

平方剰余コード

甲南大 理 伊藤 昇

Noboru Ito

F を体, V を F に成分を持つサイズ n の行ベクトル全部の作る F 上のベクトル空間とする. (線型) コード C とは V の部分空間のことである. N を非負整数全部の集合とするとき, 重さ $w: V \rightarrow N$ とは $v \in F$ に対し $w(v) = v$ の非 0 成分の個数とするものである. 各ベクトルの重さを不変にする V の自己同型全部は単項変換群 M と一致する. C の自己同型群, $\text{Aut}(C)$, とは C を不変にする M の最大部分群のことである. (代数的) コード理論の大切な問題の 2 つは (1) C の最小重さ $d = d(C) = \min_{0 \neq v \in C} w(v)$ を決定することと, (2) C の情報集合, これは $\dim_F(C) = k$ とするとき, (線型) 独立となる k 個の座標位置列をすべて決定することとである. $\text{Aut}(C)$ はこの問題を考察するのに有益な働きをすることとが期待される.

サイズ $p+1$, p は奇素数, の平方剰余コードについて上述の事柄を考察するが, とくに 2 元 (体上の) コードに興味があるので, $p \equiv \pm 1 \pmod{8}$ と仮定する. さらに記述を短縮するために $p \equiv -1 \pmod{8}$ のときだけ説明する. p

$\equiv 1 \pmod{8}$ のときは多少変更が必要である。

1. 大域的平方剰余コード

まず記号を設定する. $\mathbb{Q}$: 有理数体; $\alpha = \exp(2\pi i/p)$, $K = \mathbb{Q}(\alpha)$; L : K の下の 2 次体, $\tau: K$ から L へのトレース; $f_j: L \times K \rightarrow L$ は $(c_0, c) f_j = c_0 + \tau(c \alpha^j)$ という関数 ($0 \leq j \leq p-1$); $(c_0, c) f_\infty = i\sqrt{p} c_0$; ν : p を法として非平方な整数; $f'_j: L \times K \rightarrow L$ は $(c_0, c) f'_j = c_0 + \tau(c \alpha^{\nu j})$ という関数 ($0 \leq j \leq p-1$); $(c_0, c) f'_\infty = -i\sqrt{p} c_0$; V : L に成分を持つサイズ $p+1$ の行ベクトル全部の作る L 上のベクトル空間; $W^\perp$: W を V の部分空間とするとき W の各ベクトルと直交する V のベクトル全部の作る部分空間; $\langle c_0, c \rangle = ((c_0, c) f_0, \dots, (c_0, c) f_{p-1}, (c_0, c) f_\infty)$, $c_0 \in L$, $c \in K$.

そうすると大域的平方剰余コード A は $\langle c_0, c \rangle$ 全部の作る V の部分空間として定義される. f を f' に置きかえると, もうひとつの大域的平方剰余コード B が得られる. 証明のよい定理については文末の文献 (およびそこにある文献) を参照されたい.

定理. $p \equiv -1 \pmod{8}$ のとき. $V = A + B$, $A \cap B = 0$, $A = A^\perp$, $B = B^\perp$, とくに $\dim_L(A) = \dim_L(B) =$

$\frac{1}{2}(b+1)$. $b \equiv 1 \pmod{8}$ のときは $B = A^\perp$, $A = B^\perp$ となることも異なる.

定理. A, B の最小重さは $\frac{1}{2}(b+3)$ である.

定理. 任意 $\frac{1}{2}(b+1)$ 個の座標位置列は情報集合である.

このように大域的コードの場合には, はっきりしている最小重さと情報集合であるが, θ を $\mathbb{Z}$ の整数環とし, A, B のベクトルのうち成分が θ にあるもの全部 $A(\theta), B(\theta)$ を考察し, $\mathbb{Z}$ の θ での素イデアル分解が $\mathbb{Z} = \theta_1 \theta_2$ の形であることに注目し, $\mathbb{Z}$ 元コード $A(\mathbb{Z}), B(\mathbb{Z})$ に移行すると, おぼろおぼろとなってくる.

