Faster isomorphism testing of p-groups of Frattini class-2

Speaker: Chuanqi Zhang

Joint work with Gábor Ivanyos, Euan Mendoza, Youming Qiao, and Xiaorui Sun

Centre for Quantum Software and Information
University of Technology Sydney

UTS Groups Analysis Geometry Seminar, April 2024

Outline

- Background of finite group isomorphism.
- Relationship between p-group isomorphism and 3-tensor isomorphism.
- Our main results and an overview of our algorithm.
- Summary and open problems.

Outline

- Background of finite group isomorphism.
- Relationship between p-group isomorphism and 3-tensor isomorphism.
- Our main results and an overview of our algorithm.
- Summary and open problems.

Outline

- Background of finite group isomorphism.
- Relationship between p-group isomorphism and 3-tensor isomorphism.
- Our main results and an overview of our algorithm.
- Summary and open problems.

Outline

- Background of finite group isomorphism.
- Relationship between p-group isomorphism and 3-tensor isomorphism.
- Our main results and an overview of our algorithm.
- Summary and open problems.

Group Isomorphism Problem

Problem (Finite group isomorphism problem)

Given the multiplication tables of two finite groups, determine whether they are isomorphic.

$$G \qquad\qquad\qquad H$$

$$\begin{array}{c|cc} * & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \cong \quad \begin{array}{c|cc} \circ & a & b \\ \hline a & a & b \\ b & b & a \end{array}$$

- First algorithm: $N^{\log N + O(1)}$ time attributed to Tarjan [Miller'78]

Group Isomorphism Problem

Problem (Finite group isomorphism problem)

Given the multiplication tables of two finite groups, determine whether they are isomorphic.

$$G \qquad\qquad\qquad H$$
$$\begin{array}{c|cc} * & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \cong \quad \begin{array}{c|cc} \circ & a & b \\ \hline a & a & b \\ b & b & a \end{array}$$

- First algorithm: $N^{\log N + O(1)}$ time attributed to Tarjan [Miller'78]

Group Isomorphism Problem

Problem (Finite group isomorphism problem)

Given the multiplication tables of two finite groups, determine whether they are isomorphic.

$$
\begin{array}{c|cc} \multicolumn{3}{c}{G} \\ * & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}
\quad \cong \quad
\begin{array}{c|cc} \multicolumn{3}{c}{H} \\ \circ & a & b \\ \hline a & a & b \\ b & b & a \end{array}
$$

- First algorithm: $N^{\log N + O(1)}$ time attributed to Tarjan [Miller'78]
- Best known algorithm: $N^{\frac{1}{4}\log N + O(1)}$ time [Rosenbaum'13]
- Open question: $N^{\log N} \xrightarrow{?} \mathrm{poly}(N)$

Group Isomorphism Problem

Problem (Finite group isomorphism problem)

Given the multiplication tables of two finite groups, determine whether they are isomorphic.

$$\begin{array}{c|cc} \multicolumn{3}{c}{G} \\ * & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \cong \quad \begin{array}{c|cc} \multicolumn{3}{c}{H} \\ \circ & a & b \\ \hline a & a & b \\ b & b & a \end{array}$$

- First algorithm: $N^{\log N + O(1)}$ time attributed to Tarjan [Miller'78]
- Best known algorithm: $N^{\frac{1}{4}\log N + O(1)}$ time [Rosenbaum'13]
- Open question: $N^{\log N} \xrightarrow{?} \mathrm{poly}(N)$

Group Isomorphism Problem

Problem (Finite group isomorphism problem)

Given the multiplication tables of two finite groups, determine whether they are isomorphic.

$$
\begin{array}{c|cc}
\multicolumn{3}{c}{G} \\
* & 0 & 1 \\
\hline
0 & 0 & 1 \\
1 & 1 & 0
\end{array}
\quad \cong \quad
\begin{array}{c|cc}
\multicolumn{3}{c}{H} \\
\circ & a & b \\
\hline
a & a & b \\
b & b & a
\end{array}
$$

- First algorithm: $N^{\log N + O(1)}$ time attributed to Tarjan [Miller'78]
- Best known algorithm: $N^{\frac{1}{4}\log N + O(1)}$ time [Rosenbaum'13]
- Open question: $N^{\log N} \xrightarrow{?} \mathrm{poly}(N)$

Through the lens of group isomorphism

- Theoretical computer science: complexity in the worst case
- Computational group theory: practical algorithms (as in Magma)
- Cryptography: protocols based on isomorphism problems
  - Several such schemes have been submitted to the NIST call for post-quantum digital signatures.

All of these areas give us good motivation to study the isomorphism testing, especially on p-groups of Frattini class-2.

Definition (p-groups of Frattini class-2)

A p-group G is of *Frattini class*-2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian.

Through the lens of group isomorphism

- Theoretical computer science: complexity in the worst case
- Computational group theory: practical algorithms (as in Magma)
- Cryptography: protocols based on isomorphism problems
  - Several such schemes have been submitted to the NIST call for post-quantum digital signatures.

All of these areas give us good motivation to study the isomorphism testing, especially on p-groups of Frattini class-2.

Definition (p-groups of Frattini class-2)

A p-group G is of *Frattini class-2*, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian.

Through the lens of group isomorphism

- Theoretical computer science: complexity in the worst case
- Computational group theory: practical algorithms (as in Magma)
- Cryptography: protocols based on isomorphism problems
  - Several such schemes have been submitted to the NIST call for post-quantum digital signatures.

All of these areas give us good motivation to study the isomorphism testing, especially on p-groups of Frattini class-2.

Definition (p-groups of Frattini class-2)

A p-group G is of *Frattini class*-2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian.

Through the lens of group isomorphism

- Theoretical computer science: complexity in the worst case
- Computational group theory: practical algorithms (as in Magma)
- Cryptography: protocols based on isomorphism problems
  - Several such schemes have been submitted to the NIST call for post-quantum digital signatures.

All of these areas give us good motivation to study the isomorphism testing, especially on p-groups of Frattini class-2.

Definition (p-groups of Frattini class-2)

A p-group G is of *Frattini class*-2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian.

Through the lens of group isomorphism

- Theoretical computer science: complexity in the worst case
- Computational group theory: practical algorithms (as in Magma)
- Cryptography: protocols based on isomorphism problems
    - Several such schemes have been submitted to the NIST call for post-quantum digital signatures.

All of these areas give us good motivation to study the isomorphism testing, especially on p-groups of Frattini class-2.

Definition (p-groups of Frattini class-2)

A p-group G is of *Frattini class*-2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian.

Why p-groups of Frattini class-2

- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.

- p-groups of Frattini class-2 contain non-abelian 2-groups.

- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].

- Multilinear formalisation[1] [Higman'60]:

[1] The illustration made some simplification for convenience.

Why p-groups of Frattini class-2

- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:

[1] The illustration made some simplification for convenience.

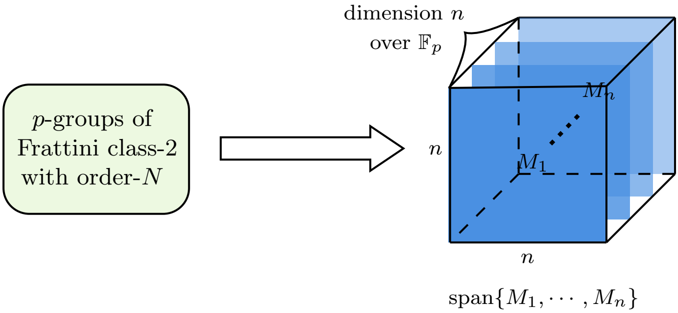
Why p-groups of Frattini class-2

- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:

[1]The illustration made some simplification for convenience.

