Automorphisms of Steiner designs

Lászlo Babai 1  John Wilmes 2

1Departments of Mathematics and Computer Science
   University of Chicago
   laci@cs.uchicago.edu

2Department of Mathematics
   University of Chicago
   wilmesj@math.uchicago.edu

AMS Special Session on Algebraic Methods in Graph Theory
   and Combinatorics
   23 March 2013
Steiner 2-designs

**Definition**

Steiner 2-design $S(2, s, v)$ has $v$ points and a set of lines:

- all lines have $s$ points
- every pair of points lies on unique line
Steiner 2-designs

**Definition**

Steiner 2-design $S(2, s, v)$ has $v$ points and a set of lines:
- all lines have $s$ points
- every pair of points lies on unique line

Example: affine space

hyperplane (size $v/s$)
Steiner 2-designs

Definition

Steiner 2-design $S(2, s, v)$ has $v$ points and a set of lines:
- all lines have $s$ points
- every pair of points lies on unique line

Trivial if $s = 2$
Main result

Theorem (Babai–W, Chen–Sun–Teng)

A nontrivial $S(2, s, v)$ has at most $v^{O(\log v)}$ automorphisms.

- Previous best: $v^{O(\sqrt{v})}$ (Babai–Pyber 94, Spielman 96)
- Bound for Steiner $t$-designs: $v^{O(t+\log v)}$ (this paper)
Main result

Theorem (Babai–W, Chen–Sun–Teng)

A nontrivial $S(2, s, v)$ has at most $v^{O(\log v)}$ automorphisms.

- Previous best: $v^{O(\sqrt{v})}$ (Babai–Pyber 94, Spielman 96)
- Bound for Steiner $t$-designs: $v^{O(t+\log v)}$ (this paper)

Goal: find small base for automorphism group – set of points with trivial pointwise stabilizer
Theorem (Babai–W, Chen–Sun–Teng)

A nontrivial $S(2, s, v)$ has at most $v^{O(\log v)}$ automorphisms.

- Previous best: $v^{O(\sqrt{v})}$ (Babai–Pyber 94, Spielman 96)
- Bound for Steiner $t$-designs: $v^{O(t+\log v)}$ (this paper)

**Goal:** find small base for automorphism group – set of points with trivial pointwise stabilizer

Theorem (Babai–W, Chen–Sun–Teng)

Exists base of size $O(\log v)$
The individualization/refinement method

Classical heuristic: coloring points/lines

- Create irregularity: **Individualize** a point
  
  (assign unique color)

- Exploit irregularity: Canonically **refine** coloring
  
  (isomorphisms preserve refined colors)
The individualization/refinement method

**Classical heuristic**: coloring points/lines

- **Create irregularity**: Individualize a point *(assign unique color)*
- **Exploit irregularity**: Canonically refine coloring *(isomorphisms preserve refined colors)*

Naive color refinement:

- Refined color of point/line: count colors of incident elements
- After \( \leq n \) refinement rounds, reach **stable refinement**.
Initially, design **highly regular**
Individualize two points
Refine coloring
Individualization and refinement

Stable refinement reached:

- Each black point: one purple, gray, and orange line
- Each purple line: two black, one blue point
Definition
Set $S$ splits $X$: after individualizing everything in $S$, each vertex of $X$ gets unique color in stable refinement

Proposition
If $S$ splits $X$ then $S$ is a base for $\text{Aut}(X)$
Gradual color refinement

(vs. CST strategy of finding pairwise distinguishers)

**Definition**

A **steady set** is a union of color classes.
Gradual color refinement

Target 1

“Hyperplane-sized” steady set ($\geq Cv/s$) with max color class size $\leq \varepsilon v/s$. $(C = 1/4, \varepsilon = 2^{-20})$
Gradual color refinement

Target 2

All color classes size $\leq \varepsilon v/s.$

($\varepsilon = 2^{-16}$)
Gradual color refinement

Target 3
Each point gets a unique color.
Target 1: Good granularity on a “hyperplane-sized” set
Granularity

Definition

The \textbf{granularity} of a steady set $A$ is $|A|/m(A)$, where $m(A)$ is the max color class size in $A$. 

\begin{align*}
\end{align*}
Strategy: Controlled growth, improved granularity

Blow-up while preserving granularity
Strategy: Controlled growth, improved granularity

Blow-up while preserving granularity

Improve granularity (size goes down)
Strategy: Controlled growth, improved granularity

Blow-up while preserving granularity

Improve granularity (size goes down)
Strategy: Controlled growth, improved granularity

Blow-up while preserving granularity

Improve granularity (size goes down)
Strategy: Controlled growth, improved granularity

Blow-up while preserving granularity

Improve granularity (size goes down)
Target 2: Good granularity everywhere
Extending the fine coloring of “hyperplane”
Extending the fine coloring of “hyperplane”

Large color class

We show it still splits in two
Extending the fine coloring of “hyperplane”

Individualize random apex
Extending the fine coloring of “hyperplane”
Extending the fine coloring of “hyperplane”

Individualize random apex
Extending the fine coloring of “hyperplane”

Naive idea...

Individualize random apex
Extending the fine coloring of “hyperplane”

Actual picture...

