Connectivity properties of the product replacement algorithm graph of finite simple groups

Shelly Garion

http://www.math.huji.ac.il/~shellyg
Outline

• The Product Replacement Algorithm (PRA) and its graph.
• Theoretical background.
• Known results.
• New results on PRA graphs of finite simple groups.
• Overview of the proofs.
The Product Replacement Algorithm (PRA)  
Motivation and history

G – finite group, given by some generating set.  
Algorithm: Construct a random element of G.

- The algorithm was proposed in 1995 by Celler, Leedham-Green, Murray, Niemeyer and O'Brien.
- Showed very good performance in practical experiments, although it has no rigorous justification.
- Was included in GAP and MAGMA.
- Widely investigated: "What do we know about the product replacement algorithm?" [Pak, 2001].
The Product Replacement Algorithm (PRA)

The graph

d(G) – minimal number of generators of G. Fix: k ≥ d(G).

The graph: X_k(G).

Vertices: V_k(G) = \{(g_1,\ldots,g_k) : <g_1,\ldots,g_k>=G\}
– the set of all generating k-tuples of G.

Edges: correspond to the Nielsen moves (1 ≤ i ≠ j ≤ k):

R_{i,j}^\pm: (g_1,\ldots,g_i,\ldots,g_k) \rightarrow (g_1,\ldots,g_i g_j^{\pm 1},\ldots,g_k),

L_{i,j}^\pm: (g_1,\ldots,g_i,\ldots,g_k) \rightarrow (g_1,\ldots,g_j^{\pm 1} g_i,\ldots,g_k),

P_{i,j}: (g_1,\ldots,g_i,\ldots,g_j,\ldots,g_k) \rightarrow (g_1,\ldots,g_j,\ldots,g_i,\ldots,g_k),

I_i: (g_1,\ldots,g_i,\ldots,g_k) \rightarrow (g_1,\ldots,g_i^{-1},\ldots,g_k).
The Product Replacement Algorithm (PRA)
Generating a random element

The algorithm corresponds to a random walk on the subgraph obtained by \( \{R_{i,j}^\pm, L_{i,j}^\pm\}_{1 \leq i \neq j \leq k} \).

The algorithm:
1. Start with some generating k-tuple (in practice: \( k=d(G)+10 \)).
2. Select uniformly a pair \((i,j)\) with \(1 \leq i \neq j \leq k\), and apply one of the four operations \(R_{i,j}^\pm, L_{i,j}^\pm\) with equal probability.
3. Repeat step (2) several times (in practice: \( \sim 100 \) times).
4. Output: a random element of the tuple that was reached.
Theoretical background: T-systems

$F_k$ – the free group on $k$ generators: $x_1, \ldots, x_k$.

The moves $\{R_{i,j}^\pm, L_{i,j}^\pm, P_{i,j}, I_i\}_{1 \leq i \neq j \leq k}$ on $(x_1, \ldots, x_k)$ can be viewed as automorphisms of $F_k$.

Theorem [Nielsen]. $Aut(F_k)$ is generated by $\{R_{i,j}^\pm, L_{i,j}^\pm, P_{i,j}, I_i\}_{1 \leq i \neq j \leq k}$.

In fact, $\langle \{R_{i,j}^\pm, L_{i,j}^\pm\}_{1 \leq i \neq j \leq k} \rangle = Aut^+(F_k)$ (an index 2 subgroup of $Aut(F_k)$).

Motivation (1950's). Study presentations of finite groups.

Presentation of $G$ (by $k$ generators and relations):

$$G = \langle x_1, \ldots, x_k ; R \rangle$$

Presentation of $G$ (by $k$ generators) = epimorphism $F_k \rightarrow G$. 
Theoretical background: T-systems

One can identify $\text{Epi}(F \to G)$ with $V_k(G)$.