Why p-groups of Frattini class-2

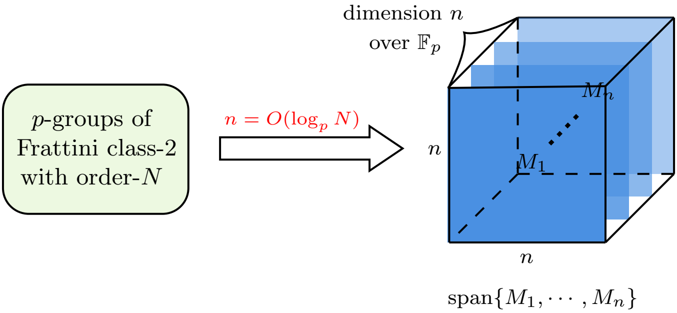
- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:



[1] The illustration made some simplification for convenience.

Why p-groups of Frattini class-2

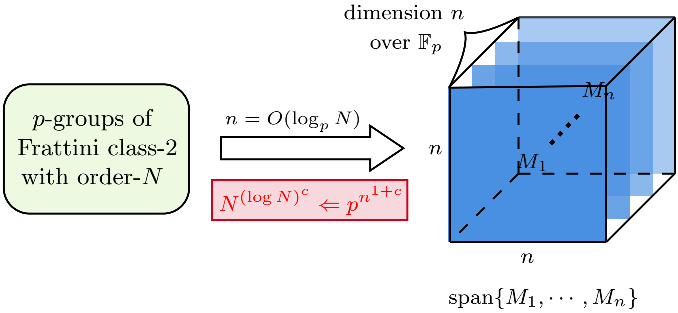
- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:



[1]The illustration made some simplification for convenience.

Why p-groups of Frattini class-2

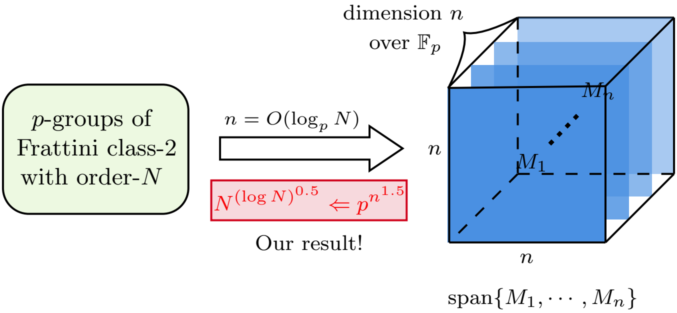
- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:



[1] The illustration made some simplification for convenience.

Why p-groups of Frattini class-2

- The isomorphism testing between p-groups of Frattini class-2 is a major bottleneck for the group isomorphism problem.
- p-groups of Frattini class-2 contain non-abelian 2-groups.
- p-groups of Frattini class-2 give a lower bound on the number of p-groups by the celebrated work of Higman [Higman'60].
- Multilinear formalisation[1] [Higman'60]:



[1] The illustration made some simplification for convenience.

Tensor Isomorphism Problem

- Isomorphism for several algebraic structures, such as algebras and polynomials, are poly-time equivalent to tensor isomorphism. [Grochow-Qiao'23]

- Isomorphisms for 3-tensors are all poly-time equivalent. [Grochow-Qiao'23]

- Isomorphism for 3-tensors under left-right actions:

$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Tensor Isomorphism Problem

- Isomorphism for several algebraic structures, such as algebras and polynomials, are poly-time equivalent to tensor isomorphism. [Grochow-Qiao'23]

- Isomorphisms for 3-tensors are all poly-time equivalent. [Grochow-Qiao'23]

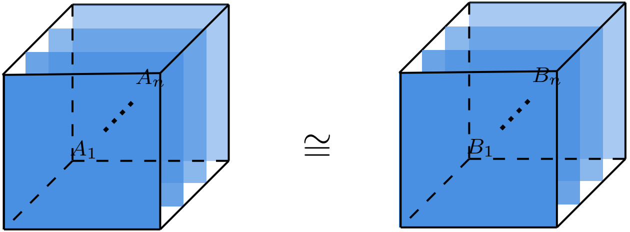
- Isomorphism for 3-tensors under left-right actions:

$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Tensor Isomorphism Problem

- Isomorphism for several algebraic structures, such as algebras and polynomials, are poly-time equivalent to tensor isomorphism. [Grochow-Qiao'23]
- Isomorphisms for 3-tensors are all poly-time equivalent. [Grochow-Qiao'23]
- Isomorphism for 3-tensors under left-right actions:



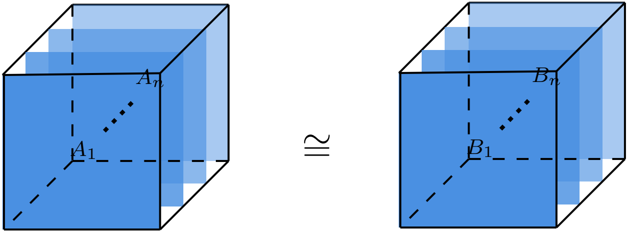
$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Tensor Isomorphism Problem

Problem (Equivalence testing of matrix spaces)

Given two $n \times n$ matrix spaces over $\mathbb{F}_q$ of dimension n, $\mathcal{A}$ and $\mathcal{B}$, determine if they are equivalent, i.e., if there exist two invertible matrices P and Q such that $\mathcal{B} = P\mathcal{A}Q := \{PAQ \mid A \in \mathcal{A}\}$.

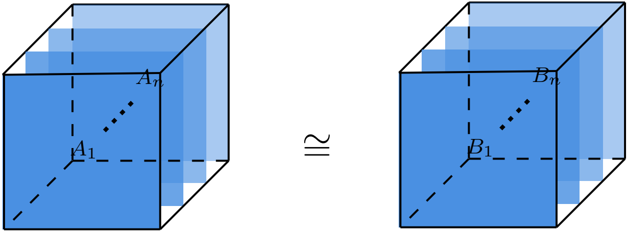


$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Previous work and our main result

- Natural upper bound: $q^{O(n^2)}$ (known since at least 1970's)
- Sun's breakthrough: $q^{O(n^{1.8}\cdot\log q)}$ [Sun'23]
- Our improvement: $q^{\tilde{O}(n^{1.5})}$ for the equivalence testing of matrix spaces

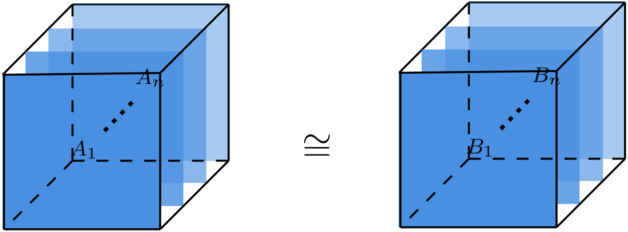


$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Previous work and our main result

