

置換群の組合せ論的可移拡大からできるデザイン

宮本 泉

IZUMI MIYAMOTO

山梨大学

UNIVERSITY OF YAMANASHI*

1 アソシエーションスキームとスーパースキーム

G は集合 $X = \{1, 2, \dots, n\}$ に作用する置換群とする。 G は可移とはすべての $i, j \in X$ に対して、 $i^g = j$ となる $g \in G$ が存在することである。(すなわち、 X 上の orbit の個数が 1 個) G の $X \times X$ への作用を $(i, j)^g = (i^g, j^g)$ で定め、 $X \times X$ を G の orbit に分ける。

例: $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$$X \times X = R_0 + R_1 + R_2 + R_3 + R_4 + R_5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 4 & 5 & 5 \\ 1 & 0 & 3 & 2 & 4 & 4 & 5 & 5 \\ 3 & 2 & 0 & 1 & 5 & 5 & 4 & 4 \\ 2 & 3 & 1 & 0 & 5 & 5 & 4 & 4 \\ 4 & 4 & 5 & 5 & 0 & 1 & 2 & 3 \\ 4 & 4 & 5 & 5 & 1 & 0 & 3 & 2 \\ 5 & 5 & 4 & 4 & 3 & 2 & 0 & 1 \\ 5 & 5 & 4 & 4 & 2 & 3 & 1 & 0 \end{pmatrix}$$

$R_0 = \{(1, 1), (2, 2), \dots, (8, 8)\}$, $R_1 = \{(1, 2), (2, 1), (3, 4), (4, 3), \dots, (7, 8), (8, 7)\}$,

$R_2 = \{(1, 3), (3, 2), (2, 4), (4, 1), \dots, (6, 8), (8, 5)\}$, ...

このとき、 $G = \text{Group}([(5, 6)(7, 8), (1, 3, 2, 4)(5, 8, 6, 7), (1, 6, 2, 5)(3, 8, 4, 7)])$ これらの orbit の組合せ論的性質が、以下に示すアソシエーションスキームとなる。

集合 $X = \{v_1, v_2, \dots, v_n\}$ とし、関係 $R_i \subset X \times X$, $0 \leq i \leq d$ とする。

定義: $(X, \{R_i\}_{0 \leq i \leq d})$ がアソシエーションスキーム

1. $R_0, R_1, \dots, R_d$ は $X \times X$ の分割
2. $R_0 = \{(v, v) | v \in X\}$
3. ${}^i R_i = \{(v_i, v_j) | (v_j, v_i) \in R_i\} = R_i$ for some i *
4. 任意の $(u, v) \in R_k$ に対して $\#\{w | (u, w) \in R_i, (w, v) \in R_j\}$ は一定。これを、 $p_{i,j,k}$ とする。

G が X 上 2 重可移とは、すべての (i_1, i_2) , $i_1 \neq i_2$, (j_1, j_2) , $j_1 \neq j_2$ に対して $(i_1^g, i_2^g) = (j_1, j_2)$ となる $g \in G$ が存在することをいう。このとき、 G は $X \times X$ 上の orbit の個数は 2 個となり、 G の作るアソシ

*imiyamoto@yamanashi.ac.jp

エーシヨンスキームによる $X \times X$ の分割は下の様になる。

$$X \times X = R_0 + R_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

G の作るアソシエーションスキームは対称群のの作るものと同じになる。そこで、対称群と対称群ではない 2 重可移群を区別するためには、 $X^3 = X \times X \times X$, $X^4 = X \times X \times X \times X$, $\dots$ 上の orbit も考える必要がある。そのために、スーパースキームを導入する。

定義: $(X, \Pi_{1 \leq l \leq t}^l)$ が t -superscheme であるとは、

1. $\Pi^l = \{R_0^l, R_1^l, \dots, R_{d_l}^l\}$ は X^l の分割 ($1 \leq l \leq t$, $t \geq 2$)
2. $\pi_l: X^l \rightarrow X^{l-1}$ ($(u_1, u_2, \dots, u_{l-1}, u_l) \rightarrow (u_1, u_2, \dots, u_{l-1})$) とおくと, $\pi_l(R_k^l) \in \Pi^{l-1}$ が成立. さらに, $\# \pi_l^{-1}((u_1, u_2, \dots, u_{l-1})) \cap R_k^l = \begin{cases} p_k^l & \text{if } (u_1, u_2, \dots, u_{l-1}) \in \pi_l(R_k^l) \\ 0 & \text{if } (u_1, u_2, \dots, u_{l-1}) \notin \pi_l(R_k^l) \end{cases}$ (regular)
3. $\sigma \in \text{SymmetricGroup}(l)$ に対して, $\sigma(R_k^l) \in \Pi^l$ が成立する。
ただし $\sigma(R_k^l) = \{(u_{\sigma(1)}, u_{\sigma(2)}, \dots, u_{\sigma(l)}) | (u_1, u_2, \dots, u_l) \in R_k^l\}$ (symmetric)

