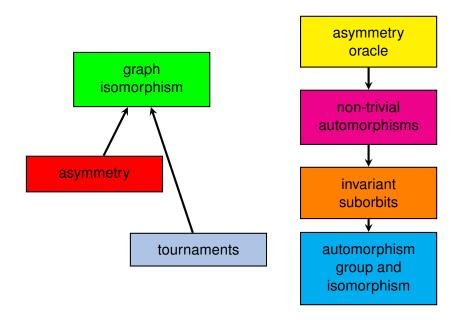
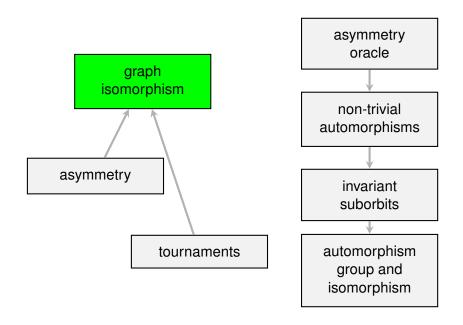
Graph isomorphism and asymmetric graphs

Pascal Schweitzer

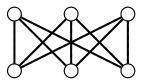
Ghent Graph Theory Workshop 2017 August 18th, Ghent







Two graphs are **isomorphic** if there is a bijection of vertices that preserves adjacency. Isomorphic graphs





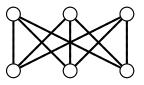
Two graphs are **isomorphic** if there is a bijection of vertices that preserves adjacency. Isomorphic graphs

Two graphs are **isomorphic** if there is a bijection of vertices that preserves adjacency.

Graph isomorphism (GI):

Algorithmic task to decide whether two graphs are isomorphic.

Isomorphic graphs





Unknown complexity

Is there an efficient algorithm for graph isomorphism?

Unknown complexity

Is there an efficient algorithm for graph isomorphism?

known

● *GI* ∈ NP NP-complete • GI NP-hard \Rightarrow SAT quasi-poly. $(\Rightarrow$ ETH false) • GI NP-hard \Rightarrow PH collapses P $(GI \in co-AM)$ unknown • $GI \in P?$ co-NP-complete Is GI NP-complete? co-AM • $GI \in co-NP?$

$$2^{O(\sqrt{(n \log n)})} \Rightarrow 2^{(\log(n)^{c})}$$
[Babai using Luks,Zemlyachenko] (1981) [Babai] (2015)

Two major open subcases:

- group isomorphism (given by multiplication table)
- tournament isomorphism

Both subcases have $2^{O(\log(n)^2)}$ -time algorithms.

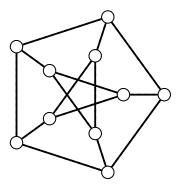
Problems equivalent to isomorphism

These following problems are polynomially equivalent:

- GI: the graph isomorphism problem
- col-GI: isomorphism problem of colored graphs
- ISO: isomorphism of general combinatorial objects
- Aut(G): compute generating set for automorphism group
- $|\operatorname{Aut}(G)|$: determine the size of $\operatorname{Aut}(G)$.

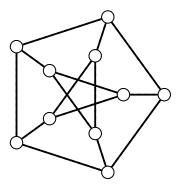
The graph isomorphism problem is actually the problem of detecting symmetries of combinatorial objects.

An automorphism is an isomorphism from a graph to itself.



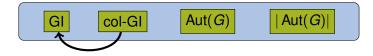
An automorphism is an isomorphism from a graph to itself.

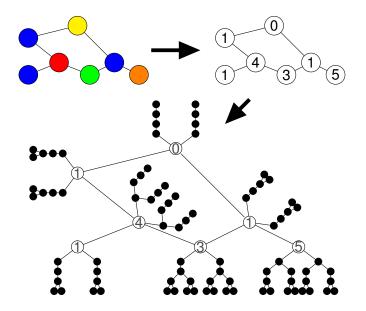
An automorphism is an isomorphism from a graph to itself.

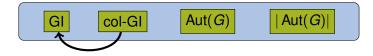


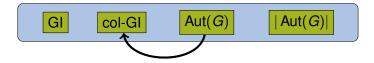
An automorphism is an isomorphism from a graph to itself.

