COMPUTATIONAL AND COMBINATORIAL ASPECTS OF FINITE SIMPLE GROUPS

Shelly Garion

SFB 878 – Groups, Geometry & Actions
Universität Münster

http://wwwmath.uni-muenster.de/u/shelly.garion/
Computational and combinatorial aspects of finite simple groups
Finite simple groups

The finite simple groups are the building blocks of all finite groups.

Definition. $G$ is simple if it has no non-trivial normal subgroups.

Theorem. Classification of the (non-abelian) Finite Simple Groups.

- Alternating groups $A_n$ ($n \geq 5$).
- Finite simple groups of Lie type $G_r(q)$
  where $r$ is the Lie rank and $q = p^e$ is the size of finite field; e.g. $\text{PSL}_{r+1}(q)$.
- 26 sporadic groups.

On the proof… thousands of pages, hundreds of articles, ~100 authors:
From Galois (1832) to Gorenstein-Lyons-Solomon (90's)…
The Product Replacement Algorithm
The problem

Basic problem in computational group theory:
How to generate a random element in a finite group $G$?

The Product Replacement Algorithm (PRA) was suggested in 1995 by
Celler, Leedham-Green, Murray, Niemeyer & O'Brien.

The PRA showed very good performance in practical experiments, but there is
no rigorous justification. It was included in GAP and MAGMA.

The PRA performs a random walk on the product replacement graph $\Gamma_n(G)$
whose vertices are the generating $n$-tuples of $G$ (for a fixed $n$):

$$\{ (g_1,\ldots,g_n) : <g_1,\ldots,g_n>=G \}$$

Question: Let $G$ be a finite simple group. Is $\Gamma_n(G)$ connected?
### The Product Replacement Algorithm

#### The results

<table>
<thead>
<tr>
<th>$n=2$</th>
<th>$n \geq 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Neumann, 1951]. $\Gamma_2(A_5)$ is disconnected.</td>
<td>Wiegold's conjecture (1980's). If $G$ is a finite simple group and $n \geq 3$ then $\Gamma_n(G)$ is connected.</td>
</tr>
<tr>
<td>[Garion-Shalev, 2009]. (Conjectured in 2002 by [Guralnick-Pak]). If $G$ is a finite simple group, then the number of connected components of $\Gamma_2(G)$ grows to infinity as $</td>
<td>G</td>
</tr>
<tr>
<td></td>
<td>• [Gilman, 1977]. $G=\text{PSL}_2(p)$, $n \geq 3$.</td>
</tr>
<tr>
<td></td>
<td>• [Evans, 1993]. $G=\text{PSL}_2(2^e)$, $\text{Sz}(2^{2e+1})$, $n \geq 3$.</td>
</tr>
<tr>
<td></td>
<td>• [Garion, 2008]. $G=\text{PSL}_2(p^e)$, $n \geq 4$.</td>
</tr>
<tr>
<td></td>
<td>• [Avni-Garion, 2008]. $G=G_r(p^e)$, $n \geq c(r)$, finite simple group of Lie type of Lie rank $r$.</td>
</tr>
</tbody>
</table>
The Product Replacement Algorithm

The methods

Can we connect any generating n-tuple of $G$ to a redundant one?

Is $\Gamma_n(G)$ connected?

What are the subgroups of $G$?

- For $G=\text{PSL}_2(q)$: the subgroups are well-known [Dickson, 1901].
- For $G=\text{G}_2(q)$ – a finite simple group of Lie type: Aschbacher’s classification of maximal subgroups (1984) – uses CFSG.
- [Avni-Garion, 2008]. For $G=\text{PSL}_2(q)$: the subgroups are well-known [Dickson, 1901].
- [Larsen-Pink, 1998] – uses algebraic geometry (not CFSG!).
- For an infinite simple Tarski monster group $G$: [Garion-Glasner].
- Any subgroup is a cyclic group of order $p$ (if $p$ is either a fixed prime or $\omega$).
- Theorem. A faithful highly transitive action of $\text{Out}(F_n)$ on a countable set.

