Algorithms for Matrix Code and Alternating Trilinear Form Equivalences via New Isomorphism Invariants

Anand Kumar Narayanan [1] Youming Qiao [2] Gang Tang [2,3]

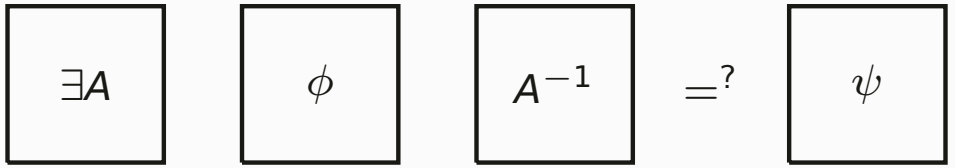
[1]SandboxAQ

[2]University of Technology Sydney

[3]University of Birmingham

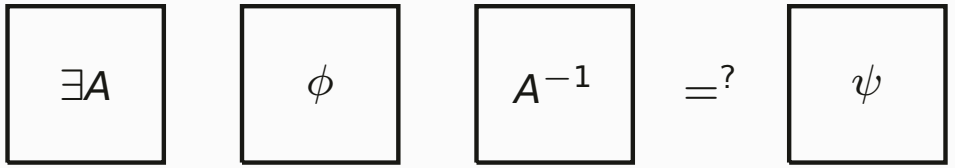
Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an A such that



Three is a shroud!

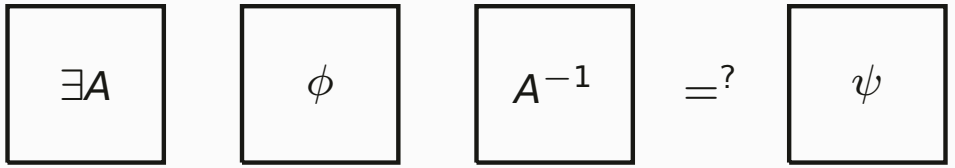
Given two square matrices ϕ and ψ, can we tell if there is an A such that



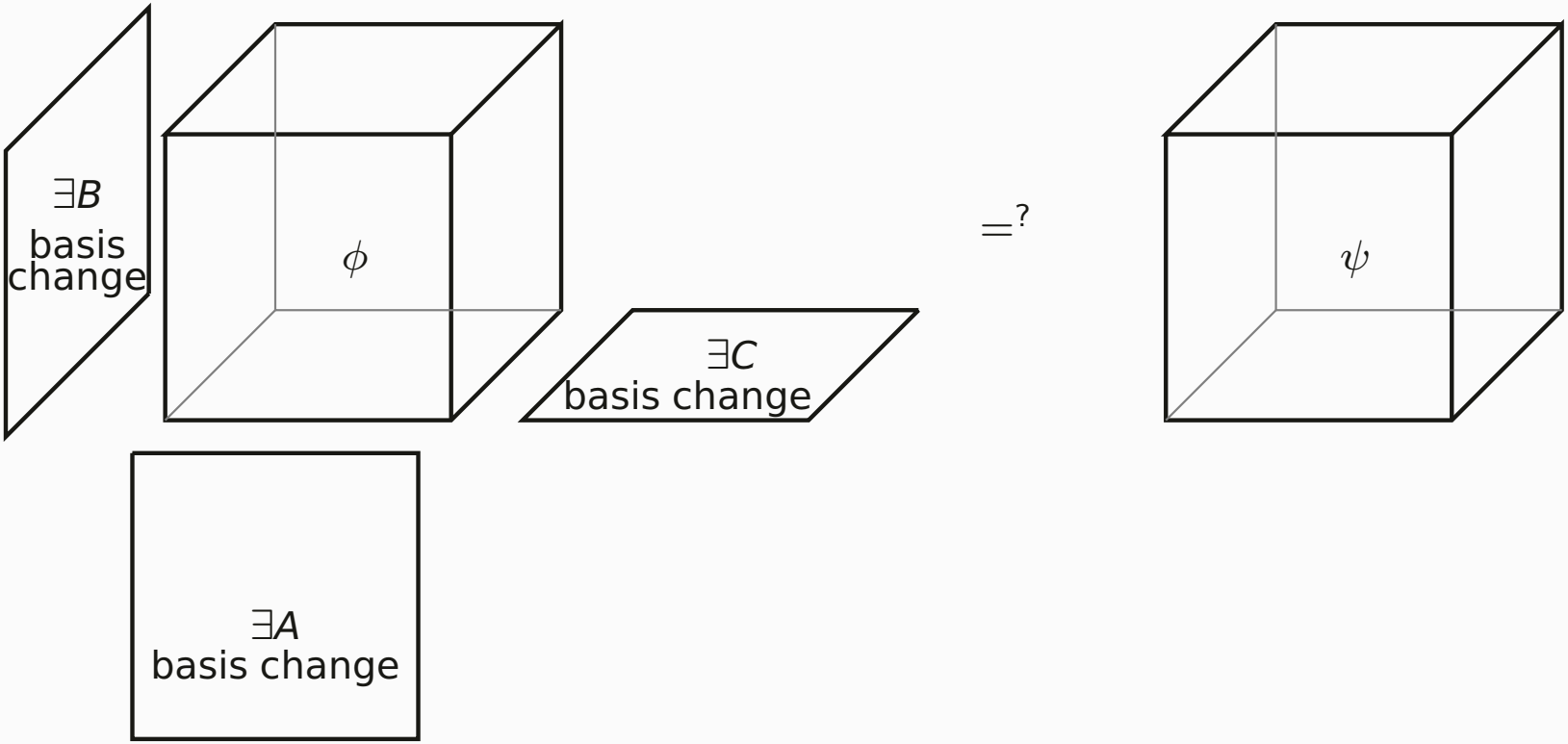
Yes, quickly!

Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an A such that

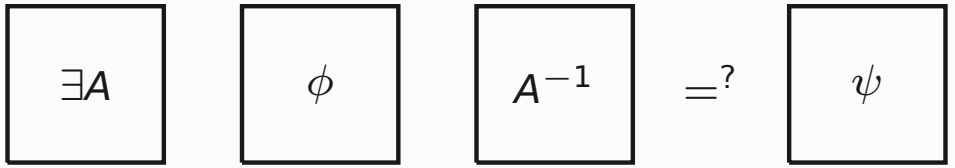


Yes, quickly! Given two tensors, is there a basis change taking one to the other?

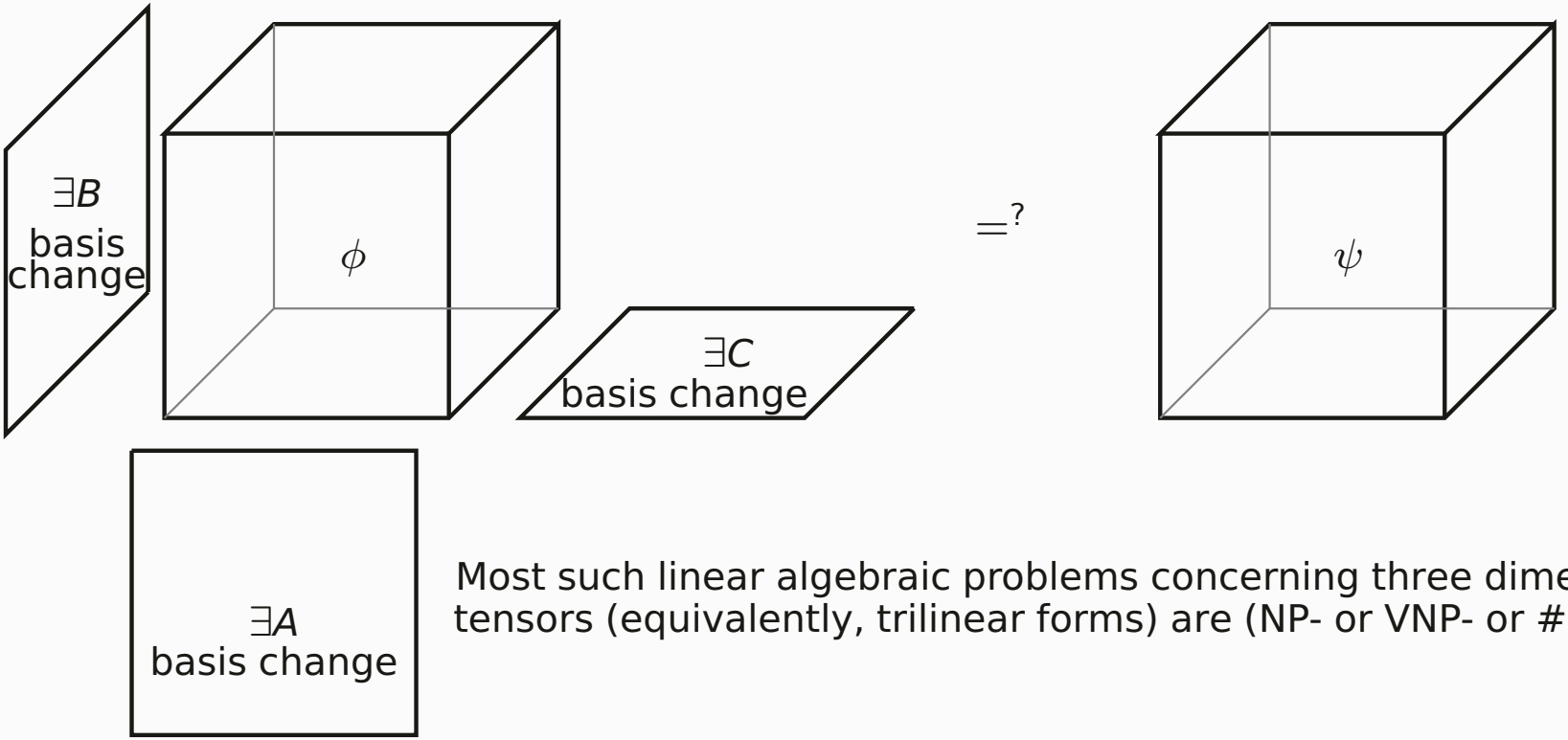


Three is a shroud!

