Average-case Algorithm for Testing Pseudo-isometry of Alternating Matrix Tuples

Peter A. Brooksbank, Joshua A. Grochow,
Yinan Li,
Youming Qiao, James B. Wilson

Full version (arXiv:1905.02518):
Incorporating Weisfeiler-Leman into algorithms for group isomorphism

21.11.2019

Bucknell University
University of Colorado Boulder
UTS
Colorado State University
CWI Centrum Wiskunde & Informatica
QuSoft Research Center for Quantum Software

Alternating Matrix Tuples

$A \in \Lambda(n,q)$	$v^t A v = 0 \ \forall \ v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	The general linear group of degree n over $\mathbb{F}_q$

$$\mathbb{G} = \left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \right)$$

$$\mathbb{H} = \left(\begin{bmatrix} 0 & -1 & 0 & -2 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ 2 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & -1 & 0 \\ -1 & 0 & -1 & -1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right)$$

Alternating Matrix Tuples

$A \in \Lambda(n, q)$	$v^t A v = 0 \ \forall \ v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n, q)$	The general linear group of degree n over $\mathbb{F}_q$

$\mathbb{G}$ and $\mathbb{H}$ are **isometric** if and only if

$$\exists T \in \mathrm{GL}(n, q), \text{ s.t. } T^t \mathbb{G} T = (T^t G_1 T, \ldots, T^t G_m T) = \mathbb{H}.$$

Alternating Matrix Tuples

$A \in \Lambda(n,q)$	$v^t A v = 0 \;\forall\; v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	The general linear group of degree n over $\mathbb{F}_q$

$\mathbb{G}$ and $\mathbb{H}$ are **isometric** if and only if

$$\exists T \in \mathrm{GL}(n,q),\ \text{s.t. } T^t \mathbb{G} T = (T^t G_1 T, \ldots, T^t G_m T) = \mathbb{H}.$$

$$\overbrace{\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}}^{T^t} \overbrace{\left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \right)}^{\mathbb{G}} \overbrace{\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}}^{T}$$

$$= \underbrace{\left(\begin{bmatrix} 0 & -1 & 0 & -2 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \\ 2 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & -1 & 0 \\ -1 & 0 & -1 & -1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \right)}_{\mathbb{H}}$$

Alternating Matrix Tuples

$A \in \Lambda(n, q)$	$v^t A v = 0 \ \forall \ v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n, q)$	The general linear group of degree n over $\mathbb{F}_q$

$\mathbb{G}$ and $\mathbb{H}$ are **isometric** if and only if

$$\exists T \in \mathrm{GL}(n, q), \text{ s.t. } T^t \mathbb{G} T = (T^t G_1 T, \ldots, T^t G_m T) = \mathbb{H}.$$

$\mathbb{G}$ and $\mathbb{H}$ are **pseudo-isometric** if and only if

$\exists T \in \mathrm{GL}(n, q)$, the linear span of $T^t \mathbb{G} T$ and $\mathbb{H}$ are the same.

Alternating Matrix Tuples

$A \in \Lambda(n,q)$	$v^t A v = 0 \ \forall \ v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	The general linear group of degree n over $\mathbb{F}_q$

$\mathbb{G}$ and $\mathbb{H}$ are **isometric** if and only if

$$\exists T \in \mathrm{GL}(n,q), \text{ s.t. } T^t \mathbb{G} T = (T^t G_1 T, \ldots, T^t G_m T) = \mathbb{H}.$$

$\mathbb{G}$ and $\mathbb{H}$ are **pseudo-isometric** if and only if

$\exists T \in \mathrm{GL}(n,q)$, the linear span of $T^t \mathbb{G} T$ and $\mathbb{H}$ are the same.

$$\overbrace{\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}}^{T^t} \left\langle \overbrace{\left(\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \right)}^{\mathbb{G}} \right\rangle \overbrace{\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}}^{T}$$

$$= \underbrace{\left\langle \left(\begin{bmatrix} 0 & 0 & -1 & -2 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -2 & 0 & -3 \\ 2 & 0 & 1 & -1 \\ 0 & -1 & 0 & -1 \\ -3 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & -2 \\ 1 & 1 & 0 & 1 \\ 1 & 2 & -1 & 0 \end{bmatrix} \right) \right\rangle}_{\mathbb{H}'}$$

Alternating Matrix Tuples

$A \in \Lambda(n,q)$	$v^t A v = 0 \ \forall \ v \in \mathbb{F}_q^n$
$\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$	m-tuples of $n \times n$ alternating matrices over $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	The general linear group of degree n over $\mathbb{F}_q$

$\mathbb{G}$ and $\mathbb{H}$ are **isometric** if and only if

$$\exists T \in \mathrm{GL}(n,q), \text{ s.t. } T^t \mathbb{G} T = (T^t G_1 T, \ldots, T^t G_m T) = \mathbb{H}.$$

$\mathbb{G}$ and $\mathbb{H}$ are **pseudo-isometric** if and only if

$\exists T \in \mathrm{GL}(n,q)$, the linear span of $T^t \mathbb{G} T$ and $\mathbb{H}$ are the same.