- Natural upper bound: $q^{O(n^2)}$ (known since at least 1970's)
- Sun's breakthrough: $q^{O(n^{1.8}\cdot \log q)}$ [Sun'23]
- Our improvement: $q^{\tilde{O}(n^{1.5})}$ for the equivalence testing of matrix spaces

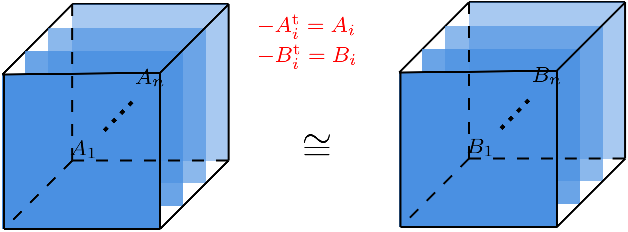


$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Previous work and our main result

- Natural upper bound: $q^{O(n^2)}$ (known since at least 1970's)
- Sun's breakthrough: $q^{O(n^{1.8} \cdot \log q)}$ [Sun'23]
  - His algorithm is for the congruence testing of skew-symmetric matrix spaces.
  -
- Our improvement: $q^{\tilde{O}(n^{1.5})}$ for the equivalence testing of matrix spaces

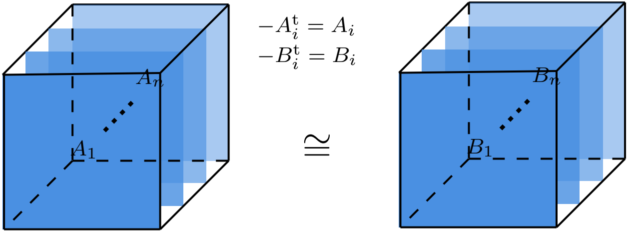


$$\mathrm{span}\{T^{\mathrm{t}} A_1 T, \cdots, T^{\mathrm{t}} A_n T\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Previous work and our main result

- Natural upper bound: $q^{O(n^2)}$ (known since at least 1970's)
- Sun's breakthrough: $q^{O(n^{1.8}\cdot\log q)}$ [Sun'23]
  - His algorithm is for the congruence testing of skew-symmetric matrix spaces.
  - This solves the isomorphism testing of p-groups of class-2 and exponent p.
- Our improvement: $q^{\tilde{O}(n^{1.5})}$ for the equivalence testing of matrix spaces

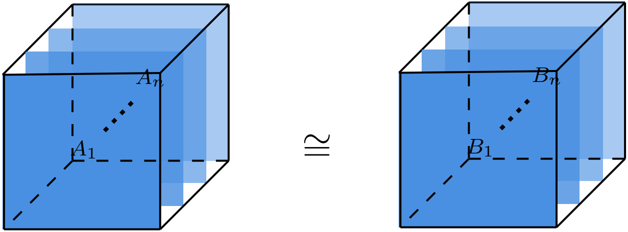


$$\mathrm{span}\{T^{\mathrm{t}}A_1T, \cdots, T^{\mathrm{t}}A_nT\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

Previous work and our main result

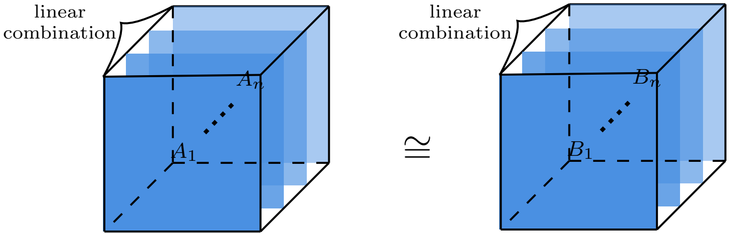
- Natural upper bound: $q^{O(n^2)}$ (known since at least 1970's)
- Sun's breakthrough: $q^{O(n^{1.8} \cdot \log q)}$ [Sun'23]
  - His algorithm is for a tensor isomorphism problem reducible to our problem.
  - This solves the isomorphism testing of a subclass of our underlying group.
- Our improvement: $q^{\tilde{O}(n^{1.5})}$ for the equivalence testing of matrix spaces



$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

invertible matrices

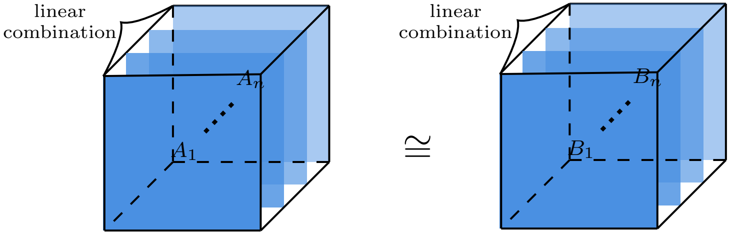
Overall strategy: from matrix spaces to matrix tuples



$$\text{span}\{PA_1Q, \cdots, PA_nQ\} = \text{span}\{B_1, \cdots, B_n\}$$

Overall strategy: reduce it to the congruence testing of matrix tuples, which is solvable in polynomial time [Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24].

Overall strategy: from matrix spaces to matrix tuples

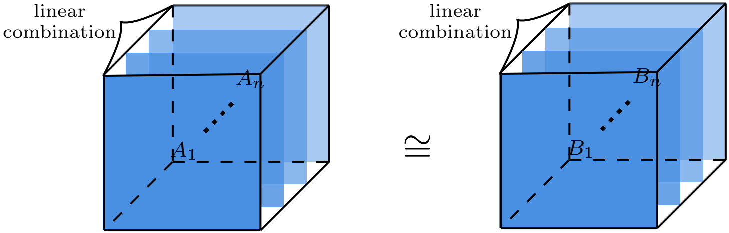


$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

Overall strategy: reduce it to the congruence testing of matrix tuples, which is solvable in polynomial time [Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24].

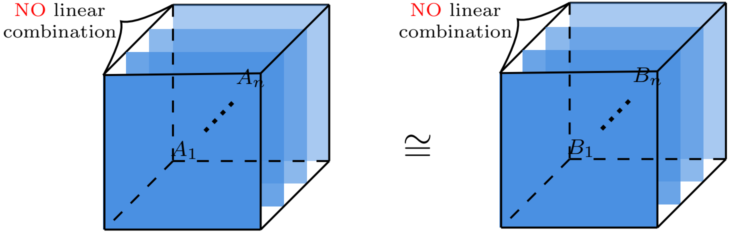
$$(T^{\mathrm{t}} A_1 T, \cdots, T^{\mathrm{t}} A_n T) = (B_1, \cdots, B_n)$$

Overall strategy: from matrix spaces to matrix tuples



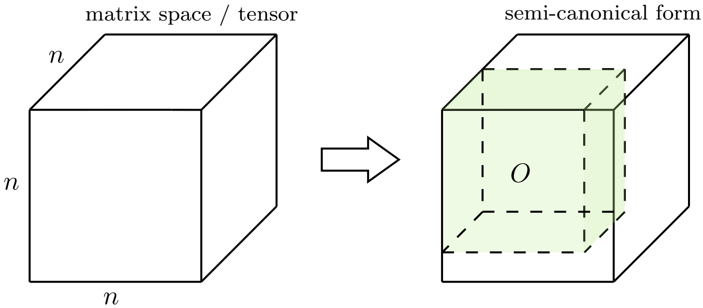
$$\mathrm{span}\{PA_1Q, \cdots, PA_nQ\} = \mathrm{span}\{B_1, \cdots, B_n\}$$

Overall strategy: reduce it to the congruence testing of matrix tuples, which is solvable in polynomial time [Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24].



