Complexity of the group isomorphism problem

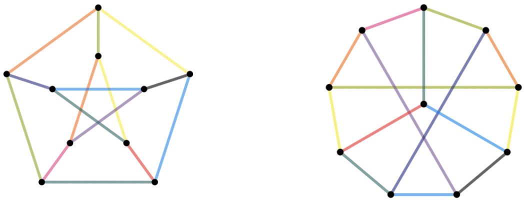
Jaroslav Hančl*, Matěj Konečný*, Jana Novotná*, Jakub Pekárek*, *Radim Předstíraný* †, Václav Rozhoň*, Jakub Svoboda*, Štěpán Šimsa*,
Advisor: Periklis Papakonstantinou♡

*Charles University, †2017, ♡Rutgers University

12. 7. 2017

Graph isomorphism

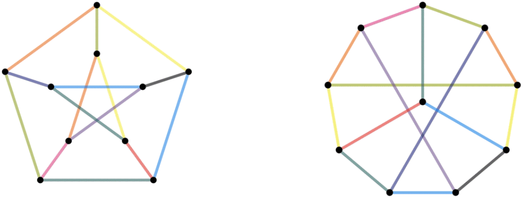
- Given two graphs decide whether their structure is the same.



Source: `https://www.quantamagazine.org/20151214-graph-isomorphism-algorithm/`

Graph isomorphism

- Given two graphs decide whether their structure is the same.



Source: `https://www.quantamagazine.org/20151214-graph-isomorphism-algorithm/`

- Graph isomorphism is in NP.
- But is believed to be easier, maybe even in P.

Theorem (Graph isomorphism is easy).

If graph isomorphism is NP-complete, something weird happens.

Graph isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP.
- Graph nonisomorphism is in IP.
- Graph nonisomorphism is in AM.
- If graph isomorphism is NP-complete, something weird happens.

Graph isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP.
- Graph nonisomorphism is in AM.
- If graph isomorphism is NP-complete, something weird happens.

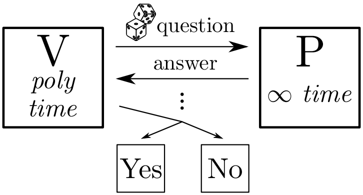
Graph isomorphism

Graph isomorphism is easy

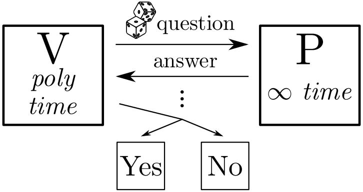
- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP.
- Graph nonisomorphism is in AM.
- If graph isomorphism is NP-complete, something weird happens.

IP protocol

- Protocol between the verifier (us, polynomial time bound) and the prover (computationally unbounded).
- We send a question to the prover (with use of randomness), he sends us an answer, this repeats several times.
- The prover is proving that the two graphs or not isomorphic (even if in fact they are isomorphic).
- We want to output the correct answer with high probability.



Graph isomorphism



Graph nonisomorphism is in IP

- We select a random graph out of the two and a random permutation of vertices.
- We send the permuted graph to the prover.
- Prover says what graph we picked in the beginning.
- If graphs were isomorphic, with $p = \frac{1}{2}$ we will know that.
- Repeat protocol to amplify probability.

Graph isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM.
- If graph isomorphism is NP-complete, something weird happens.

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens.

Graph nonisomorphism is in AM

- AM is like IP but the prover knows our randomness.
- The proof is more complicated but based on the proof for the IP protocol.

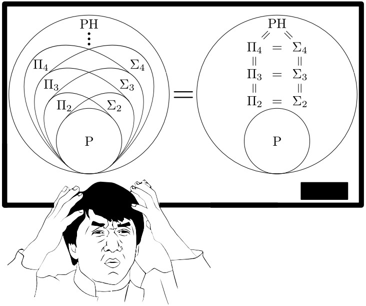
Graph isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens.

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓



Theorem (Graph isomorphism is easy).

If graph isomorphism is NP-complete, something weird happens.

Conjecture (Group isomorphism is easy).

If group isomorphism is NSC_2-complete, something weird happens.

- NSC_2 is the same as NP but the space is restricted to only $\mathcal{O}(\log^2 n)$.

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2.
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$.
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$.
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$.
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$.
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism vs Group isomorphism

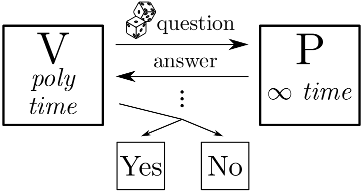
Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$.
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$.
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism



Graph nonisomorphism is in IP

- We select a random graph out of the two and a random permutation of vertices.
- We send the permuted graph to the prover.
- Prover says what graph we picked in the beginning.
- If graphs were isomorphic, with $p = \frac{1}{2}$ we will know that.
- Repeat protocol to amplify probability.

Graph isomorphism vs Group isomorphism

- For storing a random permutation we need asymptotically $n \log(n)$ space.
- So, instead we sample randomly a set of size $100 \cdot \log(n)$ that fits in our $\mathcal{O}(\log^2(n))$ space.
- For groups, this set is (with probability at least 99%) "generating", i.e. any element of the group can be represented using only elements from this set.
- We need a deterministic process that creates a permutation of vertices based on this selected set. It must not depend on the way the groups are given to us on the input.