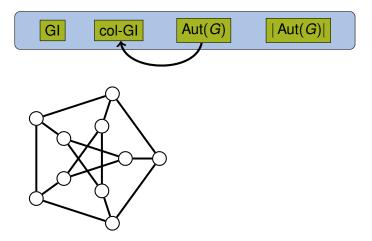


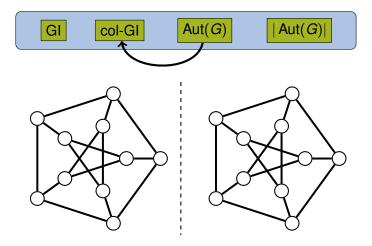


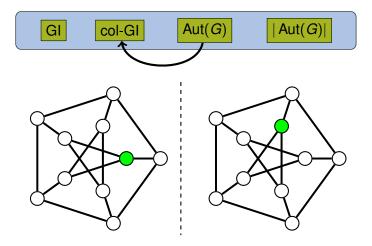


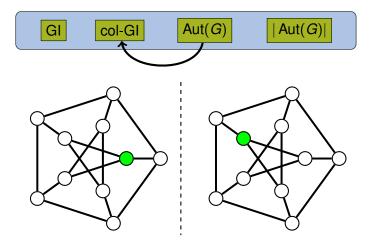






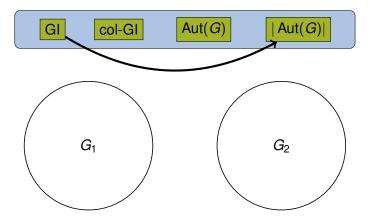


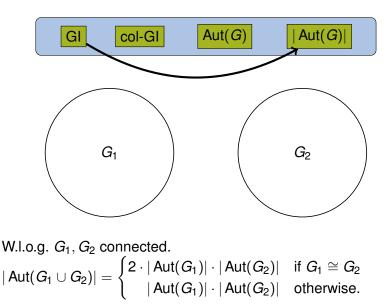


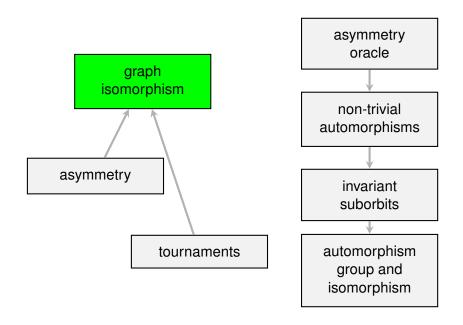


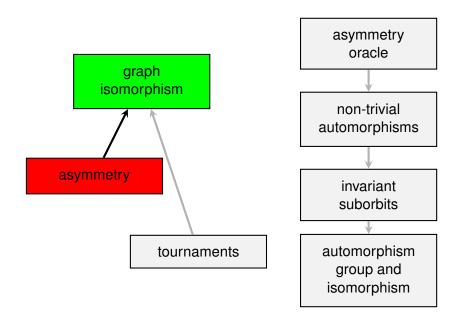












Worst Case instances for IR algorithms

What is the running time of IR algorithms (such as nauty, or traces, bliss, saucy, conauto)?

Worst Case instances for IR algorithms

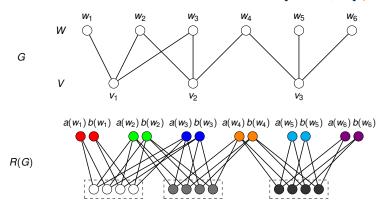
What is the running time of IR algorithms (such as nauty, or traces, bliss, saucy, conauto)?

- In the worst case IR algorithms have exponential running time. [Neuen, S.] (2017+)

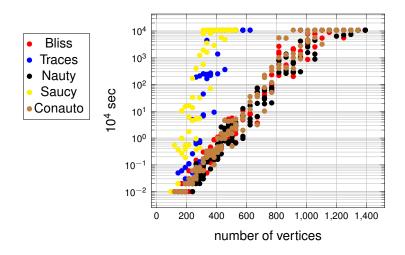
Worst Case instances for IR algorithms

What is the running time of IR algorithms (such as nauty, or traces, bliss, saucy, conauto)?

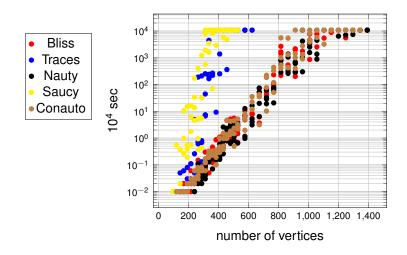
- In the worst case IR algorithms have exponential running time. [Neuen, S.] (2017+)



Benchmark graphs



Benchmark graphs



These benchmarks are asymmetric graphs (rigid).

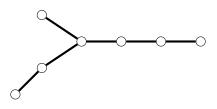
Graph asymmetry

A graph *G* is called asymmetric (or *rigid*) if it does not have a non-trivial automorphism (i.e., |Aut(G)| = 1).

Graph asymmetry

A graph *G* is called asymmetric (or *rigid*) if it does not have a non-trivial automorphism (i.e., |Aut(G)| = 1).

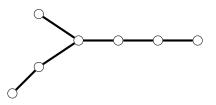
Example:



Graph asymmetry

A graph *G* is called asymmetric (or *rigid*) if it does not have a non-trivial automorphism (i.e., |Aut(G)| = 1).