Given two square matrices ϕ and ψ, can we tell if there is an A such that

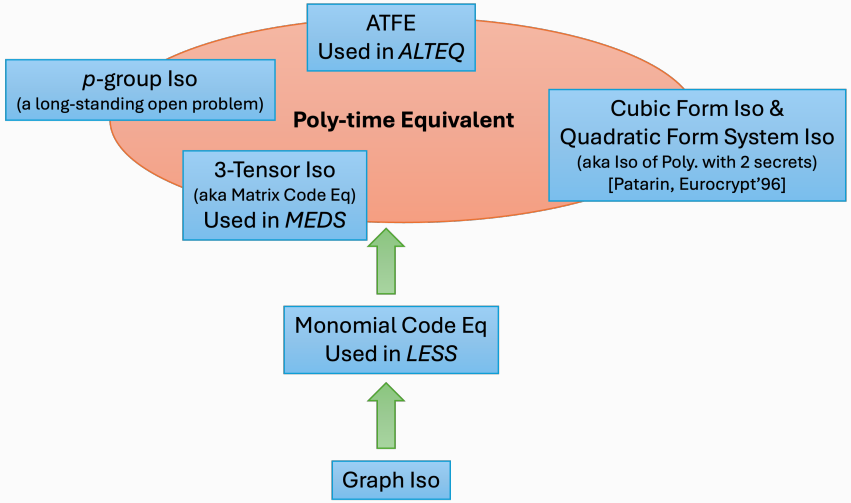


Yes, quickly! Given two tensors, is there a basis change taking one to the other?



Most such linear algebraic problems concerning three dimensional tensors (equivalently, trilinear forms) are (NP- or VNP- or #P-)hard.

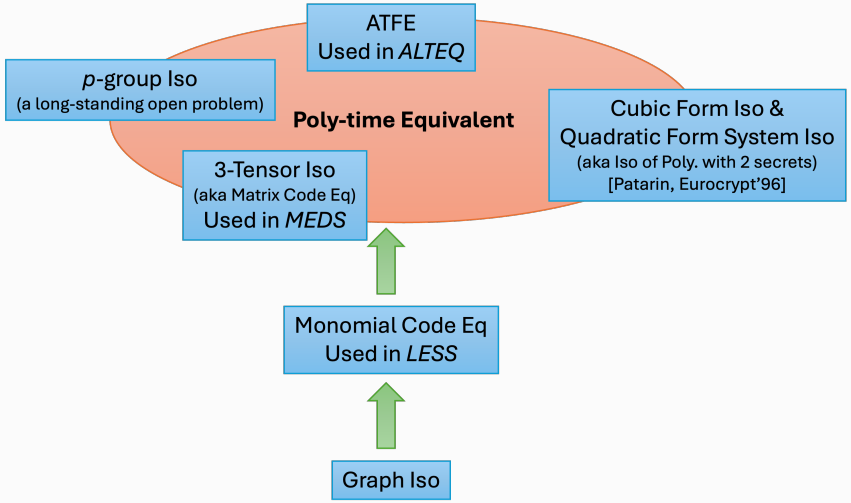
A web of complexity theoretic reductions connect the tensor isomorphism problem over finite fields (see the series ((ITCS 2021) I,II,III,IV) of papers by Grochow and Qiao), on whose hardness NIST on-ramp signatures MEDS, ALTEQ, etc. are built.



We present new algorithms for finding isomorphisms of tensors (equivalently, trilinear forms) over finite fields.

- polynomially faster than previously known
- informs the security/parameters of NIST on-ramp signatures
  - bit security of MEDS cut in half asymptotically, and suggest an easy fix
  - ALTEQ took our algorithm into account in designing the parameters
- new efficiently computable distinguishing invariants
- builds on algorithms by Bouillaguet, Fouque, and Véber (Eurocrypt 2013), and Beullens (Crypto 2023).

A web of complexity theoretic reductions connect the tensor isomorphism problem over finite fields (see the series ((ITCS 2021) I,II,III,IV) of papers by Grochow and Qiao), on whose hardness NIST on-ramp signatures MEDS, ALTEQ, etc. are built.



We present new algorithms for finding isomorphisms of tensors (equivalently, trilinear forms) over finite fields.

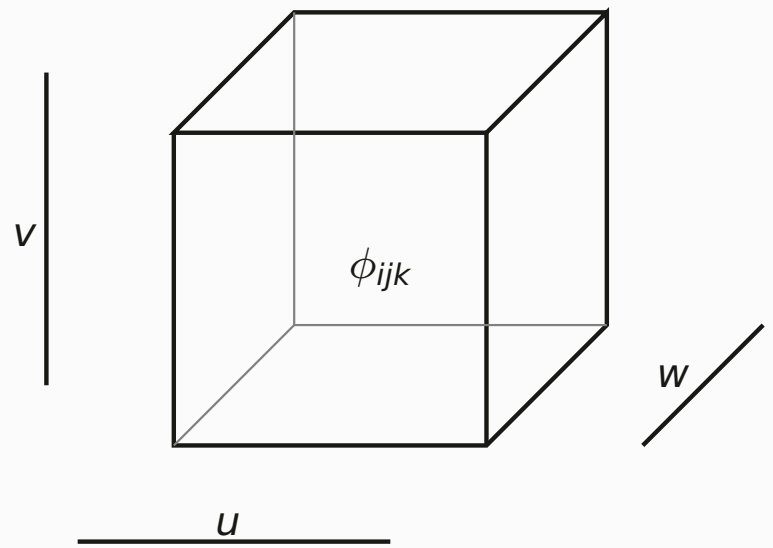
- polynomially faster than previously known
- informs the security/parameters of NIST on-ramp signatures
  - bit security of MEDS cut in half asymptotically, and suggest an easy fix
  - ALTEQ took our algorithm into account in designing the parameters
- new efficiently computable distinguishing invariants
- builds on algorithms by Bouillaguet, Fouque, and Véber (Eurocrypt 2013), and Beullens (Crypto 2023).

