡大コード :

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

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 $[n, k, \alpha]$ -コードの拡大は $[n+1, k, \alpha+1]$ -コードであり,

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

(4) Binary Golay codes これは $\mathbb{F}_2$ 上の $[23, 12, 7]$ -コード G_{23} である. この拡大コード G_{24} を Golay コードと呼ぶ. G_{24} の生成行列は次である.

$$G = \begin{array}{c|cccccccccccccccccccccccc} & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & \infty & 0' & 1' & 2' & 3' & 4' & 5' & 6' & 7' & 8' & 9' & 10' \\ \hline 1 & 1 & & & & & & & & & & & & & 1 & & & & & & & & & & & & \\ & & 1 & & & & & & & & & & & & & 1 & & & & & & & & & & & \\ & & & 1 & & & & & & & & & & & & & 1 & & & & & & & & & & \\ & & & & 1 & & & & & & & & & & & & & 1 & & & & & & & & & \\ & & & & & 1 & & & & & & & & & & & & & 1 & & & & & & & & \\ & & & & & & 1 & & & & & & & & & & & & & 1 & & & & & & & \\ & & & & & & & 1 & & & & & & & & & & & & & 1 & & & & & & \\ & & & & & & & & 1 & & & & & & & & & & & & & 1 & & & & & \\ & & & & & & & & & 1 & & & & & & & & & & & & & 1 & & & & \\ & & & & & & & & & & 1 & & & & & & & & & & & & & 1 & & & \\ & & & & & & & & & & & 1 & & & & & & & & & & & & & 1 & & \\ & & & & & & & & & & & & 1 & & & & & & & & & & & & & 1 & \\ & & & & & & & & & & & & & 1 & & & & & & & & & & & & & 1 \\ \hline \end{array}$$

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

重み分布関数 について.

Hamming コード H_n ($n=2^r-1$) の重み分布関数

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

拡大 Hamming コード H_8 に γ を z ,

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

Golay コード G_{23} , G_{24} に γ を z ,

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

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

Golay コード G_{12} に γ を z (完備) 重み分布関数

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

$$W_{G_{12}}(x, y) = x^{12} + 3y^{12} + 264x^6y^6 + 440x^3y^3.$$

自己同型群に γ を z . 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 z を y . σ が $C \subseteq \mathbb{F}_2^n$ を動かさない時 σ を C の自己同型と γ . C の自己同型全体のなす群を $\text{Aut}(C)$ と書く.

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

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

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

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) には次節の方法が有力である.

§3. Macwilliams の定理.

定義 C を $[n, k, \alpha]$ -コードとする.

$$C^\perp := \{(x_1, \dots, x_n) \in F_2^n \mid \sum_{i=1}^n x_i z_i = 0 \text{ for } (z_1, \dots, z_n) \in C\}.$$

このとき $C^\perp$ を C の 双対コード という. これは $[n, n-k, \alpha']$ -コードである (ある α' に対し). $C = C^\perp$ のとき C を 自己双対コード という. 自己双対コードにたいして $k = n/2$.

拡大 Hamming コード H_4 , Golay コード G_{12}, G_{24} は自己双対コードである. 変わ, ちよとして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 F_2 上の $\nu \times \nu$ 行列とみなせる ($\nu = n^2 + n + 1 =$ 点の個数). C を A の行ベクトルで生成された F_2^ν の部分空間とする. 組合せ論の大問題として, n が素数中であることが予想されており, 実際 $n \neq 6$ は証明されている. $n=10$ が次の問題になるが, 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.

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.

定理 (Macwilliams). C が F_2 上の $[n, k, \alpha]$ -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よう。

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

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

このとき Poisson の和公式が成立する:

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

$$\begin{aligned} (\text{証明}) \quad \sum_{u \in C} \hat{f}(u) &= \sum_{u \in C} \sum_{v \in F^n} (-1)^{u \cdot v} f(v) \\ &= \sum_{v \in F^n} \left(\sum_{u \in C} (-1)^{u \cdot v} \right) f(v). \end{aligned}$$

各 $v \in F^n$ に対し, $\chi_v: C \rightarrow \{\pm 1\}: u \mapsto (-1)^{u \cdot v}$ は C の指標

