On the Descriptive Complexity of Finite Groups

Nathaniel A. Collins (University of Colorado Boulder)
Joshua A. Grochow (University of Colorado Boulder)
Michael Levet* (University of Colorado Boulder)

Groups, Nilpotence, and Tensors 2023

April 29, 2023

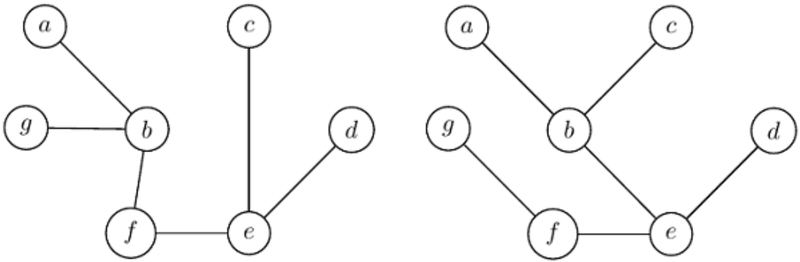
Motivation- Graph Isomorphism

Graph Isomorphism

- Graph Isomorphism is a candidate NP-intermediate problem (in NP, but neither in P nor NP-complete).
- Best algorithmic bound: $n^{\Theta(\log^2 n)}$ (Babai, 2016).
- Group Isomorphism (GpI) is strictly easier than Graph Isomorphism, under AC^0-reductions.
- Best algorithmic bound for GpI: $n^{\Theta(\log n)}$.
- Can techniques from Graph Isomorphism be fruitfully leveraged in the setting of groups? (Weisfeiler–Leman)

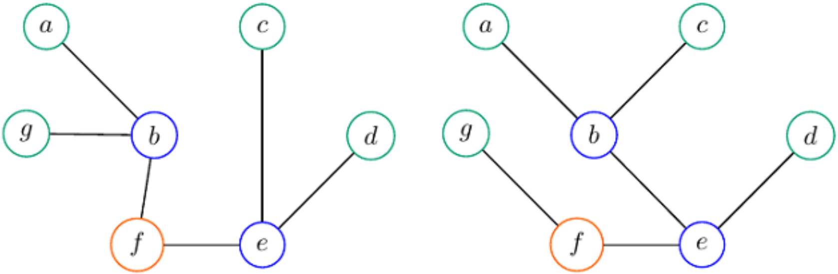
1-Dimensional Weisfeiler–Leman: Example

Input:



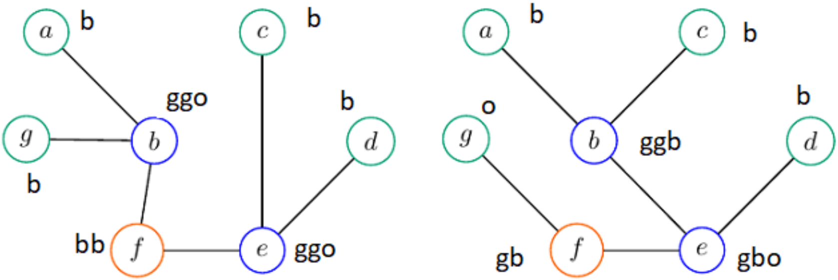
1-Dimensional Weisfeiler–Leman: Example

Initial Coloring: Color vertices by degree



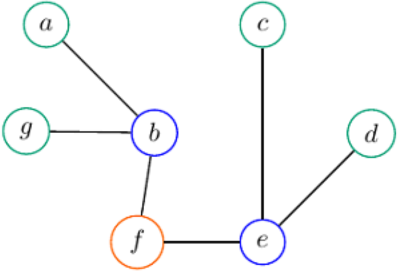
1-Dimensional Weisfeiler–Leman: Example

Refinement Step: Color each vertex based on its initial color and multiset of colors of its neighbors.



1-Dimensional Weisfeiler–Leman: Example

Refinement Step: Color each vertex based on its initial color and multiset of colors of its neighbors.



Weisfeiler–Leman

1-Dimensional Weisfeiler–Leman

- Initial Coloring: Color vertices by degree (number of neighbors)
- Refinement Step: Two vertices u, v receive the same color at round $r + 1$ if:
  - They have the same color at round r, and
  - The multiset of colors of u's neighbors is the same as for v's neighbors.
- Termination: If the multiset of colors differ at the end of a given round, we conclude that the two graphs are non-isomorphic.

Weisfeiler–Leman

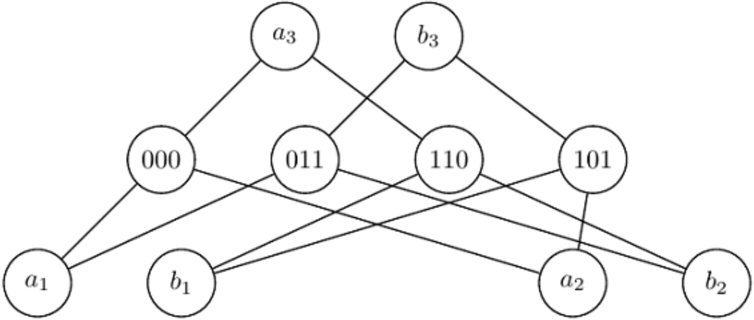
Higher-Dimensional Weisfeiler–Leman

k-dimensional Weisfeiler–Leman (k-WL):

- Color k-tuples of vertices rather than vertices.
- Initial Coloring: Color k-tuples based on their marked isomorphism type.
- Refinement Step: Color k-tuple based on its color at previous round and colors of *nearby* k-tuples (Hamming distance 1)

Weisfeiler–Leman

Counter-Example: Higher-dimensional Weisfeiler–Leman gets stuck on a construction of Cai, Fürer, & Immerman (1992). Replace each vertex with a *gadget* and connect gadgets based on edges of original graph.