(Pseudo-)Isometry Testing:

Given $\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$, determine whether $\mathbb{G}$ and $\mathbb{H}$ are (pseudo-)isometric.

Why should we care about pseudo-isometry testing of alternating matrix tuples?

p-groups and Alternating Matrix Tuples

Let G be a p-group of class 2 and exponent p of order p^ℓ (p odd).

- Class (at most) 2: $[G, G] \leq Z(G) = \{g \in G : gg' = g'g \ \forall \ g' \in G\}$.
- Abelian groups are class 1: $[G, G] = \{1\}$.
- exponent p: $g^p = 1 \ \forall \ g \in G$.

p-groups and Alternating Matrix Tuples

Let G be a p-group of class 2 and exponent p of order p^ℓ (p odd).

The commutator map $\Phi_G : G/[G,G] \times G/[G,G] \to [G,G]$:

$$\Phi_G(g_1, g_2) = [g_1, g_2],\ \forall\ g_1, g_2 \in G/[G,G]$$

is **alternating**:

$$\Phi_G(g, g) = e,\ \forall\ g \in G/[G,G].$$

p-groups and Alternating Matrix Tuples

Let G be a p-group of class 2 and exponent p of order p^ℓ (p odd).

The commutator map $\Phi_G : G/[G,G] \times G/[G,G] \to [G,G]$:

$$\Phi_G(g_1, g_2) = [g_1, g_2],\ \forall\ g_1, g_2 \in G/[G,G]$$

is **alternating**:

$$\Phi_G(g,g) = e,\ \forall\ g \in G/[G,G].$$

Note: $G/[G,G] = (\mathbb{Z}/p\mathbb{Z})^n \cong \mathbb{F}_p^n$, $[G,G] = (\mathbb{Z}/p\mathbb{Z})^m \cong \mathbb{F}_p^m$ $(m+n=\ell)$.

(The isomorphisms correspond to distinguish basis of $(\mathbb{Z}/p\mathbb{Z})^n$ and $(\mathbb{Z}/p\mathbb{Z})^m$.) $\Phi_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ is an alternating bilinear map.

p-groups and Alternating Matrix Tuples

Let G be a p-group of class 2 and exponent p of order p^ℓ (p odd).

The commutator map $\Phi_G : G/[G,G] \times G/[G,G] \to [G,G]$:

$$\Phi_G(g_1, g_2) = [g_1, g_2],\ \forall\ g_1, g_2 \in G/[G,G]$$

is **alternating**:

$$\Phi_G(g, g) = e,\ \forall\ g \in G/[G,G].$$

Note: $G/[G,G] = (\mathbb{Z}/p\mathbb{Z})^n \cong \mathbb{F}_p^n$, $[G,G] = (\mathbb{Z}/p\mathbb{Z})^m \cong \mathbb{F}_p^m$ $(m + n = \ell)$.

(The isomorphisms correspond to distinguish basis of $(\mathbb{Z}/p\mathbb{Z})^n$ and $(\mathbb{Z}/p\mathbb{Z})^m$.) $\Phi_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ is an alternating bilinear map.

$$\Phi_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m \ \Leftrightarrow\ \mathbb{G} = (A_1, \ldots, A_m) \in \Lambda(n,p)^m$$

p-groups and Alternating Matrix Tuples

Let G be a p-group of class 2 and exponent p of order p^ℓ (p odd).

The commutator map $\Phi_G : G/[G,G] \times G/[G,G] \to [G,G]$:

$$\Phi_G(g_1, g_2) = [g_1, g_2],\ \forall\, g_1, g_2 \in G/[G,G]$$

is **alternating**:

$$\Phi_G(g, g) = e,\ \forall\, g \in G/[G,G].$$

Note: $G/[G,G] = (\mathbb{Z}/p\mathbb{Z})^n \cong \mathbb{F}_p^n$, $[G,G] = (\mathbb{Z}/p\mathbb{Z})^m \cong \mathbb{F}_p^m$ $(m + n = \ell)$.

(The isomorphisms correspond to distinguish basis of $(\mathbb{Z}/p\mathbb{Z})^n$ and $(\mathbb{Z}/p\mathbb{Z})^m$.) $\Phi_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ is an alternating bilinear map.

$$\Phi_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m \ \Leftrightarrow\ \mathbb{G} = (A_1, \dots, A_m) \in \Lambda(n,p)^m$$

[Baer 1938]: $G_1 \cong G_2 \Leftrightarrow \mathbb{G}_1$ and $\mathbb{G}_2$ are pseudo-isometric.