だから, 直交関係により

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

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

$$\begin{aligned} \text{よって, } \chi_v = 1_C &\Leftrightarrow (-1)^{u \cdot v} = 1 \quad \forall u \in C \Leftrightarrow u \cdot v = 0 \quad \forall u \in C \\ &\Leftrightarrow v \in C^\perp \end{aligned}$$

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

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

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

一方ヤクトルを次のように計算すると,

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

$$\begin{aligned}
&= \sum_{(v_1, \dots, v_n) \in \mathbb{F}_q^n} (-1)^{u_1 v_1 + \dots + u_n v_n} \prod_{i=1}^n x^{1-v_i} y^{v_i} \\
&= \sum_{v_1=0}^1 \dots \sum_{v_n=0}^1 \prod_{i=1}^n (-1)^{u_i v_i} x^{1-v_i} y^{v_i} \\
&= \prod_{i=1}^n \sum_{v_i=0}^1 (-1)^{u_i v_i} x^{1-v_i} y^{v_i} \\
&= (x+y)^{n-m(u)} (x-y)^{m(u)}
\end{aligned}$$

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,

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

さへ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ゐることがわかる。

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 $h := x^2 - y^2$ の多項式として表わせる:

$$W_C(x, y) \in \mathbb{C}[g, h].$$

(証明)

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

とすれば, (1) $W_C(x, y)$ は A によ, z 不変 (Macwilliams),

(2) $W_C(x, y)$ は B によ, z 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, $G := \langle A, B \rangle \subseteq GL(2, \mathbb{C})$ とすれば, $W_C(x, y) \in R^G$.

そこで Molien (Poincare) 級数を計算すると,

$$\begin{aligned} P(R^G, t) &:= \sum_{m=0}^{\infty} (\dim R_m^G) t^m \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det(I - t\sigma)} \quad (\text{Molien の定理}) \\ &= \frac{1}{(1-t^2)^2} = (1+t^2+t^4+\dots)(1+t^2+t^4+\dots) \end{aligned}$$

不変式論より $R^G = \mathbb{C}[\varphi, \psi]$, $\varphi = x^2 + (z-1)y^2$, $\psi = 2yz - y^2$ 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 もいえる.

定理. C を $\mathbb{F}_q$ 上の $[n, k, \alpha]$ -コードとする. $\mathbb{F}_q$ の元を $\{\omega_0=0, \omega_1, \dots, \omega_{q-1}\}$ と並べておく. $\chi: \mathbb{F}_q \rightarrow \mathbb{C}$ 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.

$$V_{C^\perp}(z_0, \dots, z_{q-1}) = \frac{1}{q^k} V_C \left(\sum_{i=0}^{q-1} \chi(\omega_i \omega_1) z_i, \dots, \sum_{i=0}^{q-1} \chi(\omega_{q-1} \omega_i) z_i \right).$$

この定理の応用として, Gleason の定理を F_3 に拡張した Sloane の定理がある.

定理. $V(x, y, z) \in \mathbb{C}$, $\mathbf{1}=(1, \dots, 1)$ を含む F_3 上の自己双対 $[n, n/2, \alpha]$ -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, $\alpha_{12} = a(a^3 + \delta p^3)$, $\beta_6 = a^{12} - 12b$, $\gamma_{18} = a^6 - 20a^3p^3 - \delta p^6$, $\delta_{36} = p^3(a^3 - p^3)^3$, さらに $a = x^2 + y^2 + z^2$.

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

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

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

による不変. したがってこれから 3 種類の行列の生成する群 G により $V(x, y, z)$ は不変である. なお $|G| = 2^5 \cdot 3^4$. 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えば, 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, $R = \mathbb{C}[x_1, \dots, x_n]$ とすると, G は R に (多元環準同型として) 作用する:

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

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

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
齊次多項式のなる 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:

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

定理 (Molien, 1897)

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

定理 (Hochster-Eagon, 1971). R^G は Cohen-Macaulay 環.

したがって, 2 齊次多項式 $\theta_1, \dots, \theta_m, \eta_1, \dots, \eta_r$ が存在して,

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

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

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

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

定理. $R^G = \mathbb{C}[\theta_1, \dots, \theta_m]$ 且 $\theta_1, \dots, \theta_m$ が代数的に独立齊次
式 $\Leftrightarrow G$ が $2 = \theta$ reflection で生成される.

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

§5. 応用.