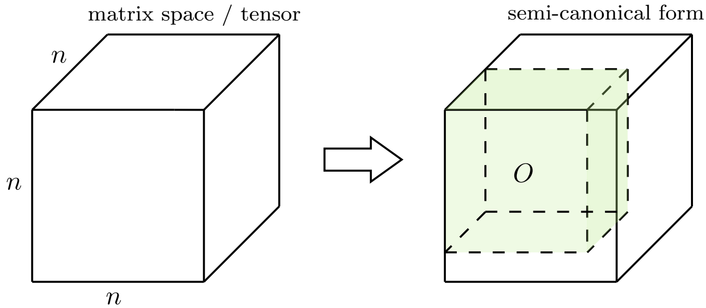
$$(T^{\mathrm{t}}A_1T, \cdots, T^{\mathrm{t}}A_nT) = (B_1, \cdots, B_n)$$

Bridge: semi-canonical forms of matrix spaces



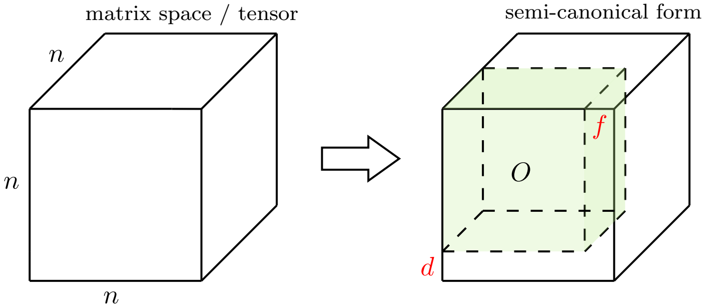
- We construct a semi-canonical form of given matrix spaces, and then construct matrix tuples from the semi-canonical forms.
- The margins are supposed to be small, to reduce the cost of enumerating the action matrices P and Q.
- The margin for the third direction, while can be large, is "local" somehow.

Bridge: semi-canonical forms of matrix spaces



- We construct a semi-canonical form of given matrix spaces, and then construct matrix tuples from the semi-canonical tensors.
- The margins are supposed to be small, to reduce the cost of enumerating the action matrices P and Q.
- The margin for the third direction, while can be large, is 'fixed' somehow.

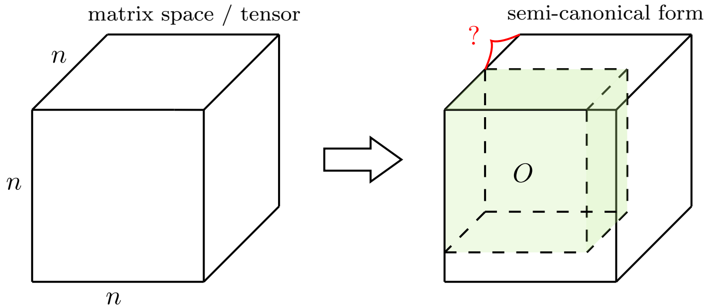
Bridge: semi-canonical forms of matrix spaces



$$d + f \ll n$$

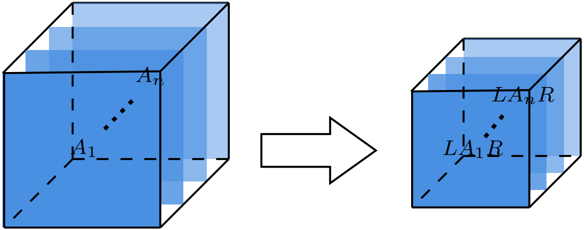
- We construct a semi-canonical form of given matrix spaces, and then construct matrix tuples from the semi-canonical tensors.
- The margins are supposed to be small, to reduce the cost of enumerating the action matrices P and Q.
- The margin for the third direction, while can be large, is 'fixed' somehow.

Bridge: semi-canonical forms of matrix spaces



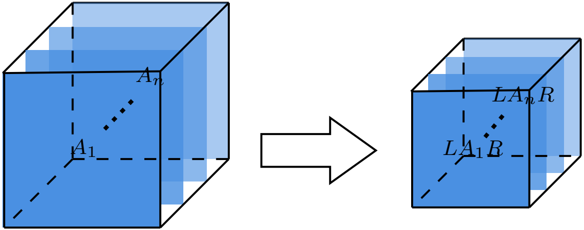
- We construct a semi-canonical form of given matrix spaces, and then construct matrix tuples from the semi-canonical tensors.
- The margins are supposed to be small, to reduce the cost of enumerating the action matrices P and Q.
- The margin for the third direction, while can be large, is 'fixed' somehow.

A special case: getting canonical forms after restrictions



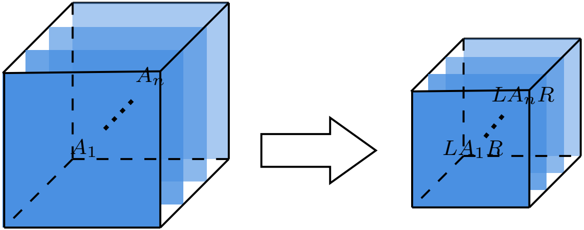
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots,$ $LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.

A special case: getting canonical forms after restrictions



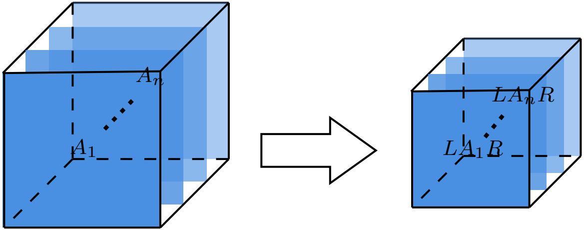
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots, LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.
  - Compute the canonical basis of $L\mathcal{A}R$.
  - Enumerate such matrices L' and R' for $\mathcal{B}$, which costs $q^{O(ns)}$.
  - Compute the canonical basis of $L'\mathcal{B}R'$ and compare it to that of $L\mathcal{A}R$.
  - The correspondence between L, L' and R, R' gives the desired equivalence between $\mathcal{A}$ and $\mathcal{B}$.
- What if $LAR = 0$ for some non-zero $A \in \mathcal{A}$?

A special case: getting canonical forms after restrictions



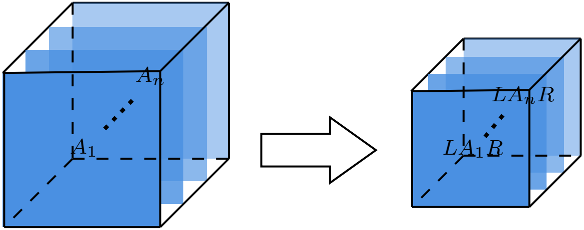
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots, LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.
  - Compute the canonical basis of $L\mathcal{A}R$.
  - Enumerate such matrices L' and R' for $\mathcal{B}$, which costs $q^{O(ns)}$.
  - Compute the canonical basis of $L'\mathcal{B}R'$ and compare it to that of $L\mathcal{A}R$.
  - The correspondence between L, L' and R, R' gives the desired equivalence between $\mathcal{A}$ and $\mathcal{B}$.
- What if $LAR = 0$ for some non-zero $A \in \mathcal{A}$?