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

$G \cong H$ if there exists a bijective map $\phi : G \to H$, such that

$$\forall\ g_1, g_2 \in G,\ \phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2).$$

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

In computation, the groups are given as the **Cayley table**:

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Cayley table of the Klein four-group

- Sparse input model ($O(\log n)$): permutations, matrices, or black-box groups. (used in CGT)
- Undecidable, if given by generators and their relations. [Adian 1957, Rabin 1958]

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

In computation, the groups are given as the **Cayley table**:

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Cayley table of the Klein four-group

- Input size of G: n^2.

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

In computation, the groups are given as the **Cayley table**:

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Cayley table of the Klein four-group

- Input size of G: n^2.
- "Efficient" algorithm: poly(n) steps.

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

In computation, the groups are given as the **Cayley table**:

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Cayley table of the Klein four-group

- Input size of G: n^2.
- "Efficient" algorithm: poly(n) steps.
- Current best algorithm: $n^{O(\log(n))}$ steps (Quasipolynomial).

The Group Isomorphism Problem

The Group Isomorphism Problem:
Given two groups G and H of order n, decide whether they are isomorphic.

In computation, the groups are given as the **Cayley table**:

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

Cayley table of the Klein four-group

- Input size of G: n^2.
- "Efficient" algorithm: poly(n) steps.
- Current best algorithm: $n^{O(\log(n))}$ steps (Quasipolynomial).
- Efficient algorithm for abelian groups.
- Barely improved from the brute-force algorithm for class 2 groups of exponent p. (Believed hard instance)

Algorithms for Pseudo-isometry Testing

Pseudo-isometry Testing:
Given $\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$, decide whether $\mathbb{G}$ and $\mathbb{H}$ are pseudo-isometric.

- Testing isomorphism for p-groups of class 2 and exponent p in polynomial time reduces to testing pseudo-isometry in time $q^{O(n+m)}$.

Algorithms for Pseudo-isometry Testing

Pseudo-isometry Testing:
Given $\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$, decide whether $\mathbb{G}$ and $\mathbb{H}$ are pseudo-isometric.

- Testing isomorphism for p-groups of class 2 and exponent p in polynomial time reduces to testing pseudo-isometry in time $q^{O(n+m)}$.
- Brute-force: $q^{n^2}\mathrm{poly}(n, m, \log q)$.

Algorithms for Pseudo-isometry Testing

Pseudo-isometry Testing:
Given $\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$, decide whether $\mathbb{G}$ and $\mathbb{H}$ are pseudo-isometric.

- Testing isomorphism for p-groups of class 2 and exponent p in polynomial time reduces to testing pseudo-isometry in time $q^{O(n+m)}$.
- Brute-force: $q^{n^2} \mathrm{poly}(n, m, \log q)$.
- Pseudo-isometry Testing should not be NP-hard under standard complexity assumptions (PH does not collapse to the second level).

Algorithms for Pseudo-isometry Testing

Pseudo-isometry Testing:
Given $\mathbb{G}, \mathbb{H} \in \Lambda(n, q)^m$, decide whether $\mathbb{G}$ and $\mathbb{H}$ are pseudo-isometric.

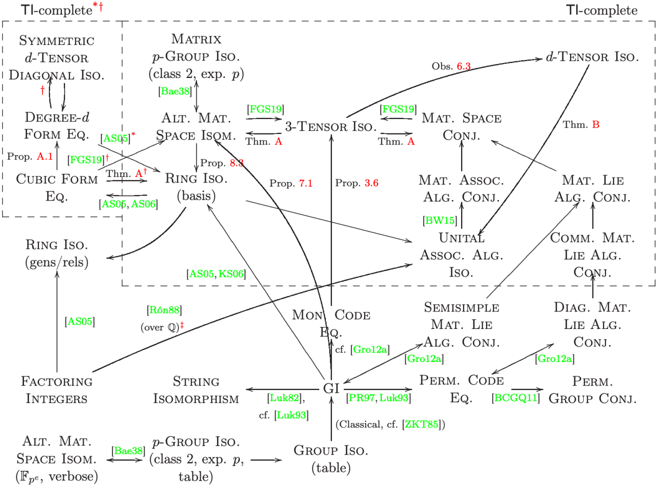
- Testing isomorphism for p-groups of class 2 and exponent p in polynomial time reduces to testing pseudo-isometry in time $q^{O(n+m)}$.
- Brute-force: $q^{n^2}\mathrm{poly}(n, m, \log q)$.
- Pseudo-isometry Testing should not be NP-hard under standard complexity assumptions (PH does not collapse to the second level).
- Slightly better bounds for pseudo-isometry testing:
  - $q^{\frac{1}{4}(n+m)^2+O(n+m)}$ for prime $q \geq 3$ [Rosenbaum 13]
  - $q^{\frac{1}{4}(n^2+m^2)+O(n+m)}$ [Li-Qiao 17]

Algorithms for Pseudo-isometry Testing

Pseudo-isometry Testing:
Given $\mathbb{G}, \mathbb{H} \in \Lambda(n,q)^m$, decide whether $\mathbb{G}$ and $\mathbb{H}$ are pseudo-isometric.