Trilinear forms

A trilinear form is a function

$$\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$
$$(u, v, w) \longmapsto \sum_i \sum_j \sum_k \phi_{ijk} u_i v_j w_k$$

that is linear in each of its three arguments. Think of it as an $n \times n \times n$ cube



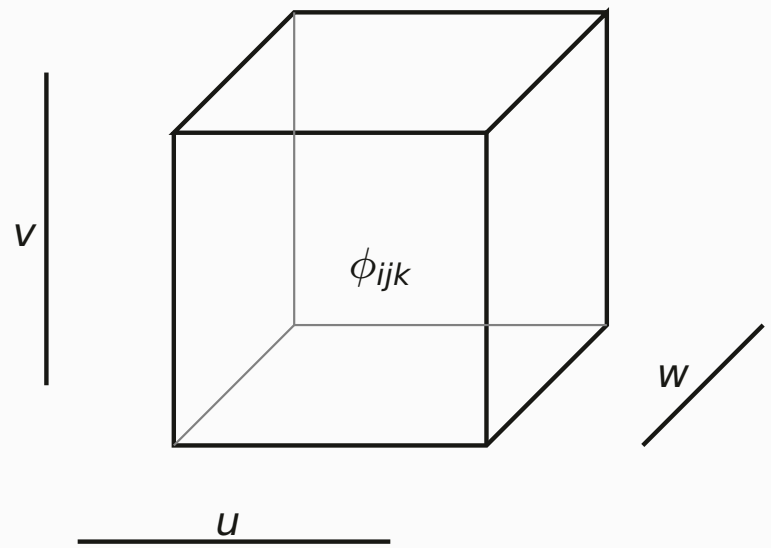
of $\mathbb{F}_q$ elements.

Trilinear forms

A trilinear form is a function

$$\phi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$
$$(u, v, w) \longmapsto \sum_i \sum_j \sum_k \phi_{ijk} u_i v_j w_k$$

that is linear in each of its three arguments. Think of it as an $n \times n \times n$ cube



of $\mathbb{F}_q$ elements. It is alternating if it satisfies the anti-symmetry constraint

$$\phi(u, u, w) = \phi(u, v, v) = \phi(w, v, w) = 0, \forall u, v, w \in \mathbb{F}_q^n.$$

Tensor Isomorphism (MEDS variant).

Triples of invertible matrices $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ act on tensors by basis change

$$((A, B, C), \phi(\star, \star, \star)) \longmapsto \phi^{A,B,C} := \phi(A\star, B\star, C\star)$$

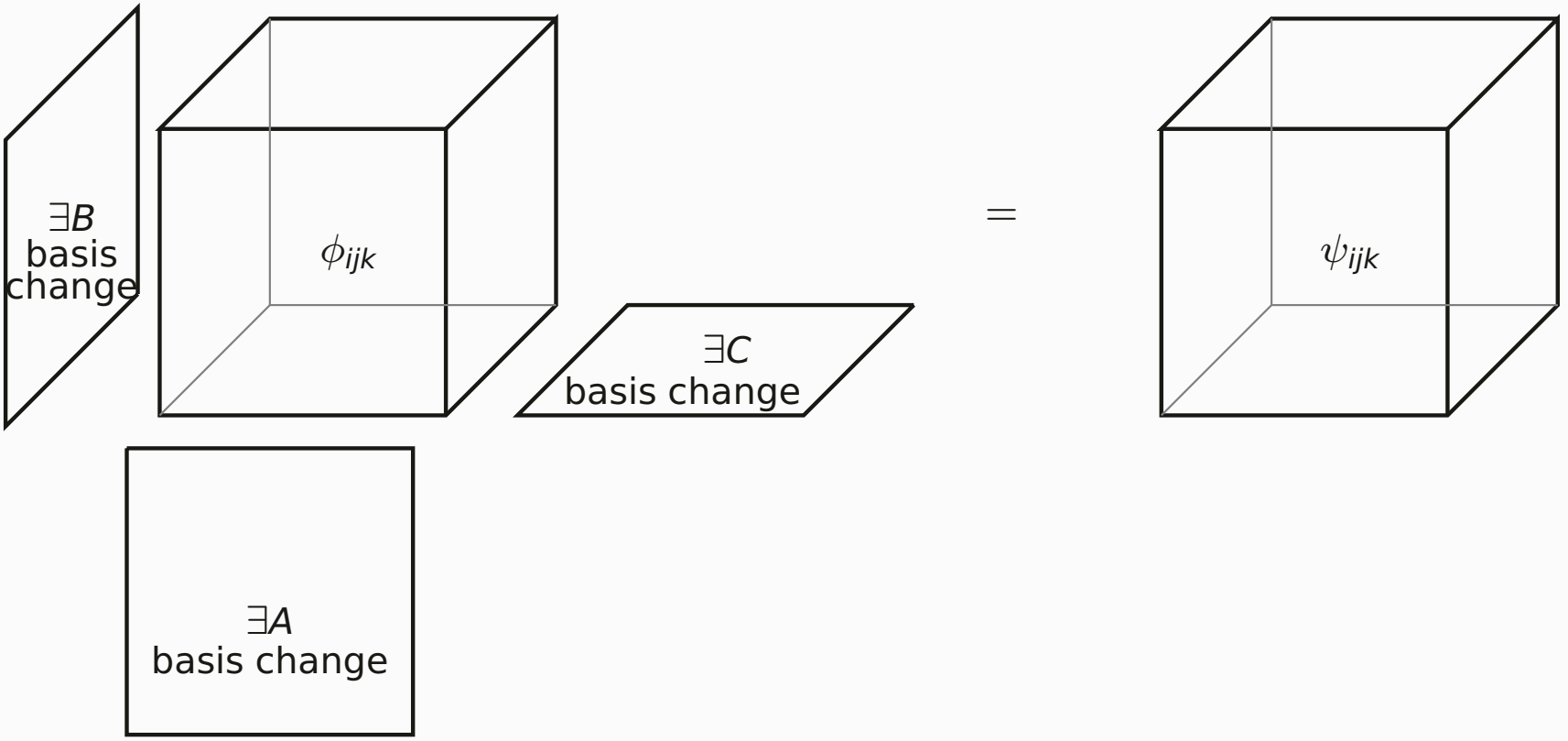
on the respective three dimensions.