Graph isomorphism vs Group isomorphism

- For storing a random permutation we need asymptotically $n \log(n)$ space.
- So, instead we sample randomly a set of size $100 \cdot \log(n)$ that fits in our $\mathcal{O}(\log^2(n))$ space.
- For groups, this set is (with probability at least 99%) "generating", i.e. any element of the group can be represented using only elements from this set.
- We need a deterministic process that creates a permutation of vertices based on this selected set. It must not depend on the way the groups are given to us on the input.

Q: What is the complexity of our algorithm?

Graph isomorphism vs Group isomorphism

- For storing a random permutation we need asymptotically $n\log(n)$ space.
- So, instead we sample randomly a set of size $100 \cdot \log(n)$ that fits in our $\mathcal{O}(\log^2(n))$ space.
- For groups, this set is (with probability at least 99%) "generating", i.e. any element of the group can be represented using only elements from this set.
- We need a deterministic process that creates a permutation of vertices based on this selected set. It must not depend on the way the groups are given to us on the input.

Q: What is the complexity of our algorithm?
A: $\approx n^{10}$

Graph isomorphism vs Group isomorphism

- For storing a random permutation we need asymptotically $n\log(n)$ space.
- So, instead we sample randomly a set of size $100 \cdot \log(n)$ that fits in our $\mathcal{O}(\log^2(n))$ space.
- For groups, this set is (with probability at least 99%) "generating", i.e. any element of the group can be represented using only elements from this set.
- We need a deterministic process that creates a permutation of vertices based on this selected set. It must not depend on the way the groups are given to us on the input.

Q: What is the complexity of our algorithm?
A: $\approx n^{10} \cdot n^{1,000,000,000}$

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$. ✓
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$.
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$. ✓
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$.
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$. ✓
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$. ✓
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$. ✓
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$. ✓
- If group isomorphism is NSC_2-complete, something weird happens.

Graph isomorphism vs Group isomorphism

Graph isomorphism is easy

- Graph isomorphism is in NP. ✓
- Graph nonisomorphism is in IP. ✓
- Graph nonisomorphism is in AM. ✓
- If graph isomorphism is NP-complete, something weird happens. ✓

Group isomorphism is easy

- Group isomorphism is in NSC_2. ✓
- Group nonisomorphism is in $\mathrm{IP}_{\mathrm{SC}_2}$. ✓
- Group nonisomorphism is in $\mathrm{AM}_{\mathrm{SC}_2}$. ✓
- If group isomorphism is NSC_2-complete, something weird happens. **?**

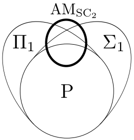
Why the last step does not work

Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

Why the last step does not work

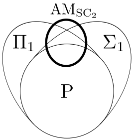
Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

What we hoped it looks like...

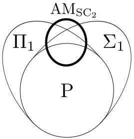


Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

What we hoped it looks like...

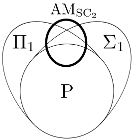


What Periklis thought
it looks like...

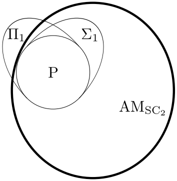


Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

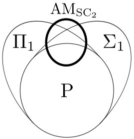
What we hoped it looks like...



What Eric thought it looks like...



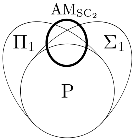
What Periklis thought it looks like...



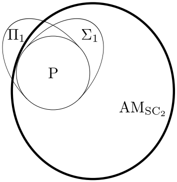
Why the last step does not work

Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

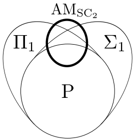
What we hoped it looks like...



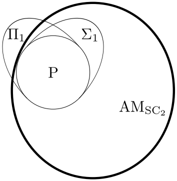
What Eric thought it looks like...



What Periklis thought it looks like...



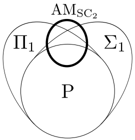
What it actually looks like...



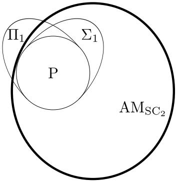
Why the last step does not work

Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

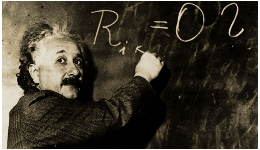
What we hoped it looks like...



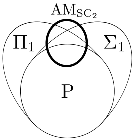
What Eric thought it looks like...



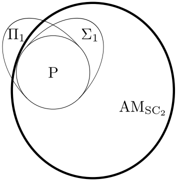
What our moms think our research looks like...



What Periklis thought it looks like...



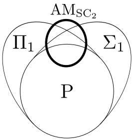
What it actually looks like...



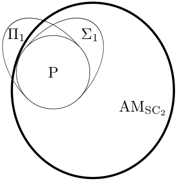
Why the last step does not work

Where is $\mathrm{AM}_{\mathrm{SC}_2}$ in the polynomial hierarchy?

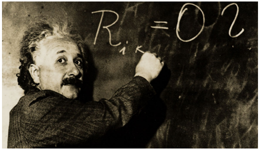
What we hoped it looks like...



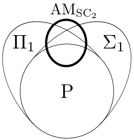
What Eric thought it looks like...



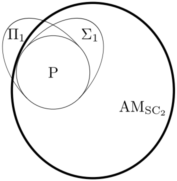
What our moms think our research looks like...



What Periklis thought it looks like...



What it actually looks like...



What it actually looks like...