Weisfeiler–Leman

Characterizations

Weisfeiler–Leman is equivalent to the following:

- 1-ary Ehrenfeucht–Fraïssé Bijective Pebble Game
- First-Order Logic with Counting Quantifiers ($\mathsf{FO} + \mathsf{C}$)
- Sherali–Adams and Lasserre Hierarchies (Linear Programming)
- (Generalized) Coherent Configurations
- Graph Neural Networks

Weisfeiler–Leman

Motivation

- What background is necessary to start reading the Weisfeiler–Leman literature (or to start collaborating)?
- Can (generalizations of) Weisfeiler–Leman do interesting things in the setting of groups?

Weisfeiler–Leman

Recent Results

Weisfeiler–Leman identifies in polynomial-time (and even in NC):

- p-groups arising from CFI graphs via Mekler's construction: (Brachter–Schweitzer, '20; Collins-L., '22)
- Coprime extensions $H \ltimes N$, where H is $O(1)$-generated and N is Abelian (Grochow–L., '22)
- Direct Products (Brachter–Schweitzer, '22; Grochow–L., '22)

Ehrenfeucht–Fraïssé Pebble Game

Spoiler: Wants to show two objects G, H are non-isomorphic

Duplicator: Wants to match or *duplicate* Spoiler's choice

- Spoiler picks up a pebble pair (p_j, p_j')
- Check: Does the induced map $p_i \mapsto p_i'$ (for all i) extend to an isomorphism?
- Duplicator picks a bijection $f : G \to H$.
- Spoiler places p_j on some $g \in G$ and p_j on $f(p_j)$.

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- The number of pebbles on the board corresponds to the Weisfeiler–Leman dimension (the k as in k-WL)
- The number of rounds of the game corresponds to the number of iterations that WL takes.

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- Recall: $[x, y] := xyx^{-1}y^{-1}$.
- Suppose Duplicator selects a bijection $f : G \to H$ such that for some $x, y \in G$, $f([x, y])$ cannot be written as $[x', y']$ for any $x', y' \in H$.

Ehrenfeucht–Fraïssé Pebble Game

- Suppose Duplicator selects a bijection $f : G \to H$ such that for some $x, y \in G$, $f([x, y])$ cannot be written as $[x', y']$ for any $x', y' \in H$.
- Spoiler pebbles $[x, y] \mapsto f([x, y])$.

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- Suppose Duplicator selects a bijection $f : G \to H$ such that for some $x, y \in G$, $f([x, y])$ cannot be written as $[x', y']$ for any $x', y' \in H$.
- Spoiler pebbles $[x, y] \mapsto f([x, y])$.
- At the next two rounds, Spoiler pebbles $x, y \in G$ and wins.

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- Let $[G, G] = \langle \{[x, y] : x, y \in G\} \rangle$.
- Suppose Duplicator selects a bijection $f : G \to H$ such $f([G, G]) \neq [H, H]$.
- Let $x \in [G, G]$ s.t. $f(x) \notin [H, H]$ (WLOG).
- Spoiler pebbles $x \mapsto f(x)$.

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- Now $x = w_1 \cdots w_\ell$, where each $w_i = [x_i, y_i]$.
- As $f(x) \notin [H, H]$, $f(x) \neq w'_1 \cdots w'_\ell$ with each $w'_i = [x'_i, y'_i]$.
- How does Spoiler win?

Weisfeiler–Leman for Groups

Ehrenfeucht–Fraïssé Pebble Game

- Now $x = w_1 \cdots w_\ell$, where each $w_i = [x_i, y_i]$.
- At the next two rounds, Spoiler pebbles $w_1 \cdots w_{\ell/2} \mapsto u'$ and $w_{\ell/2+1} \cdots w_\ell \mapsto v'$.
- WLOG, $u' \notin [H, H]$.
- Remove pebbles on x, v' and repeat the strategy.
- Spoiler wins with 3 pebbles on the board and $\leq \log_2(\ell) + O(1)$ rounds.
- Note: $\ell \leq n$.

Group Isomorphism

Fitting-free Groups

- Every finite group is built using finite simple groups.
- Composition series tell us how to "glue" the building blocks together to obtain a prescribed group G.
- Push Abelian composition factors all to the bottom:

$$0 \to \mathrm{Rad}(G) \to G \to G/\mathrm{Rad}(G) \to 0.$$

- Groups where $\mathrm{Rad}(G) = 1$ are called *Fitting-free* or *semisimple*. They do not have Abelian normal subgroups.
- Fitting-free groups admit polynomial-time isomorphism test (Babai, Codenotti, & Qiao, 2012).

Fitting-free Groups

Question

Does Weisfeiler–Leman identify Fitting-free groups in polynomial-time?

Fitting-free Groups

Higher-arity Logics

The following are equivalent (Hella 1989, 1996):

- Consider the 2-ary pebble game where Spoiler can place 1 or 2 pebbles at a given round.
- Let Q be the set of all generalized binary quantifiers, and let $\mathrm{FO}(Q)$ be the extension of first-order logic permitting quantifiers from Q.

Note that the 2-ary game trivially handles binary relational structures, such as graphs.

Fitting-free Groups

Theorem (Grochow–L., '22)

Let G be a Fitting-free group, and let H be arbitrary. If $G \not\cong H$, then in the 2-ary game, Spoiler can win with $O(1)$ pebbles and $O(1)$ rounds.

Corollary (Grochow–L., '22)

If G is Fitting-free, then G is identified by a formula in $FO(Q)$ with $O(1)$ variables and quantifier depth $O(1)$.