Example:



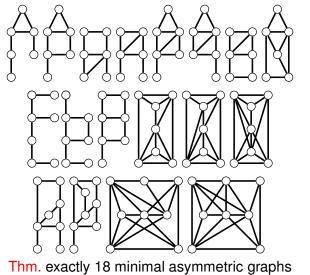
Graph asymmetry denoted GA is the algorithmic task to decide whether a given graph is asymmetric.

(Many authors call this the graph automorphism problem.)

Absence of symmetry



Absence of symmetry



Nešetřil Conjecture

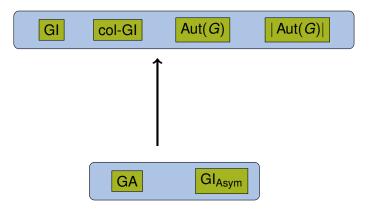
[S., Schweitzer] (2017+)

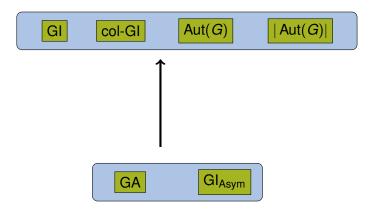
Graph isomorphism and asymmetric graphs





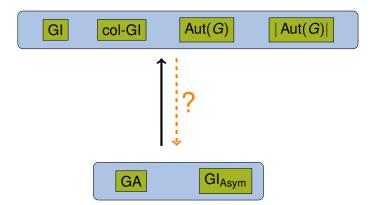






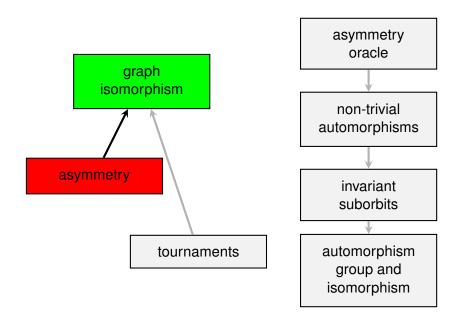
Open question:

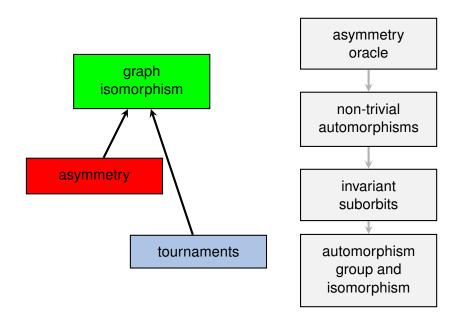
Is it harder to find all symmetries than to detect asymmetry?



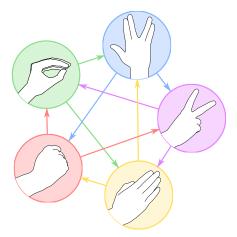
Open question:

Is it harder to find all symmetries than to detect asymmetry?





A tournament is an oriented complete graph. (exactly one directed edge between every pair of vertices) A tournament is an oriented complete graph. (exactly one directed edge between every pair of vertices)



User:Nojhan/Wikimedia Commons/CC-BY-SA-3.0

Graph isomorphism and asymmetric graphs

Symmetry problems for tournaments



- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}

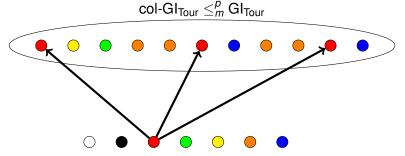


- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}

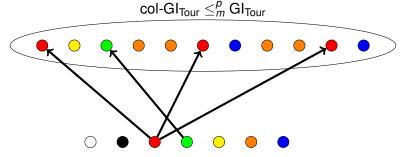




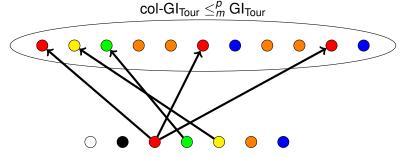
- colored tournament isomorphism \rightarrow tournament isomorphism



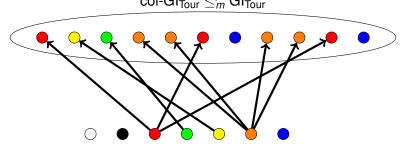
- colored tournament isomorphism \rightarrow tournament isomorphism



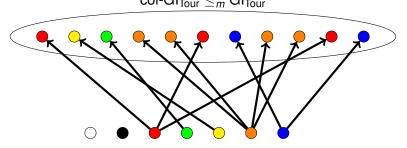
- colored tournament isomorphism \rightarrow tournament isomorphism



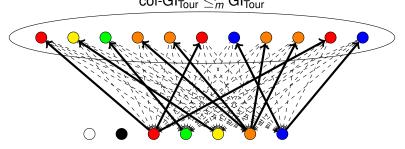
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