Individualize random apex
We show it still splits in two

Individualize random apex

Extending the fine coloring of “hyperplane”
Target 3: Complete split

Color classes still nearly “hyperplane-sized!”
Target 3: Complete split

Color classes still nearly “hyperplane-sized!”
iterated random cones
(like increasing "subspaces")
Addressing scheme

- iterated random cones
  (like increasing “subspaces”)

\[ f_1(x), f_2(x), f_3(x) \]

\[ p_0, p_1, p_2 \]
iterated random cones
(like increasing “subspaces”)

\[
\begin{align*}
f_1(x) & \quad f_2(x) \\
 p_0 & \quad p_1 \\
 p_2 & \quad p_3 \quad f_3(x)
\end{align*}
\]
iterated **random cones**
(like increasing “subspaces”)

(s − 1)-way branching
Addressing scheme

- iterated random cones
  (like increasing "subspaces")
- \((s - 1)\)-way branching

**Lemma**

At step \(d\), produces \((s - 1)^d\)
uniformly distributed,
pairwise independent points.
After \( \left( \frac{\log \nu}{\log s} \right)^2 \) rounds, each point likely has unique color via Chebyshev argument.

Points infer color from history.
Review of main results

Theorem (Babai–W, Chen–Sun–Teng)

Nontrivial $S(2, s, v)$ has base of size $O(\log v)$

Corollary

Nontrivial $S(2, s, v)$ has at most $v^{O(\log v)}$ automorphisms
Motivation: isomorphism testing

Theorem (Babai–W, Chen–Sun–Teng)

*Test isomorphism of $S(2, s, \nu)$ in time $\nu^{O(\log \nu)}$*

Theorem (Babai–Chen–Sun–Teng–W)

*Test isomorphism of SR graph in time $\exp(\tilde{O}(n^{1/5}))$*
Theorem (Neumaier '79)

A nontrivial SR graph is one of these:

1. line-graph of Steiner 2-design
2. line-graph of transversal design
3. conference graph
4. satisfies “claw bound” (eigenvalue inequality)
Theorem

Bound on number of automorphisms:

1. line-graph of Steiner 2-design: $v^{\log v}$ (this)
2. line-graph of transversal design: $v^{\log v}$ (Miller '78)
3. conference graph: $n^{\log n}$ (Babai '80)
4. satisfies “claw bound”: $\exp(\tilde{O}(n^{9/37}))$ 10am here
Outlook: automorphisms of SR graphs

Theorem

Bound on number of automorphisms:

1. line-graph of Steiner 2-design: $v^\log v$ (this)
2. line-graph of transversal design: $v^\log v$ (Miller ’78)
3. conference graph: $n^\log n$ (Babai ’80)
4. satisfies “claw bound”: $\exp(\tilde{O}(n^{9/37}))$ 10am here
Reconstruction from line-graph

To get bound on $|\text{Aut}(L(X))|$, need to reconstruct $X$ from $L(X)$

**Proposition**

*If* $s^3 - 2s^2 + 2s < v$, *then* $X$ *uniquely reconstructed from* $L(X)$;  
*If* $s^3 - 2s^2 + 2s \geq v$, *then* claw bound holds

First bound is optimal: consider 3-dim’l projective space
Non-unique reconstruction

**Theorem**

If $G = L(X)$ for $X$ nontrivial $S(2, s, v)$ with $s^2 = O(v^{1-\epsilon})$ at most $\exp(\tilde{O}(s^3/(\epsilon v)))$ reconstructions of $S(2, s, v)$ from $G$.

**Corollary**

$|\text{Aut}(X)| \leq \exp(\tilde{O}(n^{1/6}))$
### Theorem

If $G = L(X)$ for $X$ nontrivial $S(2, s, v)$ with $s^2 = O(v^{1-\varepsilon})$ at most

$$\exp(\tilde{O}(s^3/(\varepsilon v)))$$

reconstructions of $S(2, s, v)$ from $G$.

### Corollary

$$|\text{Aut}(X)| \leq \exp(\tilde{O}(n^{1/6}))$$

### Lemma

If $s^2 = O(v^{1-\varepsilon})$, then cliques of reconstructions have form $A \cup B$ where $|A| = O(1/\varepsilon)$ and $B$ is set of common neighbors of $A$. 
Non-unique reconstruction

**Theorem**

If $G = L(X)$ for $X$ nontrivial $S(2, s, v)$ with $s^2 = O(v^{1-\varepsilon})$ at most

$\exp(\tilde{O}(s^3/(\varepsilon v)))$ reconstructions of $S(2, s, v)$ from $G$

**Corollary**

$|\text{Aut}(X)| \leq \exp(\tilde{O}(n^{1/6}))$

**Challenge**

Find: $X$ an $S(2, s, v)$ such that $L(X)$ has $\Omega(n^{\varepsilon})$ reconstructions
- Find Steiner design $X$ so that $L(X)$ has $\Omega(n^\epsilon)$ reconstructions?!
- Improve $\exp(n^{1/6})$ bound for $|\text{Aut}(L(X))|$
- **Conjecture:** (Babai 1981) $|\text{Aut}(G)| = \exp(n^\epsilon)$ for SR graph
  - (Exceptions: trivial, $L(K_n)$, $L(K_{n,n})$, and complements)
  - Current best: $|\text{Aut}(G)| \leq \exp(n^{9/37})$ (Chen–Sun–Teng) (using individualization/refinement)