The group $\text{Aut}(F_k) \times \text{Aut}(G)$ acts on $V_k(G)$ by:

$$(\tau, \sigma): \phi \mapsto \sigma \circ \phi \circ \tau^{-1}$$

Where: $\tau \in \text{Aut}(F_k)$, $\sigma \in \text{Aut}(G)$ and $\phi \in \text{Epi}(F_k \to G)$.

Definition [B.H. Neumann and H. Neumann, 1951].

An orbit of $\text{Aut}(F_k) \times \text{Aut}(G)$ in $V_k(G)$ is called a $T_k$-system (for: system of transitivity).

Remark. If $k \geq 2d(G)$ then

$X_k(G)$ is connected $\iff$ $G$ has only one $T_k$-system.
## Connectivity properties of PRA graphs

### Known results

<table>
<thead>
<tr>
<th>k=d(G)</th>
<th>k≥d(G)+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>As many connected components as you want.</td>
<td>Conjectured that the PRA graph is connected.</td>
</tr>
</tbody>
</table>

- **G abelian**: $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$ where $m_1 | m_2 | \ldots | m_k$, $(d(G)=k)$.  
  - [Neumann & Neumann, 1951].
  - G has one $T_k$-system.
  - [Diaconis & Graham, 1999].
  - $X_k(G)$ has $\phi(m_1)$ connected components of equal size.
# Connectivity properties of PRA graphs

## Known results

<table>
<thead>
<tr>
<th>$k = d(G)$</th>
<th>$k \geq d(G) + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>As many connected components as you want.</td>
<td>Conjectured that the PRA graph is connected.</td>
</tr>
</tbody>
</table>

**Example** [Neumann, 1956]. Nilpotent group of order $2^{15}$, with two $T_2$-systems.

[Dunwoody, 1963]. For every $k, N, p$ there exists a $p$-group $G$ with $d(G)=k$ and at least $N$ $T_k$-systems.

[Dunwoody, 1970]. If $G$ is a finite solvable group and $k \geq d(G) + 1$, then $X_k(G)$ is connected.

[Gilman, 1977]. For any finite group $G$, if $k \geq 2 \log_2 |G|$, then $X_k(G)$ is connected.
Finite simple groups

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

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

- Alternating groups – $A_n$ ($n \geq 5$).
- Finite groups of Lie type – $L_r(q)$, where $r$ is the Lie rank and $q$ is the size of finite field.
  - Classical: linear ($\text{PSL}_n(q)$), orthogonal, unitary, symplectic.
  - Exceptional: Suzuki groups, …
- 26 sporadic groups.

Corollary. If G is a finite simple group then $d(G)=2$. 
Connectivity properties for simple groups

Known results

<table>
<thead>
<tr>
<th>k=2</th>
<th>k≥3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let: $\tau_2(G) = # \text{T}_2$-systems of $G$. $\chi_2(G) = # \text{conn. comp. of } X_2(G)$.</td>
<td></td>
</tr>
<tr>
<td>[Neumann, 1951]. $\tau_2(A_5)=2$.</td>
<td></td>
</tr>
<tr>
<td>[Pak, 2001]. $\tau_2(A_n) \to \infty$ as $n \to \infty$.</td>
<td></td>
</tr>
<tr>
<td>[Guralnick &amp; Pak, 2002]. $\tau_2(\text{PSL}_2(p)) \to \infty$ as $p \to \infty$.</td>
<td></td>
</tr>
<tr>
<td>Conjecture (2002). This is true for all finite simple groups.</td>
<td></td>
</tr>
</tbody>
</table>

| Wiegold's conjecture. If $G$ is a finite simple group and $k \geq 3$ then $X_k(G)$ is connected. |
| Known for: |
| [Gilman, 1977]. $G=\text{PSL}_2(p)$. |
| [Evans, 1993]. $G=\text{PSL}_2(2^e)$, $G=\text{Sz}(2^{2e+1})$. |
Connectivity properties for simple groups

New results

<table>
<thead>
<tr>
<th>$k=2$</th>
<th>$k \geq 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[G, Shalev]</strong>. Let $G$ be a finite simple group, then: $\tau_2(G), \chi_2(G) \to \infty$ as $</td>
<td>G</td>
</tr>
</tbody>
</table>
**k=2: many connected components**

Theorem [G, Shalev]. Let $G$ be a finite simple group, then: $\tau_2(G), \chi_2(G) \to \infty$ as $|G| \to \infty$.

