

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 の巡回射影平面を収納するものが存在するかどうか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^e (e は奇数) のデザルグ平面は duadic code に収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^e のデザルグ平面だけであること, さらに e が偶数なら $2^{2e} + 2^e + 1$ は 3 の倍数であり, e が奇数なら $2^{2e} + 2^e + 1$ 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。我々の証明の方がより構成的であることが勿論であるが、大同小異ではある。

さて Press 氏による 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を容易となる。それを含めた duadic code の定義をここで述べる。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まいと思ふので、それをも述べる。

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 は $R_n = GF(2)[x]/(x^n - 1)$ 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 $\mathbb{Z}/(n) = \{0, 1, \dots, n-1\}$ の部分集合、と置く。 $e(x)$ 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 $\langle 2 \rangle$ で環状コセットに分ける (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, $\mu_a : \mu_a(i) = ai$ 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 $S = T \cup \{0\}$, または $S = \mu_a(T) \cup \{0\}$, ここで $\{0\}$ または $\emptyset$ ($\{0\}$ がどちらか n を与えるときもある), 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.

我々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 $\text{GF}(2)$ 上の 1 の原始 n 乗根とする. μ_a は $\mu_a(\alpha^i) = \alpha^{-i}$ とすると $\{\alpha^i, 0 \leq i \leq n-1\}$ の置換であるが, 上と同じく α^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なっている. さて μ_{-1} が分裂を与えるすると, $x^n - 1 = (x - 1) f(x)$ とするとき $f(x)$ の既約因子分解が $f(x) = a_1(x) \cdots a_s(x) b_1(x) \cdots b_s(x)$, ここで $\{a_i(x), b_i(x)\}$, $1 \leq i \leq s$ は相反対である, とおける. 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 $\{a_i(x), b_i(x)\}$, $1 \leq i \leq s$ が一対一

選んだ積が duadic code となるので、このとき 2^3 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まいと思ふ。

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 $\{a_i(x), b_i(x)\}$ ($1 \leq i \leq n$) について少なくとも一つの因子を持つことであり、 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、その様子を各 i について、一対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

$n = 2^{10} + 2^5 + 1 = 1057 = 7 \cdot 151$, $| \equiv 2 \pmod{1057}$.
 $151 \equiv 15 \pmod{1057}$ 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 "ガルーア" 平面を cyclic difference set の形で与えらる, $P = C(1) \cup C(5, 5) \cup C(4, 5, 3)$ とする.
 $Pc = P$ を満足する duadic idempotent c の存在を見る (一を構成する) ともいわけである. そのために各 $C(i)$ において $P \cdot C(i) + P$ 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ににする. とも角 $P(P \cdot C(i) + P) = P$ に注意しておく. 他方 $C(i)$ 達を μ_1 -pair にわけると, 36 個の pair が出来る.

さて行のラベルを $P \cdot C(i) + P$, 列のラベルを $\{C(j), \mu_1(C(j))\}$ とし, $(P \cdot C(i) + P, \{C(j), \mu_1(C(j))\})$ - 成分は $P \cdot C(i) + P$ の表示が pair の一方だけを含む時だけ 1, 否否時は 0 として, $GF(2)$ 上の incidence matrix 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 1 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, 709-7

14