Representation Theory of Graph Isomorphism

Jacob Urisman

University of Colorado Boulder

University of Cambridge, June 9th, 2026

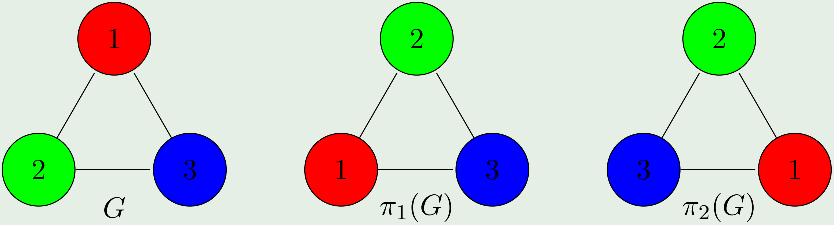
Based on joint work with Joshua A. Grochow

Graph Isomorphism in Terms of Group Actions I

S_n acts on graphs by permuting the vertices. For $\pi \in S_n$, a graph G, $\pi(G)$ by $v \mapsto \pi(v)$ for all $v \in V_G$.

Example

Let G be the triangle graph on 3 vertices. If $\pi_1 = (1, 2)$, then $\pi_1(G)$ is a reflection of the graph about the axis going through vertex 3. If $\pi_2 = (1, 2, 3)$, then $\pi_2(G)$ is a rotation of the graph.



Graph Isomorphism in Terms of Group Actions II

$G \cong H \iff$ exists $\pi \in S_n$ such that $\pi(G) = H$.

Let A_G be the adjacency matrix of a graph G and let P_π be a permutation matrix which corresponds to the permutation $\pi \in S_n$. Consider $B = P_\pi A_G P_\pi^{-1}$.

Observation

$B_{i,j} = A_{G\pi^{-1}(i),\pi^{-1}(j)}$

Weisfeiler–Leman

We evaluate our results in comparison to the power of the Weisfeiler–Leman (WL) algorithm.

Weisfeiler–Leman

We evaluate our results in comparison to the power of the Weisfeiler–Leman (WL) algorithm.

The WL algorithm is an iterative coloring algorithm which colors nodes (or k-tuples of nodes) based on the multiset of colors of a node and its neighbors (or "neighboring k-tuples").

Weisfeiler–Leman

We evaluate our results in comparison to the power of the Weisfeiler–Leman (WL) algorithm.

The WL algorithm is an iterative coloring algorithm which colors nodes (or k-tuples of nodes) based on the multiset of colors of a node and its neighbors (or "neighboring k-tuples").

The WL algorithm is a common point of comparison since it has many nice combinatorial properties, chief of which is its equivalent distinguishing power to first-order logic (Cai–Fürer–Immerman '92).

Weisfeiler–Leman

We evaluate our results in comparison to the power of the Weisfeiler–Leman (WL) algorithm.

The WL algorithm is an iterative coloring algorithm which colors nodes (or k-tuples of nodes) based on the multiset of colors of a node and its neighbors (or "neighboring k-tuples").

The WL algorithm is a common point of comparison since it has many nice combinatorial properties, chief of which is its equivalent distinguishing power to first-order logic (Cai–Fürer–Immerman '92).

k is called the dimension of the WL algorithm.

GCT Motivation

- Strongly inspired by Geometric Complexity Theory (GCT)
- Idea of GCT: use algebraic geometry and representation theory to attack complexity questions
  - Algebraic geometry: study of when systems of polynomials vanish
  - Representation theory: study of group actions on vector spaces
- ($\Rightarrow$) GCT suggests methods for proving graphs are non-isomorphic
- ($\Leftarrow$) GI as a testbed for ideas from GCT

Polynomials I

Previous work (Berkholz–Grohe '15,'17; Derksen '13; Snook–Schoenebeck–Codenotti '14; Atserias–Maneva '13) has looked at polynomials over variables x_{ij} whose vanishing forces the permutation matrix X to encode an isomorphism between G and H, i.e. $XGX^{-1} = H$.