Let: $(x,y) \in V_2(G)$.

**Commutator:** $[x,y] = x^{-1}y^{-1}xy$.

How do the Nielsen moves affect the commutator?

**Example.** $(x,y) \to (xy,y)$.

$[x,y] \to [xy,y] = y^{-1}x^{-1}y^{-1}xy = [x,y]^y$.

**Higman's lemma [Nuemann, 1956].** $[x,y]$ is preserved under Nielsen moves, up to conjugation (and inverse).
k=2: many connected components

Main idea of the proof

Theorem [G, Shalev]. Let $G$ be a finite simple group, then:
$	au_2(G)$, $\chi_2(G) \to \infty$ as $|G| \to \infty$.

Let: $S = \{g \in G: g= [x,y], \langle x, y \rangle = G\}$.

By Higman's lemma:
$\chi_2(G) \geq \#\{\text{conjugacy classes } C \text{ of elements of } S\} := k(S)$

Main step. prove that $S$ is 'large' (contains almost all $G$).

Why? $S$ is 'large' (almost all $G$) $\Rightarrow$ $k(S)$ is 'large' (almost as $k(G)$)
$\Rightarrow k(S) \to \infty$ as $|G| \to \infty$. 
Ore's conjecture
Commutators in finite simple groups

Ore's conjecture. Every element in a finite simple group $G$ is a commutator:

For any $g \in G$ there exist $x, y \in G$ s.t. $[x, y] = g$.

History:

- [Ore, 1951]. Proved it for $A_n$.
- [Thompson, 1960]. Proved it for $\text{PSL}_n(q)$.
- [Ellers & Gordeev, 1998]. Proved it for $\text{L}_r(q)$ where $q > 8$.
- [Liebeck, O'Brien, Shalev & Tiep, 2008]. Completed the proof!
Commutators distribution

Let $G$ be a finite group and $g \in G$. Denote:

$N(g) = \# \{(x, y) \in G \times G : [x, y] = g\}$.

Frobenius formula (1896).

$|G| = \sum_{\chi \in \text{Irr}(G)} \chi(g)/\chi(1)$.

When $G$ is a finite simple group:

Ore's conjecture for $G$ $N(g) \neq 0$ for every $g \in G$.

Question. Is $N(g) \approx |G|$ for almost every $g \in G$?

Answer. YES!

Denote: $N(g) = \# \{x'y \in G : x'y[=g\}$.

Let $G$ be a finite group and $g \in G$.
Equidistribution theorem

Equidistribution theorem [G, Shalev].
Every finite simple group $G$ has a subset $S=S_G \subset G$ satisfying:
1. $|S| = |G| \ (1-o(1))$.
2. $N(g) = |G| \ (1+o(1))$ uniformly for all $g \in S$.
Where $o(1)$ depends only on $G$ and tends to 0 as $|G| \to \infty$.

Remark 1. Can we take $S=G$? – NO!
$1 \notin S$ since $N(1)=|G| \cdot k(G)$,
k($G$) = #$\{\text{conjugacy classes in } G\}$, and $k(G) \to \infty$ as $|G| \to \infty$.

Remark 2. Denote the error by $\varepsilon(G)$, the proof shows that:
$\varepsilon(A_n) = O(n^{-1/2})$ , $\varepsilon(L_r(q)) = O(q^{-r/4})$. 
Corollary 1 (measure preservation).
Let $G$ be a finite simple group, and look at the commutator map:
\[ \alpha : G \times G \to G \]
\[ \alpha(x, y) = [x, y] \]

(i) For any $Y \subseteq G$: \[ \frac{|\alpha^{-1}(Y)|}{|G|^2} = \frac{|Y|}{|G|} + o(1). \]

(ii) For any $X \subseteq G \times G$: \[ \frac{|\alpha(X)|}{|G|} \geq \frac{|X|}{|G|^2} - o(1). \]

(iii) In particular, if $X \subseteq G \times G$ satisfies $|X| = (1-o(1))|G|^2$ then
\[ |\alpha(X)| = (1-o(1))|G|. \]
Equidistribution and measure preservation

Example. If $X = \{(x,y): \langle x,y \rangle = G\}$ then $|X| = (1-o(1))|G|^2$:

Theorem. Almost every pair $(x,y) \in G \times G$ generates $G$.

