数理解析研究所講究録
第794巻1992年153-160

An inequality for primitive translation association schemes

北大・理 伊藤 豊治
(Toyoharu Itoh)

translation association scheme $\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$ とは，Xがアーベル群の構造を持つ，group association scheme $\mathfrak{X}(X)$ の fusion scheme である。ここで，group association scheme とは，Gを有限群，$C_0=\{e\}, C_1, \cdots C_d$ をGの共役類とするとき，

$$R_i=\{(x,y)\in G\times G \mid yx^{-1}\in C_i\} \quad i=0,1,\cdots,d$$

によって i次の関係を定義する commutative association sheme $\mathfrak{X}(G)=(G,\{R_i\}_{0\le i\le d})$ である。また association scheme $\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$ に対して $\{0,1,\cdots,d\}$ の分割 $\{\Lambda_j\}_{0\le j\le e}$ 但し $\Lambda_0=\{0\}$ を与え，$R_{\Lambda_j}=\bigcup_{\ell\in\Lambda_j}R_\ell$ $j=0,1,\cdots,e$ とする。このとき $\mathfrak{X}'=(X,\{R_{\Lambda_j}\}_{0\le j\le e})$ が association scheme となるとき，$\mathfrak{X}'$ を $\mathfrak{X}$ の fusion scheme という。本稿では，translation association scheme の基本的性質について述べる。

以下 $\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$ を association scheme とする。

定義 (primitive association scheme)

$$\mathfrak{X}:\text{primitive} \overset{\text{def}}{\Longleftrightarrow} \Gamma_i=(X,R_i)\ :\text{graph は connected} \quad {}^\forall i=1,2,\cdots,d.$$

group association scheme $\mathfrak{X}(G)$ が primitive である為の必要十分条件が，G が単純群であることがよく知られている。

<u>定義 (translation association scheme)</u>

$\mathfrak{X}$：translation association scheme

$\overset{\text{def}}{\Longleftrightarrow}$ (i) X はアーベル群の構造をもつ。

(ii) $(x,y)\in R_i \longrightarrow (x+z, y+z)\in R_i$

for $\forall i$, $x, y, z \in X$.

以下 translation association scheme を translation scheme という。

Examples

0) G：アーベル群

このとき，$\mathfrak{X}(G)$ は translation scheme である。

1) G_i：位数 m のアーベル群　$i=1,2,\cdots,m$　　$m,n\geq 2$.

$X = G_1\times G_2\times\cdots\times G_m$

$R_i = \{(x,y)\in X\times X \mid \partial(x,y)=i\}$ $(i=1,2,\cdots,m)$.　where $\partial(x,y)=\#\{i \mid x_i \neq y_i\}$

$x=(x_1,\cdots,x_n)$
$y=(y_1,\cdots,y_n)$.

とする。このとき，$(X,\{R_i\}_{0\leq i\leq n})$ は Hamming scheme $H(n,m)$ であり，translation scheme である。

2) $q := p^n$, p：素数，α：$GF(q)$ の primitive root

$d\in\mathbb{N}$ s.t. $\frac{q-1}{d}\in\mathbb{N}$, $K\leq GF(q)^{\times}$ subgroup s.t. $|K|=\frac{q-1}{d}$.

とする。このとき，

$R_0 := \{(x, x) \mid x \in GF(q)\}$

$R_i := \{(x, y) \in GF(q) \times GF(q) \mid y - x \in \alpha^i K\}$ $i = 1, 2, \cdots, d$.

と定義すると，$(GF(q), \{R_i\}_{0 \le i \le d})$ は translation scheme になる。この association scheme を cyclotomic scheme という。

この primitive translation scheme については，次のような conjecture がある。

<u>Conjecture (Brouwer et al [2] p.68)</u>

$\mathfrak{X} = (X, \{R_i\}_{0 \le i \le d})$: primitive translation scheme

このとき，次のいずれかが成り立つ。

(i) X は elementary abelian group である。

(ii) $\mathfrak{X}$ は Hamming scheme である。

(iii) $\mathfrak{X}$ は Latin square type 又は negative Latin square type の association scheme である。

しかし，この conjecture に対して，次の様な反例がある。それは，parameter (4000, 775, 150) を持つ，$\mathbb{Z}_5^3 \times \mathbb{Z}_2^5$ 上の McFarland difference set (R.L. McFarland [3]) から得られる，strongly regular graph で parameters が $(v, k, \lambda, \mu) = (4000, 775, 150, 150)$，$r = 25$，$s = -25$ を持つものである。

