アソシエーションスキームの拡張と２重可移群の計算

宮本 泉

MIYAMOTO IZUMI*

山梨大学

UNIVERSITY OF YAMANASHI†

1 アソシエーションスキーム

置換群とアソシエーションスキームの関係を見るとき、2 重可移群の場合にはアソシエーションスキームは自明なものになり、そこからもとの 2 重可移群がどの様なものであるかを考えることはできません。ここでは、アソシエーションスキームの或る種の拡張を考えて、とくに、2 重可移群の場合に、もとの群が構成できるかどうかを調べます。すべての 2 重可移群の分類は、有限単純群の分類をもとにしてできていますが、構成的な計算法についての研究はほとんど無いようです ([2])。集合 $X = \{v_1, v_2, \cdots, v_n\}$、関係 $R_i \subset X \times X$, $0 \le i \le d$ に対して、

定義：$(X, \{R_i\}_{0 \le i \le d})$ が アソシエーションスキーム であるとは

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

例：G は X 上の可移な置換群、 R_i は G を $X \times X$ に作用させたときの orbit。$X = \{1, 2, 3, 4, 5, 6, 7, 8\}$、$G = \mathrm{Group}([\ (5,6)(7,8),\ (1,3,2,4)(5,8,6,7),\ (1,6,2,5)(3,8,4,7)\ ])$ とすると、${}^tR_2 = R_3$、それ以外は、${}^tR_i = R_i$ で、

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

*佐藤真久氏に感謝します。

†imiyamoto@yamanashi.ac.jp

この関係行列による表示は、(i,j) 成分が $k \iff k \in R_k$ により定めます。とくに、 G が X 上 2 重可移 $\iff$ G は $X \times X \backslash R_0$ 上可移 となるので、$X \times X$ の分割は、下のようになります。そして、このアソシエーションスキームの自己同型群は、X 上の対称群 $Sym(X)$ になります。

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

2 Superscheme

アソシエーションスキームの拡張して、一般に $X \times X \times X$ の分割なども考慮すします。
定義：(X, Π) が superscheme であるとは、

1. $\Pi^l = \{R_0^l, R_1^l, \cdots, R_{d_l}^l\}$ は X^l の分割 $(1 \le l \le m,\ m \ge 2)$。
2. $\pi_l : X^l \to X^{l-1} \quad (u_1, u_2, \cdots, u_{l-1}, u_l) \to (u_1, u_2, \cdots, u_{l-1})$ とおくと、 $\pi_l(R_k^l) \in \Pi^{l-1}$ が成立。
3. $(u_1, u_2, \cdots, u_{l-1}) \in \pi_l(R_k^l)$ にたいして $p_k^l = \#\pi_l^{-1}((u_1, u_2, \cdots, u_{l-1})) \cap R_k^l$ は一定。(regular)
4. $\sigma \in Sym(l)$ にたいして、$\sigma(R_k^l) \in \Pi^l$、ただし、$\sigma(R_k^l) = \{(u_{\sigma(1)}, u_{\sigma(2)}, \cdots, u_{\sigma(l)}) | (u_1, u_2, \cdots, u_l) \in R_k^l\}$。(symmetric)

superscheme には他の定義もありますが、この定義は Ivanyos のプリントを参考にしました。アソシエーションスキームの定義から自然に $R_{i,j,k} = \{(u,v,w) | (u,v) \in R_k, (u,w) \in R_i, (w,v) \in R_j\}$ による X^3 の分割が誘導され、$m = 3$ の superscheme になっています。このとき、$(u,v) \in R_k$ にたいして、$\#\pi^{-1}((u,v)) \cap R_{i,j,k} = p_{i,j,k}$ となります。アソシエーションスキームのときと同様に、X 上の (可移とは限らない) 群 G の X^l 上 orbit$(1 \le l \le m)$ は superscheme になります。16 次の場合で、アソシエーションスキームは約２００個、可移な置換群は約２０００個、可移な置換群からつくられる ($m = 3$ の) superscheme は約４００個あります。

3 計算アルゴリズム

ここでは、2 重可移群を、その 1 点固定部分群から復元することを試みます。G を $X = \{1, 2, \cdots, n\}$ 上の 2 重可移群、G_n を点 n を固定する部分群とします。2 重可移で、3 重可移ではない群 G にたいして、G_n の X^3 上の orbit を集めて、G の orbit を構成することを考えます。このことは、G_n のつくる ($m = 3$ の)superscheme による分割をもとに G のつくる superscheme を推測することを意味します。以下に、詳しく説明をして、例を紹介します。$X^{(l)} = \{(i_1, i_2, \cdots, i_l) \in X^l | j \neq k$ のとき $i_j \neq i_k\}$ とします。G の X^2 の orbit は R_0 と $X^{(2)}$、つまり、G のつくる superscheme による X^2 の分割が $\Pi^2 = \{R_0, X^{(2)}\}$ となることから、考慮するのは $X^{(l)}$ に含まれる orbit のみで十分になります。