- Testing isomorphism for p-groups of class 2 and exponent p in polynomial time reduces to testing pseudo-isometry in time $q^{O(n+m)}$.
- Brute-force: $q^{n^2}\text{poly}(n, m, \log q)$.
- Pseudo-isometry Testing should not be NP-hard under standard complexity assumptions (PH does not collapse to the second level).
- Slightly better bounds for pseudo-isometry testing:
  - $q^{\frac{1}{4}(n+m)^2+O(n+m)}$ for prime $q \geq 3$ [Rosenbaum 13]
  - $q^{\frac{1}{4}(n^2+m^2)+O(n+m)}$ [Li-Qiao 17]
- Isometry testing for alternating matrix tuples can be done in $\text{poly}(n, m, q)$ for odd q [Brooksbank-Wilson 12, Ivanyos-Qiao 18].

Relations with Other Isomorphism Problems



Conclude in [Grochow-Qiao 2019].

Problem $A \to B$ means a polynomial-time algorithm of problem B can also solve problem A in polynomial time.

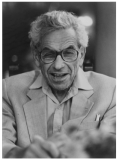
Average-case Algorithm

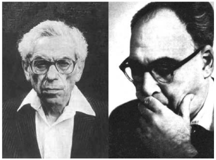
- Work for "almost all" instances sampled from a certain random model.

Average-case Algorithm

- Work for "almost all" instances sampled from a certain random model.

Random Graph Isomorphism [Babai-Erdős-Selkow 80]
For almost all graphs in the **Erdős-Rényi model**, testing isomorphism with any graph can be done in **linear** time.

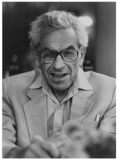



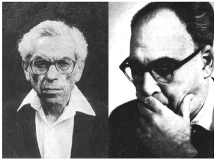


Average-case Algorithm

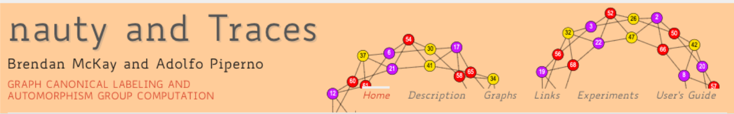
- Work for “almost all” instances sampled from a certain random model.

> **Random Graph Isomorphism** [Babai-Erdős-Selkow 80]
> For almost all graphs in the the **Erdős-Rényi model**, testing isomorphism with any graph can be done in **linear** time.



- Shares some ideas and techniques with practical algorithms.



Average-case Algorithm for Pseudo-isometry Testing

Theorem

For all but at most $1/q^{\Omega(nm)}$ fraction of $\mathbb{G} \in \Lambda(n, q)^m$, there is an algorithm which tests pseudo-isometry of $\mathbb{G}$ with an arbitrary $\mathbb{H} \in \Lambda(n, q)^m$ in time $q^{O(n+m)}$.

Average-case Algorithm for Pseudo-isometry Testing

Theorem

For all but at most $1/q^{\Omega(nm)}$ fraction of $\mathbb{G} \in \Lambda(n,q)^m$, there is an algorithm which tests pseudo-isometry of $\mathbb{G}$ with an arbitrary $\mathbb{H} \in \Lambda(n,q)^m$ in time $q^{O(n+m)}$.

The random model: Choose the strictly upper triangular parts from $\mathbb{F}_q$ independently and uniformly at random. Set the diagonal entries to 0, and the lower triangular entries according to the upper triangular ones.

$$\begin{bmatrix} 0 & \mathbf{x}_{1,2} & \mathbf{x}_{1,3} & \mathbf{x}_{1,4} \\ -\mathbf{x}_{1,2} & 0 & \mathbf{x}_{2,3} & \mathbf{x}_{2,4} \\ -\mathbf{x}_{1,3} & -\mathbf{x}_{2,3} & 0 & \mathbf{x}_{3,4} \\ -\mathbf{x}_{1,4} & -\mathbf{x}_{2,4} & -\mathbf{x}_{3,4} & 0 \end{bmatrix}$$

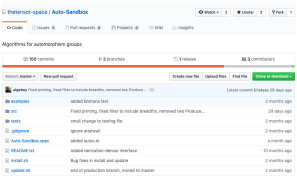
Average-case Algorithm for Pseudo-isometry Testing

Theorem
For all but at most $1/q^{\Omega(nm)}$ fraction of $\mathbb{G} \in \Lambda(n,q)^m$, there is an algorithm which tests pseudo-isometry of $\mathbb{G}$ with an arbitrary $\mathbb{H} \in \Lambda(n,q)^m$ in time $q^{O(n+m)}$.