2. 自己同型群

A, B の自己同型群は同型 (相似) である. A には以下のようき自己同型対応があり, それらは $\text{PSL}_2(\mathbb{F}_p)$ を生成する:

c : 巡回シフト

$$f_j c = f_{j+1}, \quad 0 \leq j \leq p-1, \quad \text{ただし } f_p = f_0 \text{ である,}$$

$$f_\infty c = f_\infty;$$

これは $\langle c_0, c \rangle$ の f_{j+1} はもとの f_j であるを読む (以下同様). したがって $\langle c_0, c \rangle c = \langle c_0, c \alpha^{-1} \rangle$ である.

$\mathbb{F}_p$, ここで $\mathbb{F}$ は p を法としての平方数の代表系を動く,

$\pi \neq 0$; ガロア自己同型

$$f_j \rho_\pi = f_{\pi j}, \quad f_\infty \rho_\pi = f_\infty.$$

σ :

$$f_j \sigma = \varepsilon_j f_{-j-1}, \quad \varepsilon_j = \left(\frac{j}{p} \right), \quad \text{ルジヤンドル記号}, \quad 1 \leq j \leq p-1, \quad f_0 \sigma = f_\infty, \quad f_\infty \sigma = -f_0.$$

(f'_j のとき, $p \equiv 1 \pmod{8}$ のときはそれぞれ多少の変更を要する).

さて $G = \text{Aut}(A)$ とおく. G は単項変換からできているが, そのうち対角変換であるもの全部 $D(G)$ は G の正規部分群である. またスカラー変換全部 S は G の中心に含まれる. A の最小重さを持つベクトルに $D(G)$ の元を働かしてみると, $D(G) = S$ に直ちにわかる. また π で単項変換を置換変換にする射影写像とすると, $G\pi \cong G/D(G)$ は次数 $p+1$ の $\text{PSL}_2(p)$ を含む 2 重可移群になる. 例外 ($p=7, 23$) を除いて $G\pi = \text{PSL}_2(p)$ を示すのが目的である. 単純群分類完了の一帰結として, 正則可移正規部分群を含まない 2 重可移群の分類も完了しているので, 以下のことを示せば充分である:

(i) $|N(\langle \sigma \rangle)| = \frac{1}{2} p(p-1)$ である. ここで N は $G\pi$ の中で正規化群をとる作用素を示す.

(ii) $\text{Alt}(p+1)$ は $G\pi$ に含まれない.

(iii) $p > 7$ ならば $G\pi$ は正則可移正規部分群を含まない

(i) の証明. 計算しやすいため V の標準基 $(e_0, e_1, \dots, e_{p-1}, e_\infty)$ をとり, 行列の語に直す. $GF(p)^X$ の指数 2 の部分群を $R = \langle \pi_0 \rangle$, $R^* = GF(p)^X - R$ とおく. さて $N(\langle \pi \rangle)$ に位数 $p+1$ の元 ρ があるとしてみる. $\rho^2 = \rho \pi_0 \circ I_{p+1}$, $\lambda \in L$, ここで I_{p+1} は次数 $p+1$ の単位行列である, とする. $e_i \rho = c_i e_{i\rho}$, $i \in \{0, 1, \dots, p-1, \infty\}$ とおく. $e_\infty \rho = c_\infty e_\infty$ だから, ρ を $\rho \cdot c_\infty^{-1} I_{p+1}$ とおきかえて, $\rho^2 = \rho \pi_0$ と仮定出来る. そうすると $e_0 \rho = c_0 e_0$ となり, $c_0^2 = c_\infty^2 = 1$. $e_1 \rho = c_1 e_{1\rho}$, $1\rho \in R$ とすると $e_1 \rho \rho_{1\rho}^{-1} = c_1 e_1$ となる. $\rho \rho_{1\rho}^{-1}$ は $N(\langle \pi \rangle)$ の元であるから, $\rho \rho_{1\rho}^{-1} = \lambda' I$, $\lambda' \in L$ となる. $\lambda' = c_0 = c_\infty$ だから $\lambda'^2 = 1$. $D(G)$ を法とする位数は ρ が $p-1$, $\rho_{1\rho}$ が $\frac{1}{2}(p-1)$ であるから, これはいけない. したがって ρ は R と R^* を交接するものと仮定出来る. $e_i \rho = c_i e_{i\rho}$, $e_i \rho^2 = e_i \pi_0 = c_i c_{i\rho}$. $e_i \rho^2$ から $c_i c_{i\rho} = 1$, $c_{i\rho} c_{i\rho^2} = 1$, $c_i = c_{i\rho^2}$ となるから c_i は c_π , $\pi \in R$, c_n , $n \in R^*$ の 2 種類で, $c_\pi c_n = 1$ となっている.