G_n の $X^{(3)}$ 上の orbit には、次の 3 種類があります。

1. 点 n を含まないもの $\cdots$ G_n の $X\backslash\{n\}$ 上の superscheme
2. (i_1,i_2,n) を含むもの $\cdots$ π_3 を通して、G_n の $X\backslash\{n\}$ 上のアソシエーションスキーム
3. 残り、(i_1,n,i_2),(n,i_1,i_2) を含む $\cdots$ $\sigma(\{(i_1,i_2,n)\})$ により得られる。

これらの orbit を集めて、π_3 による像が $X^{(2)}$ になり、さらに、superscheme の定義にある性質３と４を満たすようにします。具体的には、projection π_3 による対応が $p^3_k:1$ の一定になること、性質４の対称性から、定義には入れてない projection についても同様の対応になっていることです。さらに、対称性で orbit がどの様に動くかも考慮します。G の $X^{(3)}$ 上の orbit で点 n を含む組と、G_n の orbit の種類２と３のものが対応しているので、G の $X^{(3)}$ 上の orbit には種類２と３の orbit がそれぞれ丁度１つ含まれています。そこでの π_3 の対応から、p^3_k の値が定まり、したがって、含まれる orbit はサイズが等しいこともわかります。`GAP` を使って書いた計算プログラムは、この条件をみたす G_n の $X^{(3)}$ 上の orbit の組合せを全て求めます。プログラムでは、G_n の $X^{(3)}$ 上の orbit に番号を付けて、その番号で答を返します。条件を満たす組合せが無いときは、空の答 [ ] を返します。このことは、特に、G_n を１点固定群とする２重可移群は存在しないことを意味します。また、G が３重可移以上のときは、$m=3$ の superscheme に代えて、適当な $m\geq 4$ の superscheme を考えます。この場合の例も次節にありますので、参照下さい。

表 1：$GL(3,2)$ on $\{1,2,\cdots,7\}$ の orbit と π_3 による対応表

orbit 番号	1	2	3	4	5	6	7	8	9	10	11
代表	[7,1,6]	[7,1,2]	[1,7,6]	[1,7,2]	[1,6,7]	[1,2,7]	[1,2,3]	[1,2,4]	[1,2,5]	[1,2,6]	[1,6,2]
π_3	[7,1] 1	[7,1] 4	[1,7] 1	[1,7] 4	[1,6] 1	[1,2] 1	[1,2] 1	[1,2] 1	[1,2] 1	[1,2] 1	[1,6] 4
$[\sigma_1,\sigma_2]$	[3,5]	[4,6]	[1,3]	[2,4]	[5,1]	[6,2]	[7,7]	[8,8]	[10,11]	[9,10]	[11,9]
種類	3	3	3	3	2	2	1	1	1	1	1
size	6	24	6	24	6	24	24	24	24	24	24

例：2 重可移群 $G=$GL(3,2)、 $X=\{1,2,\cdots,7\}$、G は $X^{(3)}$ 上に、 長さ 42 と 168 の 2 個の orbit をもつ。G_7 の $(X\backslash\{7\})^{(2)}$ 上の orbit は２個、長さ 6 と 24、(それぞれ $[1,6]$、$[1,2]\in X^{(2)}$ を含む)、G_7 の $(X\backslash\{7\})^{(3)}$ 上の orbit、 長さ 24 が 5 個したがって、G_7 の $X^{(3)}$ 上の orbit は、 $6+5=11$ 個、表 1 を参照してください。G_7 の $X^{(3)}$ 上の orbit の π_3 による像は G_7 の $X^{(2)}$ 上の orbit になることに注意して計算します。G の $X^{(3)}$ 上の orbit を作るために、最初、おなじサイズの種類２、３の orbit １、３、５番を集めて π_3 による像を考慮すると、この時点で不足しているのは像が [1,2] を含む orbit になり、その対応が 1:1 である orbit で、orbit 番号７、８、９、１０が候補になります。そこで対称性を考慮すると９、１０番は除外されます。ここで得られる答は、[1,3,5,7] と [1,3,5,8] の２つになります。さらに、π_3 以外の projection に関する条件を考慮し、残った部分も同様にして、プログラムの答は

$$
\begin{array}{l}
[\ [\ [1,3,5,7],[2,4,6,8,9,10,11]\ ],\\
\ \ [\ [1,3,5,8],[2,4,6,7,9,10,11]\ ]\ ]
\end{array}
$$

の２つになります。
今回得られた答の自己同型群を計算すると最初に与えられた GL(3,2) と、その 7 次対称群における共役群になり、いずれも正しい答を与えています。

4　計算例

例：前節の群 G_7 のつくる $\{1,2,\cdots,6\}$ 上のアソシエーションスキームをもとに G を復元できるかを見ます。このアソシエーションスキームの関係行列は

$$\begin{pmatrix} 0 & 1 & 2 & 2 & 2 & 2 \\ 1 & 0 & 2 & 2 & 2 & 2 \\ 2 & 2 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 & 0 & 1 \\ 2 & 2 & 2 & 2 & 1 & 0 \end{pmatrix}$$