Tensor Isomorphism (MEDS variant).

Triples of invertible matrices $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ act on tensors by basis change

$$((A, B, C), \phi(\star, \star, \star)) \longmapsto \phi^{A,B,C} := \phi(A\star, B\star, C\star)$$

on the respective three dimensions. Two forms ϕ, ψ are isomorphic if there exists such a basis change $(A, B, C) \in GL_n(\mathbb{F}_q)^3$ taking one to the other, as pictured.



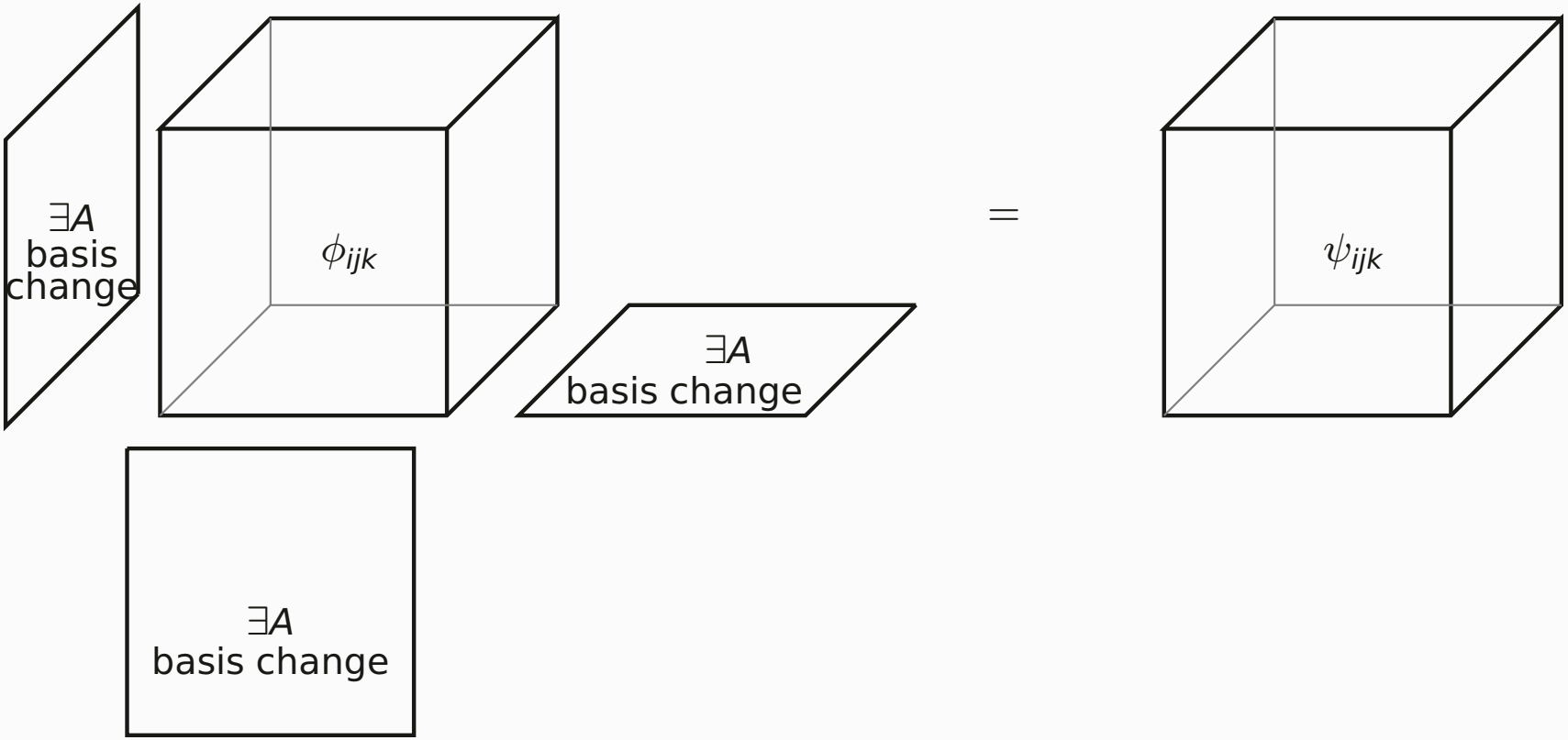
Given two isomorphic tensors, find an isomorphism between them (if it exists).

Tensor Isomorphism (ALTEQ variant).

Invertible matrices $A \in GL_n(\mathbb{F}_q)$ act on alternating tensors by the same basis change

$$(A, \phi(\star,\star,\star)) \longmapsto \phi^A := \phi(A\star, A\star, A\star)$$

on each of the three dimensions. Two alternating trilinear forms ϕ, ψ are isomorphic if there exists such a basis change $A \in GL_n(\mathbb{F}_q)$ taking one to the other, as pictured.



Given two isomorphic alternating tensors, find an isomorphsim between them (if it exists).