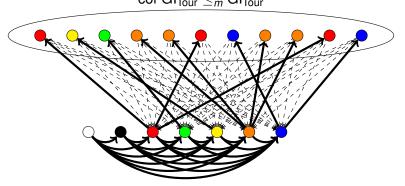
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



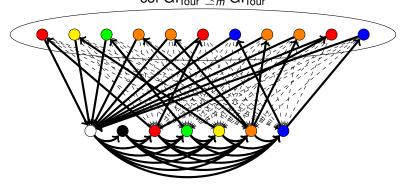
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



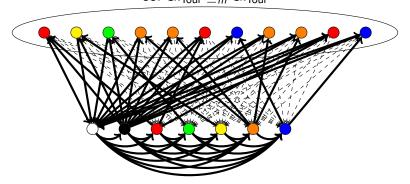
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



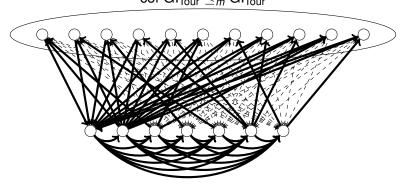
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



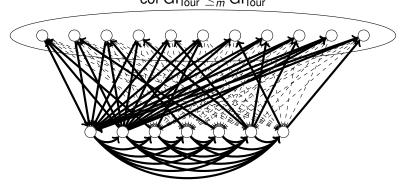
- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



- colored tournament isomorphism \rightsquigarrow tournament isomorphism col-GI_{Tour} \leq_m^p GI_{Tour}



[Arvind, Das, Mukhopadhyay] (2010)

- colored tournament asymmetry \rightsquigarrow tournament asymmetry col-GA_{Tour} \leq_m^p GA_{Tour}

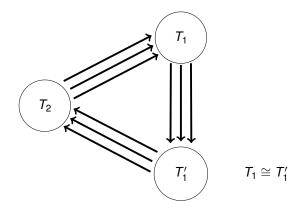


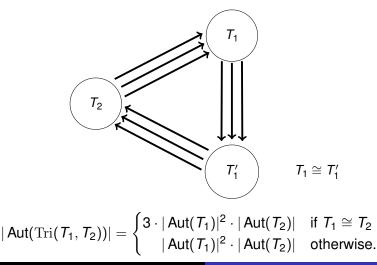








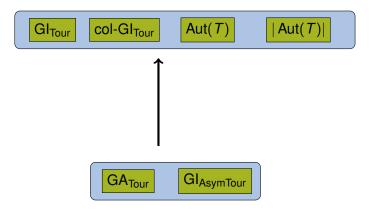


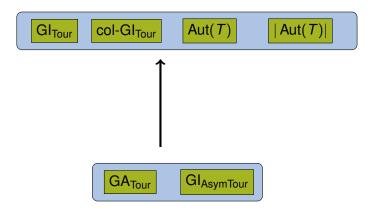








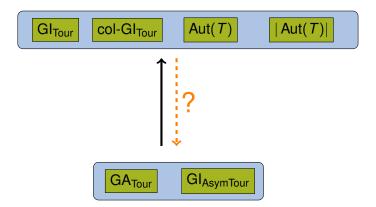




Open question:

Is it harder to find all symmetries than to detect asymmetry?

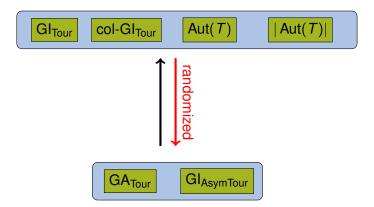
Asymmetry vs isomorphism for tournaments



Open question:

Is it harder to find all symmetries than to detect asymmetry?

Asymmetry vs isomorphism for tournaments



Open question:

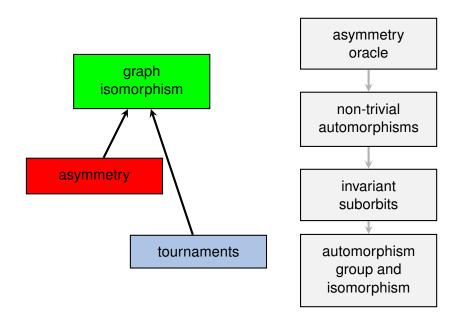
Is it harder to find all symmetries than to detect asymmetry?