となり、この自己同型群は $Sym(2) \wr Sym(3) \supset G_7$ になります。このアソシエーションスキームが誘導する $(X\backslash\{7\})^{(3)}$ の分割は、 サイズ 48、24、24、24 の集合で構成されていて、superscheme で考えた場合と対比して示すと表 2 になります。

表 2：G_7 のアソシエーションスキームの誘導する $X^{(3)}$ の分割

分割を構成する集合のサイズ	6	24	6	24	6	24	48	24	24	24
対応する G_7 の orbit 番号	1	2	3	4	5	6	7,8	9	10	11
種類	3	3	3	3	2	2	1	1	1	1

この分割を構成する集合を集めて、G のつくる superscheme を構成するのですが、プログラムのだす答は空 [ ] になります。これは前節の例の結果から推測できることです。なぜなら、前節の例の答ではいずれも orbit ７と８番が G の異なる orbit に含まれるのに、アソシエーションスキームによる分割では、この２つの orbit が１つになってしまっているからです。

例：GL(3,2) の作る７次の superscheme($m=4$) を拡張して、 8 次の superscheme($m=4$) を構成することを試みます。GL(3,2) の $\{1,2,\cdots,8\}^{(4)}$ 上の orbit は、 $8+5=13$ 個、 サイズ [42, 168, 42, 168, 42, 168, 42, 168, 168, 168, 168, 168, 168]、答は一つ [[[1, 3, 5, 7, 13], [2, 4, 6, 8, 9, 10, 11, 12]]]。拡張で得られる群は、 AGL(3,2)= 2^3GL(3,2)。
さらに、 AGL(3,2) の作る８次の superscheme($m=5$) を拡張して、 9 次の superscheme($m=5$) を構成することを試みます。AGL(3,2) の $\{1,2,\cdots,9\}^{(5)}$ 上の orbit は、$10+5=15$ 個で、サイズは [1344, 336, 1344, 336, 1344, 336, 1344, 336, 1344, 336, 1344, 1344, 1344, 1344, 1344]、答は空 [ ] になります。
以上、前節の例とこの例の計算時間はそれぞれ 20、 230、 2540 msec。PentiumIII 933MHz、メモリー 256MB の Linux パソコンで実行しました。

例：15 次の 2 重可移群 A(7)/GL(3,2) $\subset$ GL(4,2)。この 2 つの群の 1 点固定群の作る superscheme は異なるが、 拡張を計算すると両者一致します。したがって、A(7) の 1 点固定群から得られるのは、A(7) ではなくて、GL(4,2) になります。
この様に、G の部分群 H の拡大を計算しても、G の拡大になってしまう例は多く出てきます。それでも、次節に述べている範囲の 2 重可移群の計算では、５７個の中で２例を除き、$|G:H| \leq 3$ になります。例外の１例が上に述べたもので、$|G:H|=8$ になっています。もう１例は Mathieu 群 M(22) に関係した PSL(3,4) で、$|G:H|=6$ になります。これらの例とは逆の意味で、次の命題が成立します。

Proposition 1 可移な部分群 $H \subset G$ の両方が $m-1$ で同じ *superscheme* を与えるとする。 このとき、H の拡大が無いならば、 G の拡大も無い。

ここで計算している superscheme は、 ($m = 3, 4, 5$ で) $X^{(m-1)} \in \Pi^{m-1}$ となるものばかりですが、群からは作られない例が、かなりたくさんでてきます。
例：C(6) の拡大の計算。 答は 4 個、 そのうち 2 個は 7 次の 2 重可移群 7:6 を与えます。残りの 2 個は、7 次の superscheme($m = 3$) を与えるが、 それから自然に誘導される $\{1, 2, \cdots, 7\}^4$ の分割では、 7 次の superscheme($m = 4$) になりません。
例:7 次の 2 重可移群 7:6 の拡大の計算。答は 2 個、１つは 3 重可移群 PGL(2,7)、もう１つは superscheme($m = 4$) を与えるますが、その誘導 superscheme($m = 5$) は存在しません。

5 計算の現状

`GAP` のデータベース `TransitiveGroup`$(n-1, i)$ と `PrimitiveGroup`$(n-1, i)$ に入っている群について、その群を G_n として、拡大の計算を試みました。固定群 G_n の $(X \backslash \{n\})^{(3)}$ 上の orbit(種類１の orbit) の個数が７０位まで計算可能です。regular な群では１０次までになります。Mathieu 群 M(10) から M(11) の計算はできますが、M(11) の superscheme ($m = 6$) の計算はメモリーサイズ不足で計算できません。２重可移で３重可移では無い群 G に対して、G_n から G を求めるとき、種類１の orbit は５０個以下の条件下で、８１次 $G \cong 3^4$:SL(4,3) の場合まで計算できます。

参 考 文 献

[1] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version4*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany and School of Mathematical and Computational Sciences, Univ. St. Andrews, Scotland, 1997.

[2] B. Huppert and N. Blackburn. *Finite Groups III.* Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[3] G. Ivanyos. On the combinatorics of evdokimov's deterministic factorization. *Draft preprint*, 1997.

[4] W. M. Kantor. Some consequences of the classification of finite simple groups. *Contemporary Math.*, 45:159–173, 1985.