One can apply various algebraic proof systems to these equations and many complexity measures on those proof systems turn out to be equivalent to WL.

- (monomial variant of) Polynomial Calculus (Berkholz–Grohe '15)
  - Between Nullstellensatz and regular PC
- Sherali–Adams Hierarchy (Atserias–Maneva '13)

In our work, we take a different approach.

Polynomials II

- Our work: x_{ij} is the (i,j)-th entry of A_G
- What can be expressed as polynomials evaluated on G?

Example

$\sum_{i,j} x_{ij}$ is an invariant polynomial which computes the total number of edges of G.

Polynomials III

We will be looking for isomorphism-invariant properties which are defined by the *vanishing* of (sets of) polynomials.

Example

$-|E_G| + \sum_{i,j} x_{ij}$ vanishes on G, but not any graph with a different number of edges.

Polynomials IV

Note that S_n acts on these polynomials the same way it does on adjacency matrices.

Sometimes it is more natural to describe invariant properties using the vanishing of sets of polynomials rather than individual ones.

Polynomials V

Example

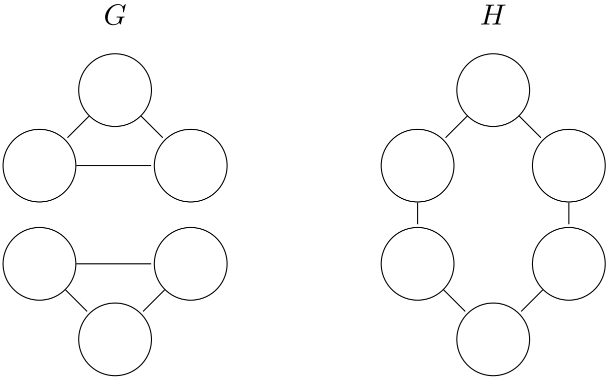
The following invariant polynomial vanishes iff all vertices have the same out-degree.

$$\sum_{\substack{i,i' \in [n] \\ i \neq i'}} \left(\sum_{j \neq i} x_{ij} - \sum_{j \neq i'} x_{i'j} \right)^2$$

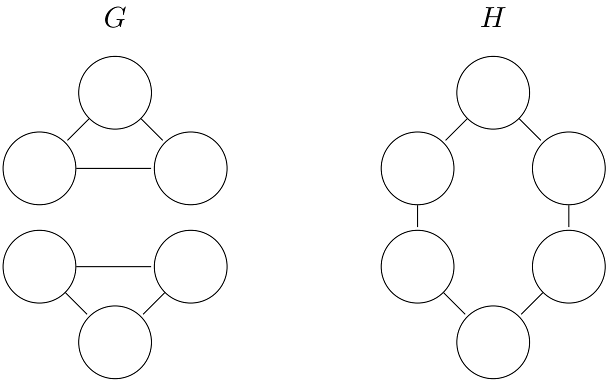
The following set of polynomials vanishes under the same condition.

$$\left\{ \sum_{j \neq i} x_{ij} - \sum_{j \neq i'} x_{i'j} \mid i, i' \in [n], i \neq i' \right\}$$

Example



Example



$$T = \{x_{ij}x_{ik}x_{jk} \mid i, j, k \in [n], \text{distinct } i, j, k\}$$

$$T(G) \neq \{0\}, T(H) = \{0\}$$

Separating Modules

Definition

A *test module* (for graph isomorphism) is a vector space $T \subseteq \mathbb{F}[x_{ij} : i, j \in [n]]/\langle x_{ij}^2 - x_{ij} : i, j \in n\rangle$ such that for all $p \in T, \pi \in S_n, \pi(p) \in T$.

A *separating module* for two graphs $G \ncong H$ is a test module such that all $p \in T$ vanish on A_G and some $p \in T$ does not vanish on A_H.