This was a conjecture of Dixon (1969), who proved it for $A_n$.

The case of $L_r(q)$ was proved by Kantor-Lubotzky (1990) and Liebeck-Shalev (1995).

Corollary 2. Almost every element $g$ in a finite simple group $G$ can be represented as a commutator $g = [x,y]$ where $\langle x,y \rangle = G$.

We deduce:

Theorem [G, Shalev]. Let $G$ be a finite simple group, then:

$\tau_2(G), \chi_2(G) \to \infty$ as $|G| \to \infty$. 
Proving the connectivity of PRA graphs

[Avni, G]. There is a function $c(r)$ s.t. if $G=L_r(q)$ then $X_k(G)$ is connected for all $k \geq c(r)$.

Previous bound: [Nikolov, Larsen-Pink].

$$k \geq Cr^2e \quad (q=p^e \text{ is the defining field}).$$

Our bound: Independent on the size of the defining field of $G$. However, at least exponential in the Lie rank $r$. 
Redundant generating tuples

[Avni, G]. There is a function $c(r)$ s.t. if $G = L_r(q)$ then $X_k(G)$ is connected for all $k \geq c(r)$.

**Definition.** A generating $k$-tuple $(g_1, \ldots, g_k)$ is **redundant** if there is some index $j$ s.t. $\langle \{g_i\}_{i \neq j} \rangle = G$.

**Main idea.** Prove that there is $c = c(r)$ s.t. if $k \geq c$, any generating $k$-tuple is connected to a redundant one.

**Why?** By replacing $c$ with $c+1$, if $k \geq c+1$ we can connect:

$$(x_1, \ldots, x_k) \rightarrow (y_1, \ldots, y_{k-2}, y_{k-1}, 1) \rightarrow (z_1, \ldots, z_{k-2}, 1, 1)$$

$$\rightarrow (z_1, \ldots, z_{k-2}, a_1, a_2) \rightarrow (1, \ldots, 1, a_1, a_2),$$

where $G = \langle a_1, a_2 \rangle$. 
Sketch of the proof

[Avni, G]. There is a function \( c(r) \) s.t. if \( G=L_r(q) \) then \( X_k(G) \) is connected for all \( k \geq c(r) \).

Sketch of the proof. If \( (g) = (g_1, \ldots, g_k) \) is NOT redundant:

\( \Rightarrow \) Let \( m<k \). What can be: \( <g_1, \ldots, g_m> \) ?

\( \Rightarrow \) Study the possible subgroups of \( G \).

\( \Rightarrow \) Connect \( (g) \) to a redundant \( k \)-tuple on a case-by-case basis.

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

For \( G=\text{L}_r(q) \): The maximal subgroups are known.

- Aschbacher’s classification – use CFSG.
- [Larsen-Pink, 1998] – use algebraic geometry (not CFSG!).
Finite simple groups of Lie type

$p$ – a prime number, $q=p^e$ a prime power.

$\overline{F}_p$ – the algebraic closure of $F_p$ (and $F_q$).

$\text{GL}_n(\overline{F}_p) \supseteq \Gamma$ – simple, connected algebraic group.

