Coherent configurations with nonsolvable automorphism group

Andrey Vasil'ev

Sobolev Institute of Mathematics and Novosibirsk State University

«Symmetry vs Regularity»
Conference in Algebraic Graph Theory

Pilsen, Czech Republic, 01.07.-07.07.2018

Setup

Ω is a finite set of size n, I is a set of colors

$\mathcal{X} = (\Omega, R)$ is a (colored) coherent configuration (a scheme)
$R = \{r_i : i \in I\}$ is a partition of $\Omega \times \Omega$

Setup

Ω is a finite set of size n, I is a set of colors

$\mathcal{X} = (\Omega, R)$ is a (colored) coherent configuration (a scheme)
$R = \{r_i : i \in I\}$ is a partition of $\Omega \times \Omega$

$\mathcal{X}' = (\Omega, R')$ is another scheme with the same set of colors
$\mathrm{Iso}(\mathcal{X}, \mathcal{X}') = \{\varphi \in \mathrm{Sym}(\Omega) : r_i\varphi = r_i', i \in I\}$

Setup

Ω is a finite set of size n, I is a set of colors

$\mathcal{X} = (\Omega, R)$ is a (colored) coherent configuration (a scheme)
$R = \{r_i : i \in I\}$ is a partition of $\Omega \times \Omega$

$\mathcal{X}' = (\Omega, R')$ is another scheme with the same set of colors
$\mathrm{Iso}(\mathcal{X}, \mathcal{X}') = \{\varphi \in \mathrm{Sym}(\Omega) : r_i\varphi = r_i', i \in I\}$

If $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ is non-empty, then it is a coset in $\mathrm{Sym}(\Omega)$ of
$\mathrm{Aut}(\mathcal{X}) = \{\varphi \in \mathrm{Sym}(\Omega) : r_i\varphi = r_i, i \in I\}$

Problems

$\mathcal{K}$ (resp. $\mathcal{K}_n$) is a class (closed w.r.t isomorphisms) of schemes (resp. of schemes of size n)

ISO$_{\mathcal{K}}$: Given $\mathcal{X}, \mathcal{X}' \in \mathcal{K}$, find $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$

Problems

$\mathcal{K}$ (resp. $\mathcal{K}_n$) is a class (closed w.r.t isomorphisms) of schemes (resp. of schemes of size n)

ISO$_{\mathcal{K}}$: Given $\mathcal{X}, \mathcal{X}' \in \mathcal{K}$, find $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$

AUT$_{\mathcal{K}}$: Given $\mathcal{X} \in \mathcal{K}$, find $\mathrm{Aut}(\mathcal{X})$

Problems

$\mathcal{K}$ (resp. $\mathcal{K}_n$) is a class (closed w.r.t isomorphisms) of schemes (resp. of schemes of size n)

$\mathsf{ISO}_{\mathcal{K}}$: Given $\mathcal{X}, \mathcal{X}' \in \mathcal{K}$, find $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$

$\mathsf{AUT}_{\mathcal{K}}$: Given $\mathcal{X} \in \mathcal{K}$, find $\mathrm{Aut}(\mathcal{X})$

$\mathcal{C}$ is the class of all schemes

$\mathsf{RCG}_{\mathcal{K}}$: Given $\mathcal{X} \in \mathcal{C}$, determine whether $\mathcal{X} \in \mathcal{K}$ or not

Why does a solvability of $\mathsf{Aut}(\mathcal{X})$ matter?

Why does a solvability of $\mathrm{Aut}(\mathcal{X})$ matter?

The composition width $cw(H)$ of a group H is a least positive integer d such that every nonabelian composition factor of a group H can be embedded in $\mathrm{Sym}(d)$

Claim (Babai–Lucks, 1983)

Let $\mathcal{X} = (\Omega, R)$ be a scheme. Given $H \leq \mathrm{Sym}(\Omega)$ with $cw(H) \leq d$, the group $\mathrm{Aut}(\mathcal{X}) \cap H$ can be found in time $n^{f(d)}$

Schemes associated with groups: Cayley schemes

Let $\Omega = G$ for some group G
$\mathcal{X} = (\Omega, R)$ is called a Cayley scheme over G if $\mathrm{Aut}(\mathcal{X})$ includes a regular subgroup G_{right} isomorphic to G