- $\{G : p(G) = 0, \forall p \in T\}$ is an isomorphism-invariant set.
- Conversely, $\{p : p(H) = 0, \forall H \cong G\}$ is a test module.

Quadratic Mismatch

- $x_{ij} :=$ the (i, j)-th entry of A_G.
- It inherently encodes edges.

Quadratic Mismatch

- $x_{ij} :=$ the (i, j)-th entry of A_G.
- It inherently encodes edges.
- WL deals with vertices.

Quadratic Mismatch

- $x_{ij} :=$ the (i, j)-th entry of A_G.
- It inherently encodes edges.
- WL deals with vertices.
- We get a (worst-case) quadratic mismatch!

Support-Degree

Definition

The *support-degree* of a monomial $x_{i_1 j_1} \cdots x_{i_d j_d}$ is

$$\text{supp-deg} := |\{i_1, \ldots, i_d, j_1, \ldots, j_d\}|$$

The support-degree of a polynomial is the maximum support-degree of any of its monomials

This is a "vertex respecting" notion of degree.

Results On Degree

Theorem (Grochow–U.)

For all d and all graphs G, H, the following are equivalent:

- *G, H are distinguishable by the initial round of d-WL.*
- *G, H admit a separating module of support-degree $\Theta(d)$.*
- *G, H admit a separating invariant of support-degree $\Theta(d)$.*

Results On Degree

Theorem (Grochow–U.)

For all d and all graphs G, H, the following are equivalent:

- *G, H are distinguishable by the initial round of d-WL.*
- *G, H admit a separating module of support-degree $\Theta(d)$.*
- *G, H admit a separating invariant of support-degree $\Theta(d)$.*

In particular, separating modules of degree or support-degree d are strictly weaker than d-WL (follows from WL round lower bound of Fürer '01).

Results On Degree

Theorem (Grochow–U.)

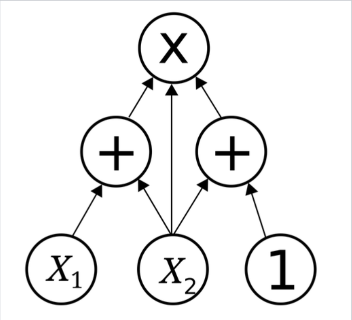
For all d and all graphs G, H, the following are equivalent:

- *G, H are distinguishable by the initial round of d-WL.*
- *G, H admit a separating module of support-degree $\Theta(d)$.*
- *G, H admit a separating invariant of support-degree $\Theta(d)$.*

In particular, separating modules of degree or support-degree d are strictly weaker than d-WL (follows from WL round lower bound of Fürer '01).

Proof relies on symmetric algebraic circuits.

Algebraic Circuits



A simple arithmetic circuit computing $(x_1 + x_2)x_2(x_2 + 1)$.

*Wikipedia

Also called “arithmetic circuits.”

Symmetric Algebraic Circuits

Definition (Dawar–Wilsenach '25)

If Γ is a permutation group acting on the input variables of a circuit C, we say C is Γ-*symmetric* if every $\pi \in \Gamma$ extends to at least one automorphism of C.
When $\Gamma \leq S_{n^2}$ (or $S_n \times S_n$) is the action of S_n on ordered pairs $\pi(x_{i,j}) = x_{\pi^{-1}(i),\pi^{-1}(j)}$, we call C *square-symmetric*.

Symmetric Algebraic Circuits

Definition (Dawar–Wilsenach '25)

If Γ is a permutation group acting on the input variables of a circuit C, we say C is Γ-*symmetric* if every $\pi \in \Gamma$ extends to at least one automorphism of C.
When $\Gamma \leq S_{n^2}$ (or $S_n \times S_n$) is the action of S_n on ordered pairs $\pi(x_{i,j}) = x_{\pi^{-1}(i),\pi^{-1}(j)}$, we call C *square-symmetric*.