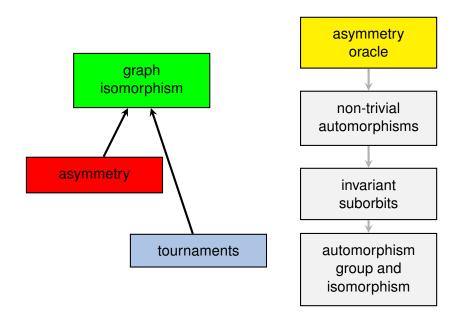
Theorem

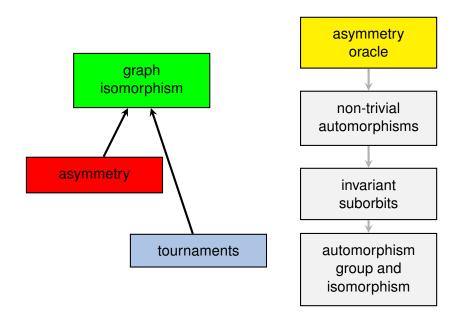
There is a polynomial-time randomized reduction from tournament isomorphism to tournament asymmetry.

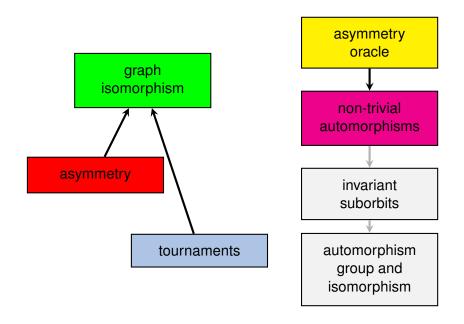
Thus:

For tournaments finding all symmetries and detecting asymmetry are polynomially equivalent.









Technique 1:

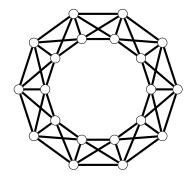
asymmetry test \rightsquigarrow non-trivial automorphism sampler

Technique 1:

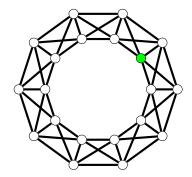
asymmetry test \rightsquigarrow non-trivial automorphism sampler

Strategy

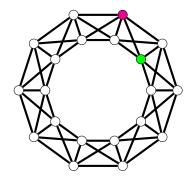
- fix more and more vertices until graph is asymmetric
- make a copy of the graph
- undo last fixing in copy
- find alternative vertex to the vertex fixed last
- find isomorphism from original to copy