例: X 上の置換群 G の X^l 上 orbit ($1 \leq l \leq t$) は t -superscheme

例: アソシエーションスキームは次のような 3-スーパースキームとなっている。アソシエーションスキームから自然に誘導される X^3 の分割 $R_{i,j,k} = \{(u, v, w) | (u, v) \in R_k, (u, w) \in R_i, (w, v) \in R_j\}$ を考えると、 $\pi: X^3 \rightarrow X^2$, $(u, v, w) \rightarrow (u, v)$ とおくと、 $\# \pi^{-1}((u, v)) \cap R_{i,j,k} = \begin{cases} p_{i,j,k} & \text{if } (u, v) \in R_k \\ 0 & \text{if } (u, v) \notin R_k \end{cases}$ となっている。

2 置換群の可移拡大への応用

G の点 n の固定部分群を $G_n = \{g \in G | n^g = n\}$ で表す。 $X \setminus \{n\}$ 上、可移な置換群として H を与えて、点 n の固定部分群が $G_n = H$ となる 2 重可移群 G を構成する。あるいは、 G が存在しないことを示す。 G を $X = \{1, 2, \dots, n\}$ 上の 2 重可移群とすると、点 n を fix する部分群 G_n から G を復元する。これらのことを、群を使わずに、 G_n の作るスーパースキームから G が存在するならばそれによって作られるはずのスーパースキームを構成することによって行う ([5, 6])。

方法: G_n の作る 3-superscheme の X^3 上の orbit を集めて、可能な G の 3-superscheme を構成する。これを、superscheme の性質をチェックすることによって行う。

G_n の $(X \setminus \{n\})^{(3)} = \{(i, j, k) | \text{相異なる } i, j, k \in X \setminus \{n\} \text{ 上の orbit の個数が } 64 \text{ 以下程度で計算できた。本研究の計算機による実験は、GAP システムを使って行っている。GAP システムのライブラリにある } 2499 \text{ 次までの primitive な群で上の条件を満たすものについてスーパースキームを構成した結果を表 1 に示す [7]。さらに、superscheme ができても、可移拡大の群が存在しないことがある。そのような例の応用として、t-デザインの構成を試みる [7]。}$

表 1: GAP のライブラリにある 2499 次までの原始的置換群で条件を満たすものの可移拡大の計算

	total	次数		
		≤ 99	$100 \leq * \leq 999$	$1000 \leq$
G_0	1637	333	808	496
superscheme	226	124	85	17
assoc scheme	77	54	16	7
可移拡大	71	48	16	7

3 orbit-like set と t -デザイン

定義: (X, B) が t -(v, k, λ) デザイン $\iff$

- $v = |X|$
- B は、 X の k 点部分集合の multi-set。 B に属する k 点部分集合 b をブロックという。
- X のどの t 点部分集合も、ちょうど λ 個のブロックに属する。

G を X の l 点部分集合に $\{x_1, x_2, \dots, x_l\}^g = \{x_1^g, x_2^g, \dots, x_l^g\}$ により作用させる。 G が X の t 点部分集合全体の上に可移、つまり、任意の t 点部分集合 $\{x_1, x_2, \dots, x_t\}$ と $\{y_1, y_2, \dots, y_t\}$ に対して、 $\{x_1, x_2, \dots, x_t\}^g = \{y_1, y_2, \dots, y_t\}$ となる $g \in G$ が存在するとき、 t -homogeneous という。このとき、 G の X の k 点部分集合上の orbit を B とすると t -($|X|, k, \lambda$) デザインができる。

$X^{(l)} = \{(x_1, x_2, \dots, x_l) | x_1, x_2, \dots, x_l \in X (\text{相異なる})\}$ とする。スーパースキームの定義にある分割 $\Pi^l = \{R_0^l, R_1^l, \dots, R_d^l\}$ が、ある m で $R_m^l = X^{(l)}$ となるとき、 l -homogeneous であると定める。可移拡大は存在しないが、スーパースキームが構成できたとき、orbit の様な集合を考えてデザインを作る。以下に、例で示す。