Definition (Dawar–Wilsenach '25)

(With the previous assumptions) we say C is (Γ-)*rigid* if any permutation of the inputs that comes from Γ extends to at most one automorphism of C.

Symmetric Algebraic Circuits for Separating Modules

If we have an irreducible separating module V, we want a multi-output circuit whose output polynomials are a spanning set for V.

Rigidity and square-symmetry apply in the same way to multi-output circuits.

Proof Outline (separating modules weaker than WL)

1. Symmetric algebraic circuits simulate separating modules using low depth.

Proof Outline (separating modules weaker than WL)

1. Symmetric algebraic circuits simulate separating modules using low depth.
2. Symmetric algebraic circuits also simulate invariants using low depth

Proof Outline (separating modules weaker than WL)

1. Symmetric algebraic circuits simulate separating modules using low depth.
2. Symmetric algebraic circuits also simulate invariants using low depth
   - Implies separating modules and invariants are basically equivalent in distinguishing power (differ by factor of 2 in degree/support-degree).

Proof Outline (separating modules weaker than WL)

1. Symmetric algebraic circuits simulate separating modules using low depth.
2. Symmetric algebraic circuits also simulate invariants using low depth
   - Implies separating modules and invariants are basically equivalent in distinguishing power (differ by factor of 2 in degree/support-degree).
3. Construct a basis for invariants.
   - This basis will be equivalent to the initial round of WL.

Proof Sketch I

Lemma (Grochow–U.)

If there exists an irreducible separating module V for graphs G, H in degree/support-degree $\leq d$, there exists a rigid square-symmetric multi-output circuit C of total bit-size $n^{O(d)}/2^{O(d^2)}n^{O(d)}$ and depth 2 whose outputs are a spanning set for V.

Proposition (3.9)

If G, H admit separating modules in degree/support-degree $\leq d$, then they are separated by an invariant of degree/support-degree $\leq 2d$ which can be computed by a symmetric algebraic circuit of bit-size $n^{O(d)}/2^{O(d^2)}n^{O(d)}$ and depth 2.

Proof Sketch II

To characterize their power, we construct an explicit basis for invariant polynomials. If K is a subgraph of G.

$$S_K := \frac{1}{|\mathrm{Aut}(K)|} \sum_{\sigma \in S_n} \sigma \left(\prod_{(i,j) \in E_K} x_{ij} \right)$$

S_K counts the number of distinct copies of K in G. This is the initial round of WL.

Observation (3.10)

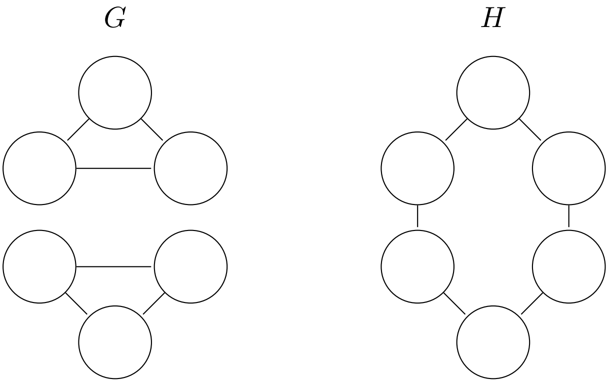
Every degree/support-degree d homogeneous invariant polynomial is a linear combination of the S_K polynomials where $d = |E_K|/|V_K|$.

Proof Sketch III

Theorem (Fürer '01)

For every dimension $d \geq 1$*, there exist non-isomorphic pairs of graphs distinguishable by d-WL, but which cannot be distinguished in fewer than* $\Omega(n)$ *rounds.*

Example



$$T = \{x_{ij}x_{ik}x_{jk} \mid i, j, k \in [n], \text{distinct } i, j, k\}$$

$$T(G) \neq \{0\}, T(H) = \{0\}$$

Our Next Idea

We wondered whether symmetric algebraic circuit size could be used more directly as a complexity measure on polynomials.