The random model: Choose the strictly upper triangular parts from $\mathbb{F}_q$ independently and uniformly at random. Set the diagonal entries to 0, and the lower triangular entries according to the upper triangular ones.

$$\begin{bmatrix} 0 & \mathbf{x}_{1,2} & \mathbf{x}_{1,3} & \mathbf{x}_{1,4} \\ -\mathbf{x}_{1,2} & 0 & \mathbf{x}_{2,3} & \mathbf{x}_{2,4} \\ -\mathbf{x}_{1,3} & -\mathbf{x}_{2,3} & 0 & \mathbf{x}_{3,4} \\ -\mathbf{x}_{1,4} & -\mathbf{x}_{2,4} & -\mathbf{x}_{3,4} & 0 \end{bmatrix}$$

Practically Implemented using **Magma**.
(https://github.com/thetensor-space).



Key idea about Average-case Algorithms

- Define “easy to check” properties which hold for “almost all” objects sampled from the random model.
- For objects satisfying these properties, isomorphism can be checked “efficiently”.

Observation: If T is a pseudo-isometry from $\mathbb{G}$ to $\mathbb{H}$, for every $c \in [m]$, T is an **isometry** from $(G_1, \ldots, G_c)$ to some $(H'_1, \ldots, H'_c)$ in $\langle \mathbb{H} \rangle^c$.

Individualizing Alternating Matrix Tuples

Observation: If T is a pseudo-isometry from $\mathbb{G}$ to $\mathbb{H}$, for every $c \in [m]$, T is an **isometry** from $(G_1, \ldots, G_c)$ to some $(H'_1, \ldots, H'_c)$ in $\langle \mathbb{H} \rangle^c$.

To test pseudo-isometry, fix the images of $G_1, \ldots, G_c$.

$$\begin{array}{ccc} (G_1, & \cdots & G_c) \\ \downarrow & & \downarrow \\ (H'_1, & \cdots & H'_c) \end{array} \quad \in \langle \mathbb{H} \rangle^c$$

Individualizing Alternating Matrix Tuples

Observation: If T is a pseudo-isometry from $\mathbb{G}$ to $\mathbb{H}$, for every $c \in [m]$, T is an **isometry** from $(G_1, \ldots, G_c)$ to some $(H'_1, \ldots, H'_c)$ in $\langle \mathbb{H} \rangle^c$.

To test pseudo-isometry, fix the images of $G_1, \ldots, G_c$.

$$\begin{array}{cccc} (G_1, & \cdots & G_c) & \\ \downarrow & & \downarrow & \\ (H'_1, & \cdots & H'_c) & \in \langle \mathbb{H} \rangle^c \end{array}$$

Identify the isometry $T \in \mathrm{GL}(n, q)$:

$$(T^t G_1 T, \ldots, T^t G_c T) = (H'_1, \ldots, H'_c),$$

check if T is a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$. (By solving linear equations.)

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n, q)^m$ can be done in time $\text{poly}(n, m, q)$ when q is odd.
% The outputs are a coset representative and a set of generators.

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n, q)^m$ can be done in time poly(n, m, q) when q is odd.
% The outputs are a coset representative and a set of generators.

Pseudo-isometry Testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant c.

- Enumerate all c-tuples $\mathbb{H}_c$ in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n, q)^m$ can be done in time $\mathrm{poly}(n, m, q)$ when q is odd.
% The outputs are a coset representative and a set of generators.

Pseudo-isometry Testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant c.

- Enumerate all c-tuples $\mathbb{H}_c$ in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H_1', \ldots, H_c')$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Running time is dominated by two For-loops:

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n,q)^m$ can be done in time poly(n,m,q) when q is odd.
% The outputs are a coset representative and a set of generators.

Pseudo-isometry Testing for odd q

Input: $\mathbb{G} = (G_1, \dots, G_m), \mathbb{H} = (H_1, \dots, H_m) \in \Lambda(n,q)^m$, constant c.

- Enumerate all c-tuples $\mathbb{H}_c$ in $\langle H_1, \dots, H_m \rangle$;
- For each $\mathbb{H}_c = (H_1', \dots, H_c')$, test isometry with $\mathbb{G}_c = (G_1, \dots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Running time is dominated by two For-loops:

- Enumerate c-tuples: q^{cm}. % $H_i' = \alpha_{i,1} H_1 + \cdots + \alpha_{i,m} H_m$ for $i \in [c]$

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n,q)^m$ can be done in time poly(n,m,q) when q is odd.
% The outputs are a coset representative and a set of generators.

Pseudo-isometry Testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n,q)^m$, constant c.

- Enumerate all c-tuples $\mathbb{H}_c$ in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H_1', \ldots, H_c')$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Running time is dominated by two For-loops:

- Enumerate c-tuples: q^{cm}. % $H_i' = \alpha_{i,1}H_1 + \cdots + \alpha_{i,m}H_m$ for $i \in [c]$
- Enumerate Isometries: For each $\mathbb{H}_c$, $|\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|$.

The Main Algorithm

Theorem ([Brooksbank-Wilson 12, Ivanyos-Qiao 18])
Testing isometry of alternating matrix tuples in $\Lambda(n,q)^m$ can be done in time $\mathrm{poly}(n,m,q)$ when q is odd.
% The outputs are a coset representative and a set of generators.

Pseudo-isometry Testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n,q)^m$, constant c.