Schemes associated with groups: Cayley schemes

Let $\Omega = G$ for some group G
$\mathcal{X} = (\Omega, R)$ is called a Cayley scheme over G if $\mathrm{Aut}(\mathcal{X})$ includes a regular subgroup G_{right} isomorphic to G

A Cayley scheme over G is central if $\mathrm{Aut}(\mathcal{X})$ includes $\langle G_{left}, G_{right} \rangle$

Schemes associated with groups: Cayley schemes

Let $\Omega = G$ for some group G
$\mathcal{X} = (\Omega, R)$ is called a Cayley scheme over G if $\mathrm{Aut}(\mathcal{X})$ includes a regular subgroup G_{right} isomorphic to G

A Cayley scheme over G is central if $\mathrm{Aut}(\mathcal{X})$ includes $\langle G_{left}, G_{right} \rangle$

Remark. If $\Gamma = \mathrm{Cay}(G, X)$ is an ordinary Cayley graph over G with a connection set X, then the Weisfeiler–Leman closure of the partition with three relations consisting of the diagonal, the edges, and the non-edges forms the corresponding Cayley scheme $\mathcal{X}$.

Cayley graph is central if its connection set is a normal subset of G.

Central Cayley schemes over almost simple groups

S is a nonabelian simple group (in particular, $S \simeq \mathrm{Inn}(S)$)
G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$

Central Cayley schemes over almost simple groups

S is a nonabelian simple group (in particular, $S \simeq \mathrm{Inn}(S)$)
G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$

$\mathcal{CCS}$ the class of central Cayley schemes over almost simple groups

Theorem 1 (Ponomarenko–V., 2017)

The problem $\mathrm{ISO}_{\mathcal{CCS}_n}$ can be solved in time $\mathrm{poly}(n)$

Central Cayley schemes over almost simple groups

S is a nonabelian simple group (in particular, $S \simeq \mathrm{Inn}(S)$)
G is called an almost simple group, if $S \leq G \leq \mathrm{Aut}(S)$

$\mathcal{CCS}$ the class of central Cayley schemes over almost simple groups

Theorem 1 (Ponomarenko–V., 2017)

The problem $\mathrm{ISO}_{\mathcal{CCS}_n}$ can be solved in time poly(n)

Remark on simple groups

Grechkoseeva–PV., to appear:

Let G be a finite simple group, X a normal subset of G. Then the Cayley graph $\Gamma = \mathrm{Cay}(G, X)$ has at most two nonequivalent Cayley representations. Moreover, Γ is CI-graph if and only if $X = X^{-1}$

Proof of Theorem 1: Key ingredients

1. In the analysis of possible structure of $\mathrm{Aut}(\mathcal{X})$ we apply the classification of primitive permutation groups with a regular almost simple subgroup (Liebeck–Praeger–Saxl, 2010), while in the imprimitive case the key is a concept of the generalized wreath product of groups (and schemes)
2. In the algorithmic part we use the Weisfeiler–Leman algorithm and methods developed by Evdokimov and Ponomarenko for isomorphism testing of circulants.

Proof of Theorem 1: Key ingredients

1. In the analysis of possible structure of $\mathrm{Aut}(\mathcal{X})$ we apply the classification of primitive permutation groups with a regular almost simple subgroup (Liebeck–Praeger–Saxl, 2010), while in the imprimitive case the key is a concept of the generalized wreath product of groups (and schemes)
2. In the algorithmic part we use the Weisfeiler–Leman algorithm and methods developed by Evdokimov and Ponomarenko for isomorphism testing of circulants.
3. In the proof of the CI-property for simple groups we (prove) and exploit the following fact:
   Each nonabelian finite simple group S contains an involution t such that $\mathrm{Aut}(S) = S \cdot C_{\mathrm{Aut}(S)}(t)$.