To do this, we need support.

Supports I

Definition (Blass–Gurevich–Shelah '99, Dawar–Wilsenach '25)

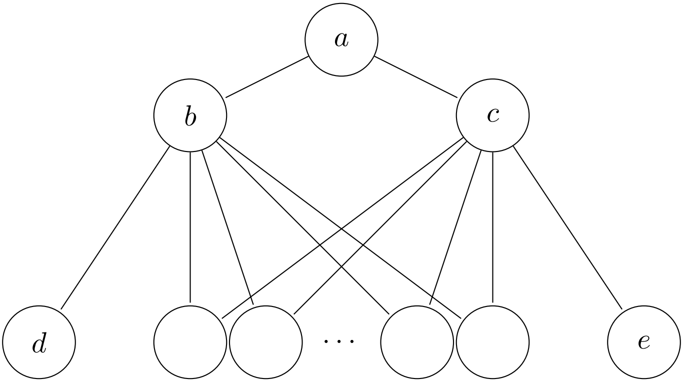
Suppose S_n acts on a set Ω. A *support* of $\omega \in \Omega$ is a subset $X \subseteq [n]$ such that every element in the pointwise stabilizer of X also stabilizes ω, i.e.

$$\bigcap \mathrm{stab}_{S_n}(x) \subseteq \mathrm{stab}_{S_n}(\omega)$$

Definition (ibid.)

The *support size* of $\omega \in \Omega$ is the minimum size of any support of ω. The support size of Ω is the maximum support size over all $\omega \in \Omega$.

Supports II



Results On Symmetric Circuit Size

Proposition

A spanning set for an irreducible separating modules can be computed by rigid square-symmetric algebraic circuits. Conversely, the outputs of a rigid square-symmetric algebraic circuits are a spanning set for an irreducible separating module.

Results On Symmetric Circuit Size

Proposition

A spanning set for an irreducible separating modules can be computed by rigid square-symmetric algebraic circuits. Conversely, the outputs of a rigid square-symmetric algebraic circuits are a spanning set for an irreducible separating module.

Theorem (Grochow–U.)

Two graphs are distinguished by separating modules (and thus invariant polynomials) computed by symmetric algebraic circuits of size $n^{O(k)}$ iff they are distinguished by $O(k)$-WL.

Key Tools (overly simplified)

Theorem (Grohe–Verbitsky '06, Thm. 3.2)

WL is simulated by boolean threshold circuits.

Theorem (Anderson–Dawar '17, Lem. 12(2))

Boolean threshold circuits are simulated by WL.

Theorem (Dawar–Wilsenach '25, Thm. 11)

Symmetric algebraic circuits are simulated by boolean threshold circuits.

Proof Sketch

$\Leftarrow$

- We modify the Grohe–Verbitsky circuit (key tool 1) to make it rigid square-symmetric.

Proof Sketch

$\Leftarrow$

- We modify the Grohe–Verbitsky circuit (key tool 1) to make it rigid square-symmetric.
- We convert the modified GV circuit to an algebraic circuit using the simple folklore conversion (which maintains rigidty and square-symmetry).