- Enumerate all c-tuples $\mathbb{H}_c$ in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Running time is dominated by two For-loops:

- Enumerate c-tuples: q^{cm}. % $H'_i = \alpha_{i,1} H_1 + \cdots + \alpha_{i,m} H_m$ for $i \in [c]$
- Enumerate Isometries: For each $\mathbb{H}_c$, $|\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|$.

$\forall\ \mathbb{H}_c,\ |\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}| \leq q^{O(n)} \Rightarrow$ time bound $q^{O(n+m)}$.

Given $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$,

$$\forall\ \mathbb{H}_c \in \langle \mathbb{H} \rangle^c,\ |\{T \in \mathrm{GL}(n, q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}| \leq q^{O(n)}$$

is not true in general.

Given $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$,

$$\forall\ \mathbb{H}_c \in \langle \mathbb{H} \rangle^c,\ |\{T \in \mathsf{GL}(n, q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}| \leq q^{O(n)}$$

is not true in general.

But it holds for any $\mathbb{G}$ chosen uniformly at random!

Average-case Analysis: Adjoint Algebra

Observation: For every $\mathbb{H}_c$,

$$\underbrace{|\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|}_{\text{Coset}} \leq \underbrace{|\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}|}_{\text{Autometry group}}$$

Claim:
For a random $\mathbb{G} \in \Lambda(n,q)^m$, with high probability we have

$$|\mathrm{Autm}(\mathbb{G}_c)| = |\{T \in \mathrm{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}| \leq q^{O(n)}.$$

Average-case Analysis: Adjoint Algebra

Observation: For every $\mathbb{H}_c$,

$$\underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|}_{\text{Coset}} \leq \underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}|}_{\text{Autometry group}}$$

Claim:
For a random $\mathbb{G} \in \Lambda(n,q)^m$, with high probability we have

$$|\mathrm{Autm}(\mathbb{G}_c)| = |\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}| \leq q^{O(n)}.$$

Random graphs have automorphism group size $O(1)$ with high probability [Erdős-Rényi 1963]

Average-case Analysis: Adjoint Algebra

Observation: For every $\mathbb{H}_c$,

$$\underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|}_{\text{Coset}} \leq \underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}|}_{\text{Autometry group}}$$

Claim:
For a random $\mathbb{G} \in \Lambda(n,q)^m$, with high probability we have

$$|\mathrm{Autm}(\mathbb{G}_c)| = |\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}| \leq q^{O(n)}.$$

The adjoint algebra and adjoint space:

$$\mathrm{Adj}(\mathbb{G}_c) = \{(A,D) \in \mathbb{M}(n,q) \oplus M(n,q) : A\mathbb{G}_c = \mathbb{G}_c D\}.$$

$$\mathrm{Adj}(\mathbb{G}_c, \mathbb{H}_c) = \{(A,D) \in \mathbb{M}(n,q) \oplus M(n,q) : A\mathbb{G}_c = \mathbb{H}_c D\}.$$

Average-case Analysis: Adjoint Algebra

Observation: For every $\mathbb{H}_c$,

$$\underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{H}_c\}|}_{\text{Coset}} \leq \underbrace{|\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}|}_{\text{Autometry group}}$$

> **Claim:**
> For a random $\mathbb{G} \in \Lambda(n,q)^m$, with high probability we have
>
> $$|\mathrm{Autm}(\mathbb{G}_c)| = |\{T \in \mathsf{GL}(n,q) : T^t \mathbb{G}_c T = \mathbb{G}_c\}| \leq q^{O(n)}.$$

The adjoint algebra and adjoint space:

$$\mathrm{Adj}(\mathbb{G}_c) = \{(A, D) \in \mathbb{M}(n,q) \oplus M(n,q) : A\mathbb{G}_c = \mathbb{G}_c D\}.$$

$$\mathrm{Adj}(\mathbb{G}_c, \mathbb{H}_c) = \{(A, D) \in \mathbb{M}(n,q) \oplus M(n,q) : A\mathbb{G}_c = \mathbb{H}_c D\}.$$

- $|\mathrm{Autm}(\mathbb{G}_c)| \leq |\mathrm{Adj}(\mathbb{G}_c)|$ as $T \in \mathrm{Autm}(\mathbb{G}_c) \Rightarrow (T^t, T^{-1}) \in \mathrm{Adj}(\mathbb{G}_c)$.
- If $\mathbb{G}_c$ and $\mathbb{H}_c$ are isometric, $|\mathrm{Adj}(\mathbb{G}_c, \mathbb{H}_c)| = |\mathrm{Adj}(\mathbb{G}_c)|$
- Can be efficiently computed by solving systems of linear equations.

Average-case Analysis: Stable Alternating Tuples

Stable (Alternating) matrix tuple:

For every nontrivial subspace U of $\mathbb{F}_q^n$,

$$\dim(\mathbb{G}_c(U)) = \dim(\langle G_1 U, \ldots, G_c U \rangle) > \dim(U).$$

% The stable concept comes from geometric invariant theory.