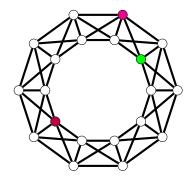




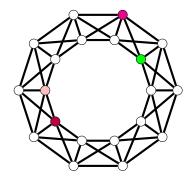




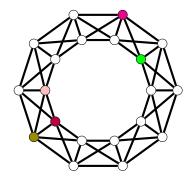




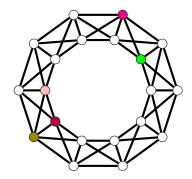




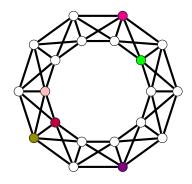




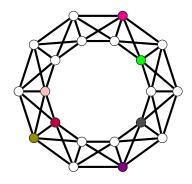




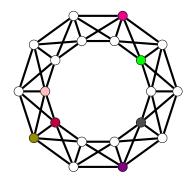




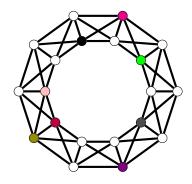




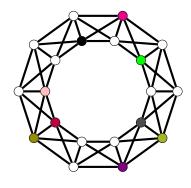


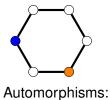


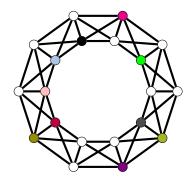




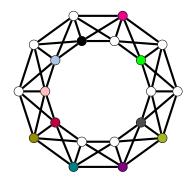


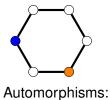


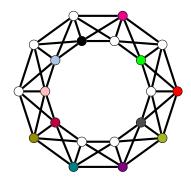




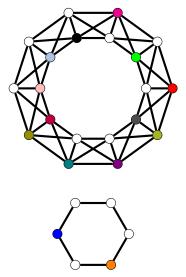


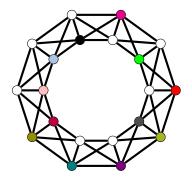




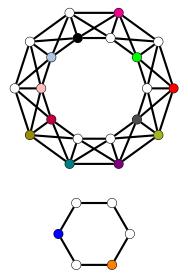


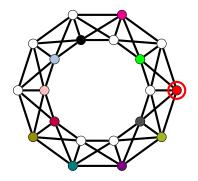




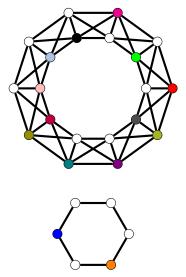


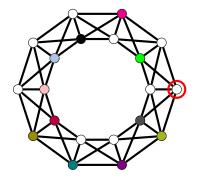




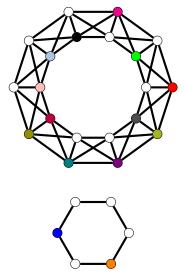


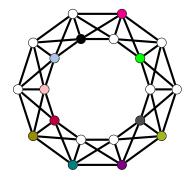




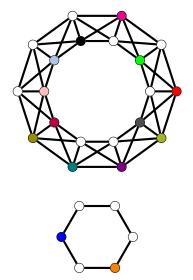


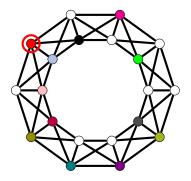




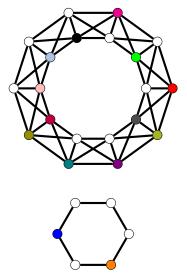


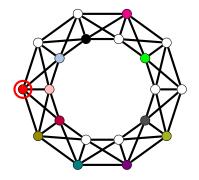




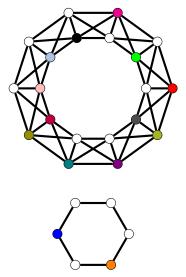


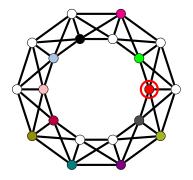




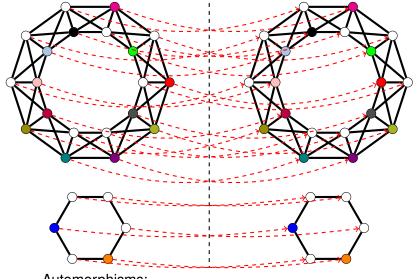


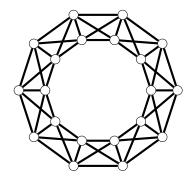






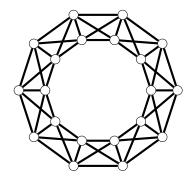






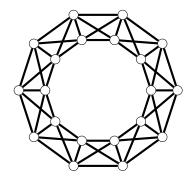


Automorphisms: φ_1



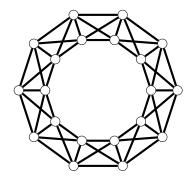


Automorphisms: φ_1





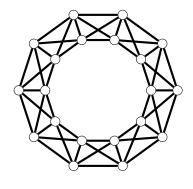
Automorphisms: φ_1, φ_2





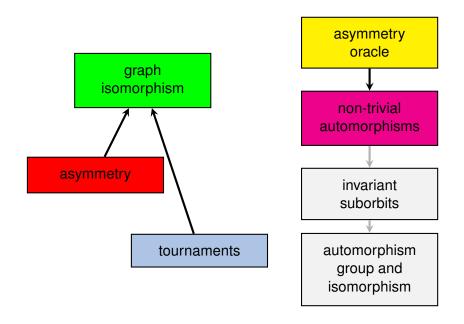
Automorphisms: φ_1 , φ_2 , φ_3

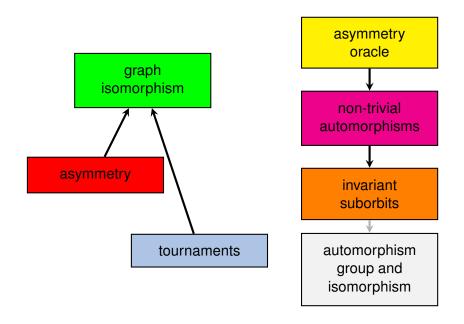
How to get automorphisms — Illustration





Automorphisms: $\varphi_1, \varphi_2, \varphi_3, \ldots$





A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$.

A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$. Only invariant sets of automorphisms are useful.

A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$. Only invariant sets of automorphisms are useful. Technique 2: sampling invariant subsets

A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$. Only invariant sets of automorphisms are useful. Technique 2: sampling invariant subsets There is a technique to extract invariant subsets with high probability. (Sample often and apply Chernoff bounds.)

A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$. Only invariant sets of automorphisms are useful.

Technique 2: sampling invariant subsets There is a technique to extract invariant subsets with high probability. (Sample often and apply Chernoff bounds.)

But: The number of samples required is polynomial in |Aut(G)|, which may be exponential in |G|.

A set of automorphisms $M' \subseteq \operatorname{Aut}(G)$ is invariant if $M'^{\varphi} = M'$ for all $\varphi \in \operatorname{Aut}(G)$. Only invariant sets of automorphisms are useful.

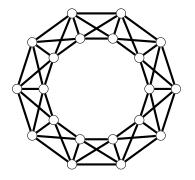
Technique 2: sampling invariant subsets There is a technique to extract invariant subsets with high probability. (Sample often and apply Chernoff bounds.)

But: The number of samples required is polynomial in |Aut(G)|, which may be exponential in |G|.

