The Replacement Property for PSL(2, q) and C-group Theory

Hector Li[1] Hy Lam[2]
Directed by Professor R. Keith Dennis and Ravi Fernando

[1] Cornell University

[2] University of California, Berkeley

2017 SPUR Undergraduate Research Forum
August 9th, 2017

Notations

- G finite group
- $\mathrm{PSL}(2, q)$: projective special linear group obtained from $\mathrm{SL}(2, q)$ by quotienting out the scalar matrices. $(q > 3)$
- $s = (s_1, ..., s_k)$ is a length-k irredundant generating sequence for G .
- $m(G) = m$ is the maximal length of an irredundant generating sequence for G.

Replacement Property

- $s = (s_1, ..., s_k)$ is said to *satisfy the replacement property* if for any nontrivial element $g \in G$, there is a slot i-th in s so that g can replace g_i to give a new generating (not necessary independent) sequence for G.
- G is said to *satisfy the replacement property* if for all s of maximal length m, s satisfies the replacement property.

Maximal subgroups in general position

- A given collection of subgroups $H_i \leq G$ indexed by set I is said to be in *general position* if, for every index i, $\bigcap_{j \in I - \{i\}} H_j \supsetneq \bigcap_{j \in I} H_j$.

Theorem (H. Lam, 2017)

Let G be a finite group, for any $k \leq m(G)$, let $s = (g_1, ..., g_k)$ an irredundant generating sequence for G. For any corresponding collection of maximal subgroups in general positions $(M_1, ..., M_k)$, there exists r in $\{1, ..., k\}$ such that the following hold:
(1) $M_r = \langle g_i : i \neq r \rangle$
(2) $m(M_r) = k - 1$
(3) M_r *satisfies the replacement property ,*
s satisfies the replacement property.

Preliminary results

Theorem (B. Nachman, 2014)

- *For prime $p \equiv 1 mod 8$, $\mathrm{PSL}(2, p)$ fails the replacement property if m=3.*
- *If m=4, $\mathrm{PSL}(2, p)$ satisfies the replacement property for any prime p.*

Q: What are the possible values m for $\mathrm{PSL}(2, q)$?

Theorem (Whiston and Saxl, 2002*)

Let $G = \mathrm{PSL}(2, p)$, p prime then, $3 \leq m \leq 4$. For $G = \mathrm{PSL}(2, p^k)$, $m \leq max(6, \pi(k) + 2)$ where $\pi(k)$ is the number of distinct prime divisors of k.

Theorem (B. Nachman, 2014)

Except for $\mathrm{PSL}(2, 7)$, which has $m = 4$, if $p \neq \pm 1 mod 10$, $m = 3$.

Involutions for PSL$(2, q)$

Theorem (B. Nachman, 2014)

For $p = \pm 1 mod 8$ but $\neq \pm 1 mod 10$, if $m = 4$, any s of length 4 is made of only involutions.

Theorem (H. Lam, 2017)

For prime $p > 5$, $\mathrm{PSL}(2, p^2)$ and $m \geq 4$, any s made of only involutions has length at most 4.

- The question of whether or not PSL(n, q) can be irredundantly generated by involutions is completely settled, at least for length 3. PSL(2,q), we can have such a length-3 s of involutions and two of which commute iff q$\notin \{2, 3, 7, 9\}$. $\rightarrow$ Classification of number of embeddings of $Z_2 \times Z_2$ into PSL(n, q) based on the number of conjugacy classes of involutions in PSL(n, q)[M.B. Cherkassoff, 1988].

Dickson's classification of maximal subgroups for PSL(2, q)

- $PGL(2,q) := GL(2,q)/\{\alpha I\} \cong$ group of all Mobius transformation from $P_1(F_q) = F_q \cup \{\infty\}$ via natural isomorphism $\rho : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (z \mapsto \frac{az+b}{cz+d})$. $\rho|_{\mathrm{PSL}(2,q)}$ is then an isomorphism from $PSL(2,q)$ to group of Mobius transformations whose determinant is a square in F_q^*. $\Rightarrow$ we regard $PSL(2,q)$ as group acting as permutations on the projective line.