$X = \{1, 2, \dots, 20, 21\}$, $|X| = 21$, $G_{21} = PSL(2, 19)$ on $X \setminus \{21\}$ とする。2 重可移で 3-homogeneous となっている。このとき、 G_{21} から、3-homogeneous 4-superschemes が得られるが、群 G_{21} の可移拡大は存在しない。 $\Pi^{(4)} = \{R_1^4, R_2^4\}$, $p_{1,4}^4 = 9$ 、つまり、orbit (の様な集合) 2 個で、9 個の 4 点対が $[x, y, z, w_1], [x, y, z, w_2], \dots, [x, y, z, w_9] \in R_1^4$ となるので、9 点部分集合 $\{w_1, w_2, \dots, w_9\}$ を、可移拡大が存在した場合に、 x, y, z を固定する部分群の orbit と考える。 x, y, z を動かしたときにできるこの 9 点部分集合は 1520 個が 3 回繰返して現れ、570 個が 6 回繰返して現れる。これらをブロックとすると、3-design (with repeated blocks) が得られる。群の拡大が存在したら、4 デザインになっているはずであるが、そうっていない。

4 A Generalization

Let a group G_0 be t -homogeneous on $X \setminus \{0\}$. Choose some orbits of G_0 on the $(k+1)$ -point subsets of X such that

B_0 a orbit such that $0 \in b_0 \in B_0$,

B_1, B'_1 orbits such that $0 \notin b_1 \in B_1 \cup B'_1$.

Let g_0, g_1, g'_1 be the orders of the stabilizers of $(k+1)$ -point subsets of these orbits in G_0 , respectively. In the following theorem $c_j B_j$ means that any block in B_j is repeated c_j times.

定理 1 ([9])

Let $B = c_0 B_0 \cup c_1 B_1 \cup c'_1 B'_1$, where c_0, c_1 and c'_1 satisfy

$$\frac{(n-k)c_0}{(k+1)g_0} = \frac{c_1}{g_1} + \frac{c'_1}{g'_1}.$$

Then (X, B) is a t -($n+1, k+1, \lambda$) design, where

$$\lambda = \frac{c_0 g \binom{k}{t-1}}{g_0 \binom{n}{t-1}}$$

In particular, if $c'_1 = 0$, then $B = c_0 B_0 \cup c_1 B_1$ and the above condition becomes

$$\frac{c_1}{c_0} = \frac{g_1(n-k)}{g_0(k+1)}.$$

Proof.

$$\begin{aligned} & \frac{\#\{(T, b) | T \text{ } t\text{-subset} \not\ni 0, b \in c_0 B_0 \cup c_1 B_1 \cup c'_1 B'_1\}}{\binom{n}{t}} \\ &= \frac{\frac{c_1 g}{g_1} \binom{k+1}{t} + \frac{c'_1 g}{g'_1} \binom{k+1}{t} + \frac{c_0 g}{g_0} \binom{k}{t}}{\binom{n}{t}} \\ &= \frac{\frac{k+1}{t} \binom{k}{t-1} \left\{ \frac{c_1 g}{g_1} + \frac{c'_1 g}{g'_1} \right\} + \frac{k-t+1}{t} \frac{c_0 g}{g_0} \binom{k}{t-1}}{\frac{n-t+1}{t} \binom{n}{t-1}} \\ &= \frac{\left\{ \frac{k+1}{t} \left\{ \frac{c_1 g}{g_1} + \frac{c'_1 g}{g'_1} \right\} + \frac{k-t+1}{t} \frac{c_0 g}{g_0} \right\} \binom{k}{t-1}}{\frac{n-t+1}{t} \binom{n}{t-1}} \\ &= \frac{\#\{(T, b) | T \text{ } t\text{-subset} \ni 0, b \in c_0 B_0\}}{\binom{n}{t-1}} = \frac{\frac{c_0 g}{g_0} \binom{k}{t-1}}{\binom{n}{t-1}} \end{aligned}$$

Example: $G = PSL(2, q)$ or $PGL(2, q)$ acting on projective line $\mathbf{P} = \{1, 2, \dots, q+1\}$. If $G = PSL(2, q)$, we assume that $q \equiv 3 \pmod{4}$. Then G is 3-homogeneous. Let $G_{1,2}$ be the stabilizer of the points 1 and 2 in G . We assume $q \equiv 1 \pmod{6}$. Then $3|q-1$. $G_{1,2}$ has subgroups of order 3 and of order $\frac{1}{2}(q-1)$ having $\frac{1}{3}(q-1)$ orbits of length 3 and two orbits of length $\frac{1}{2}(q-1)$ respectively. We use some of these orbits to

construct blocks.