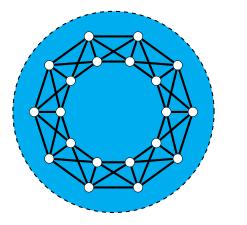
However, we can sample pairs of vertices lying in a common orbit. There are less than n^2 such pairs.

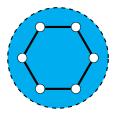
We call a partition $\pi = \{C_1, ..., C_t\}$ of the vertices a partition into invariant suborbits if

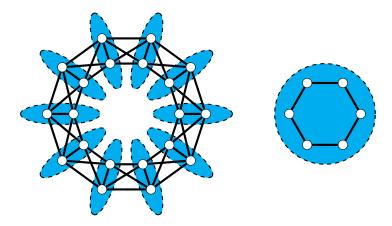
- every C_i is contained in an orbit
- π is invariant under Aut(G) (i.e., $\pi^{\varphi} = \pi$ for all $\varphi \in Aut(G)$)

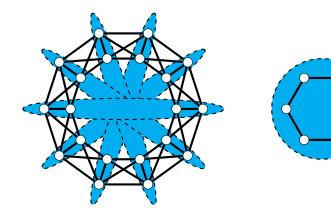


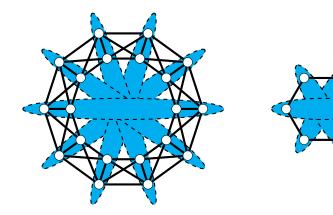


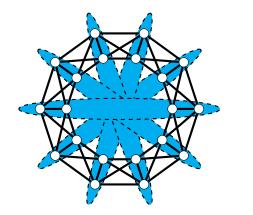


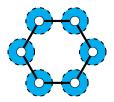


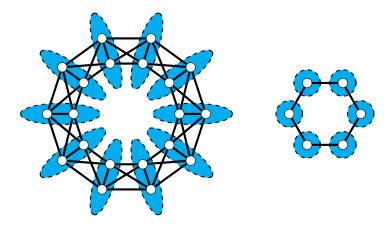












Lemma

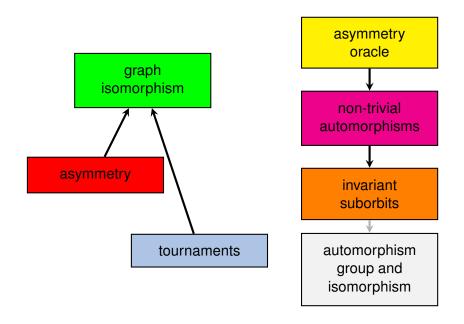
Given an invariant sampler we can compute in polynomial time invariant suborbits (with high probability).

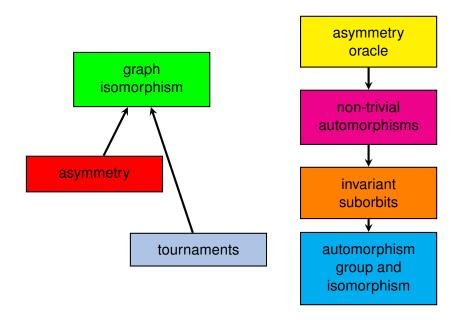
Proof technique:

- repeatedly sample $\varphi \in Aut(G)$ and randomly pick pair

 $(x,\varphi(x))$ with $x \in V(G)$

- extract characteristic set of pairs
- compute the transitive closure of the relation induced by pairs





Theorem (Luks (1982))

For a solvable permutation group Γ on V and a graph G on vertex set V we can compute $\Gamma \cap Aut(G)$ in polynomial time.

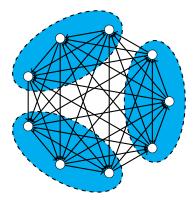
Facts:

- Tournaments have solvable automorphism group.
- Wreath products of solvable groups are solvable.

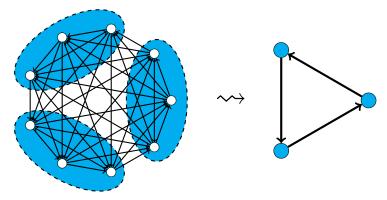
T: a tournament; $\pi = \{C_1, \ldots, C_t\}$: a partition of the vertices

T: a tournament; $\pi = \{C_1, ..., C_t\}$: a partition of the vertices The quotient tournament T/π has the vertex set $\{C_1, ..., C_t\}$. The direction of the edge between C_i and C_k is the **majority direction** between C_i and C_k in *T*.

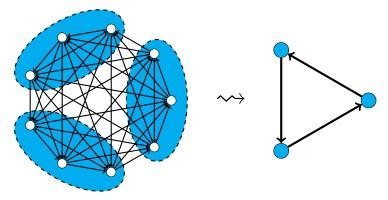
T: a tournament; $\pi = \{C_1, ..., C_t\}$: a partition of the vertices The quotient tournament T/π has the vertex set $\{C_1, ..., C_t\}$. The direction of the edge between C_i and C_k is the **majority direction** between C_i and C_k in *T*.