The standard Frobenius map.

$$\text{Frob}_q : \text{GL}_n(\overline{F}_p) \rightarrow \text{GL}_n(\overline{F}_p)$$

$$(x_{ij}) \rightarrow (x_{ij}^q).$$

A homomorphism $F: \Gamma \rightarrow \Gamma$ is called a Frobenius map if $\exists k, m, e$ ($q=p^e$) and a faithful representation $\rho: \Gamma \rightarrow \text{GL}_m(\overline{F}_p)$, satisfying $F^k|_{\rho(\Gamma)} = \text{Frob}_q|_{\rho(\Gamma)}$ (where $\text{Frob}_q: \text{GL}_m(\overline{F}_p) \rightarrow \text{GL}_m(\overline{F}_p)$).
Finite simple groups of Lie type

Notation. \( \Gamma^F = \{ g \in \Gamma : F(g) = g \} \).
\( q_F = p^{e/k} \) (usually this is the size of the defining field of \( \Gamma^F \)).

A finite simple group of Lie type is a group of the form:
\( G = (\Gamma^F)^{\text{der}} = [\Gamma^F, \Gamma^F] \).

Denote: \( r = \text{Lie rank of } \Gamma = \text{Lie rank of } G = (\Gamma^F)^{\text{der}}. \)

Examples.

- \( \Gamma^F \) (and \( (\Gamma^F)^{\text{der}} \)) is always a finite group.
- \( \Gamma \subseteq \text{GL}_n(\overline{F}_p) \), \( F = \text{Frob}_q \) corresponds to \( \rho: \Gamma \subseteq \text{GL}_m \), then \( \Gamma^F = \Gamma(\overline{F}_q) \).
- \( \Gamma = \text{PSL}_n(\overline{F}_p) \), \( F \) is defined by \( g \rightarrow \text{Frob}_p((g^T)^{-1}) \), then \( G = \text{PSU}_n(p) \) (Unitary groups).
Maximal subgroups of groups of Lie type

Theorem [Larsen & Pink, 1998]. The subgroups of $G=(\Gamma^F)^{\text{der}}$ are:

1. **Very small:** their size is bounded by a function of $r$.

2. **Structural subgroups:** fix a line in some representation $\rho_\Gamma: \Gamma \to \text{GL}_d(F_p)$, where $d=d(r)$ depends only in the Lie type of $\Gamma$. (Types $C_1$, $C_2$, $C_3$, $C_4$, $C_6$, $C_7$, $C_8$ and $S$ of Aschbacher).

3. **Subfield subgroups:** are 'almost' $\Gamma^{F_0}$ (= between $\Gamma^{F_0}$ and $(\Gamma^{F_0})^{\text{der}}$) for some Frobenius $F_0$, s.t. $F$ is a power of $F_0$. (Type $C_5$ of Aschbacher).

Remark. $[\Gamma^F:(\Gamma^F)^{\text{der}}] \leq 2r.$
Maximal subgroups of groups of Lie type

Example. \( G = \text{SL}_n(q) \), acts on \( V = \mathbb{F}_q^n \).

Structural subgroups. A parabolic subgroup (type \( C_1 \)) stabilizes some subspace \( U \subset V \) (\( \dim U = m < n \)):

\[
\begin{pmatrix}
  m \times m & * \\
  0 & (n-m) \times (n-m)
\end{pmatrix}
\]

\( \Leftrightarrow \) stabilizes a line in \( \wedge^m V \) (the m-th exterior product of \( V \)).

The dimension \( d = \dim (\wedge^m V) \) of this representation is maximal when \( m = n/2 \), and then \( d = \binom{n}{n/2} = O(2^n) \).

The other types of subgroups fix direct sums, tensor products etc.

Subfield subgroups. \( \text{SL}_n(p^f) \) where \( f | e \) (\( q = p^e \)).
Main steps of the proof

[Avni, G]. There is a function $c(r)$ s.t. if $G=L_r(q)$ then $X_k(G)$ is connected for all $k \geq c(r)$.

**Our aim:** Show that there is $c=c(r)$ s.t. if $k \geq c$, any generating $k$-tuple $(x_1, \ldots, x_k)$ of $G$ is connected to a redundant $k$-tuple.