Set

$$b_0 = \bigcup \frac{1}{6}(q-7) \text{ orbits of length } 3 \cup \{0, 1, 2\}$$

$$b_1 = \bigcup \frac{1}{6}(q-1) \text{ orbits of length } 3$$

$$b'_1 = \text{a orbit of length } \frac{1}{2}(q-1)$$

Then $k+1 = \frac{1}{2}(q-1)$ (block size). The orders of the stabilizers of the blocks b_0, b_1, b'_1 should be $g_0 = 3c_0$, $g_1 = 3c_1$, $g'_1 = \frac{c'_1}{2}(q-1)$, respectively. Set $B = c_0B_0 \cup c_1B_1 \cup c'_1B'_1$. Then we have

$$\frac{(n-k)c_0}{(k+1)g_0} = \frac{q+1-\frac{1}{2}(q-3)}{\frac{1}{2}(q-1) \times 3} = \frac{q+5}{3(q-1)}$$

$$\frac{c_1}{g_1} + \frac{c'_1}{g'_1} = \frac{1}{3} + \frac{2}{q-1} = \frac{q+5}{3(q-1)}$$

$|G| = \frac{1}{m}(q+1)q(q-1)$, where $m = 2$ or 1 according as $G = PSL(2, q)$ or $PGL(2, q)$.

$$\lambda = \frac{(q-1)(q-3)(q-5)}{12m}$$

定理 2 ([8])

$(P \cup \{0\}, B)$ is a $3-(q+2, \frac{1}{2}(q-1), \frac{1}{12m}(q-1)(q-3)(q-5))$ design.

G is as above. Similarly we chose 3 subsets of $P \cup \{0\}$ of size $\frac{1}{2}(q+1)$ so that the stabilizers are of order $g_0 = c_0$, $g_1 = c_1$, $g'_1 = \frac{c'_1}{2}(q+1)$

定理 3

$(P \cup \{0\}, B)$ is a $3-(q+2, \frac{1}{2}(q+1), \frac{1}{4m}(q-1)^2(q-3))$ design.

5 Experiments

We use GAP system [3] in our experiments. $G = PSL(2, 31) = \text{PrimitiveGroup}(32, 4)$. Then we can choose the blocks of size $\frac{1}{2}(q-1) = 15$ so that the stabilizers are of order 3, 3, 15. Therefore we have that $(P \cup \{33\}, B)$ is a simple $3-(33, 15, 910)$ design.

$G = PGL(2, 25) = \text{PrimitiveGroup}(26, 2)$. We can choose the blocks of size $\frac{1}{2}(q-1) = 12$ so that the stabilizers are of order 6, 6, 24. So by Theorem 2 $c_0 = c_1 = c'_1 = 2$, which implies $B = 2B_0 \cup 2B_1 \cup 2B'_1$. In this case, if we set $B = B_0 \cup B_1 \cup B'_1$, we have a simple $3-(27, 12, 440)$ design.

$G = PGL(2, 25) = \text{PrimitiveGroup}(26, 2)$. We can choose the blocks of size $\frac{1}{2}(q+1) = 13$ so that the stabilizers are of order 2, 2 and 26. So by Theorem 3 $c_0 = c_1 = c'_1 = 2$. We have a simple $3-(27, 13, 1584)$ design if we set $B = B_0 \cup B_1 \cup B'_1$.

$G = PSL(2, 19) = \text{PrimitiveGroup}(20, 1)$. We can choose subsets of size $\frac{1}{2}(q+1) = 10$ so that the stabilizers are of order 1, 1, 10. So by Theorem 3 $c_0 = c_1 = c'_1 = 1$. We have a simple $3-(21, 10, 648)$ design.

The subgroups of $PSL(2, q)$ are well known (cf. [2]). Probably we will be able to get simple $3-(q+2, k, \lambda)$ designs, $k = \frac{1}{2}(q-1)$ and $\frac{1}{2}(q+1)$, generally ([9]).