[Garion, 2008]. For $G=\text{PSL}_2(q)$: the subgroups are well-known [Dickson, 1901].


[Garion-Glasner]. For an infinite simple Tarski monster group $G$: Any subgroup is a cyclic group of order $p$ (if $p$ is either a fixed prime or $\omega$).

Theorem. A faithful highly transitive action of $\text{Out}(F_n)$ on a countable set.
Word maps in groups
The problem

A word $w = w(x_1, \ldots, x_n)$ is an element in $F_n = \langle x_1, \ldots, x_n \rangle$.

For a group $G$, a word map is given by:

$$ w: G^n \rightarrow G $$

$$(g_1, \ldots, g_n) \mapsto w(g_1, \ldots, g_n) $$

Questions:
- Let $G$ be a finite simple group and let $w \neq 1$. What is the image $w(G^n)$? Is $w: G^n \rightarrow G$ surjective?
- What are the sizes of the fibers of a word map? Is $w: G^n \rightarrow G$ almost equidistributed? e.g. $|w^{-1}(g)| \approx |G|^{n-1}$ for almost all $g \in G$.

Investigated by Guralnick, Larsen, Liebeck, Segal, Shalev, O'Brien, Tiep, …
Word maps in groups

The results

Commutator word: \( e_1 = [x,y] = x y x^{-1} y^{-1} \in F_2 \)

Theorem (Ore’s Conjecture) [Ore, 1951; Thompson, 1960's; Ellers-Gordeev, 1998; Liebeck-O'Brien-Shalev-Tiep, 2008; …]
Any element in a finite simple group is a commutator.

[Garion-Shalev, 2009].
The commutator map on finite simple groups is almost equidistributed.

Engel words: \( e_n = [e_{n-1},y] = [...] [[x,y],y],...,y \in F_2 \)
[Bandman-Garion-Grunewald]. Surjectivity and equidistribution of \( e_n \) on \( PSL_2(q) \).

Two-power words: \( w = x^a y^b \in F_2 \) [Guralnick-Malle, 2012; LOST, 2012].
[Bandman-Garion, 2012]. Surjectivity and equidistribution of \( x^a y^b \) on \( PSL_2(q) \).
Word maps in groups
The methods

Commutator word:
[Frobenius, 1896]. \# \{(x,y) \in G \times G: [x,y]=g \} = |G| \cdot \sum_{\chi \in \text{Irr}(G)} \chi(g)/\chi(1)

Words in SL₂(q):
Trace map Theorem [Fricke-Klein, 1897; Vogt, 1889].
\[
\text{word } w(x,y) \text{ in } \text{SL}_2(q) \Rightarrow \text{tr}(w) = P(s,t,u) \text{ is a polynomial in } s=\text{tr}(x), t=\text{tr}(y), u=\text{tr}(xy) \text{ over } F_q
\]

Examples:

w=[x,y] \Rightarrow \text{tr}(w) = s^2 + t^2 + u^2 - stu - 2

[Bandman-Garion-Grunewald]. w=e_n(x,y) \Rightarrow s_n = \text{tr}(e_n) = s_{n-1}^2 + 2t^2 - s_{n-1}t^2 - 2

[Bandman-Garion, 2012]. w=x^a y^b \Rightarrow \text{tr}(w) = u \cdot f_{a,b}(s,t) + h_{a,b}(s,t)

By induction, compute \text{tr}(w) for any \( w \in F_2 \)
Beauville surfaces
The problem

Beauville surface [Beauville, 1978; Catanese, 2000]. \( S = (C_1 \times C_2)/G \)

\( S \) is an infinitesimally rigid complex surface, where \( C_1 \) and \( C_2 \) are curves of genus \( \geq 2 \) and \( G \) is a finite group acting freely on their product.