A special case: getting canonical forms after restrictions



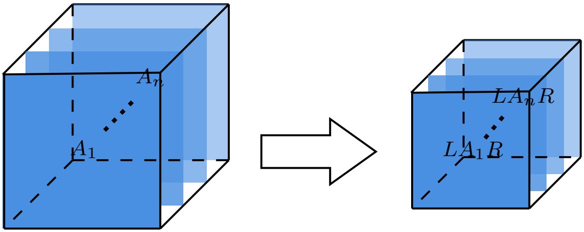
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots, LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.
  - Compute the canonical basis of $L\mathcal{A}R$.
  - Enumerate such matrices L' and R' for $\mathcal{B}$, which costs $q^{O(ns)}$.
  - Compute the canonical basis of $L'\mathcal{B}R'$ and compare it to that of $L\mathcal{A}R$.
  - The correspondence between L, L' and R, R' gives the desired equivalence between $\mathcal{A}$ and $\mathcal{B}$.
- What if $LAR = 0$ for some non-zero $A \in \mathcal{A}$?

A special case: getting canonical forms after restrictions



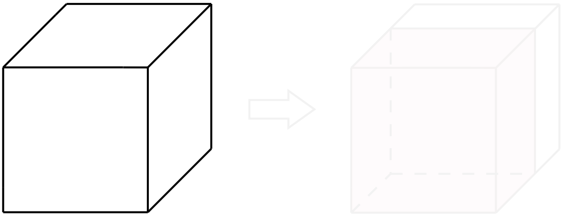
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots, LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.
  - Compute the canonical basis of $L\mathcal{A}R$.
  - Enumerate such matrices L' and R' for $\mathcal{B}$, which costs $q^{O(ns)}$.
  - Compute the canonical basis of $L'\mathcal{B}R'$ and compare it to that of $L\mathcal{A}R$.
  - The correspondence between L, L' and R, R' gives the desired equivalence between $\mathcal{A}$ and $\mathcal{B}$.
- What if $L\mathcal{A}R = 0$ for some non-zero $A \in \mathcal{A}$?

A special case: getting canonical forms after restrictions



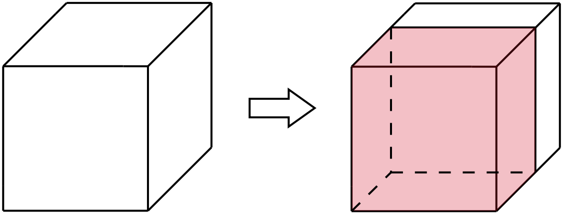
- Assume $L \leq \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \leq \mathrm{M}(n \times s, \mathbb{F}_q)$ satisfy that $LA_1R, \cdots, LA_nR \leq \mathrm{M}(s \times s, \mathbb{F}_q)$ are linearly independent.
  - Compute the canonical basis of $L\mathcal{A}R$.
  - Enumerate such matrices L' and R' for $\mathcal{B}$, which costs $q^{O(ns)}$.
  - Compute the canonical basis of $L'\mathcal{B}R'$ and compare it to that of $L\mathcal{A}R$.
  - The correspondence between L, L' and R, R' gives the desired equivalence between $\mathcal{A}$ and $\mathcal{B}$.
- What if $LAR = 0$ for some non-zero $A \in \mathcal{A}$?

Technique 1: individualisation by left-right restrictions



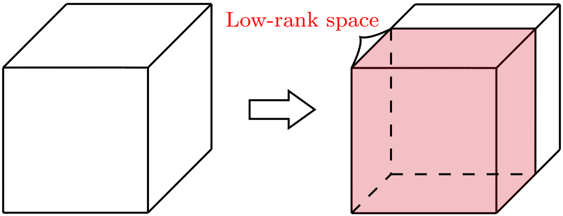
- Given a matrix space $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$.
- Basic idea: sort the basis matrices (subject to choices of L, R) such that
  - the first ones span $\mathrm{Ker}_{L,R}(\mathcal{A}) := \mathrm{span}\{A \in \mathcal{A} \mid LAR = 0\}$, and
  - the remaining ones form a canonical basis of the quotient space $\mathcal{A} / \mathrm{Ker}_{L,R}(\mathcal{A})$.
- Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Technique 1: individualisation by left-right restrictions



- Given a matrix space $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$.
- Basic idea: sort the basis matrices (subject to choices of L, R) such that
  - the first ones span $\mathrm{Ker}_{L,R}(\mathcal{A}) := \mathrm{span}\{A \in \mathcal{A} \mid LAR = 0\}$, and
  - the remaining ones form a canonical basis of the quotient space $\mathcal{A}/\,\mathrm{Ker}_{L,R}(\mathcal{A})$.
- Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Technique 1: individualisation by left-right restrictions



- Given a matrix space $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$.
- Basic idea: sort the basis matrices (subject to choices of L, R) such that
  - the first ones span $\mathrm{Ker}_{L,R}(\mathcal{A}) := \mathrm{span}\{A \in \mathcal{A} \mid LAR = 0\}$, and
  - the remaining ones form a canonical basis of the quotient space $\mathcal{A}/\,\mathrm{Ker}_{L,R}(\mathcal{A})$.
- Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Technique 1: individualisation by left-right restrictions

Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Lemma (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$ be a matrix space of dimension n. Then with at least probability of $1 - \frac{1}{q^r}$, $\mathrm{Ker}_{L,R}(\mathcal{A})$ consists of matrices of rank $\leq r$ for uniformly randomly sampled $L \in \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \in \mathrm{M}(n \times s, \mathbb{F}_q)$.

Why is this an advantage?

Technique 1: individualisation by left-right restrictions

Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Lemma (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$ *be a matrix space of dimension* n*. Fix some* $r \in [n]$*, and let*

$$s = \lceil 3 \cdot \max\{\frac{n}{r}, r\} \rceil.$$

Then with at least probability of $1 - \frac{1}{q^r}$, $\mathrm{Ker}_{L,R}(\mathcal{A})$ *consists of matrices of rank* $\leq r$ *for uniformly randomly sampled* $L \in \mathrm{M}(s \times n, \mathbb{F}_q)$ *and* $R \in \mathrm{M}(n \times s, \mathbb{F}_q)$.

Why is this an advantage?

Technique 1: individualisation by left-right restrictions

Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Lemma (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$ be a matrix space of dimension n. Let $r = \sqrt{n}$ and

$$s = O(\sqrt{n}).$$

Then with at least probability of $1 - \frac{1}{q^r}$, $\mathrm{Ker}_{L,R}(\mathcal{A})$ consists of matrices of rank $\leq r$ for uniformly randomly sampled $L \in \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \in \mathrm{M}(n \times s, \mathbb{F}_q)$.

Why is this an advantage?

Technique 1: individualisation by left-right restrictions

Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Lemma (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$ be a matrix space of dimension n. Let $r = \sqrt{n}$ and

$$s = O(\sqrt{n}).$$

Then with at least probability of $1 - \frac{1}{q^r}$, $\mathrm{Ker}_{L,R}(\mathcal{A})$ consists of matrices of rank $\leq r$ for uniformly randomly sampled $L \in \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \in \mathrm{M}(n \times s, \mathbb{F}_q)$.

