

An inequality for primitive translation association schemes

北大・理 伊藤 豊治

(Toyoharu Itoh)

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

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

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

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

定義 (primitive association scheme)

$\mathcal{X}$: primitive $\xLeftrightarrow{\text{def}} \Gamma_i = (X, R_i)$ graph は connected
 $\forall i = 1, 2, \dots, d.$

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

定義 (translation association scheme)

$\mathcal{X}$: translation association scheme

$\stackrel{\text{def}}{\iff} (i) X$ 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 とする。

Examples

0) G : アーベル群

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

1) G_i : 位数 m の アーベル群 $i=1, 2, \dots, n$ $m, n \geq 2$

$$X = G_1 \times G_2 \times \dots \times G_n$$

$$R_i = \{(x, y) \in X \times X \mid \partial(x, y) = i\} \quad \text{where } \partial(x, y) = \#\{i \mid x_i \neq y_i\}$$

$(i=1, 2, \dots, n)$.

$$x = (x_1, \dots, x_n)$$

$$y = (y_1, \dots, y_n).$$

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

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

とする。このとき,

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

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

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

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

Conjecture (Brouwer et al [2] p.68)

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

のとき, 次のいずれかが成り立つ。

- (i) X は elementary abelian group である。
- (ii) Σ は Hamming scheme である。
- (iii) Σ は Latin square type または negative Latin square type の association scheme である。

しかし, この conjecture に対し, 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。

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$: translation scheme, $|X| = n$ とする.

そして $x \in X$ に対し $n \times n$ -matrix P_x を次のように定義

する. $\forall a, b \in X$ に対し

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

この行列 P_x ($x \in X$) は group association scheme $\mathcal{X}(X)$ の adjacency matrix であり、次の事をみたとす.

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

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

$$A_i = \sum_{x \in N_i} P_x.$$

for all i

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

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

(0 は X の単位元)

いま X をアーベル群とすると、

$\text{rank}(X) :=$ the minimal cardinality of generating set of X .

とする。

補題. 1.

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

このとき,

Σ は primitive $\iff X = \langle N_i \rangle \quad \forall i=1, 2, \dots, d.$

がある。

証明. $(\implies)$ [2] p.67. proposition 2.10.4 (i).

$(\impliedby)$ いま Σ 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.

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

k_i : R_i の valency

このとき, 次の成り立つ。

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

(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。

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

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

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

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

(ii) $\mathcal{A}$ は $\mathcal{C}$ を $\mathcal{C}$ の Bose-Mesner algebra とし, $k_1 = r$ と仮定する. (i.e. $\lambda = 1$ とする) $\therefore N_1 = \{x_1, \dots, x_r\}$

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

となる。このとき

$$A_1^2 = \sum_{i=1}^r P_{2x_i} + 2 \sum_{1 \leq i < j \leq r} P_{x_i + x_j} \quad \dots \dots \dots (*)$$

である。また、 X の rank が $r = k_1$ なのだから

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

Case 1. $2x_i$ ($1 \leq i \leq r$) はすべて異なる。又は $2x_i = 0 \quad \forall i$.

$\mathcal{A}$ は $B_m = \sum_{1 \leq i_1 < \dots < i_m \leq r} P_{x_{i_1} + \dots + x_{i_m}}$ とすると、仮定より

$B_2 \in \mathcal{C}$, また $B_m \in \mathcal{C}$ ($m \geq 2$) と仮定すると,

$$A_1 B_m = (m+1) B_{m+1} + \sum_{1 \leq i_1 < \dots < i_m \leq r} \sum_{j=1}^m P_{x_{i_1} + \dots + 2x_{i_j} + \dots + x_{i_m}}$$

となり, $B_{m+1} \in \mathcal{C}$ が得られる。よって m についての帰納法により,

$B_r \in \mathcal{C}$ i.e. $P_{x_1 + \dots + x_r} \in \mathcal{C}$ となる。すなわち, $\exists k \neq 0$

で $N_k = \{x_1 + \dots + x_r\}$ となるものが存在する。よって補題 1 と,

$\mathcal{C}$ の primitivity より, X は素数位数の巡回群となる。

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

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

仮定より, もし $2x_i = 0 \quad \forall i$, ならば $P_{11}^0 = \delta_{11} \neq 0$. よって,
 $x_i + x_j \neq 0 \quad (1 \leq i \leq j \leq r)$, 仮定より $2x_i = 0 \quad (\forall i)$. これは仮定に反する
 ので, $2x_i \neq 0 \quad \forall i$.

(i) より $k_i \geq r \quad (\forall i \neq 0)$ であり, (*) より, 行列 $\sum_{i=1}^r P_{2x_i}$ の要素
 は 0 または 2 仮定より r は偶数である。いま $r = 2s$ とし,

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

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 $2y_i \quad (1 \leq i \leq s)$ はすべて異なる, 且 D は $(0,1)$ -行列.

仮定より $C_3 \in \mathcal{OL}$ となる。また $C_t \in \mathcal{OL}$, $(t-1)y_i \quad (1 \leq i \leq s)$ は
 すべて異なる ($t \geq 3$) と仮定すると, C_t はある adjacency matrix と一
 致することになり, $ty_i \quad (1 \leq i \leq s)$ はすべて異なることになり。

$$\text{また} \quad A_1 C_t = 2C_{t+1} + \sum_{i \neq j} (P_{ty_i + y_j} + P_{ty_i + z_j} + P_{(t-1)y_i + z_i + y_j} + P_{(t-1)y_i + z_i + z_j})$$

で, $\sum(\dots)$ は $(0,1)$ -行列なので $C_{t+1} \in \mathcal{OL}$ となる。よって

t についての帰納法により $C_t \in \mathcal{OL} \quad t=3, 4, 5, \dots$, 且 2

実際 C_L はある adjacency matrix と一致する。しかし、これは、
 $\exists t, t y_i = 0$ 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 $k_i \geq t+1$ ($\forall i \neq 0$) なので $\frac{|X|-1}{t+1} \geq d$ は明らか。

注意: 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 $\frac{p^q-1}{q}$ の $GF(p^{q-1})$ 上の cyclotomic scheme は primitive であり, $k_i = q$ ($\forall i \neq 0$), $\text{rank}(GF(p^{q-1})) = q-1$ 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.