数理解析研究所講究録
第 429 巻 1981 年 18-24

18

Cyclic Neofield と Cyclic 2-design

東京理科大理工　神保　雅一

cyclic neofield と $S_2(2,3,v)$ design との間には、密接な関係があることが知られている。ここでは、ある種の cyclic neofield と $S(2,4,v)$ design との間にも同様の関係があることを示す。

§1 Neofield

まず、neofield の定義と2,3の簡単な性質を挙げておく。

定義1　有限集合 S ($|S| = n \geq 2$) が二項演算 $+$, $\cdot$ に関して閉じているとする。このとき、$N_n = \langle S, +, \cdot \rangle$ が位数 n の finite neofield であるとは、次の条件を満足することである。

i) S が $+$ に関して loop をなす（この零元を0とする）。

ii) $S-\{0\}$ が $\cdot$ に関して群をなす（この単位元を1とする）

iii) 両側の分配法則が成立つ。

特に、$\langle S-\{0\}, \cdot \rangle$ が巡回群であるとき N_n を cyclic neofield といい、S の元を $0, 1, a, a^2, \cdots, a^{n-2}$ と表わすことにする。

cyclic neofield に関して次の性質が知られている。

補題1 (Paige)　N_n を finite cyclic neofield とする。このとき、

$$(-1) = \begin{cases} 1 & n \text{ が偶数のとき} \\ a^{\frac{n-1}{2}} & n \text{ が奇数のとき} \end{cases}$$

が成立つ．但し(-1)は、$1+x=0$ となる x のことである．

定義2　neofield N_n の元 g に対して、

$$x+(y+g)=y \qquad \forall y \in N_n$$

となるような x が（y によらず）存在するとき、x を g の交換逆元（exchange inverse）といい、N_n の任意の元が交換逆元をもつとき、N_n は XIP-neofield であるという。

$\mathbb{Z}_n$ を n を法とする剰余群とし、$\mathbb{Z}_{n-1}^{*}=\begin{cases}\mathbb{Z}_{n-1}\setminus\{0\} & (n\text{が偶数})\\ \mathbb{Z}_{n-1}\setminus\{\frac{n-1}{2}\} & (n\text{が奇数})\end{cases}$

とおく。N_n を cyclic XIP-neofield とし、

$$T=\{(k,n)\ ;\ 1+a^k=-a^n\ ,\ k,n\in\mathbb{Z}_{n-1}^{*}\} \cdots (1)$$

なる順序対の集合を考えると、T は次の性質をもつ。

(i)　$(k,n)\in T \implies (n-k,-k)\in T$

$\qquad\qquad (-n,\ k-n)\in T$

(ii)　任意の $k\in\mathbb{Z}_{n-1}^{*}$ に対して $(k,n)\in T$ なる $n\in\mathbb{Z}_{n-1}^{*}$ が唯一つ存在する。また、$(m,k)\in T$ なる $m\in\mathbb{Z}_{n-1}^{*}$ が唯一つ存在する。

また、逆に、性質(i)，(ii)をもつ $\mathbb{Z}_{n-1}^{*}$ の順序対の集合 T が存在するならば、$(k,n)\in T$ に対して $1+a^k=-a^n$ と定義することにより、XIP-neofield が得られる。（Hsu[ ] 参照）

§2 cyclic XIP-neofield と cyclic 2-design

点の数 v, ブロック上の点の数 k, 会合数 λ の t-design を $S_\lambda(t,k,v)$ design と書く。特に $\lambda=1$ の時には、$S(t,k,v)$ design と書くことにする。また、点上正則な巡回群を自己同型群の部分群として持つような $S_\lambda(t,k,v)$ design を cyclic $S_\lambda(t,k,v)$ design ということにする。

cyclic XIP-neofield と cyclic $S_\lambda(2,3,v)$ design の関係については、Johnsen and Stover [ ], Doner [ ], Hsu [ ] らによって研究されている。ここでは、ある種の cyclic XIP-neofield と cyclic $S(2,4,v)$ design の存在が同値であることを示す。

まず、位数 n が偶数の場合に、cyclic neofield N_n の元 g に対して、$1+(1+(\cdots+(1+(1+g))\cdots))=g$ となる 1 の数の最小値を元 g の characteristic ということにする。このとき、次の定理が成立つ。

定理1: n が偶数であるとすると、$0,1$ 以外のすべての元の characteristic が 3 の cyclic XIP-neofield N_n が存在することと cyclic $S(2,4,\frac{n-1}{3})$ design が存在することは同値である。

この定理を証明するために、次の補題を準備しておく。

補題2 N_n を定理1の性質を持つ neofield とし、順序対

の集合Tを(1)の如く定義すると、Tは(i)，(ii)の性質に加えて次の性質も持つ。

(iii) (k,m)，$(m,l)\in T$ ならば $k\neq l$ であり

$(l,k)\in T$

また、Tが(i)，(ii)，(iii)を満足するならば N_n は定理1の性質をもつ neofield である。

証明　$1+a^k=a^m$　$1+a^m=a^l$ である（なぜならば $-1=1$）。また a^k の charcteristic が3であるから $1+a^l=a^k$。逆も同様。