$G = AGL(2, 5) = \text{PrimitiveGroup}(25, 22)$. $|G| = 12000$ We can choose b_0 and b_1 of size 5 so that the stabilizers of these blocks are of order 80 and 400. Then

$$\frac{g_1(n-k)}{g_0(k+1)} = \frac{400(25-4)}{80(4+1)} = 21.$$

So if we set $B = B_0 \cup 21B_1$, then we have a 2-(26,5,24) design by Theorem 1. We can also choose subsets of size 6 so that the stabilizers are of order 400 and 12. Then

$$\frac{g_1(n-k)}{g_0(k+1)} = \frac{12(25-5)}{400(5+1)} = \frac{1}{10}.$$

So if we set $B = 10B_0 \cup B_1$, then we have a 2-(26,6,60) design.

$G = \text{MathieuGroup}(24) = \langle (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23), (3, 17, 10, 7, 9)(4, 13, 14, 19, 5)(8, 18, 11, 12, 23)(15, 20, 22, 21, 16), (1, 24)(2, 23)(3, 12)(4, 16)(5, 18)(6, 10)(7, 20)(8, 14)(9, 21)(11, 17)(13, 22)(15, 19) \rangle$ in the GAP library. G acts on $\{1, 2, \dots, 24\}$. We take 25 as the additional point and set

$$\begin{aligned} b_0 &= \{3, 4, 6, 7, 10, 12, 13, 14, 17, 21, 22, 25\}, \\ b_1 &= \{3, 4, 5, 6, 7, 10, 11, 12, 14, 18, 21, 23\} \text{ and} \\ b'_1 &= \{1, 2, 3, 4, 5, 6, 8, 11, 13, 15, 18, 24\}. \end{aligned}$$

The stabilizers of these blocks are of order 7920, 95040 and 6912 respectively. Set $c_0 = 5$, $c_1 = 10$ and $c'_1 = 4$ and set $B = 5B_0 \cup 10B_1 \cup 4B'_1$. Then

$$\frac{(24-11) \times 5}{(11+1) \times 7920} = \frac{13}{19008} = \frac{10}{95040} + \frac{4}{6912}$$

and $\lambda = 4800$. So (X, B) is a 5-(25,12,4800) design, since G is 5-homogeneous. Moreover we see that (X, B) is a 6-(25,12,1680) design.

サイズ v が決まっていれば、コンピュータを使ったデザインの構成は様々に行われている (例えば, [1])。ここには、定理の応用例としての実験を示した。また、デザインについては [4] 等を参照されたい。

参 考 文 献

- [1] A. Betten, E. Haberberger, R. Laue, A. Wassermann, DISCRETA - a program to construct t-designs with prescribed automorphism group. <http://www.mathe2.uni-bayreuth.de/discreta/>
- [2] P. J. Cameron, H.R.Maimani, G.R.Omidi and B. Tayfeh-Rezaie, 3-Designs from $\text{PSL}(2, q)$. *Discrete Math.*, 3063–3073, 306 (2006).
- [3] The GAP Groups. Gap - groups, algorithms and programming, version 4. *Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany and School of Mathematical and Computational Sciences, Univ. St. Andrews, Scotland*, 2000.
- [4] G. B. Khosrovshahi and R. Laue, t-Designs with $t \geq 3$, in *Handbook of Combinatorial Designs (2nd Edition)*, CRC Press Series on Discrete Mathematics and its Applications, C. J. Colbourn and J. H. Dinitz (eds.) CRC Press, Boca Raton, FL, (2006) 79–101.
- [5] 宮本泉, アソシエーションスキームの拡張と 2 重可移群の計算. *Computer Algebra, Algorithms, Implementations and Applications*, 数理解析研究所講究録 185–189, 1394 (2004)
- [6] 宮本泉, 置換群の可移拡大の計算法, *Computer Algebra, Algorithms, Implementations and Applications*, 数理解析研究所講究録 35–39, 1456 (2005)
- [7] I. Miyamoto, A Computation of Some Multiply Homogeneous Superschemes from Transitive Permutation Groups. In: Brown, C.W. (ed) *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation*. ACM press, 293–298 (2007)

- [8] I. Miyamoto, A construction of designs from $PSL(2, q)$ and $PGL(2, q)$, $q \equiv 1 \pmod{6}$, on $q + 2$ points. *to appear in Algorithmic Algebraic Combinatorics and Gröbner Bases, edited by G. Jones, A. Jurisic, M. Muzychuk and I. Ponomarenko* Springer.
- [9] I. Miyamoto, A construction of designs on $n + 1$ points from multiply homogeneous permutation groups of degree n . in preparation.