T: a tournament; $\pi = \{C_1, ..., C_t\}$: a partition of the vertices The quotient tournament T/π has the vertex set $\{C_1, ..., C_t\}$. The direction of the edge between C_i and C_k is the **majority direction** between C_i and C_k in *T*.



T: a tournament; $\pi = \{C_1, ..., C_t\}$: a partition of the vertices The quotient tournament T/π has the vertex set $\{C_1, ..., C_t\}$. The direction of the edge between C_i and C_k is the **majority direction** between C_i and C_k in *T*.



Note: if all C_i have odd size this operation is well defined.

Technique 3: invariant suborbits \rightsquigarrow automorphism group Input: A tournament T; invariant suborbit oracle Technique 3: invariant suborbits \rightsquigarrow automorphism group **Input:** A tournament *T*; invariant suborbit oracle • compute a partition $\pi = \{C_1, \dots, C_t\}$ into invariant suborbits For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic. Technique 3: invariant suborbits \rightsquigarrow automorphism group **Input:** A tournament *T*; invariant suborbit oracle • compute a partition $\pi = \{C_1, \dots, C_t\}$ into invariant suborbits For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π

(quotient tournament)

Input: A tournament T; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π

(quotient tournament)

• compute $\Delta := \operatorname{Aut}(T/\pi)$

Input: A tournament T; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π

(quotient tournament)

- compute $\Delta := \operatorname{Aut}(T/\pi)$
- compute $\Theta := \operatorname{Aut}(T[C_1])$

Input: A tournament T; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π

• compute $\Delta := \operatorname{Aut}(T/\pi)$

- compute $\Theta := \operatorname{Aut}(T[C_1])$
- compute $\Gamma := \Theta \wr \Delta$

(quotient tournament)

(wreath product)

Input: A tournament T; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π

• compute $\Delta := \operatorname{Aut}(T/\pi)$

- compute $\Theta := \operatorname{Aut}(T[C_1])$
- compute $\Gamma := \Theta \wr \Delta$
- compute $\Gamma \cap \operatorname{Aut}(T)$

(quotient tournament)

(wreath product)

Input: A tournament *T*; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π (quotient tournament) • compute $\Delta := \operatorname{Aut}(T/\pi)$ • compute $\Theta := \operatorname{Aut}(T[C_1])$ • compute $\Gamma := \Theta \wr \Delta$ • compute $\Gamma \cap \operatorname{Aut}(T)$

Output: Aut(T) = $\Gamma \cap$ Aut(T)

(wreath product)

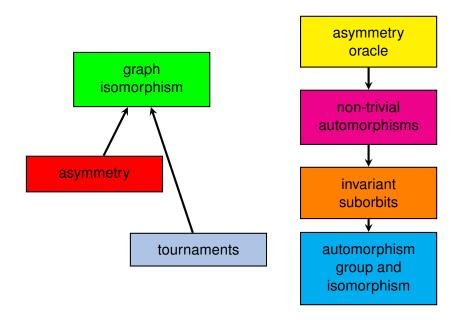
Input: A tournament T; invariant suborbit oracle

• compute a partition $\pi = \{C_1, \ldots, C_t\}$ into invariant suborbits

For simplicity assume all induced subtournaments $T[C_i]$ are isomorphic.

• compute T/π (quotient tournament) • compute $\Delta := \operatorname{Aut}(T/\pi)$ • compute $\Theta := \operatorname{Aut}(T[C_1])$ • compute $\Gamma := \Theta \wr \Delta$ (wreath product) • compute $\Gamma \cap \operatorname{Aut}(T)$ Output: $\operatorname{Aut}(T) = \Gamma \cap \operatorname{Aut}(T)$

A more careful case distinction and some running time analysis show that the overall process runs in polynomial time.



Theorem

There is a polynomial-time randomized reduction from tournament isomorphism to tournament asymmetry.

Theorem

There is a polynomial-time randomized reduction from tournament isomorphism to tournament asymmetry.

Open: How about for graphs? How about for groups?

Theorem

There is a polynomial-time randomized reduction from tournament isomorphism to tournament asymmetry.

Open: How about for graphs? How about for groups?

Related results:

Canonization: With [Arvind, Das, Mukhopadhyay] (2010) we get an analogous result for canonization.

Hardness: tournament asymmetry is hard for NL, C₌L, PL, DET, and MOD_kL under AC⁰ reductions. [Wager] (2007)

Cumulative Prize Money

Prize for a proof that $GI \in P$ or $GI \notin P$!



Prize for a proof that $GI \in P$ or $GI \notin P!$



Prize for a proof that $GI \in P$ or $GI \notin P$!