Proof Sketch

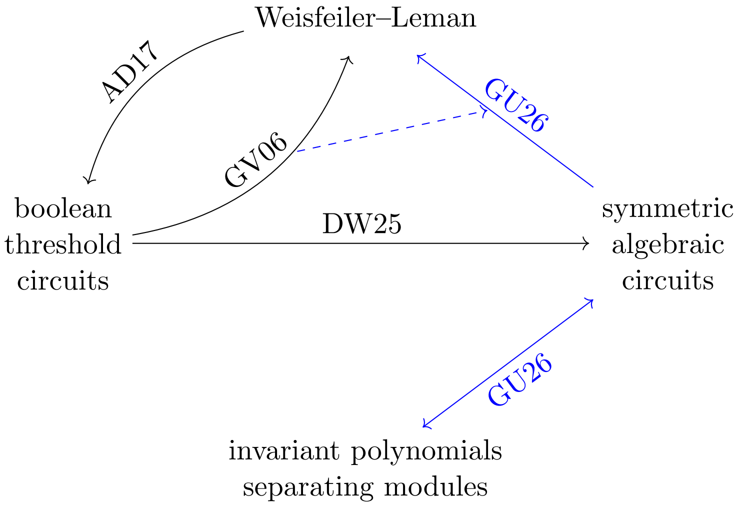
$\Leftarrow$

- We modify the Grohe–Verbitsky circuit (key tool 1) to make it rigid square-symmetric.
- We convert the modified GV circuit to an algebraic circuit using the simple folklore conversion (which maintains rigidty and square-symmetry).

$\Rightarrow$

- Implicit in Dawar–Wilsenach '25 (key tool 3).
  - Uses results from Anderson–Dawar '17 (key tool 2).

$(A \to B) :=$ A simulates B



My Favorite Result of Ours

Recall that we want to use Graph Isomorphism as a testbed for GCT.

GCT relies on multiplicity obstructions.

Test Module Equivalence I

Two test modules T, T' are said to be equivalent if there is a bilinear map $f : T \to T'$ such that $f(\pi p) = \pi f(p)$ for all $p \in T, \pi \in S_n$.

Test Module Equivalence II

Example

$$T_1 = \left\{ \sum_{j \neq i} x_{ij} - \sum_{j \neq i'} x_{i'j} \mid i, i' \in [n], i \neq i' \right\}$$

$$T_2 = \left\{ \sum_{j \neq i} x_{ji} - \sum_{j \neq i'} x_{ji'} \mid i, i' \in [n], i \neq i' \right\}$$

$$T_3 = \left\{ \sum_{j,k : |\{i,j,k\}|=3} x_{ij}x_{jk}x_{ki} - \sum_{j,k : |\{i',j,k\}|=3} x_{i'j}x_{jk}x_{ki'} : i, i' \in [n] \right\}$$

$$T_4 = \{ x_{ij}x_{ik}x_{jk} \mid i, j, k \in [n], \text{distinct } i, j, k \}$$

$$T_1 \sim T_2 \sim T_3 \neq T_4$$

Multiplicity Obstructions

One can then ask, given a test module T, how many test modules equivalent to T vanish on G. This is called the multiplicity of T.

A multiplicity obstruction of the isomorphism of G, H is a test module T with different multiplicity on G, H.

Characterization of Multiplicity Information

- Mulmuley and Sohoni in their GCT papers propose to separate complexity classes via representation-theoretic multiplicity obstructions.
- There has not been a characterization of multiplicity information as a simple combinatorial property of symmetry groups.

Characterization of Multiplicity Information

- Mulmuley and Sohoni in their GCT papers propose to separate complexity classes via representation-theoretic multiplicity obstructions.
- There has not been a characterization of multiplicity information as a simple combinatorial property of symmetry groups.
- Until now!

Results on Multiplicities

Theorem (Grochow–U.)

Two n-vertex graphs G, H are distinguished by multiplicities iff the counts of cycle types of elements in $\mathrm{Aut}(G) \leq S_n$ and $\mathrm{Aut}(H) \leq S_n$ are distinct.

Results on Multiplicities

Theorem (Grochow–U.)

Two n-vertex graphs G, H are distinguished by multiplicities iff the counts of cycle types of elements in $\mathrm{Aut}(G) \leq S_n$ and $\mathrm{Aut}(H) \leq S_n$ are distinct.

Corollary

Any two graphs with conjugate automorphism groups cannot be distinguished by multiplicity information.

Results on Multiplicities

Theorem (Grochow–U.)

Two n-vertex graphs G, H are distinguished by multiplicities iff the counts of cycle types of elements in $\mathrm{Aut}(G) \leq S_n$ and $\mathrm{Aut}(H) \leq S_n$ are distinct.