さて A は, $\langle 1, 0 \rangle = (1, \dots, 1, i\sqrt{p})$ および

$1 + 2\gamma = \sqrt{p}$, $1 + \gamma + \gamma' = 0$ で γ , γ' を定義し, V のベクトルの座標を $0, R$ の元, R^* の元, ∞ の順序で書くとすると, $\langle 0, 1 \rangle = (\frac{1}{2}(p-1), \gamma, \dots, \gamma', \dots, 0)$ があるので, $(\frac{1}{2}(p-1) - \gamma, 0, \dots, \gamma' - \gamma, \dots, -\sqrt{p}\gamma)$ を含む. $\langle 1, 0 \rangle \neq \langle 0, 1 \rangle$ から同じ様にする, $(\frac{1}{2}(p-1)c_0 - \gamma'c_0, 0, \dots, c_\pi(\gamma - \gamma'), \dots, -c_\infty\sqrt{p}\gamma')$ を含むと仮定する. それで, $c_0(\frac{1}{2}(p-1) - \gamma') / (\frac{1}{2}(p-1) - \gamma) = -c_\pi = c_\infty$ を得る. $c_\infty = 1$ なら, $c_0 = -1$ したがって $\gamma + \gamma' = p-1$ となってしまう. $c_\infty = -1$ のときも同様に矛盾が得られる.

(ii) の証明. $A\gamma(p+1)$ が G に含まれていると仮定しよう. そうすると $e_0 f = a e_1$, $e_1 f = b e_2$, $e_2 f = c e_0$, $e_i f = \delta_i e_i$, $i \in \{3, \dots, p-1, \infty\}$ という元が G にある. そうすると $abc = \delta_3^3 = \dots = \delta_\infty^3$, $(\delta_i \delta_j^{-1})^3 = 1$ となる. ④ $(\sqrt{-p})$ の単元は ± 1 だけである. $\delta_3 = \dots = \delta_\infty = \delta$ とおき, f を $f \delta^{-1} I_{p+1}$ で置き換え, $\delta = 1$ と仮定出来る. $(\frac{1}{2}(p-1), \gamma, \dots, \gamma', \dots, 0)$ に f を作用させると, $2 \in R$ なので, $(\gamma, \frac{1}{2}(p-1)a, \gamma b, \dots)$ となり, したがって, $\frac{1}{2}(p-1) = \gamma c$, $\gamma = \frac{1}{2}(p-1)a$, $\gamma = \gamma b$, それで $b = 1$,

$ac = 1$ を得る. 今度は $(1, \dots, 1, i\sqrt{p})$ に ρ を作用させると, $(c, a, 1, \dots)$ とまり, $\dots$ のところは不変であるので, $a = c = 1$ を得る. したがって $\frac{1}{2}(p-1) = 2$ となるが, これは明らかに矛盾である.

