Some Open Problems in Computational Group Theory

Bireswar Das

IIT Gandhinagar

Pre-Conference School, CALDAM 2023

7 Feb, 2023

Groups

Definition

A non-empty set G is said to form a group under a binary operation $. : G \times G \longrightarrow G$ if

- for all $a, b, c \in G$, $(a.b).c = a.(b.c)$ (associativity).

Groups

Definition

A non-empty set G is said to form a group under a binary operation $. : G \times G \longrightarrow G$ if

- for all $a, b, c \in G$, $(a.b).c = a.(b.c)$ (associativity).
- there exists an element $e \in G$ such that for all $a \in G$, $e.a = a.e = a$ (e is called the identity).

Groups

Definition

A non-empty set G is said to form a group under a binary operation $. : G \times G \longrightarrow G$ if

- for all $a, b, c \in G$, $(a.b).c = a.(b.c)$ (associativity).
- there exists an element $e \in G$ such that for all $a \in G$, $e.a = a.e = a$ (e is called the identity).
- for all $a \in G$ there exists $b \in G$ such that $a.b = b.a = e$. (b is called the inverse of a).

Cayley Table of a Group

*	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	2	1	3	4
6	6	5	7	8	1	2	4	3
7	7	8	5	6	4	3	2	1
8	8	7	6	5	3	4	1	2

Problems

- The Group Isomorphism Problem (GrIso)

Problems

- The Group Isomorphism Problem (GrIso)
- Some problems from permutation group theory

Problems

- The Group Isomorphism Problem (GrIso)
- Some problems from permutation group theory
- Minimum Generating Set Problem (MIN-GEN)

Problems

- The Group Isomorphism Problem (GrIso)
- Some problems from permutation group theory
- Minimum Generating Set Problem (MIN-GEN)
- Group Factorization Problem (GrFact)

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.
- Let $S \subseteq G$. The intersection of all subgroups containing S is the *subgroup generated by* S, denoted $\langle S \rangle$.

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.
- Let $S \subseteq G$. The intersection of all subgroups containing S is the *subgroup generated by* S, denoted $\langle S \rangle$.
- Computing $\langle S \rangle$ in polytime.

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.
- Let $S \subseteq G$. The intersection of all subgroups containing S is the *subgroup generated by* S, denoted $\langle S \rangle$.
- Computing $\langle S \rangle$ in polytime.
- H is generated by $S \subseteq G$ if $H = \langle S \rangle$. (Analogous to spanning sets).

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.
- Let $S \subseteq G$. The intersection of all subgroups containing S is the *subgroup generated by* S, denoted $\langle S \rangle$.
- Computing $\langle S \rangle$ in polytime.
- H is generated by $S \subseteq G$ if $H = \langle S \rangle$. (Analogous to spanning sets).
- Cosets $Hg = \{hg | g \in G\}$.

Preliminary

- A subset H of a group G is called a subgroup if H is a group under the inherited binary operation. Notation $H \leq G$.
- Intersection of two groups is a group.
- Let $S \subseteq G$. The intersection of all subgroups containing S is the *subgroup generated by* S, denoted $\langle S \rangle$.
- Computing $\langle S \rangle$ in polytime.
- H is generated by $S \subseteq G$ if $H = \langle S \rangle$. (Analogous to spanning sets).
- Cosets $Hg = \{hg | g \in G\}$.
- Lagrange Theorem: $G = H \uplus Hg_1 \uplus Hg_2 \uplus \ldots \uplus Hg_k$.

A Lemma

Lemma

Every group G with n elements has a generating set of size $\log n$.

A Lemma

Lemma

Every group G with n elements has a generating set of size $\log n$.

Such set can be computed very efficiently.

Homomorphism and Isomorphism

- A map $\phi : G_1 \longrightarrow G_2$ is called a *homomorphism* is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$.

Homomorphism and Isomorphism

- A map $\phi : G_1 \longrightarrow G_2$ is called a *homomorphism* is $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$.
- A bijective homomorphism is called an isomorphism.

The Group Isomorphism Problem

GrIso

Input: Two groups G_1 and G_2 given by their Cayley table.
Decide: If G_1 and G_2 are isomorphic.

- In NP.

The Group Isomorphism Problem

GrIso

Input: Two groups G_1 and G_2 given by their Cayley table.
Decide: If G_1 and G_2 are isomorphic.

- In NP.
- Very unlikely to be NP-complete.

The Group Isomorphism Problem

GrIso

Input: Two groups G_1 and G_2 given by their Cayley table.
Decide: If G_1 and G_2 are isomorphic.

- In NP.
- Very unlikely to be NP-complete.
- Open: Is it in P?

Tarjan's Algorithm

Input: Two groups G_1 and $_2$

1. Find a generating set S of size $\log n$ in G_1.

Tarjan's Algorithm

Input: Two groups G_1 and $_2$

1. Find a generating set S of size $\log n$ in G_1.
2. Try all possible mappings of S to G_2.

Tarjan's Algorithm

Input: Two groups G_1 and $_2$

1. Find a generating set S of size $\log n$ in G_1.
2. Try all possible mappings of S to G_2.
3. Do sanity check.

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n+O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n+O(1)}$ for some $\alpha < 1$? Good hunting."