Average-case Analysis: Stable Alternating Tuples

Stable (Alternating) matrix tuple:

For every nontrivial subspace U of $\mathbb{F}_q^n$,

$$\dim(\mathbb{G}_c(U)) = \dim(\langle G_1 U, \ldots, G_c U \rangle) > \dim(U).$$

% The stable concept comes from geometric invariant theory.

- If $\mathbb{G}_c$ is stable, then every nonzero elements in $\mathrm{Adj}(\mathbb{G}_c)$ is invertible. (Exercise!)

Average-case Analysis: Stable Alternating Tuples

Stable (Alternating) matrix tuple:

For every nontrivial subspace U of $\mathbb{F}_q^n$,

$$\dim(\mathbb{G}_c(U)) = \dim(\langle G_1 U, \ldots, G_c U \rangle) > \dim(U).$$

% The stable concept comes from geometric invariant theory.

- If $\mathbb{G}_c$ is stable, then every nonzero elements in $\mathrm{Adj}(\mathbb{G}_c)$ is invertible. (Exercise!)
- $\mathrm{Adj}(\mathbb{G}_c)$ is a finite division algebra over $\mathbb{F}_q$ which contains identity.

Average-case Analysis: Stable Alternating Tuples

Stable (Alternating) matrix tuple:

For every nontrivial subspace U of $\mathbb{F}_q^n$,

$$\dim(\mathbb{G}_c(U)) = \dim(\langle G_1 U, \ldots, G_c U\rangle) > \dim(U).$$

% The stable concept comes from geometric invariant theory.

- If $\mathbb{G}_c$ is stable, then every nonzero elements in $\mathrm{Adj}(\mathbb{G}_c)$ is invertible. (Exercise!)
- $\mathrm{Adj}(\mathbb{G}_c)$ is a finite division algebra over $\mathbb{F}_q$ which contains identity.
- $\mathrm{Adj}(\mathbb{G}_c)$ is a field by Wedderburn's little theorem. And we can conclude

Theorem: $\mathbb{G}_c$ is stable $\Rightarrow$ $|\mathrm{Adj}(\mathbb{G}_c)| \leq q^n$.

Upper Bound the Probability of being Unstable

Claim: With probability $1 - \frac{1}{q^{\Omega(n)}}$, a random $\mathbb{G}_c$ is stable.

Upper Bound the Probability of being Unstable

Claim: With probability $1 - \frac{1}{q^{\Omega(n)}}$, a random $\mathbb{G}_c$ is stable.

- Convert 4 random alternating matrices into 1 random matrix.
- Upper bound the probability of a random tuple of 5 matrices being nonstable.

Upper Bound the Probability of being Unstable

Claim: With probability $1 - \frac{1}{q^{\Omega(n)}}$, a random $\mathbb{G}_c$ is stable.

- Convert 4 random alternating matrices into 1 random matrix.
- Upper bound the probability of a random tuple of 5 matrices being nonstable.

Theorem:
For $c \geq 20$, with probability $1 - \frac{1}{q^{\Omega(n)}}$, a random $\mathbb{G}_c \in \Lambda(n, q)^c$ satisfies $|\mathrm{Autm}(\mathbb{G}_c)| \leq q^{O(n)}$.

The Main Algorithm, Revisited

Pseudo-isometry testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant c.

- Enumerate all c-tuples in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H_1', \ldots, H_c')$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

The Main Algorithm, Revisited

Pseudo-isometry testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant $c \geq 20$.

- Compute a generating set of $\mathrm{Autm}(\mathbb{G}_c)$;
- If $|\mathrm{Autm}((G_1, \ldots, G_c))| > q^n$, terminate;
- Enumerate all c-tuples in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

The Main Algorithm, Revisited

Pseudo-isometry testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant $c \geq 20$.

- Compute a generating set of $\mathrm{Autm}(\mathbb{G}_c)$;
- If $|\mathrm{Autm}((G_1, \ldots, G_c))| > q^n$, terminate;
- Enumerate all c-tuples in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Theorem

For odd q and $m \geq 20$, the above algorithm tests pseudo-isometry for almost but $\frac{1}{q^{\Omega(n)}}$ fraction of $\mathbb{G} \in \Lambda(n, q)^m$ with arbitrary $\mathbb{H} \in \Lambda(n, q)^m$ in time $q^{O(n+m)}$.

The Main Algorithm, Revisited

Pseudo-isometry testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant $c \geq 20$.

- Compute a generating set of $\mathrm{Autm}(\mathbb{G}_c)$;
- If $|\mathrm{Autm}((G_1, \ldots, G_c))| > q^n$, terminate;
- Enumerate all c-tuples in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Theorem

For odd q and $m \geq 20$, the above algorithm tests pseudo-isometry for almost but $\frac{1}{q^{\Omega(n)}}$ fraction of $\mathbb{G} \in \Lambda(n, q)^m$ with arbitrary $\mathbb{H} \in \Lambda(n, q)^m$ in time $q^{O(n+m)}$.