Schemes associated with groups: Schurian schemes

$G \leq \mathrm{Sym}(\Omega)$ acts componentwisely on $\Omega \times \Omega$

$S = \mathrm{Orb}_2(G, \Omega)$ is the set of orbits of this action (2-orbits)

Schemes associated with groups: Schurian schemes

$G \leq \mathrm{Sym}(\Omega)$ acts componentwisely on $\Omega \times \Omega$

$S = \mathrm{Orb}_2(G, \Omega)$ is the set of orbits of this action (2-orbits)

$\mathrm{Inv}(G) = \mathrm{Inv}(G, \Omega) = (\Omega, S)$ is a schurian scheme

Claim

$\mathcal{X}$ is schurian if and only if $\mathcal{X} = \mathrm{Inv}(\mathrm{Aut}(\mathcal{X}))$

Schemes associated with groups: Schurian schemes

$G \le \mathrm{Sym}(\Omega)$ acts componentwisely on $\Omega \times \Omega$

$S = \mathrm{Orb}_2(G, \Omega)$ is the set of orbits of this action (2-orbits)

$\mathrm{Inv}(G) = \mathrm{Inv}(G, \Omega) = (\Omega, S)$ is a schurian scheme

Claim

$\mathcal{X}$ is schurian if and only if $\mathcal{X} = \mathrm{Inv}(\mathrm{Aut}(\mathcal{X}))$

If G is a finite group and $H \le G$, then G acts on the set $\Omega = G/H$ of right cosets by right multiplications

$\mathcal{X} = \mathrm{Inv}(G, H)$ is a (homogeneous) scheme w.r.t this action

Cartan schemes over simple groups of Lie type

G is a finite group with a (B, N)-pair
$H = B \cap N$ is the Cartan subgroup of G
$\mathcal{X} = \mathrm{Inv}(G, H)$ is called a Cartan scheme

Cartan schemes over simple groups of Lie type

G is a finite group with a (B, N)-pair
$H = B \cap N$ is the Cartan subgroup of G
$\mathcal{X} = \mathrm{Inv}(G, H)$ is called a Cartan scheme

Claim

Every finite simple group of Lie type is a group with a (B, N)-pair

Cartan schemes over simple groups of Lie type

G is a finite group with a (B, N)-pair
$H = B \cap N$ is the Cartan subgroup of G
$\mathcal{X} = \mathrm{Inv}(G, H)$ is called a Cartan scheme

Claim

Every finite simple group of Lie type is a group with a (B, N)-pair

L is a simple group of Lie type of rank l over the field of order q

$\mathcal{L}$ is the class of Cartan schemes for such groups L (with additional condition $l \geq 7$ and $q \geq 4l$ in the case of classical groups)

Theorem 2 (Ponomarenko–V.,2016)

The problems $\mathrm{RCG}_{\mathcal{L}_n}$ and $\mathrm{ISO}_{\mathcal{L}_n}$ can be solved in time $\mathrm{poly}(n)$

Proof of Theorem 2: Key ingredients

1. Combinatorial part. A sufficient condition for any scheme to have the combinatorial base of size at most 2
2. Group-theoretical part. Proving that the above condition holds for Cartan scheme over groups from $\mathcal{L}$
3. Algorithmic part. The Weisfeiler–Leman algorithm and the fact that the combinatorial base of $\mathcal{X}$ is at most 2

AUT for Schurain schemes and 2-Closure problem

$\mathcal{SCH}$ is the class of all Schurian schemes

$\mathcal{X} = (\Omega, R) \in \mathcal{SCH} \Leftrightarrow$ there is $G \leq \mathrm{Sym}(\Omega)$ s.t. $R = \mathrm{Orb}(G, \Omega^2)$

AUT for Schurain schemes and 2-Closure problem

$\mathcal{SCH}$ is the class of all Schurian schemes

$\mathcal{X} = (\Omega, R) \in \mathcal{SCH} \Leftrightarrow$ there is $G \leq \mathrm{Sym}(\Omega)$ s.t. $R = \mathrm{Orb}(G, \Omega^2)$

It follows that $\mathrm{AUT}_{\mathcal{SCH}}$ is equivalent to the following

2-Closure Problem

Given a permutation group G, find $G^{(2)}$

Wielandt, 1969: $G^{(2)} = \mathrm{Aut}(\mathrm{Inv}(G))$ is the 2-closure of G

AUT for Schurain schemes and 2-Closure problem

$\mathcal{SCH}$ is the class of all Schurian schemes

$\mathcal{X} = (\Omega, R) \in \mathcal{SCH} \Leftrightarrow$ there is $G \leq \mathrm{Sym}(\Omega)$ s.t. $R = \mathrm{Orb}(G, \Omega^2)$

It follows that $\mathrm{AUT}_{\mathcal{SCH}}$ is equivalent to the following

2-Closure Problem

Given a permutation group G, find $G^{(2)}$

Wielandt, 1969: $G^{(2)} = \mathrm{Aut}(\mathrm{Inv}(G))$ is the 2-closure of G

Remark. One can consider the 2-closure problem as dual to

APART Problem

Given a partition P of Ω^2, find $\mathrm{Inv}(\mathrm{Aut}(P))$

Known Results

Theory (Wielandt et al.)