Dickson's classification of maximal subgroups for $\mathrm{PSL}(2, q)$ (continued)

Theorem (L.E Dickson, 1901?)

Given a maximal subgroup in $\mathrm{PSL}(2, q)$*, it is an isomorphic copy of the following classes :*

- *A point stabliser of order q(q-1) i.e* $C_q \rtimes C_{(q-1)/2}$.
- *A pair stabliser of form* D_{q-1} *for q odd,* $D_{2(q-1)}$ *for q even.*
- *A pair stabliser of form* D_{q+1} *for q odd,* $D_{2(q+1)}$ *for q even.*
- *subfield group* $PSL(2, q_1)$ *for q an odd prime power of* q_1, $PGL(2, q_1)$ *for* $q = q_1^2$, *q odd*
- S_4, A_4, A_5 *with classification of modulo 8 and 10.*

Further results

Theorem (H. Lam, 2017)

- *If prime $p \equiv \pm 1$ mod 10 and 1 mod 4,* $\mathrm{PSL}(2,p)$ *fails the replacement property if $m = 3$.*
- *If $p \equiv \pm 3$ mod 10,* $\mathrm{PSL}(2,p^2)$ *fails the replacement property if $m = 3$.*
- *If $p \equiv \pm 3$ mod 8, the same result holds for* $\mathrm{PSL}(2,p^2)$*.*
- *If $m \geq 4$ and $p > 5$, any s of length-4 consisting of involutions satisfies the replacement property in* $\mathrm{PSL}(2,p)$*.*

Useful propositions

- (Whiston Saxl) There cannot be more than three maximal subgroups are of the first 3 types. If there are three, then $m \lnsim 4$.
- Let D_{2p} be a dihedral group of order $2p$ in $G = PGL(2, p^2)$, for any odd prime p, $N_G(D_{2p})$ is isomorphic to $C_p \rtimes \mathrm{C}_{p-1}$.
- For $p{=}{\pm}1$ mod4, there exists a unique subgroup H of G such that $H \cong PSL(2, p)$, and H contains D_{2p}. $\rightarrow$ We can generalize the proof for n where $2n | p \pm 1$.
- Suppose H_1, H_2 are subfield subgroups of $PSL(2, p^2)$, if the intersection of H_1 and H_2 contains a dihedral subgroup of order $2n$, where $2n$ divides $p \pm 1$. $H_1 \cap H_2$ is also a subfield subgroup.(In fact, the intersection is isomorphic to either one of them.)

Coxeter Groups

Definition (Coxeter Groups)

A (finitely generated) Coxeter group (G, S) is a group G together with a set $S = \{r_0, \cdots, r_{n-1}\}$ that admits the following presentation

$$G = \langle r_0, \cdots, r_{n-1} \,|\, (r_i r_j)^{m_{ij}} = 1 \rangle$$

where

- $m_{ii} = 1$;
- $2 \leq m_{ij} \leq \infty$, for $i \neq j$.

In other words, G is a group generated by involutions $r_0, \cdots, r_{n-1}$; the only relations between the generators are the orders of their pairwise products.

Coxeter Groups (continued)

The Coxeter-Dynkin diagram of the Coxeter group (G, S) is an undirected labelled graph such that

- vertices are indexed by involutions $r_0, \cdots, r_{n-1}$;
- the pair $\{r_i, r_j\}$ is an edge iff $m_{ij} \geq 3$ (i.e. iff r_i and r_j do not commute);
- the edge $\{r_i, r_j\}$ is labelled with the order $p_{ij} = o(r_i r_j)$.

C-groups

Definition (Intersection property)

A generating set $S = \{s_0, s_1, \cdots, s_{n-1}\}$ of G satisfies the intersection property (a.k.a. strongly independent property) if for all subsets $I, J \subseteq \{0, \cdots, n-1\}$, the following property is satisfied.

$$\langle s_i \mid i \in I \rangle \cap \langle s_j \mid j \in J \rangle = \langle s_k \mid k \in I \cap J \rangle$$

Definition (C-groups of rank n)

A C-group of rank n is a pair (G, S) such that G is a group and S is a generating set of n involutions of G that satisfies the intersection property.
The C-rank of a group G is the largest rank of a C-group representation of G.