補題3　N_n を定理1の性質をもつ neofield とする。そして $1+a^k=a^m$，$1+a^m=a^l$，$1+a^l=a^k$ であるとすると、$k,m,l,-k,-m,-l,k-l,k-m,l-k,l-m,m-k,m-l$ はすべて異る。（但しこれらは $\mathbb{Z}_{n-1}^*$ の元と見なす）

証明：k,m,l は互いに異ることは明らか。$k\equiv -k \pmod{n-1}$ とすると $2k\equiv 0 \pmod{n-1}$　n は偶数であるから $k\equiv 0 \pmod{n-1}$ よって $k\in\mathbb{Z}_{n-1}^*$ 仰えに $k\neq -k \pmod{n-1}$。$k\equiv -m \pmod{n-1}$ とすると $(-m,m)\in T$ よって $(2m,m)\in T$ 従って $-m\equiv 2m \pmod{n-1}$。$3m\equiv 0 \pmod{n-1}$。従って、このような $m\in\mathbb{Z}_{n-1}^*$ が存在するには、$n-1$ が3で割り切れなければならない。ところが N_n は0，1以外のすべての元の charateristic が3であるから $n-2$ が3で割り切れる。これ

は矛盾．よって $k \not\equiv -m \pmod{n-1}$．他のものについても同様にして調べれば良い。

定理1の証明： cyclic $S(2,4,n-1)$ design は、$\mathbb{Z}_{n-1}$ を点の集合として持ち、$\mathbb{Z}_{n-1}$ の 4-subsets をブロックとして持つと見なして一般性を失なわない。今、$(0, k, m, \ell)$ をブロックとして持つならば、このブロックを cyclic に回した次のブロック $(-k, 0, m-k, \ell-k)$, $(-m, k-m, \ell-m)$, $(-\ell, k-\ell, m-\ell, 0)$ も存在するはずであり、$\lambda = 1$ であることより $k, m, \ell, -k, -m, -\ell, m-k, \ell-k, k-m, \ell-m, k-\ell, m-\ell$ はすべて異る。これらから次の順序対を作るとこれらは、性質(i), (iii)を満す。

(k, m) $(m-k, -k)$ $(-m, k-m)$

(m, ℓ) $(\ell-m, -m)$ $(-\ell, m-\ell)$

(ℓ, k) $(k-\ell, -\ell)$ $(-k, \ell-k)$

$(\ell-k, m-k)$ $(m-\ell, k-\ell)$ $(k-m, \ell-m)$

また、今使われなかったブロック $(0, k', m', \ell')$ について同様に行なう。これをくり返すと、順序対の集合 T は(i), (ii), (iii)を満し、従って求める neofield N_n を得る。

逆に定理1の性質をもつ neofield N_n から $1+a^k = a^m$, $1+a^m = a^\ell$, $1+a^\ell = a^k$ を満す $k, m, \ell \in \mathbb{Z}_{n-1}^*$ を取ることができる。ここで $(0, k, m, \ell)$ を初期ブロックと

して $(i, k+i, m+i, l+i) \pmod{n-1}$ なるブロック
を作る。このとき補題3に注意すると $(0, k, m, l)$
$(-k, 0, m-k, l-k)$, $(-m, k-m, 0, l-m)$, $(-l, k-l, m-l, 0)$
の各ブロックに現れる非零元はすべて異る。同様に

$$1+a^{k'}=a^{m'}, \quad 1+a^{m'}=a^{l'}, \quad 1+a^{l'}=a^{k'}$$

なる $k'\ l'\ m'$ を用いて $n-1$ 個のブロックを作る。これを
くり返すと、このようにしてできたブロックは、cyclic
$S(2, 4, n-1)$ design となっている。　　証明終

注意　$S(2, 4, v)$ design が存在するための必要十分条件は
$v \equiv 1$ or $4 \pmod{12}$ となることである。(Hanani)　また、
$v \equiv 1 \pmod{12}$ で v が素数であれば、cyclic $S(2, 4, v)$ design
が存在する(Bose)。

上のように、位数が偶数の場合には、0, 1以外の元の characteristic が3の
neofield の存在と $S(2, 4, v)$ design の存在が同値であることが
言えるが、位数が奇数の場合にも同様の結果が得られる。

定理2　n が奇数 $(= 12m+5)$ のときには、$0, 1, a^s, a^{2s}, a^{3s}$
$(s = 3m+1)$ 以外のすべての元について、

$$1-(1-(1-g)) = g$$

が成立つ cyclic XIP-neofield Nの存在と、cyclic $S(2, 4, n-1)$
design の存在とは同値である。

この証明は、n が偶数の場合とほぼ同様であるので省略す

るが、この場合には、$n-1$が4で割り切れるため、$(0, S, 25, 35)$なる形のブロックを持つことを注意しておく。

定理1，定理2によって cyclic neofield と cyclic $S(2, 4, v)$ design との関係がわかったが、残念ながら、定理1及び2の性質を満足するような neofield の構成方法はまだ知られていない。

[1] Doner,J.R., CIP-neofields and Combinatorial Designs. Ph.D. dissertation, The University of Michigan,1972.

[2] Johnsen,e.c. and Storer,T.F., Combinatorial Structures in Loops II. Commutative Inverse Property Cyclic Neofields of Prime Power Orders, Pacific J. of Math. 52, No. 1, 115-127, 1974.

[3] Hsu,D.F., Cyclic Neofields and Combinatorial Designs, Springer Lecture Note in Math. 824, 1980.