1. G is abelian $\Rightarrow G^{(2)}$ is abelian
2. G is a p-group $\Rightarrow G^{(2)}$ is a p-group
3. G is nilpotent $\Rightarrow G^{(2)}$ is nilpotent
4. G is of odd order $\Rightarrow G^{(2)}$ is of odd order
5. G is imprimitive Frobenius $\Rightarrow G^{(2)} = G$
6. $(G \times H)^{(2)} = G^{(2)} \times H^{(2)}$ (in both cases)
7. $(G \wr H)^{(2)} = G^{(2)} \wr H^{(2)}$ (an imprimitive wreath product)

Known Results

Theory (Wielandt et al.)

1. G is abelian $\Rightarrow G^{(2)}$ is abelian
2. G is a p-group $\Rightarrow G^{(2)}$ is a p-group
3. G is nilpotent $\Rightarrow G^{(2)}$ is nilpotent
4. G is of odd order $\Rightarrow G^{(2)}$ is of odd order
5. G is imprimitive Frobenius $\Rightarrow G^{(2)} = G$
6. $(G \times H)^{(2)} = G^{(2)} \times H^{(2)}$ (in both cases)
7. $(G \wr H)^{(2)} = G^{(2)} \wr H^{(2)}$ (an imprimitive wreath product)

Algorithms

The 2-closure problem for a permutation group G of degree n can be solved in time poly(n) in the following cases

1. G is nilpotent (Ponomarenko, 1994)
2. G is of odd order (Evdokimov–P., 2001)

Obstacles

1. G is solvable $\not\Rightarrow$ $G^{(2)}$ is solvable

   If $G = C_p \rtimes C_{p-1}$ of degree p then $G^{(2)} = \mathrm{Sym}(p)$

Obstacles

1. G is solvable $\not\Rightarrow$ $G^{(2)}$ is solvable

   If $G = C_p \rtimes C_{p-1}$ of degree p then $G^{(2)} = \mathrm{Sym}(p)$

2. Primitive case $\not\Rightarrow$ general case

   Let $G = C_{p^2} \rtimes C_{p-1}$ and $H = C_{p^2} \rtimes C_{p(p-1)}$ of degree p^2.

   Let $\mathcal{D}$ be the imprimitivity system consisting of p blocks of size p each, and let Δ is one of this blocks. Then

   $G^{\Delta} = H^{\Delta} = C_p \rtimes C_{p-1}$, so $(G^{\Delta})^{(2)} = (H^{\Delta})^{(2)} = \mathrm{Sym}(p)$

   $G_{\mathcal{D}} = H_{\mathcal{D}} = C_p \rtimes C_{p-1}$, so $(G_{\mathcal{D}})^{(2)} = (G_{\mathcal{D}})^{(2)} = \mathrm{Sym}(p)$.

   It can be easily verified that $H^{(2)} = \mathrm{Sym}(p) \wr \mathrm{Sym}(p)$,

Obstacles

1. G is solvable $\not\Rightarrow$ $G^{(2)}$ is solvable

   If $G = C_p \rtimes C_{p-1}$ of degree p then $G^{(2)} = \mathrm{Sym}(p)$

2. Primitive case $\not\Rightarrow$ general case

   Let $G = C_{p^2} \rtimes C_{p-1}$ and $H = C_{p^2} \rtimes C_{p(p-1)}$ of degree p^2.

   Let $\mathcal{D}$ be the imprimitivity system consisting of p blocks of size p each, and let Δ is one of this blocks. Then

   $G^{\Delta} = H^{\Delta} = C_p \rtimes C_{p-1}$, so $(G^{\Delta})^{(2)} = (H^{\Delta})^{(2)} = \mathrm{Sym}(p)$

   $G_{\mathcal{D}} = H_{\mathcal{D}} = C_p \rtimes C_{p-1}$, so $(G_{\mathcal{D}})^{(2)} = (G_{\mathcal{D}})^{(2)} = \mathrm{Sym}(p)$.