(iii) の証明. G の位数 $p+1$ の正則正規部分群 L を含むとしてみる. L は基本アーベル 2 群であるから, とくに $p+1 = 2^m$ である. L は $N(\langle c \rangle)$ の忠実な表現加群と考えられ, 他方 $N(\langle c \rangle)$ の忠実な既約表現の次数はすくなくとも $\frac{1}{2}(p-1)$ であるから, $m \geq 2^{m-1} - 1$ を得る. これより $m = 3$, $p = 7$ まででくる.

最小重さ, 情報集合とことまり, 自己同型群は $A(\theta)$, $A(2)$ にスムーズに移行する. $D(G) \cap A(\theta)$ は θ の単数群に同型なので, $p \equiv 1 \pmod{8}$ のときは無限群である.

3. 2元平斉剰余コード

最小重さの移行の仕事はまったくわかっていないといつてよいと思えば, $A(2)$, $B(2)$ を直接考察した次の様な結果が知られている.

定理. $(d-1)^2 \geq p+2$. $p \equiv -1 \pmod{8}$ のときは, さらに $(d-1)^2 - (d-1) + 1 \geq p$ かつ $d \equiv 0 \pmod{4}$.

改良されるのは、今のところ $p \equiv -1 \pmod{8}$ のときに
かぎられているらしい。

定理 $p \equiv -1 \pmod{8}$ とする. $(d-1)^2 - (d-1)$
 $+ 1 = p$ なら, 座標位置を点, 最小重さベクトルが 1 を持
 つ座標位置の集合をブロックとみると, 対称 $2-(p, d-1, 1)$ デザイン (射影平面) とある. さらに $p = 7, d =$
 4 に限る.

前半は van Tilborg, 後半は Calderbank による. Calder
 bank はこの結果も含めて, 限界をいろいろと改良している.

情報集合の移行の仕方については, Newhant がしらべてい
 るが, 具体的な定理という形では, $PSL_2(p)$ の位数 $\frac{1}{2}(p+1)$
 の元が, その 2 つのサイクル L_1, L_2 に巡回的に働いている
 ので, 長さ $\frac{1}{2}(p+1)$ の巡回コードが $A(2), B(2)$ に収納
 されているという事実にもとづくものに限られる様である.

定理 (Jensen). $p \equiv 1 \pmod{8}$ とする. $l = \frac{1}{2}(p+1)$
 $1)$ は素数であるとする. $GF(l)^X = \langle \alpha \rangle$ または
 $\alpha^l - 1 = (\alpha - 1) f(\alpha) g(\alpha)$ で $f(\alpha), g(\alpha)$ が既約
 $(GF(2) \text{ 上})$ であるとする. そうすると L_1 も L_2 も情報
 集合である.

定理 (Pless). $p \equiv 1 \pmod{8}$ とする. $\frac{1}{2}(p+1)$
 $\equiv 0 \pmod{3}$ とする. そうすると L_1 が情報集合ならば,

L_2 は情報集合でない。

Jenson はまた計算機によつて, L_1 も L_2 も情報集合にふらふ p の例の最小なものとして, $p \equiv 1 \pmod{8}$ のときは $p = 89$ を, $p \equiv -1 \pmod{8}$ のときは $p = 167$ をあげている。この様に定理は $p \equiv 1 \pmod{8}$ のときにのみ述べられているが, $p \equiv -1 \pmod{8}$ のときでも, 似た様な定理を述べることは出来ると思う。然し L_1, L_2 に $A(2)$, $B(2)$ の平方剰余性が反映している様な結果がほしいのであるが, 将来に待たなければふらふ様な様である。

文献

F. J. MacWilliams - N. J. A. Sloane, The theory of Error-Correcting Codes, North-Holland 1977

D. A. Jenson, A double circulant presentation of quadratic residue codes, IEEE Trans. of Information Theory 26 (1980) 223 - 227

V. Pless, When is a cycle an information set?
Annals N.Y. Academy of Sciences 319 (1979)
429 - 435