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n + O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n + O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n + \log n / \log\log n}$ [Rosenbaum'13].

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n + O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n + O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n + \log n / \log\log n}$ [Rosenbaum'13].
- For solvable groups $n^{1/4 \log_p n + \log n / \log\log n}$. [Rosenbaum'13]

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n+O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n+O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n+\log n/\log\log n}$ [Rosenbaum'13].
- For solvable groups $n^{1/4\log_p n+\log n/\log\log n}$. [Rosenbaum'13]
- $n^{(1/4)\log_p n+\log n/\log\log n}$ [Rosenbaum'13, Arxiv].

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n + O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n + O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n + \log n / \log\log n}$ [Rosenbaum'13].
- For solvable groups $n^{1/4 \log_p n + \log n / \log\log n}$. [Rosenbaum'13]
- $n^{(1/4)\log_p n + \log n / \log\log n}$ [Rosenbaum'13, Arxiv].
- Open: Is GrIso in co-NP?

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n+O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n+O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n+\log n/\log\log n}$ [Rosenbaum'13].
- For solvable groups $n^{1/4\log_p n+\log n/\log\log n}$. [Rosenbaum'13]
- $n^{(1/4)\log_p n+\log n/\log\log n}$ [Rosenbaum'13, Arxiv].
- Open: Is GrIso in co-NP?
- It is "almost" in co-NP for solvable groups [Arvind-Torán'11]

GrIso: Known and Open

- R. J. Lipton: " Please solve the GrIso problem. Or at least break below the $n^{\log n + O(1)}$ time, which is the best known now for decades. Can you prove $n^{\alpha \log n + O(1)}$ for some $\alpha < 1$? Good hunting."
- $n^{(1/2)\log_p n + \log n / \log\log n}$ [Rosenbaum'13].
- For solvable groups $n^{1/4 \log_p n + \log n / \log\log n}$. [Rosenbaum'13]
- $n^{(1/4)\log_p n + \log n / \log\log n}$ [Rosenbaum'13, Arxiv].
- Open: Is GrIso in co-NP?
- It is "almost" in co-NP for solvable groups [Arvind-Torán'11]
- Problem: Does the result of Arvind and Torán hold for groups all of whose non-abelian composition factors are bounded?

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.
- GrIso for Abelian Groups in linear time [T. Kavitha'07]

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.
- GrIso for Abelian Groups in linear time [T. Kavitha'07]
- Hamiltonian groups (linear), and some generalization of Abelian groups in nearly linear time. [D-Sharma'19]

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.
- GrIso for Abelian Groups in linear time [T. Kavitha'07]
- Hamiltonian groups (linear), and some generalization of Abelian groups in nearly linear time. [D-Sharma'19]
- Can Kavitha's result be generalized even further?

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.
- GrIso for Abelian Groups in linear time [T. Kavitha'07]
- Hamiltonian groups (linear), and some generalization of Abelian groups in nearly linear time. [D-Sharma'19]
- Can Kavitha's result be generalized even further?
- Nearly linear for most all order. [Dietrich-Wilson'21]

GrIso: Restricted Classes of Groups

- GrIso for Abelian Groups in P.
- GrIso for Abelian Groups in linear time [T. Kavitha'07]
- Hamiltonian groups (linear), and some generalization of Abelian groups in nearly linear time. [D-Sharma'19]
- Can Kavitha's result be generalized even further?
- Nearly linear for most all order. [Dietrich-Wilson'21]
- Open: GrIso for nilpotent groups of class 2?

Group Representations

- Cayley table representations.

Group Representations

- Cayley table representations.
- Permutation representations.

Group Representations

- Cayley table representations.
- Permutation representations.
- Generator-relator representations.

Group Representations

- Cayley table representations.
- Permutation representations.
- Generator-relator representations.
- Depending on what representation is used a computational problem can become easy or extremely challenging.

Permutation Group Representation

- Computer algebra systems (GAP, MAGMA,..) use this.

Permutation Group Representation

- Computer algebra systems (GAP, MAGMA,..) use this.
- Connection to group isomorphism.

Permutation Group Representation

- Computer algebra systems (GAP, MAGMA,..) use this.
- Connection to group isomorphism.
- Cayley's Theorem: Every group is a subgroup of $Sym(\Omega)$ for some Ω.

Permutation Group Representation

- Computer algebra systems (GAP, MAGMA,..) use this.
- Connection to group isomorphism.
- Cayley's Theorem: Every group is a subgroup of $Sym(\Omega)$ for some Ω.
- $G \leq S_n$

Generators

(Groups can be given by generators. Action representation on elements and sets.)

Polynomial Time Algorithms

The following problems have polynomial time algorithms:
Membership,
Testing normality,
Solvability,
Nilpotency,
Intersection with normal subgroups,
Finding core,
Socle etc.

Set Transporter Problem

STRANS

Input: A group $G \leq S_n$ and $\Delta_1, \Delta_2 \subseteq [n]$.
Decide: Does there exists $\sigma \in G$ such that $\Delta_1^\sigma = \Delta_2$?