Corollary

Any two graphs with conjugate automorphism groups cannot be distinguished by multiplicity information.

Open question

Are all graphs with non-conjugate automorphism groups distinguished by multiplicity obstructions?

Open question

Is cycle-index GI-hard?

Multiplicities and Occurrences I

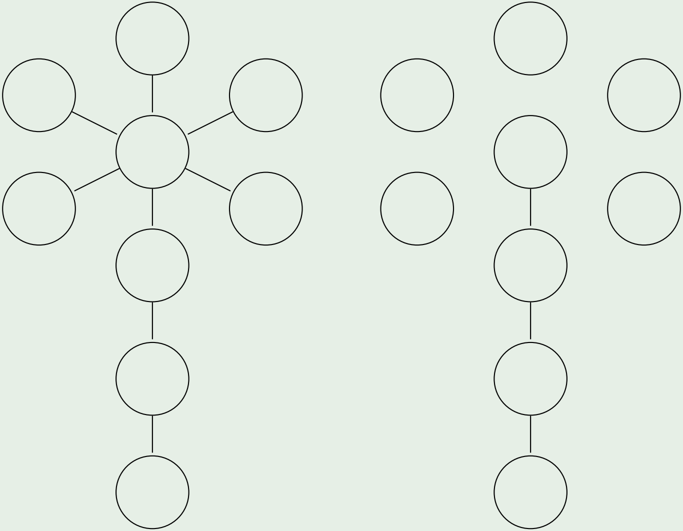
We know that occurrence obstructions are strictly weaker than multiplicity obstructions for algebraic complexity lower bounds (Dörfler–Ikenmeyer–Panova '20).

Proposition (Grochow–U.)

For all $n \geq 6$, there are pairs of simple undirected graphs $G \ncong H$ on n vertices such that G and H are separated by multiplicity obstructions but not by occurrence obstructions.

Multiplicities and Occurrences II

Example



Bonus Result on Graph Reconstruction

Theorem (Forman '04, Grochow–U.)

Let k be a positive integer, and let G be a finite simple undirected graph with $k < |E_G|$.

- *G is k-edge reconstructible iff it is identified by invariant polynomials of degree at most $|E_G| - k$.*
- *G is k-vertex reconstructible iff it is identified by invariant polynomials of support-degree at most $|V_G| - k$.*

Future Work

- Explore supports more.
  - Seems to underlie any problem which can be viewed as groups acting on a structure.
  - Representation theory of the symmetric group (GCT).

Future Work

- Explore supports more.
  - Seems to underlie any problem which can be viewed as groups acting on a structure.
  - Representation theory of the symmetric group (GCT).
- Can supports can help us extend these results to tensor isomorphism?
- Can supports provide insight into orbit closure intersection?
- Γ-symmetries for continuous groups Γ (e.g. $\mathfrak{sl}_2$)?

Open Questions

A graph is characterized by its symmetries if it is the only graph (up to isomorphism) with its automorphism group.

- Is every pair of graphs that are characterized by their symmetries distinguished by multiplicity obstructions?
- Is every graph characterized by its symmetries also characterized by its multiplicities?
- Can isomorphism of symmetry-characterized graphs be decided in polynomial time?

Open Questions

A graph is characterized by its symmetries if it is the only graph (up to isomorphism) with its automorphism group.

- Is every pair of graphs that are characterized by their symmetries distinguished by multiplicity obstructions?
- Is every graph characterized by its symmetries also characterized by its multiplicities?
- Can isomorphism of symmetry-characterized graphs be decided in polynomial time?
- Is there an algorithm to find a separating module/multiplicty obstruction in degree $\leq d$ faster than $n^{O(d)}$ time?
- Can algorithmic results on counting subgraphs H (of G on n-vertices) be 'implemented' using symmetric algebraic circuits of size/bit-size $n^{O(hdtw(H))}$ or $f(H)n^{O(tw(H))}$?

Thank you!