Again, to find L', R' such that $\mathcal{B}$ is individualised correspondingly to $\mathcal{A}$, we still need to enumerate all L', R' in such size, which costs $q^{O(ns)}$. Why is this an advantage?

Technique 1: individualisation by left-right restrictions

Advantage: $\mathrm{Ker}_{L,R}(\mathcal{A})$ is a low-rank space with a high probability.

Lemma (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

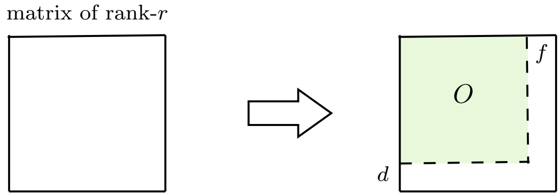
Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F}_q)$ be a matrix space of dimension n. Let $r = \sqrt{n}$ and

$$s = O(\sqrt{n}).$$

Then with at least probability of $1 - \frac{1}{q^r}$, $\mathrm{Ker}_{L,R}(\mathcal{A})$ consists of matrices of rank $\leq r$ for uniformly randomly sampled $L \in \mathrm{M}(s \times n, \mathbb{F}_q)$ and $R \in \mathrm{M}(n \times s, \mathbb{F}_q)$.

Why is this an advantage?

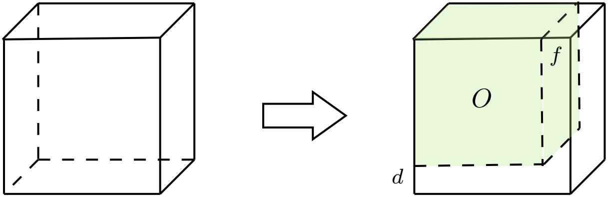
Low-rank matrix characterisation



$$d + f = O(r)$$

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



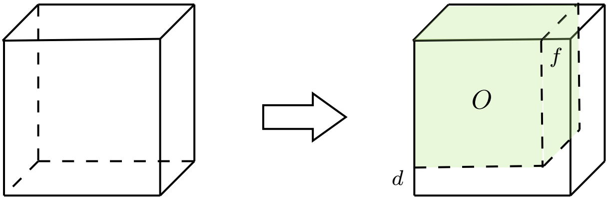
$$d + f = O(r)$$

over field of order $\geq r+1$

[Flanders'62, Atkinson-Lloyd'81]

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



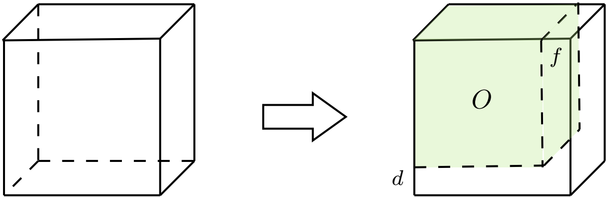
$$d + f = O(r^2)$$

[Sun'23]

Our new perspective:

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



$$d + f = O(r \log r)$$

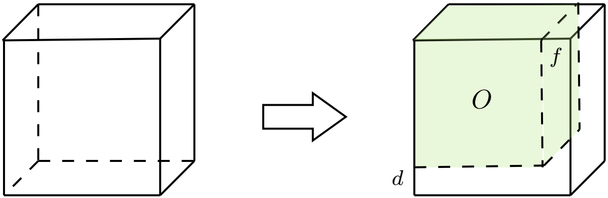
[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

- For $U \leq \mathbb{F}^n$, $\mathcal{K}(U) := \mathrm{span}\{\cup_{K \in \mathcal{K}} K(U)\}$. Then U is a *g-shrunk subspace* of $\mathcal{K}$, if $\dim(U) - \dim(\mathcal{K}(U)) \geq g$.
- The *non-commutative corank* of $\mathcal{K} := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{K}\}$.
- $\text{nc-corank}(\mathcal{K}) + d + f = n$.
- We can 'fix' the zero block by computing the canonical maximum shrunk subspace of $\mathcal{K}$ [Ivanyos-Qiao-Subrahmanyam'18].

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



$$d + f = O(r \log r)$$

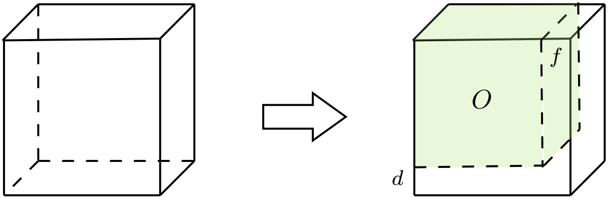
[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

- For $U \leq \mathbb{F}^n$, $\mathcal{K}(U) := \text{span}\{\cup_{K \in \mathcal{K}} K(U)\}$. Then U is a *g-shrunk subspace* of $\mathcal{K}$, if $\dim(U) - \dim(\mathcal{K}(U)) \geq g$.
- The *non-commutative corank* of $\mathcal{K} := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{K}\}$.
- $\text{nc-corank}(\mathcal{K}) + d + f = n$.
- We can 'fix' the zero block by computing the canonical maximum shrunk subspace of $\mathcal{K}$ [Ivanyos-Qiao-Subrahmanyam'18].

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



$$d + f = O(r \log r)$$

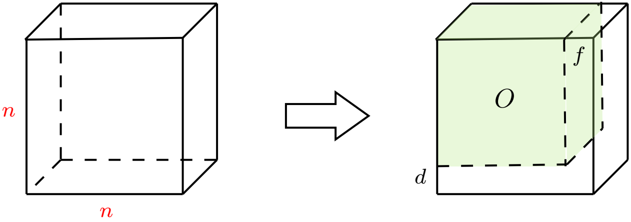
[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

- For $U \leq \mathbb{F}^n$, $\mathcal{K}(U) := \operatorname{span}\{\cup_{K \in \mathcal{K}} K(U)\}$. Then U is a *g-shrunk subspace* of $\mathcal{K}$, if $\dim(U) - \dim(\mathcal{K}(U)) \geq g$.
- The *non-commutative corank* of $\mathcal{K} := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{K}\}$.
- nc-corank$(\mathcal{K}) + d + f = n$.
- We can 'fix' the zero block by computing the canonical maximum shrunk subspace of $\mathcal{K}$ [Ivanyos-Qiao-Subrahmanyam'18].

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



$$d + f = O(r \log r)$$

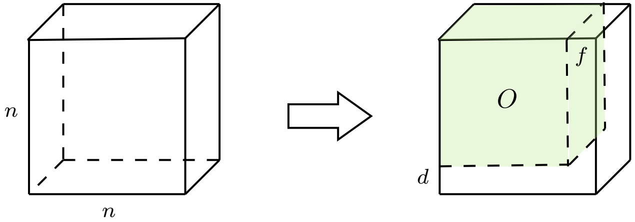
[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

- For $U \leq \mathbb{F}^n$, $\mathcal{K}(U) := \text{span}\{\cup_{K \in \mathcal{K}} K(U)\}$. Then U is a *g-shrunk subspace* of $\mathcal{K}$, if $\dim(U) - \dim(\mathcal{K}(U)) \geq g$.
- The *non-commutative corank* of $\mathcal{K} := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{K}\}$.
- $\text{nc-corank}(\mathcal{K}) + d + f = n$.
- We can 'fix' the zero block by computing the canonical maximum shrunk subspace of $\mathcal{K}$ [Ivanyos-Qiao-Subrahmanyam'18].