Beauville structure [Bauer-Catanese-Grunewald, 2005]. (\( x_1, y_1, z_1; x_2, y_2, z_2 \))

- \( x_1y_1z_1 = 1 = x_2y_2z_2 \),
- \( <x_1, y_1> = G = <x_2, y_2> \),
- no non-identity power of \( x_1, y_1, z_1 \) is conjugate in \( G \) to a power of \( x_2, y_2, z_2 \).

The type of \( (x_1, y_1, z_1; x_2, y_2, z_2) \) is the 6 orders of \( x_1, y_1, z_1; x_2, y_2, z_2 \).

Questions [Bauer-Catanese-Grunewald, 2005].

1) Which finite simple groups admit a Beauville structure?
2) Which types can occur in a Beauville structure?
Beauville surfaces

The results

Conjecture 1 [BCG, 2005].
All finite simple groups (except $A_5$) admit a Beauville structure.

Proved for:
- $A_n$ ($n \geq 6$) [BCG, 2005; Fuertes, González-Diez, 2009].
- $\text{PSL}_2(q)$ ($q \geq 7$) [Fuertes-Jones, 2011; Garion-Penegini].
- Almost all finite simple groups [Garion-Larsen-Lubotzky, 2012].
- All finite simple groups ($\neq A_5$) [Fairbairn-Magaard-Parker; Guralnick-Malle].

Conjecture 2 [BCG, 2005] – proved by [Garion-Penegini].
For any two hyperbolic triples of integers $(k_1, l_1, m_1; k_2, l_2, m_2)$ almost all alternating groups $A_n$ admit a Beauville structure of type $(k_1, l_1, m_1; k_2, l_2, m_2)$.

[Garion]. Characterization of the types of Beauville structures for $\text{PSL}_2(q)$. 
Beauville surfaces

The methods

G admits a Beauville structure of type \((k_1,l_1,m_1;k_2,l_2,m_2)\).

\[ \iff \]

G is a quotient of \(\Delta(k_1,l_1,m_1)\) and \(\Delta(k_2,l_2,m_2)\) + "disjoint" condition.

Triangle group: \(\Delta(k,l,m) = \langle x, y : x^k = y^l = (xy)^m = 1 \rangle\)

Question: Which finite simple groups are quotients of a given \(\Delta(k,l,m)\)?

- \(A_n\) – Higman 1960s; Conder 1980; Everitt 2000; Liebeck-Shalev 2004,…
- \(\text{PSL}_2(q)\) – Macbeath 1968; Rosenberger et al. 1989; Marion 2009.
- \(\text{Gr}(q)\) – open! Luccini-Tamburini-Wilson 2000; Liebeck-Shalev 2005,…

[Frobenius, 1890s]. \(X,Y,Z\) – conjugacy classes in G (of orders \(k,l,m\)).

\[
\# \{x,y,z : x \in X, y \in Y, z \in Z, xyz=1\} = |X|\cdot|Y|\cdot|Z|/|G| \cdot \sum_{\chi \in \text{Irr}(G)} \chi(x)\chi(y)\chi(z)/\chi(1)
\]
Computational and combinatorial aspects of finite simple groups
Future plans

Continue my research in group theory, focusing on finite simple groups, while interacting with other fields of mathematics such as algebraic geometry, number theory, representation theory, dynamics…

Some specific research problems…

Word maps

- Analysis of general words in $\text{PSL}_2(q)$.
- Generalize the trace map method to $\text{PSL}_n(q)$ and $G_r(q)$.
- Generalizations to $\text{SL}_2(\mathbb{Z}_p)$ and $\text{SL}_2(\mathbb{Z})$.

Beauville surfaces

- What is the probability of admitting a Beauville structure?
- Constructing Beauville surfaces with specific properties (e.g. reality).
- Investigating the moduli space of Beauville surfaces.