Finding tensor isomorphism (MEDS variant)

We design a fast computable invariant, pairing trilinear forms ϕ with co-rank one projective points $\hat{u} \in \mathbb{P}(\mathbb{F}_q^n)$,

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle$$

Finding tensor isomorphism (MEDS variant)

We design a fast computable invariant, pairing trilinear forms ϕ with co-rank one projective points $\hat{u} \in \mathbb{P}(\mathbb{F}_q^n)$,

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle$$

satisfying, for all $\phi, \hat{u}, A, B, C$,

$$\langle \phi, \hat{u} \rangle = \left\langle \phi^{A,B,C}, A^{-1}\hat{u} \right\rangle .$$

Finding tensor isomorphism (MEDS variant)

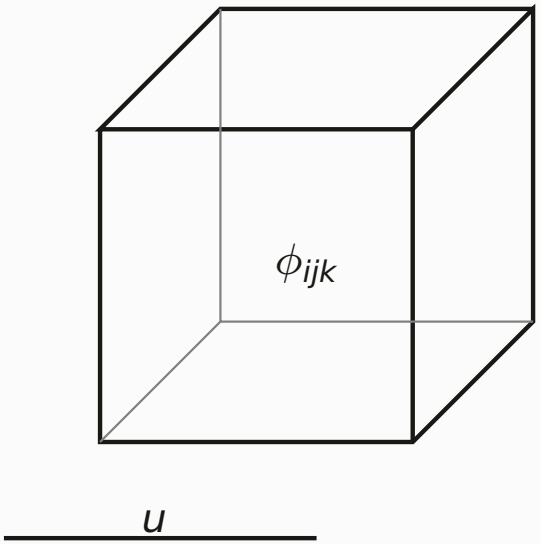
We design a fast computable invariant, pairing trilinear forms ϕ with co-rank one projective points $\hat{u} \in \mathbb{P}(\mathbb{F}_q^n)$,

$$(\phi, \hat{u}) \longmapsto \langle \phi, \hat{u} \rangle$$

satisfying, for all $\phi, \hat{u}, A, B, C$,

$$\langle \phi, \hat{u} \rangle = \left\langle \phi^{A,B,C}, A^{-1}\hat{u} \right\rangle .$$

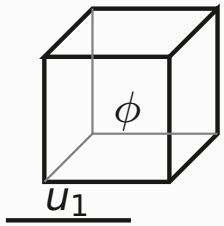
Co-rank one points are $u \in \mathbb{F}_q^n$ such that $\phi(u, \star, \star)$ is co-rank one. That is, the matrix



has rank $n - 1$. Denote the set of projective co-rank 1 vectors $\hat{u}$ as $\mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.

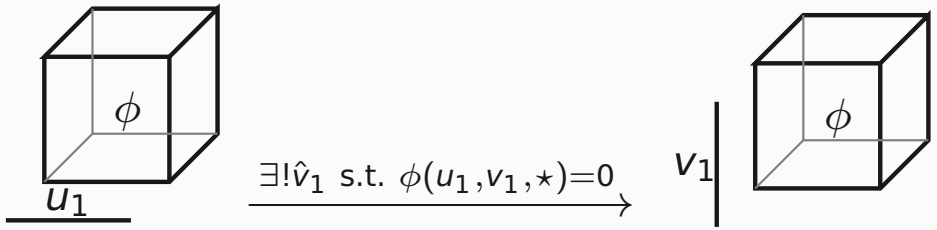
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.



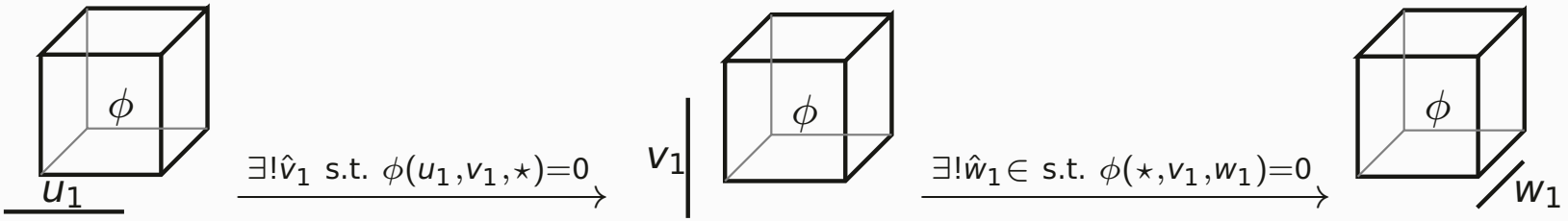
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.