C-groups (continued)

Proposition

If a generating sequence $S = \{s_0, s_1, \cdots, s_{n-1}\}$ of G satisfies the intersection property, then S is irredundant.

Proof.

Suppose S satisfies the intersection property and is redundant. Let $I = \{0, 1, \cdots, n-1\}$. There exists $k \in I$ such that $\langle s_i \mid i \in I \rangle = \langle s_i \mid i \in I \backslash \{k\} \rangle$. Since $\{k\} \cap I \backslash \{k\} = \varnothing$, we have $\langle s_k \rangle \cap \langle s_i \mid i \in I \backslash \{k\} \rangle = \langle \varnothing \rangle = \{1\}$, so $\langle s_k \rangle$ is not a subgroup of $\langle s_i \mid i \in I \backslash \{k\} \rangle$. However, we know $\langle s_k \rangle$ is a subgroup of $\langle s_i \mid i \in I \rangle$, which is a contradiction. □

Examples of C-groups

Proposition

For any n, the symmetric group S_n is a C-group of rank $n-1$.

Theorem (Whiston, 1999)

For an irredundant set inside S_n, the size of the set is at most $n-1$, with equality only if the set generates the whole group S_n.

Theorem (Cameron, Cara, 2002)

For $n \geq 7$, any irredundant generating set for S_n of size $n-1$ satisfies the intersection property.

Examples of C-groups (continued)

Theorem (Cameron & Cara, 2002)

Let S be an irredundant generating set for S_n of size $n-1$, where $n \geq 7$. Then there is a tree T on $\{1, \cdots, n\}$ such that one of the following holds

- $S = S(T)$;
- *for some element $s \in S(T)$, we have*

$$S = \{s\} \cup \left\{ (st)^{\epsilon(t)} \mid t \in S(T) \backslash \{s\} \right\}, \textit{where } \epsilon(t) = \pm 1$$

Conversely, each of these sets is an irredundant generating set for S_n.

String C-groups

Definition (String C-groups)

A C-group is a string C-group provided its generating involutions can be reordered in such a way that $(r_i r_j)^2 = 1$ for all i, j with $|i - j| > 1$. Equivalently, string C-groups are C-groups with string Coxeter-Dynkin diagrams.

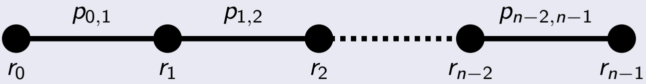


Figure: Coxeter-Dynkin diagrams of String C-groups

Example

The symmetric group S_n is a string C-group.

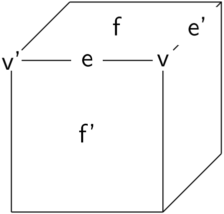
Polytopes I

The polytope, as partially ordered set, has the following properties:

- Every maximal chain has the same length. (In the case of the cube, a maximal chain has the form (empty set, vertex, edge, face, cube).) We can talk about the dimension of a "face": the empty set has dimension -1, a vertex dimension 0, an edge dimension 1, and so on.
- A connectedness condition: we can move from any "face" to any other by a sequence of steps in which consecutive "faces" are incident; we can further assume that every "face" in the sequence except the first and last has dimension i or j, where i and j are two given dimensions.

Polytopes II

- If f and g are incident "faces" of dimensions i and $i+2$ respectively, then there are exactly two "faces" of dimension $i+1$ incident with both f and g. (In our picture of the cube, v and v' are the "faces" incident with the empty set and e; e and e' are incident with v and f; and f and f' are incident with e and with the whole polytope.)



Automorphisms of polytopes

Definition (Automorphisms of polytopes)

An automorphism of a polytope is a permutation of the "faces" preserving the partial order (and hence preserving the dimensions of "faces").

