数理解析研究所講究録
第475巻 1982年 147-155

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$w: V \to N$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，$Aut(C)$，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．$Aut(C)$はこの問題を考察するのに有益な働らきをすることが期待される．

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，T：KからLへのトレエス；$f_j : L \times K \to L$は$(c_0, c) f_j = c_0 + T(c\alpha^j)$という関数$(0 \le j \le p-1)$；$(c_0, c) f_\infty = i\sqrt{p}\, c_0$；$\nu$：$p$を法として非平方な整数；$f_j' : L \times K \to L$は$(c_0, c) f_j' = c_0 + T(c\alpha^{\nu j})$という関数$(0 \le j \le p-1)$；$(c_0, c) f_\infty' = -i\sqrt{p}\, c_0$；$V$：$L$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；$\langle c_0, c \rangle = ((c_0, c) f_0, \cdots, (c_0, c) f_{p-1}, (c_0, c) f_\infty)$，$c_0 \in L$，$c \in K$．

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'におきかえると，もうひとつの大域的平方剰余コードBが得られる．証明のな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$\dim_L(A) = \dim_L(B) =$

$\frac{1}{2}(p+1)$. $p \equiv 1 \pmod 8$ のときは $B = A^{\perp}$, $A = B^{\perp}$ とあるところが異なる.

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

定理. 任意 $\frac{1}{2}(p+1)$ 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, はっきりしこいる最小重さと情報集合であるが, $\mathfrak{o}$ を $\mathbb{L}$ の整数環とし, A, B のベクトルのうち成分が $\mathfrak{o}$ にあるもの全部 $A(\mathfrak{o})$, $B(\mathfrak{o})$ を考察し, 2 の $\mathfrak{o}$ での素イデアル分解が $2 = \mathfrak{p}_1\mathfrak{p}_2$ の形であることに注目し, 2元コード" $A(2)$, $B(2)$ 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 には以下のような自己同型対応があり, それらは $PSL_2(p)$ を生成する:

τ : 巡回シフト

$f_j\tau = f_{j+1}$, $0 \le i \le p-1$, ただし $f_p = f_0$ である,

$f_\infty\tau = f_\infty$;

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

S_π, ここで π は p を法としての平方数の代表系を動く,

π キ 0 ; ガロア自己同型

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

σ :

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

(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 $G = \mathrm{Aut}(A)$ とおく . G は単項変換からできているから , 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 $D(G)$ の元を働らかしてみると , $D(G) = S$ が直ちにわかる . また元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 $PSL_2(p)$ を含む 2 重可移群になる . 例外 ($p = 7$, 23) を除いて $G\pi = PSL_2(p)$ 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) $|N(\langle \tau \rangle)| = \frac{1}{2} p(p-1)$ 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) $Alt(p+1)$ は $G\pi$ に含まれない .

(iii) $p>7$ ならば G_π 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 $(e_0, e_1, \cdots, e_{p-1}, e_\infty)$ をとり, 行列の話に直す. $GF(p)^\times$ の指数2の部分群を $R=\langle \pi_0 \rangle$, $R^*=GF(p)^\times - R$ とおく. さて $N(\langle \tau \rangle)$ に位数 $p+1$ の元 σ があるとしてみる. $\sigma^2 = \sigma\pi_0 \cdot \lambda I_{p+1}$, $\lambda \in L$, ここで I_{p+1} は次数 $p+1$ の単位行列である, とする. $e_i\sigma = c_i\, e_{i\sigma}$, $i \in \{0, 1, \cdots, p-1, \infty\}$ とおく. $e_\infty \sigma = c_\infty e_\infty$ だから, σ を $\sigma \cdot c_\infty^{-1} I_{p+1}$ でおきかえて, $\sigma^2 = \sigma\pi_0$ と仮定出来る. そうすると $e_0\sigma = c_0 e_0$ となり, $c_0^2 = c_\infty^2 = 1$. $e_1\sigma = c_1 e_{1\sigma}$, $1\sigma \in R$ とすると $e_1 \sigma \sigma_{1\sigma}^{-1} = c_1 e_1$ となる. $\sigma\sigma_{1\sigma}^{-1}$ は $N(\langle \tau \rangle)$ の元であるから, $\sigma\sigma_{1\sigma}^{-1} = \lambda' I$, $\lambda' \in L$ となる. $\lambda' = c_0 = c_\infty$ だから $\lambda'^2 = 1$. $D(G)$ を法とする位数は σ が $p-1$, $\sigma_{1\sigma}$ が $\frac{1}{2}(p-1)$ であるから, これはいけない. したがって σ は R と R^* を交換することがわかる. $e_i\sigma = c_i e_{i\sigma}$, $e_i\sigma^2 = e_i\pi_0 = c_i c_{i\sigma} \cdot e_{i\sigma^2}$ から $c_i c_{i\sigma} = 1$, $c_{i\sigma} c_{i\sigma^2} = 1$, $c_i = c_{i\sigma^2}$ となるから c_i 達は c_π, $\pi \in R$, c_η, $\eta \in R^*$ の2種類で, $c_\pi c_\eta = 1$ となっている.

