数理解析研究所講究録
587巻 1986年 167-172

Duadic codeについて

甲南大理 伊藤 昇 (Noboru Ito)

1. はじめに

この集会が開かれた時点では, duadic codeで位数 2^5 の巡回射影平面を收納するものが存在するかどうかが未解決の問題であったので, 存在するというのが話の主題であった([1]).

集会後間もなく, 平峰豊氏の巡回表示を用いて, 位数 2^b (bは奇数)のデザルグ平面はduadic codeに收納されることを証明出来た. 偶数位数の巡回射影平面で知られているものは位数 2^b のデザルグ平面だけであること, さらに b が偶数なら $2^{2b} + 2^b + 1$ は3の倍数であり, b が奇数なら $2^{2b} + 2^b + 1$ の各素因数は8を法として ± 1 に合同であることを注意する.

その後 Plessの通信により, 彼女が位数が4の倍数で, $n = m^2 + m + 1$ の各素因子は8を法として ± 1 に合同である

様な巡回射影平面はduadic codeに収納されるという定理を証明したことが判明した．我我の証明の方がより構成的であること勿論であるが，大同小異ではある．

さてPless達によるduadic codeの定義は巾等生成元によるものであるが，それは生成多項式によってでも与えられる．さらに後者によると，どの巡回コードがどのduadic codeに含まれるかを包含定理という形に述べることが容易となる．それを含めたduadic codeの定義をまず述べる．また集会で話した証明は上二つのと異なり，それはそれで面白いかも知れないと思うので，それをまず述べる．

2. Duadic codeの定義

Cを長さn（nは奇数）の2元巡回コード，すなわちCを$R_n = GF(2)[x]/(x^n-1)$のイデアルとする．R_nは半単純な単項イデアル環であるから，Cは生成多項式$g(x)$，巾等生成元$e(x)$を持つ．$e(x) = \sum_{i\in S} x^i$，Sは$\mathbb{Z}/(n) = \{0, 1, \cdots, n-1\}$の部分集合，とおく．$e(x)$が巾等元なので，$i\in S$なら$2i\in S$である．$\mathbb{Z}/(n)$を2で生成される乗法群$\langle 2\rangle$で環状コセットにわける（例えば$n=7$なら，$\{0\}$，$\{1, 2, 4\}$，$\{3, 6, 5\}$が環状コセットである）と，Sはいくつかの環状コセットの合併集合で

ある．aがnと素な整数であると，μ_a : $\mu_a(i) = ai$ は$\mathbb{Z}/(n)$の置換であるが，環状コセットの集合の置換であることも見易い．

もし $\mathbb{Z}/(n) - \{0\} = T \cup \mu_a(T)$, $T \cap \mu_a(T) = \emptyset$ となるならば，この分解をμ_aによる分裂と呼ぶ．さて $S = T \cup E$, または $= \mu_a(T) \cup E$, ここで $E = \{0\}$ または $= \emptyset$ (Eがどちらかはnを与えるときまる)，のときCを duadic code という．duadic pair を定義する方がより適切かも知れない．

我我が今興味を持つのは $a = -1$ という場合なので，以下これを仮定する．

αをGF(2)上の1の原始n乗根とする．μ_aは$\mu_a(\alpha^i) = \alpha^{ai}$ とすると $\{\alpha^i, 0 \le i \le n-1\}$の置換であるが，上と同じく$\alpha^i$達の最小多項式達の置換であることも見易い．$a = -1$としたので各多項式はその相反多項式にうつる．さて$\mu_{-1}$が分裂を与えるとすると，$x^n - 1 = (x-1)h(x)$とおくとき$h(x)$の既約因子分解が $h(x) = a_1(x) \cdots a_s(x)\, b_1(x) \cdots b_s(x)$, ここで $\{a_i(x), b_i(x)\}$, $1 \le i \le s$ は相反対である，とまっている．逆も成立する．そして $g(x) = a_1(x) \cdots a_s(x)$ である．実際には $\{a_i(x), b_i(x)\}$, $1 \le i \le s$ が一つずつ

選んだ積が duadic code となるので，このとき 2^5 個の duadic code が作られる．ただし duadic code の等価問題は今のところ完全には解決されていないと思う．

ともかくある巡回コード D が duadic code に含まれるためには，D の生成多項式が，各 $\{a_i(x), b_i(x)\}$ $(1 \leq i \leq \lambda)$ について少なくとも一方を因子に持つことであり，D を含むものは $a_i(x)b_i(x)$ が D の生成多項式の因子になっているとき，その様な各 i について，一方だけを選んで得られることも見易いであろう．

3. 2^5 のとき．

$n = 2^{10} + 2^5 + 1 = 1057 = 7 \cdot 151$，$|2 \bmod 151| = |2 \bmod 1057| = 15$ である．したがって環状コセットは $\{0\}, \{151, 302, 604\}, \{453, 906, 755\}$ を除くと，サイズ 15 である．

各環状コセットを，そこに含まれる最小数 i により $C(i)$ と表記する．例えば $C(1) = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 991, 925, 793, 529\}$ である．さらに $C(i)$ に対応する中等元も $C(i)$ で表わす：$C(i) = \sum_{j \in C(i)} \alpha^j$ である．このとき合併集合と和とが対応する．

位数 2^5 のデザルグ平面を cyclic difference set の形で与えると，$P = C(1) \cup C(55) \cup C(453)$ となる．$Pe = P$ を満足する duadic idempotent e の存在を見る（一を構成する）とよいわけである．そのために各 $C(i)$ について $P \cdot C(i) + P$ を $C(j)$ 達の和として表示する．その際単位元 $C(0)$ は何時でも調整出来るので無視することにする．とも角 $P(PC(i) + P) = P$ に注意しておく．他方 $C(i)$ 達を μ_{-1} - pair に分けると，36個の pair が出来る．

さて行のラベルを $PC(i) + P$，列のラベルを $\{C(j), \mu_{-1}(C(j))\}$ とし，$(PC(i) + P, \{C(j), \mu_{-1}(C(j))\})$ - 成分は $PC(i) + P$ の表示が pair の一方だけを含む時だけ 1，でない時は 0 として，$GF(2)$ 上の incidence mathix を作る．この行列 M のサイズは $(72, 36)$ である．

いくつかの行の和が全ベクトルになる時が duadic idempotent に対応する．それが可能になるのは M の階数が 36 なら明白であるが，後者を見ることは多少時間をとるとしても困難ではない．

文献

1. J. Leon, J.M. Masley and V. Pless, Duadic code,

IEEE Trans. on Inform. Theory, IT-30, 709-714