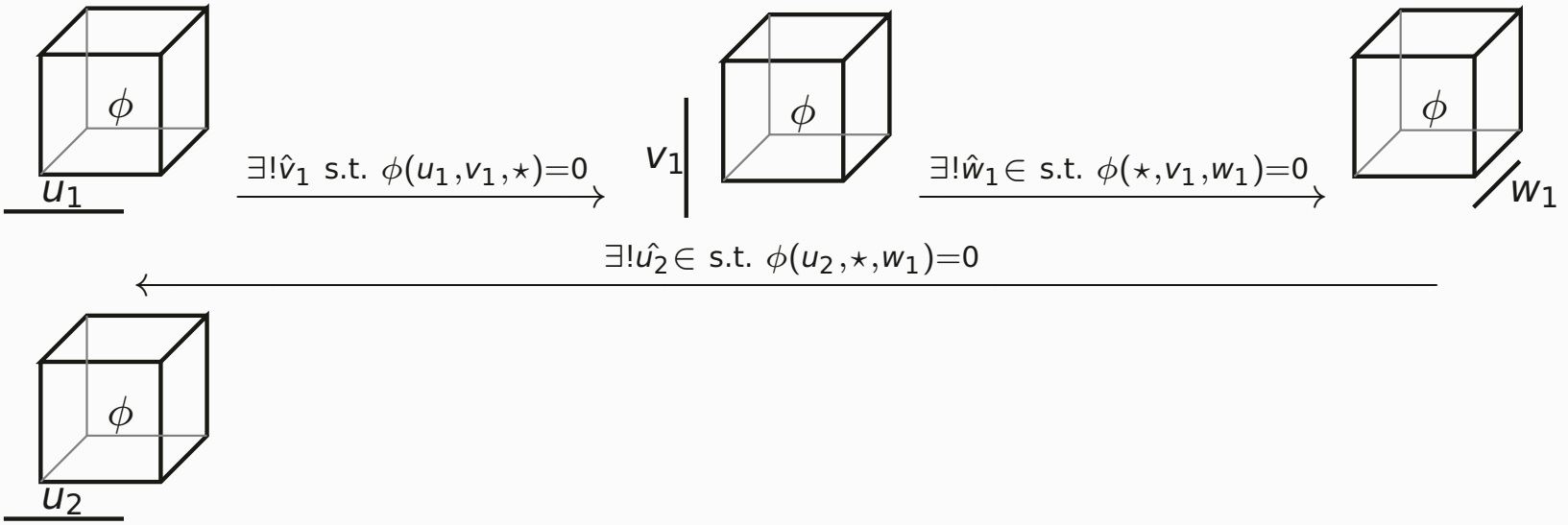
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.



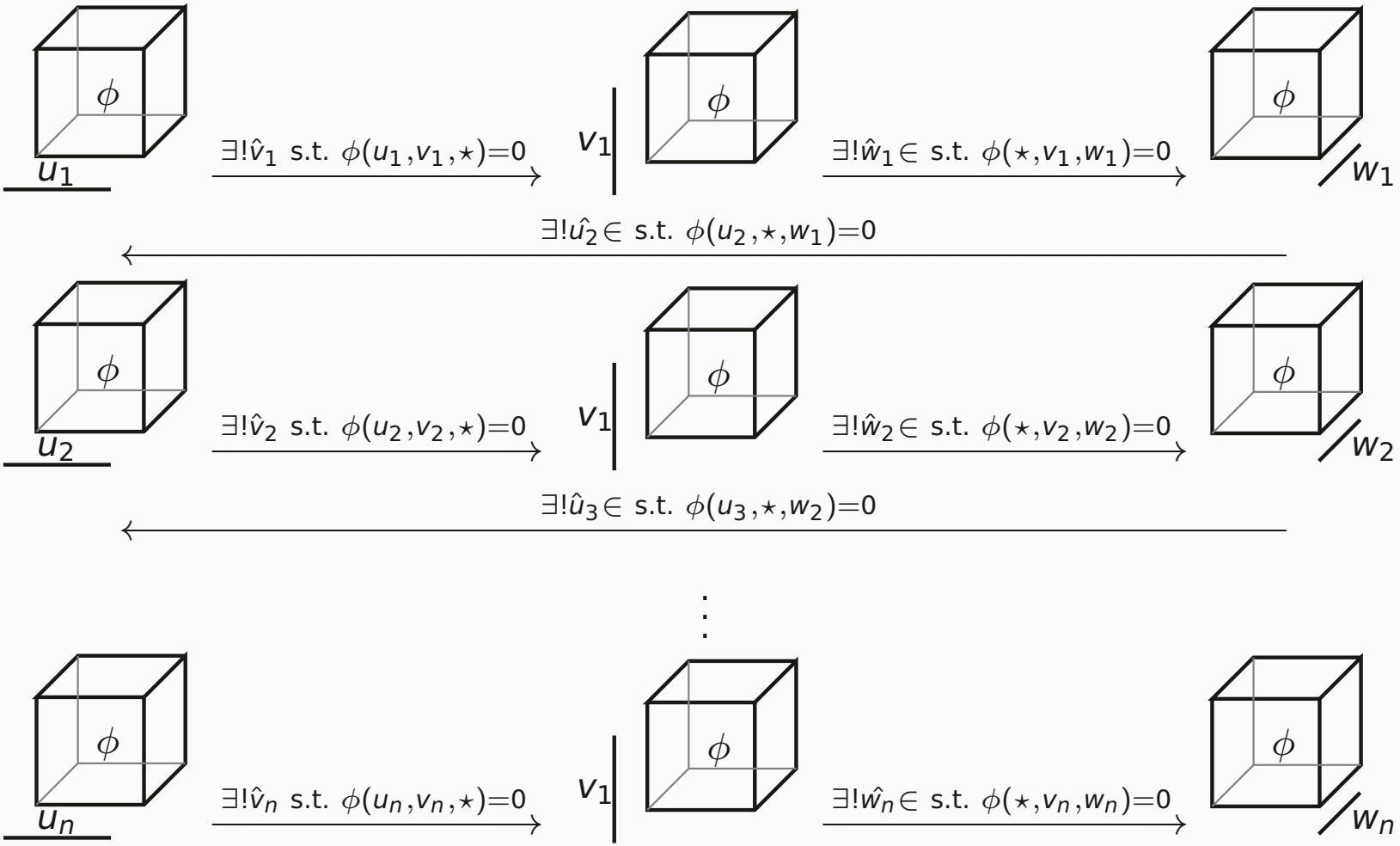
Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.