Technique 2: low-rank matrix space characterisation

Low-rank space $\mathcal{K}$ bounded by rank-r



$$d + f = O(r \log r)$$

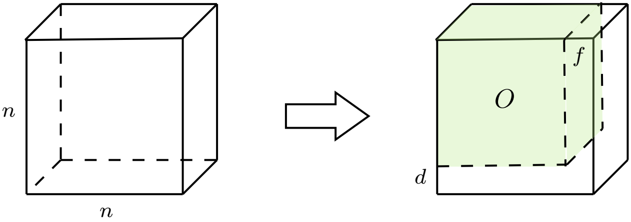
[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

- For $U \leq \mathbb{F}^n$, $\mathcal{K}(U) := \text{span}\{\cup_{K \in \mathcal{K}} K(U)\}$. Then U is a *g-shrunk subspace* of $\mathcal{K}$, if $\dim(U) - \dim(\mathcal{K}(U)) \geq g$.
- The *non-commutative corank* of $\mathcal{K} := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{K}\}$.
- $\text{nc-corank}(\mathcal{K}) + d + f = n$.
- We can 'fix' the zero block by computing the canonical maximum shrunk subspace of $\mathcal{K}$ [Ivanyos-Qiao-Subrahmanyam'18].

Technique 2: low-rank matrix space characterisation

Low-rank space bounded by rank-$\sqrt{n}$



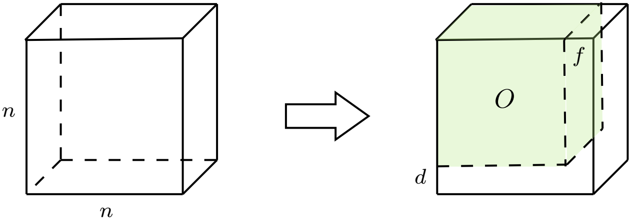
$$d + f = O(\sqrt{n}\log n)$$

[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

Our new perspective:

Technique 2: low-rank matrix space characterisation

Low-rank space bounded by rank-$\sqrt{n}$

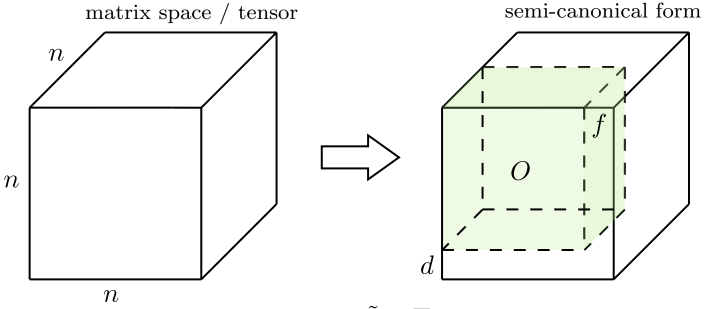


$$d + f = \tilde{O}(\sqrt{n})$$

[Ivanyos-Mendoza-Qiao-Sun-Zhang'24]

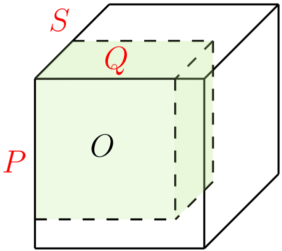
Our new perspective:

From semi-canonical forms to skew-symmetric matrix tuples

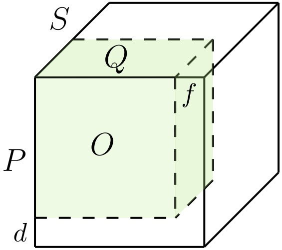


$$d + f = \tilde{O}(\sqrt{n})$$

From semi-canonical forms to skew-symmetric matrix tuples



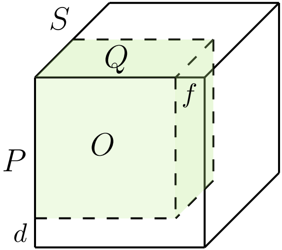
From semi-canonical forms to skew-symmetric matrix tuples



Upon enumeration which costs $q^{\tilde{O}(n^{1.5})}$,

$$P = \begin{bmatrix} P_1 & P_2 \\ O & P_3 \end{bmatrix} \qquad Q = \begin{bmatrix} Q_1 & Q_2 \\ O & Q_3 \end{bmatrix} \qquad S = \begin{bmatrix} S_1 & S_2 \\ O & I \end{bmatrix}$$

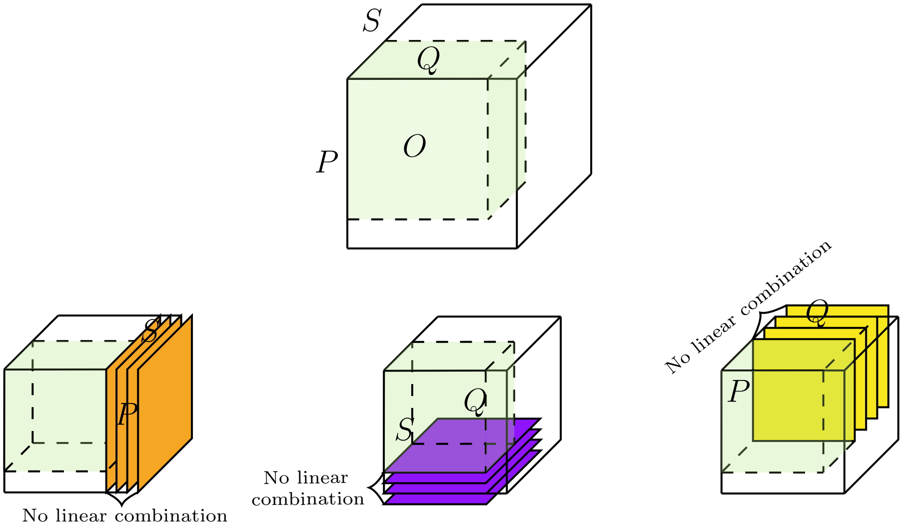
From semi-canonical forms to skew-symmetric matrix tuples



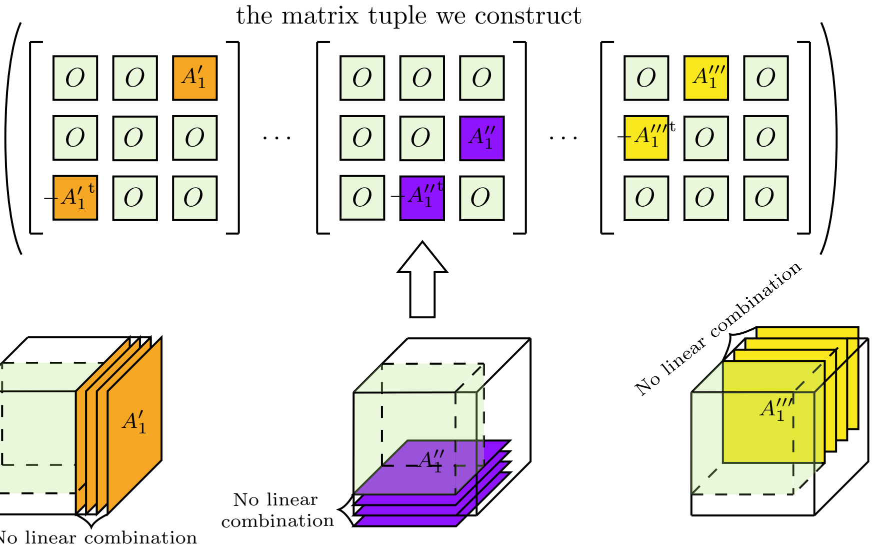
Upon enumeration which costs $q^{\tilde{O}(n^{1.5})}$,

$$P = \begin{pmatrix} P_1 & O \\ O & I_d \end{pmatrix} \qquad Q = \begin{pmatrix} Q_1 & O \\ O & I_f \end{pmatrix} \qquad S = \begin{pmatrix} S_1 & S_2 \\ O & I \end{pmatrix}$$