Set Transporter and Graph Isomorphism

Book keeping through groups

(all isomorphism from a graph to another, small to big)

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.
- These problems are in NP$\cap$ co-AM.

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.
- These problems are in NP$\cap$ co-AM.
- They have statistical zero knowledge proofs [Arvind-D]

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.
- These problems are in NP$\cap$ co-AM.
- They have statistical zero knowledge proofs [Arvind-D]
- Babai gave a quasipolynomial time algorithm for Coset Intersection.

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.
- These problems are in NP$\cap$ co-AM.
- They have statistical zero knowledge proofs [Arvind-D]
- Babai gave a quasipolynomial time algorithm for Coset Intersection.
- Open: P? In coNP?

Some Other Problems

- Coset intersection, Set Stabilizer, Double coset equality, Conjugacy,..
- These problems are polytime (Turing) equivalent.
- These problems are in NP$\cap$ co-AM.
- They have statistical zero knowledge proofs [Arvind-D]
- Babai gave a quasipolynomial time algorithm for Coset Intersection.
- Open: P? In coNP?
- What happens when we restrict the group classes?

The Minimum Generating Set Problem

MIN-GEN

Input: A group G and an integer k.
Decide: If G has a generating set of size at most k.

- It is in NP.

The Minimum Generating Set Problem

MIN-GEN

Input: A group G and an integer k.
Decide: If G has a generating set of size at most k.

- It is in NP.
- It has an $n^{\log n}$ algorithm.

Examples

(Simple groups, product of groups, product of simple groups)

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]
- Recently we obtained the following results (joint work with Dhara Thakkar):

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]
- Recently we obtained the following results (joint work with Dhara Thakkar):
  1. Solvable groups (both Cayley table and permutation representation).

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]
- Recently we obtained the following results (joint work with Dhara Thakkar):
  1. Solvable groups (both Cayley table and permutation representation).
  2. $n^{1/4 log_p n + O(1)}$ for general groups.

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]
- Recently we obtained the following results (joint work with Dhara Thakkar):
  1. Solvable groups (both Cayley table and permutation representation).
  2. $n^{1/4 log_p n + O(1)}$ for general groups.
  3. Product of simple groups (Cayley table)

Known Results

- It is in P for nilpotent groups (Cayley table) [Arvind-Torán'06]
- Recently we obtained the following results (joint work with Dhara Thakkar):
  1. Solvable groups (both Cayley table and permutation representation).
  2. $n^{1/4 log_p n + O(1)}$ for general groups.
  3. Product of simple groups (Cayley table)
  4. Some of Menegazzo's questions on permutation group: Primitive groups (quasipolynomial time)

MIN-GEN: Not yet known

- Product of groups from two easily manageable classes.

MIN-GEN: Not yet known

- Product of groups from two easily manageable classes.
- In co-AM?

MIN-GEN: Not yet known

- Product of groups from two easily manageable classes.
- In co-AM?
- Quasipolymonila time algorithm for permutation group.

MIN-GEN: Not yet known

- Product of groups from two easily manageable classes.
- In co-AM?
- Quasipolymonila time algorithm for permutation group.
- Product of simple groups (permutation representation).

Group Factorization

PGF

Input: A group G, a subset S of G, $x \in G$, and a budget k.
Decide: Can x be written as the product of a sequence of length at most k with elements from S?

- Is in NP-hard [Even-Goldreich81]

Group Factorization

PGF

Input: A group G, a subset S of G, $x \in G$, and a budget k.
Decide: Can x be written as the product of a sequence of length at most k with elements from S?

- Is in NP-hard [Even-Goldreich81]
- NP complete if the budget is given in unary and PSPACE complete if k is in binary [Jerrum85].

Group Factorization

PGF

Input: A group G, a subset S of G, $x \in G$, and a budget k.
Decide: Can x be written as the product of a sequence of length at most k with elements from S?

- Is in NP-hard [Even-Goldreich81]
- NP complete if the budget is given in unary and PSPACE complete if k is in binary [Jerrum85].
- W[1]-hard [Cai et al.'97], in W[P] (Cai et al. '97).

Group Factorization

PGF

Input: A group G, a subset S of G, $x \in G$, and a budget k.
Decide: Can x be written as the product of a sequence of length at most k with elements from S?

- Is in NP-hard [Even-Goldreich81]
- NP complete if the budget is given in unary and PSPACE complete if k is in binary [Jerrum85].
- W[1]-hard [Cai et al.'97], in W[P] (Cai et al. '97).
- What is the exact parameterized complexity of this problem?

Group Factorization

PGF

Input: A group G, a subset S of G, $x \in G$, and a budget k.
Decide: Can x be written as the product of a sequence of length at most k with elements from S?

- Is in NP-hard [Even-Goldreich81]
- NP complete if the budget is given in unary and PSPACE complete if k is in binary [Jerrum85].
- W[1]-hard [Cai et al.'97], in W[P] (Cai et al. '97).
- What is the exact parameterized complexity of this problem?
-

Thank You!