$\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$: translation scheme , $|X|=n$ とする。

そして $x\in X$ に対して $n\times n$-matrix P_x を次のように定義する。 $\forall a,b\in X$ に対して

$$P_x(a,b)=\begin{cases}1 & \text{if } x+a=b\\ 0 & \text{otherwise}\end{cases}$$

この行列 $P_x\ (x\in X)$ は group association scheme $\mathfrak{X}(X)$ の adjacency matrix であって、次の事をみたす。

$$P_xP_y=P_yP_x=P_{x+y}\ ,\ (P_x)^s=P_{sx}\ ,\quad P_x^t=P_{-x}$$

for all $x,y\in X$, $s\in \mathbb{Z}$,

$$A_i=\sum_{x\in N_i}P_x \qquad \text{for all } i$$

但し A_i は $\mathfrak{X}$ の i 次の adjacency matrix ,

$N_i=\{x\in X\mid (0,x)\in R_i\}$ $i=0,1,2,\cdots,d$.

(0 は X の単位元)

いま X をアーベル群とするとき、

rank(X) := the minimal cardinality of generating set of X .

とする。

補題。1.

$\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$: translation scheme of class d.

このとき、

$\mathfrak{X}$ は primitive $\rightleftarrows$ $X=\langle N_i\rangle$ $\forall i=1,2,\cdots,d$.

である。

証明. ($\longrightarrow$) [2] P.67 proposition 2.10.4 (i).

($\longleftarrow$) いま $\mathfrak{X}$ を imprimitive であるとする。よって $\exists i(\neq 0)$ で $\Gamma_i=(X,R_i)$ が disconnected となるものがある。これは $\langle N_i\rangle$ が X の proper subgroup であることを意味する。//.

定理。2.

$\mathfrak{X}=(X,\{R_i\}_{0\le i\le d})$: primitive translation scheme of class d, where X is of rank r.

k_i : R_i の valency

このとき、次が成り立つ。

(i) $k_i \geqq r$ for any $i=1,2,\cdots,d$, i.e. $\frac{|X|-1}{r}\geqq d$

(ii) もし $k_i=r$ for some $i(\neq 0)$, ならば X は素数位数の巡回群である。

(iii) もし X が素数位数の巡回群でなければ，次の不等式

が成り立つ。

$$\frac{|X|-1}{r+1} \geqq d.$$

証明 (i) 補題1より $k_i = |N_i| \geqq r.$ ($^\forall i \neq 0$)

よって $|X| = \sum_{i=0}^{d} k_i = 1 + \sum_{i=1}^{d} k_i \geqq 1 + rd.$

$$\therefore \frac{|X|-1}{r} \geqq d.$$

(ii) いま $\mathfrak{A}$ を $\mathfrak{X}$ の Bose-Mesner algebra とし, $k_1 = r$ と仮定する。(i.e. $i=1$ とする) $\therefore N_1 = \{x_1, \cdots, x_r\}$

$$A_1 = P_{x_1} + P_{x_2} + \cdots + P_{x_r}$$

となる。このとき

$$A_1^2 = \sum_{i=1}^{r} P_{2x_i} + 2 \sum_{i \lneqq j} P_{x_i + x_j} \quad \text{------} (*).$$

である。また X の rank が $r = k_1$ なので

$2x_i \notin \{x_i + x_j \mid 1 \leqq i \lneqq j \leqq r\}$, $x_i + x_j$ ($1 \leqq i \lneqq j \leqq r$) はすべて異なる。

Case 1. $2x_i$ ($1 \leqq i \leqq r$) はすべて異なる, 又は $2x_i = 0$ $^\forall i$.

いま $$B_m = \sum_{1 \leqq i_1 \lneqq \cdots \lneqq i_m \leqq r} P_{x_{i_1} + \cdots + x_{i_m}}$$ とすると, 仮定より $B_2 \in \mathfrak{A}$, また $B_m \in \mathfrak{A}$ ($m \geqq 2$) と仮定すると,

$$A_1 B_m = (m+1) B_{m+1} + \sum_{1 \leqq i_1 \lneqq \cdots \lneqq i_m \leqq r} \sum_{j=1}^{m} P_{x_{i_1} + \cdots + 2x_{i_j} + \cdots + x_{i_m}}$$