   It can be easily verified that $H^{(2)} = \mathrm{Sym}(p) \wr \mathrm{Sym}(p)$,

   but G is imprimitive Frobenius, so $G^{(2)} = G$.

Some New Results (not published yet)

Theorem 3 (Ponomarenko–V.)

The 2-closure problem for a permutation group G of degree n can be solved in time poly(n), if

1. G is supersolvable
2. G is metabelain

Some New Results (not published yet)

Theorem 3 (Ponomarenko–V.)

The 2-closure problem for a permutation group G of degree n can be solved in time poly(n), if

1. G is supersolvable
2. G is metabelain

A transitive permutation group is said to be $\frac{3}{2}$-transitive, if nontrivial orbits of a point stabilizer are all of the same size.

Theorem 4 (Churikov–V.)

The 2-closure problem for a $\frac{3}{2}$-transitive permutation group G of degree n can be solved in time poly(n)

Primitive case

Liebeck–Praeger–Saxl 1988, and PS 1992

If $G \leq \mathrm{Sym}(\Omega)$ is primitive, then either $\mathrm{Soc}(G) = \mathrm{Soc}(G^{(2)})$, or one of the following holds:

1. G is 2-transitive
2. G and $G^{(2)}$ are known almost simple groups
3. G and $G^{(2)}$ preserve a product decomposition $\Omega = \Delta^m$, $m \geq 2$, and G^Δ and $(G^{(2)})^\Delta$ are groups from (1) and (2).

Primitive case

Liebeck–Praeger–Saxl 1988, and PS 1992

If $G \leq \mathrm{Sym}(\Omega)$ is primitive, then either $\mathrm{Soc}(G) = \mathrm{Soc}(G^{(2)})$, or one of the following holds:

1. G is 2-transitive
2. G and $G^{(2)}$ are known almost simple groups
3. G and $G^{(2)}$ preserve a product decomposition $\Omega = \Delta^m$, $m \geq 2$, and G^Δ and $(G^{(2)})^\Delta$ are groups from (1) and (2).

We have (due to Savelii Skresanov and GAP) a bunch of examples, where G is a maximal subgroup in $\mathrm{A\Gamma L}_1(p^d)$ and $G^{(2)}$ is a subgroup of $\mathrm{AGL}_d(p)$ which contains a composition factor isomorphic to a simple group of Lie type (here $p \in \{2, 3\}$ and $d \in \{6, 8\}$).

Primitive case

Liebeck–Praeger–Saxl 1988, and PS 1992

If $G \leq \mathrm{Sym}(\Omega)$ is primitive, then either $\mathrm{Soc}(G) = \mathrm{Soc}(G^{(2)})$, or one of the following holds:

1. G is 2-transitive
2. G and $G^{(2)}$ are known almost simple groups
3. G and $G^{(2)}$ preserve a product decomposition $\Omega = \Delta^m$, $m \geq 2$, and G^Δ and $(G^{(2)})^\Delta$ are groups from (1) and (2).

We have (due to Savelii Skresanov and GAP) a bunch of examples, where G is a maximal subgroup in $\mathrm{A\Gamma L}_1(p^d)$ and $G^{(2)}$ is a subgroup of $\mathrm{AGL}_d(p)$ which contains a composition factor isomorphic to a simple group of Lie type (here $p \in \{2, 3\}$ and $d \in \{6, 8\}$).

Remark. Most of these examples are groups of rank 3.

Open Problems

Find a polynomial-time algorithm that solves the 2-closure problem

Open Problems

Find a polynomial-time algorithm that solves the 2-closure problem, in particular, for

1. solvable groups
2. groups of rank 3.

Open Problems

Find a polynomial-time algorithm that solves the 2-closure problem, in particular, for

1. solvable groups
2. groups of rank 3.

Find a polynomial-time algorithm that solves the recognition problem for schurian schemes

Open Problems

Find a polynomial-time algorithm that solves the 2-closure problem, in particular, for

1. solvable groups
2. groups of rank 3.

Find a polynomial-time algorithm that solves the recognition problem for schurian schemes, in particular, for

1. schurian eqiuvalenced schemes
2. Coxeter schemes.