- odd $q \Rightarrow$ all q: Replace all isometry tests by computing adjoint algebra and adjoint space.

The Main Algorithm, Revisited

Pseudo-isometry testing for odd q

Input: $\mathbb{G} = (G_1, \ldots, G_m), \mathbb{H} = (H_1, \ldots, H_m) \in \Lambda(n, q)^m$, constant $c \geq 20$.

- Compute a generating set of $\mathrm{Autm}(\mathbb{G}_c)$;
- If $|\mathrm{Autm}((G_1, \ldots, G_c))| > q^n$, terminate;
- Enumerate all c-tuples in $\langle H_1, \ldots, H_m \rangle$;
- For each $\mathbb{H}_c = (H'_1, \ldots, H'_c)$, test isometry with $\mathbb{G}_c = (G_1, \ldots, G_c)$;
- If they are isometric, check whether every isometry T is also a pseudo-isometry between $\mathbb{G}$ and $\mathbb{H}$.

Theorem

For odd q and $m \geq 20$, the above algorithm tests pseudo-isometry for almost but $\frac{1}{q^{\Omega(n)}}$ fraction of $\mathbb{G} \in \Lambda(n, q)^m$ with arbitrary $\mathbb{H} \in \Lambda(n, q)^m$ in time $q^{O(n+m)}$.

- odd $q \Rightarrow$ all q: Replace all isometry tests by computing adjoint algebra and adjoint space.
- $\frac{1}{q^{\Omega(n)}} \Rightarrow \frac{1}{q^{\Omega(nm)}}$: Enumerate all c-tuples of $\mathbb{G}$ until one stable tuple is found.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.
- Reduce the enumeration cost: Choose low-rank matrices.

  % When q is small, #low-rank matrices in a random alternating tuple is expected to be much smaller than q^m and no less than 3.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.
- Reduce the enumeration cost: Choose low-rank matrices.
  % When q is small, #low-rank matrices in a random alternating tuple is expected to be much smaller than q^m and no less than 3.

Experiments:

- Randomly generate $\mathbb{G}, \mathbb{H} \in \Lambda(5,3)^4$ and test isometry.
- Randomly generate $\mathbb{G} \in \Lambda(5,3)^4$ and $T \in \mathrm{GL}(5,3)$ and test isometry between $\mathbb{G}$ and $T^t \mathbb{G} T$.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.
- Reduce the enumeration cost: Choose low-rank matrices.
  % When q is small, #low-rank matrices in a random alternating tuple is expected to be much smaller than q^m and no less than 3.

Experiments:

- Randomly generate $\mathbb{G}, \mathbb{H} \in \Lambda(5,3)^4$ and test isometry.
- Randomly generate $\mathbb{G} \in \Lambda(5,3)^4$ and $T \in \mathrm{GL}(5,3)$ and test isometry between $\mathbb{G}$ and $T^t \mathbb{G} T$.

Brute-force: Fail to complete. % $5^{10} \ll 3^{25}$

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.
- Reduce the enumeration cost: Choose low-rank matrices.

  % When q is small, #low-rank matrices in a random alternating tuple is expected to be much smaller than q^m and no less than 3.

Experiments:

- Randomly generate $\mathbb{G}, \mathbb{H} \in \Lambda(5,3)^4$ and test isometry.
- Randomly generate $\mathbb{G} \in \Lambda(5,3)^4$ and $T \in \mathrm{GL}(5,3)$ and test isometry between $\mathbb{G}$ and $T^t \mathbb{G} T$.

Brute-force: Fail to complete. % $5^{10} \ll 3^{25}$

Our (Modified) Algorithm: Complete with correct answer in 2 minutes.

Practical Implementation

Implementation Trick:

- Tolerable enumeration in a laptop: 5^{10}.
- Solution: $c = 3$ is normally sufficient in practice.
- Reduce the enumeration cost: Choose low-rank matrices.
  % When q is small, #low-rank matrices in a random alternating tuple is expected to be much smaller than q^m and no less than 3.

Experiments:

- Randomly generate $\mathbb{G}, \mathbb{H} \in \Lambda(5,3)^4$ and test isometry.
- Randomly generate $\mathbb{G} \in \Lambda(5,3)^4$ and $T \in \mathrm{GL}(5,3)$ and test isometry between $\mathbb{G}$ and $T^t \mathbb{G} T$.

Brute-force: Fail to complete. % $5^{10} \ll 3^{25}$

Our (Modified) Algorithm: Complete with correct answer in 2 minutes.

Other results (not in this talk)

- A general strategy for group isomorphism which combines recent algebraic techniques with the Weisfeiler-Leman refinement technique for Graph Isomorphism.
- A new random model for finite groups, and average-case results to support the "filter and WL" refinement.
- Worst-case polynomial-time algorithms for testing isomorphism of groups with "genus-2 radicals".

arXiv:1905.02518

Thanks for your Attention!