以下では $\mathbb{F}_2$ 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 δ を与えたとき, $\mathbb{F}_2$ 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.

$$\alpha^* := \max \left\{ \alpha(C) \mid \begin{array}{l} C \text{ は } \mathbb{F}_2 \text{ 上の長さ } n \text{ の} \\ \text{自己双対コード} \end{array} \right\}.$$

一般に $\alpha = \alpha(C)$ のとき, C の重み分布関数について,

$$W_C(x, y) = x^n + A_\alpha x^{n-\alpha} y^\alpha + A_{\alpha+1} x^{n-\alpha-1} y^{\alpha+1} + \dots$$

$$A_1 = \dots = A_{\alpha-1} = 0, \quad A_\alpha \neq 0, \quad A_i \geq 0 \quad (\forall i).$$

定理 (Gleason, Pierce, Turyn). $t > 1$ を自然数とする. 任意の $u \in C$ に対し $w(u)$ 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	δ	t	$\alpha(C)$
I*	2	2	$\leq 2 \lfloor n/8 \rfloor + 2$
II	2	4	$\leq 4 \lfloor n/24 \rfloor + 4$
III	3	3	$\leq 3 \lfloor n/12 \rfloor + 3$
IV	4	2	$\leq 2 \lfloor n/6 \rfloor + 2$

*) Type II に属するもの. $\lfloor \cdot \rfloor$ は Gauss 記号

以下 Type II のコード C に対し $\alpha := \alpha(C) \leq 4\lceil n/24 \rceil + 4$ を示そう, $w(x) \equiv 0(4) (\forall x \in C)$ だから,

$$i \neq 0(4) \Rightarrow A_i := \#\{u \in C \mid w(u) = i\} = 0.$$

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

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

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

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

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

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

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

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

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.

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

系. $n \equiv 0 \pmod{8}$.

$W^*(x, y) = \sum_{i=0}^n a_i \theta_8^{j-3i} \varphi_{24}^i \in \mathbb{C}[\theta_8, \varphi_{24}]$, $i = 2^r$, $n = 8j = 24m + 8v$, $v = 0, 1, 2$ としたとき, $m+1$ 個の $a_1, a_2, \dots \in \mathbb{C}$ をうまく選んで,

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

の形にできる. しかも $A_{4m+4}^* > 0$ であるから,

$$n = 24m \Rightarrow A_{4m+4}^* = \binom{n}{5} \binom{5m-2}{m-1} / \binom{4m+4}{5} > 0.$$

したがって, 重み分布関数の係数に $n \geq 2$, $A_1 = \dots = A_{4m+3} = 0$ とはできるが, $A_1 = \dots = A_{4m+4} = 0$ とはできない.

$$\therefore d(C) = \min_{0 \neq u \in C} w(u) \leq 4m + 4 = 4 \left\lfloor \frac{n}{24} \right\rfloor + 4.$$

以上によつて

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

定義. 上の不等式で等号が成立するとき, extremal と言う. (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 $A_{4m+8} < 0$ だから. $n = 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 136$ に対しは Type II のコードの存在が知られている. $n = 8$ のときは, 16 大 Hamming コード H_8 , $n = 16$ のときは $H_8 \oplus H_8$, $n = 24$ のときは 16 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.

§ 5. あとがき.

(1) 有限群 G が可換環 R に作用しとけるとする. 写像

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

($H \leq G$) を考える. 各 $r \in R^H$ に対し,

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

となるから, $|H|G : |H|$ 個の写像

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

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, $R^H = R^G \oplus \ker T_H^G$ 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形関数を連想させる. 実際 *Sloane* 等がこのことを指摘しとける. 対応するものとしては次のものがあげられる:

コード $\longleftrightarrow$ 格子, 重み分布関数 $\longleftrightarrow$ *theta* 関数,

不変式 $\longleftrightarrow$ 保形関数, $\theta_8 \longleftrightarrow E_2$ (Eisenstein級数),

$\varphi_{24} \longleftrightarrow \Delta$, $H_8 \longleftrightarrow E_8$, $G_{24} \longleftrightarrow \Lambda_{24}$ (Leech lattice).

その他, "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詰めるが秘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、 $L(C) := \{x \in \mathbb{R}^n \mid \sqrt{2}x \bmod 2 \in C\}$ とすることにより、2格子が得られる。

(3) この講演の内容は *Monthly* (vol 84, 1977) にのって 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-correcting 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. Combin. 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.