From semi-canonical forms to skew-symmetric matrix tuples



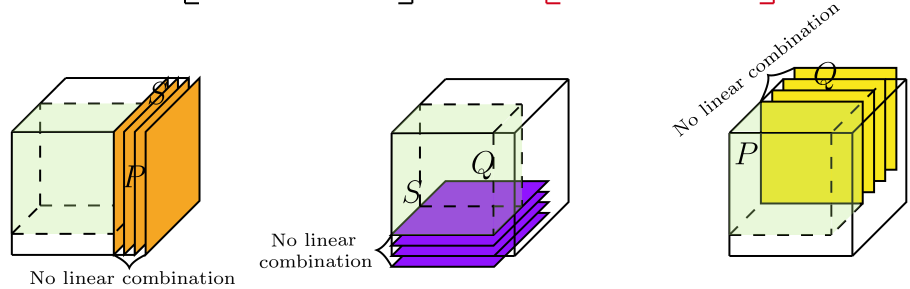
From semi-canonical forms to skew-symmetric matrix tuples



Some colourful slices may be transposed appropriately to match the action matrices.

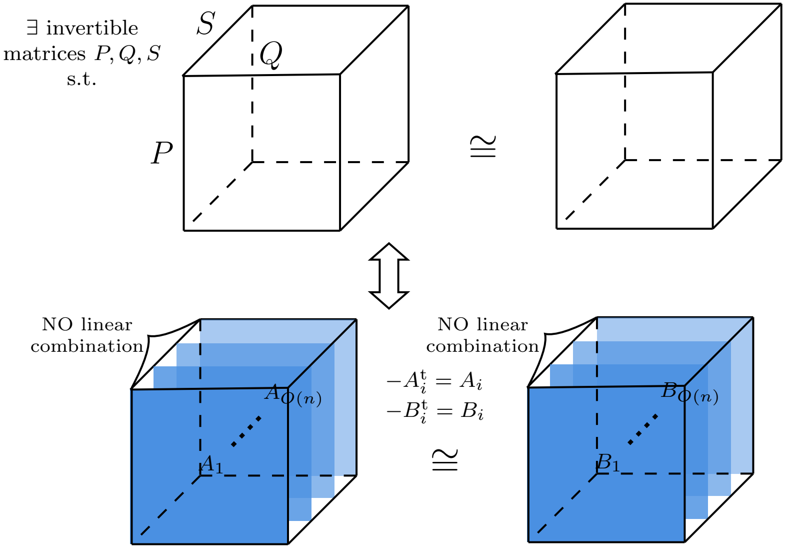
From semi-canonical forms to skew-symmetric matrix tuples

$$\begin{array}{c|ccc} & P^{\mathrm{t}} & Q^{\mathrm{t}} & S^{\mathrm{t}} \\ \hline P & O & & \\ Q & & O & \\ S & & & O \end{array} \qquad T = \begin{bmatrix} P & & \\ & Q & \\ & & S \end{bmatrix}$$



Some colourful slices may be transposed appropriately to match the action matrices.

From tensor isomorphism to tuple isomorphism



∃ an invertible matrix T s.t. $(T^{\mathrm{t}} A_1 T, \cdots, T^{\mathrm{t}} A_{O(n)} T) = (B_1, \cdots, B_{O(n)})$

T is conditioned in a special form, but it is still reducible to the general problem.

Wrap-up of the results

Theorem (Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24)

Given two matrix tuples over $\mathbb{F}_q$, there exists a polynomial-time algorithm that decides whether they are congruent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two $n \times n$ matrix spaces over $\mathbb{F}_q$ of dimension-m, there exists an algorithm in time $q^{\tilde{O}((n+m)^{1.5})}$ that decides whether they are equivalent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two p-groups of Frattini class-2 of order N, there exists an algorithm in time $N^{\tilde{O}((\log N)^{1/2})}$ to decide whether they are isomorphic.

Wrap-up of the results

Theorem (Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24)

Given two matrix tuples over $\mathbb{F}_q$, there exists a polynomial-time algorithm that decides whether they are congruent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two $n \times n$ matrix spaces over $\mathbb{F}_q$ of dimension-m, there exists an algorithm in time $q^{\tilde{O}((n+m)^{1.5})}$ that decides whether they are equivalent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two p-groups of Frattini class-2 of order N, there exists an algorithm in time $N^{\tilde{O}((\log N)^{1/2})}$ to decide whether they are isomorphic.

Wrap-up of the results

Theorem (Ivanyos-Qiao'19, Brooksbank-Kassabov-Wilson'24)

Given two matrix tuples over $\mathbb{F}_q$, there exists a polynomial-time algorithm that decides whether they are congruent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two $n \times n$ matrix spaces over $\mathbb{F}_q$ of dimension-m, there exists an algorithm in time $q^{\tilde{O}((n+m)^{1.5})}$ that decides whether they are equivalent.

Theorem (Ivanyos-Mendoza-Qiao-Sun-Zhang'24)

Given two p-groups of Frattini class-2 of order N, there exists an algorithm in time $N^{\tilde{O}((\log N)^{1/2})}$ to decide whether they are isomorphic.

What's next?

- Can we improve the algorithm for general group isomorphism to $N^{(\log N)^c}$ time for some $c < 1$?
- Or for other subclasses of p-groups...
- Can we design more faster practical algorithms to break isomorphism-based cryptography protocols?
  - [Narayanan-Qiao-Tang'24] made a heuristic one running in time $q^{O(n/2)}$ for the average case of the equivalence testing of matrix spaces.

What's next?

- Can we improve the algorithm for general group isomorphism to $N^{(\log N)^c}$ time for some $c < 1$?

- Or for other subclasses of p-groups...

- Can we design more faster practical algorithms to break isomorphism-based cryptography protocols?

What's next?

- Can we improve the algorithm for general group isomorphism to $N^{(\log N)^c}$ time for some $c < 1$?
- Or for other subclasses of p-groups...
- Can we design more faster practical algorithms to break isomorphism-based cryptography protocols?
  - [Narayanan-Qiao-Tang'24] made a heuristic one running in time $q^{O(n/2)}$ for the average case of the equivalence testing of matrix spaces.

What's next?

- Can we improve the algorithm for general group isomorphism to $N^{(\log N)^c}$ time for some $c < 1$?
- Or for other subclasses of p-groups...
- Can we design more faster practical algorithms to break isomorphism-based cryptography protocols?
  - [Narayanan-Qiao-Tang'24] made a heuristic one running in time $q^{O(n/2)}$ for the average case of the equivalence testing of matrix spaces.

Question and Answer

Thank you so much!