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

$1+2\zeta=\sqrt{-p}$, $1+\zeta+\zeta'=0$ で ζ,ζ' を定義し，V のベクトルの座標を 0，R の元，R^* の元，∞ の順序で書くことにすると，$\langle 0,1\rangle=(\frac{1}{2}(p-1),\zeta,\cdots,\zeta',\cdots,0)$ があるので，$(\frac{1}{2}(p-1)-\zeta,0,\cdots,\zeta'-\zeta,\cdots,-\sqrt{-p}\zeta)$ を含む．$\langle 1,0\rangle_S$，$\langle 0,1\rangle_S$ から同じ様にすると，$(\frac{1}{2}(p-1)c_0-\zeta' c_0,0,\cdots,c_\pi(\zeta-\zeta'),\cdots,-c_\infty\sqrt{-p}\zeta')$ を含むことがわかる．それで，$c_0(\frac{1}{2}(p-1)-\zeta')/(\frac{1}{2}(p-1)-\zeta)=-c_\pi=c_\infty$ を得る．$c_\infty=1$ なら，$c_0=-1$ したがって $\zeta+\zeta'=p-1$ となってしまう．$c_\infty=-1$ のときも同様な矛盾が得られる．

(ii) の証明．$Alt(p+1)$ が G に含まれていると仮定しよう．そうすると $e_0S=ae_1$，$e_1S=be_2$，$e_2S=ce_0$，$e_iS=\delta_i e_i$，$i\in\{3,\cdots,p-1,\infty\}$ という元が G にある．そうすると $abc=\delta_3^3=\cdots=\delta_\infty^3$，$(\delta_i\delta_j^{-1})^3=1$ となる．$\mathbb{Q}(\sqrt{-p})$ の単元は ±1 だけである．$\delta_3=\cdots=\delta_\infty=\delta$ とおき，S を $S\delta^{-1}I_{p+1}$ でおきかえると，$\delta=1$ と仮定出来る．$(\frac{1}{2}(p-1),\zeta,\cdots,\zeta',\cdots,0)$ に S を作用させると，$2\in R$ なので，$(\zeta,\frac{1}{2}(p-1)a,\zeta b,\cdots)$ となり，したがって，$\frac{1}{2}(p-1)=\zeta c$，$\zeta=\frac{1}{2}(p-1)a$，$\zeta=\zeta b$，それで $b=1$，

$ac=1$ を得る．今度は $(1,\cdots,1,c,0)$ に ρ を作用させると，$(c,a,1,\cdots)$ となり，$\cdots$ 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 が位数 $p+1$ 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 $N(\langle\tau\rangle)$ の忠実な表現加群と考えられ，他方 $N(\langle\tau\rangle)$ 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．これから $m=3$，$p=7$ がでてくる．

最小重さ，情報集合ということより，自己同型群は $A(\theta)$，$A(2)$ にスムーズに移行する．$D(G)\wedge A(\theta)$ は θ の奇数群に同型なので，$p\equiv 1\pmod 8$ のときは無限群である．

3. 2元平方剰余コード

最小重さの移行の仕方はまったくわかっていないといってよいと思うが，$A(2)$，$B(2)$ 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 $(d-1)^2-(d-1)+1\geq p$ から $d\equiv 0\pmod 4$．

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）となる．さらに $p = 7$，$d = 4$ に限る．

前半は van Tilborg，後半は Calderbank による．Calderbank 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，Newhart 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 に巡回的に働らいているので，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ずくものに限られる様である．

定理（Jensen）．$p \equiv 1 \pmod 8$ とする．$l = \frac{1}{2}(p+1)$ は素数であるとする．$GF(l)^X = \langle 2 \rangle$ または $x^l - 1 = (x-1) f(x) g(x)$ で $f(x)$，$g(x)$ が既約（$GF(2)$ 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はまた計算機によって，L_1 も L_2 も情報集合にならない 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 $p \equiv 1 \pmod 8$ のときに限られているが，$p \equiv -1 \pmod 8$ 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 $A(z)$, $B(z)$ 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ならない様である．

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