となり, $B_{m+1} \in \mathfrak{A}$ が得られる。よって m についての帰納法により, $B_r \in \mathfrak{A}$ i.e. $P_{x_1 + \cdots + x_r} \in \mathfrak{A}$ となる。すなわち, $^\exists k (\neq 0)$ で $N_k = \{x_1 + \cdots + x_r\}$ となるものが存在する。よって補題1と, $\mathfrak{X}$ の primitivity より, X は素数位数の巡回群となる。

Case 2. $\exists i \neq j$ に対して $2x_i = 2x_j$ 又は，$2x_i \neq 0$ $\exists i$

$$A_1^2 = \sum_{k=0}^{d} p_{11}^k A_k$$

なので，もし $2x_i = 0$ $\exists i$，ならば $p_{11'}^0 = \delta_{11'} r \neq 0$．よって，$x_i + x_j \neq 0$ $(1 \leqq i < j \leqq r)$，なので $2x_i = 0$ $(\forall i)$．これは仮定に反するので，$2x_i \neq 0$ $\forall i$。

(1)より $k_i \geqq r$ $(\forall i \neq 0)$ であり，(*)より，行列 $\sum_{i=1}^{r} P_{2x_i}$ の要素は 0 又は 2 なので r は偶数である。いま $r = 2s$ とし，

$$x_{2i-1} = y_i, \ x_{2i} = z_i \quad \text{such that} \quad 2z_i = 2y_i \ (1 \leqq i \leqq s).$$

とする。よって $$A_1 = \sum_{i=1}^{s} (P_{y_i} + P_{z_i})$$ となる。

いま A_1^3 を計算すると，$A_1^3 = 4C_3 + 6D$，但し．

$$C_t = \sum_{i=1}^{s} (P_{ty_i} + P_{(t-1)y_i + z_i}).$$

$$D = \sum_{i \neq j} (P_{y_i + 2y_j} + P_{z_i + 2y_j}) + \sum_{i,j,k \text{ distinct}} (P_{y_i + y_j + y_k} + P_{z_i + z_j + z_k})$$

$$+ \sum_{i<j} \sum_{k=1}^{s} (P_{y_i + y_j + z_k} + P_{z_i + z_j + y_k}).$$

このとき $2y_i$ $(1 \leqq i \leqq s)$ はすべて異なり，そして D は $(0,1)$-行列なので $C_3 \in \mathfrak{A}$ となる。また $C_t \in \mathfrak{A}$，$(t-1)y_i$ $(1 \leqq i \leqq s)$ はすべて異なる $(t \geqq 3)$ と仮定すると，C_t はある adjacency matrix と一致することになり，ty_i $(1 \leqq i \leqq s)$ はすべて異なることになる。

また $$A_1 C_t = 2C_{t+1} + \sum_{i \neq j} (P_{ty_i + y_j} + P_{ty_i + z_j} + P_{(t-1)y_i + z_i + y_j} + P_{(t-1)y_i + z_i + z_j})$$ で，$\sum(\cdots)$ は $(0,1)$-行列なので $C_{t+1} \in \mathfrak{A}$ となる。よって t についての帰納法により $C_t \in \mathfrak{A}$ $t = 3, 4, 5, \cdots\cdots$，そして

実際 C_t は、ある adjacency matrix と一致する。しかし、これは、$\exists t$ s.t. ${}^t y_1 = 0$ に反する。

以上より X は素数位数の巡回群である。

(iii) (ii) より $k_i \geqq r+1$ ($^\forall i \neq 0$) なので $\frac{|X|-1}{r+1} \geqq d$ は明らか。//

<u>注意：</u> 定理2(iii) の不等式で等号が成り立つ例。

p, q：素数 s.t. p は $GF(q)$ の primitive root.

このとき、class $\frac{p^{q-1}-1}{q}$ の $GF(p^{q-1})$ 上の cyclotomic scheme は primitive であり、$k_i = q$ ($^\forall i \neq 0$)，$\mathrm{rank}(GF(p^{q-1})) = q-1$ である。この translation scheme は定理2(iii)の不等式で等号が成り立つものである。

参考文献

[1] E. Bannai and T. Ito, "Algebraic Combinatorics I. Association scheme,"

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, "Distance-Regular Graphs,"

[3] R. L. McFarland, A family of difference sets in non-cyclic groups, Journal of Combinatorial Theory (A) 15 (1973), 1-10.

[4] T. Itoh and A. Munemasa, An inequality for primitive translation association schemes, preprint.