Constructing the invariant

Start with a co-rank one $\hat{u} = \hat{u}_1 \in \mathbb{P}_\phi \subseteq \mathbb{P}(\mathbb{F}_q^n)$.



$U = \{u_1, u_2, \ldots, u_n\}$ $V = \{v_1, v_2, \ldots, v_n\}$ $W = \{w_1, w_2, \ldots, w_n\}$

Constructing the invariant

If each list U, V, W has n-linearly independent vectors, then we can construct three unique invertible matrices A_U, B_V, C_W to act. The resulting tensor

$$\left\langle \phi, \hat{u} \right\rangle := \phi^{A_U, B_V, C_W}$$

(not merely the isomorphism class) is the invariant. Some subtle choices are made to resolve the ambiguity from the representatives of the projective points.

Constructing the invariant

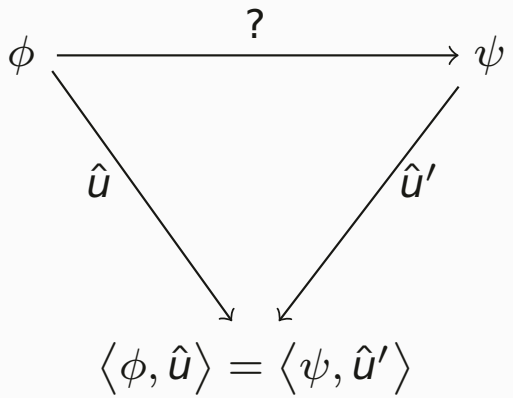
If each list U, V, W has n-linearly independent vectors, then we can construct three unique invertible matrices A_U, B_V, C_W to act. The resulting tensor

$$\langle \phi, \hat{u} \rangle := \phi^{A_U, B_V, C_W}$$

(not merely the isomorphism class) is the invariant. Some subtle choices are made to resolve the ambiguity from the representatives of the projective points.

Algorithm: Input ϕ, ψ.

Sample from $\left\{ \langle \phi, \hat{u} \rangle, \hat{u} \in \mathbb{P}_\phi \right\}$ and $\left\{ \langle \psi, \hat{u}' \rangle, \hat{u}' \in \mathbb{P}_\psi \right\}$ to look for a collision



Roughly $\sqrt{|\mathbb{P}_\phi|} \approx \sqrt{|\mathbb{P}_\psi|} \approx q^{\frac{n-2}{2}}$ samples each suffice.

Runtime

Assuming certain heuristics, the expected runtime of our algorithm is

$$O(q^{\frac{n-2}{2}} \cdot (q \cdot n^3 + n^4) \cdot (\log(q))^2).$$

Consequently, the bit security estimates of the MEDS scheme is reduced, as indicated in the table below.

parameter set	n	q	**Algebraic**	**Leon-like**	**Ours**
MEDS-I	14	4093	148.1	170.68	102.59
MEDS-III	22	4093	218.41	246.95	152.55
MEDS-V	30	2039	298.82	297.77	186.57

Remedy. Enlarge q (doubling bit length asymptotically) to meet the security demand. Does not affect the running times much, but increases the signature size.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Find a collision $\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Find a collision $\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Heuristic runtime: Roughly $q^{k/2}$ times the cost to sample co-rank r points, assuming canonical forms. Already taken into account in the design of ALTEQ.

Finding tensor isomorphism (ALTEQ variant)

For a projective point $\hat{u}$ of large co-rank r, let $K_{\hat{u}} := \ker(\phi(u, \star, \star))$. Then

$$(\phi, \hat{u}) \longmapsto \left\langle \phi, \hat{u} \right\rangle := (\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q) \bmod (GL(K_{\hat{u}}) \times GL(n, q))$$

is an invariant. On the right is the isomorphism class of the restriction $\phi : K_{\hat{u}} \times \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ modulo $GL(K_{\hat{u}})$ acting on the first dimension and $GL(n, q)$ acting on the other two.

Given $(\hat{u}, \hat{u}')$ as partial information, we can test using Gröbner basis if

$$\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle .$$

Isomorphism testing the tensor restriction $\Rightarrow$? Canonical forms.

Algorithm. Input two alternating trilinear forms ϕ, ψ. Let the number of co-rank r points roughly be q^k.

- Sample a set U_ϕ of $q^{k/2}$ co-rank r points with respect to ϕ.
- Sample a set U_ψ of $q^{k/2}$ co-rank r points with respect to ψ.
- Find a collision $\left\langle \phi, \hat{u} \right\rangle =_? \left\langle \psi, \hat{u}' \right\rangle$ for some $\hat{u} \in U_\phi$ and $\hat{u}' \in U_\psi$.

Heuristic runtime: Roughly $q^{k/2}$ times the cost to sample co-rank r points, assuming canonical forms. Already taken into account in the design of ALTEQ.

Quantum Collision Finding

Using Szegedy's quantum random walks or Tani's claw finding, we get cubic (instead of quadratic) speedups on quantum computers.

Quantum Collision Finding

Using Szegedy's quantum random walks or Tani's claw finding, we get cubic (instead of quadratic) speedups on quantum computers.

An Open Problem

Tensor isomorphism problems are easy to phrase as hidden subgroup problems over (products of) general linear groups. General linear groups are notorious hard cases, due to large dimensional irreducible representations.

Do generic hidden subgroup problems over general linear groups reduce to tensor isomorphism problems?