Observation

It follows from the three conditions above that the identity is the only automorphism fixing a maximal chain. (In the case of the cube, suppose that an automorphism fixes v, e and f. Then it must fix v', the only other vertex incident with e; similarly it must fix e' and f'. Using the connectedness, we can work from any maximal chain to any other, and find that everything is fixed.)

Automorphisms of polytopes (continued)

Corollary

The number of automorphisms does not exceed (and, indeed, is a divisor of) the number of maximal chains. The most symmetric polytopes are thus the ones in which the number of automorphisms is equal to the number of maximal chains, and so the group of automorphisms acts sharply transitively on the maximal chains. These are the regular polytopes.

Regular Polytopes and string C-groups

Let P be a regular polytope of dimension d and $C = (f_{-1}, \cdots, f_d)$ be a maximal chain. For any i with $0 \leq i \leq d-1$, there is a unique maximal chain C_i which agrees with C in every dimension except i, and there exists a unique automorphism ρ_i which maps C to C_i. Then ρ_i also maps C_i back to C, and so $\rho_i^2 = 1$.
Since the polytopes satisfy the connectedness condition, the automorphism groups can be generated by these involutions.
Specifically, these involutions satisfy the following two properties:

- If $|i-j| \geq 2$, then ρ_i and ρ_j commute.
- The automorphism group with the generating set of these involutions satisfies the intersection property.

PSL(2, q) as a C-group I

Definition (Rank)

The rank of a "face" F is defined as $(m-2)$, where m is the maximum length of chains $(f_{-1}, \cdots, F)$.

The rank of an abstract polytope is the largest rank of its "faces."

Remark. The rank of an abstract polytope is the C-rank of its automorphism group.

Theorem (Sjerve & Cherkassoff, 1993)

The $\mathrm{PSL}(2,q)$ *group may be generated by three involutions, two of which commute, if and only if* $q \neq 2, 3, 7$ *or* 9*.*

Theorem (Leemans & Vauthier, 2006)

Let $G \cong \mathrm{PSL}(2,q)$*. If* P *is a polytope on which* G *acts regularly, then the rank of* P *is at most 4.*

PSL$(2, q)$ as a C-group II

Theorem (Leemans & Schulte, 2007)

If PSL$(2, q)$ *is the full automorphism group of a regular polytope of rank* 4*, then* $q = 11$ *or* 19*.*

If we drop the condition that the Coxeter-Dynkin diagram of the C-group is a string, then we have the following result.

Theorem (Connor, Jambor & Leemans, 2014)

Let $G \cong$ PSL$(2, q)$ *for some prime power* $q \geq 4$*. The C-rank of* G *is* 4 *if and only if* $q \in \{7, 9, 11, 19, 31\}$*. Otherwise it is 3.*

References

Julius Whiston (1999).
Maximal independent generating sets of the symmetric group.
Journal of Algebra 232 (2000), 255 – 268.

Peter J. Cameron and Philippe Cara (2002).
Independent generating sets and geometries for symmetric groups.
Journal of Algebra 258 (2002), 641 – 650.

Dennis Sjerve and Michael Cherkassoff (1993).
On groups generated by three involutions, two of which commute.
Journal of Algebra 258 (2002), 641 – 650.

Dimitri Leemans and Laurence Vauthier (2006).
An atlas of abstract regular polytopes for small groups.
Aequationes Mathematicae 72 (2006), 313 – 320.

Dimitri Leemans and Egon Schulte (2007).
Groups of type $L_2(q)$ acting on polytopes.
Advances in Geometry 7(4) (2007), 529 – 539.

Thomas Connor, Sebastian Jambor and Dimitri Leemans (2015).
C-groups of PSL$(2, q)$ and PGL$(2, q)$.
Journal of Algebra 427 (2015), 455 – 466.

Peter J. Cameron (2014).
Regular polytopes, 1.
https://cameroncounts.wordpress.com/2014/09/01/regular-polytopes-1/

Hy P.G Lam (2017)
The Replacement Property of PSL$(2, p)$ and PSL$(2, p^2)$.
https://arxiv.org/abs/1709.08745

Acknowledgement

Special thanks to Professor Dennis and Ravi for their support and guidance. Thank you for listening.