**Step 1:** There is a constant $c_1=c_1(r)$ s.t. for any $k \geq c_1$, every generating $k$-tuple $(x_1, \ldots, x_k)$ contains a subset of $c_1$ generators, say $\{x_1, \ldots, x_{c_1}\}$, s.t. $H_0 = <x_1, \ldots, x_{c_1}> \approx \Gamma^{F_0}$ for some $F_0$ (where $F$ is some power of $F_0$).

**Remark.** Here we use at least exponentially many generators.
Main steps of the proof

Step 2: Connect \((x_1, \ldots, x_{c_1}, x_{c_1+1}, \ldots, x_k) \rightarrow (x_1, \ldots, x_{c_1}, w, \ldots, x_k)\) s.t. \(w\) is a regular semisimple element.

Example. \(G=\text{SL}_n(q)\). a regular semisimple element \(w\) has \(n\) different eigen values (in \(\overline{F}_p\)).

Step 3: Now we have the \(k\)-tuple \((x_1, \ldots, x_{c_1}, w, y_1, \ldots, y_m, z_1, \ldots, z_m, \ldots)\), where: \(m=m(r), c=c_1+1+2m\) and \(k \geq c\).

Let: \(H_1 = <x_1, \ldots, x_{c_1}, w, y_1, \ldots, y_m>\) and \(H_2 = <x_1, \ldots, x_{c_1}, w, z_1, \ldots, z_m>\), then: \(H_1, H_2 \supseteq H_0 \cong \Gamma^{F_0}\).

Therefore, by [Larsen & Pink]: \(H_1 \cong \Gamma^{F_1}\) and \(H_2 \cong \Gamma^{F_2}\) (for some \(F_1, F_2\) which are powers of \(F_0\)).
Main steps of the proof

Step 4:

- If $F_{H1} = F_{H2}$: then $H_1$ and $H_2$ are almost equal (both contain $(\Gamma_{H1}^{F})^{\text{der}}$ and contained in $\Gamma_{H1}^{F}$), so we get redundant generators.

- If $|F_{H1}| < |F_{H2}|$:

Remark. The centralizer of a regular semisimple element $w$ 'measures' the size of the defining field: $|F_G| = [C_G(w)^{1/r}]$.

Example. $G=\text{SL}_n(q)$. $w$ is totally split $\Rightarrow C_G(w) = (q-1)^{n-1} \approx q^{n-1}$.

$w$ is totally non-split $\Rightarrow C_G(w) = (q^{n-1})/(q-1) \approx q^{n-1}$.

Therefore:

$$|F_{H1}| < |F_{H2}| \iff |C_{H1}(w)| < |C_{H2}(w)|.$$
Main steps of the proof

Trick. We can connect by Nielsen moves:

\[(x_1, \ldots, x_{c_1}, w, y_1, \ldots, y_m, z_1, \ldots, z_m, \ldots) \rightarrow (x_1, \ldots, x_{c_1}, w, y_1', \ldots, y_m', z_1, \ldots, z_m, \ldots)\]

s.t.  \[\Delta_1' = \langle x_1, \ldots, x_{c_1}, w, y_1', \ldots, y_m' \rangle\] satisfies:

\[|C_{H1'}(w)| \geq |C_{H2}(w)| \Rightarrow |F_{H1'}| \geq |F_{H2}|.\]

Therefore:

\[|F_{H1'}| + |F_{H2}| \geq |F_{H1}| + |F_{H2}|.\]

Since this sum is bounded (by \(2|F_G|\)), we are done.
Summary

We study the connectivity problem of the Product Replacement Algorithm graph for finite simple groups. The vertices of this graph are the generating k-tuples of G, and the connected components correspond to the transitivity classes of the action of the automorphism group of the free group $\text{Aut}(F_k)$ on the set of epimorphisms $F_k \rightarrow G$.

We distinguish two kinds of behavior:

1. When $k=2$, there are many connected components.
2. When $k$ is large enough, the graph is connected. It was conjectured by Wiegold that $k=3$ is enough for connectivity.