Tensors and Graphs II: questions and techniques

Training Workshop at Tensors: Algebra-Geometry-Applications

Youming Qiao
University of Technology Sydney

30 May 2024

Last lecture

* Recipes of constructing tensors from graphs

* Three correspondences of structures

Graphs	Tensors
Perfect matching	Non-zero det
Isomorphism	Isomorphism
Independent sets	Totally-isotropic space

Matrices of linear forms: where graphs and tensors meet

* You've (probably) seen matrices of linear forms

- One way to encode 3-tensors

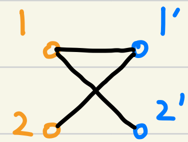
e.g.

$$\begin{bmatrix} 3x_1 - 2x_2 & -x_1 + x_2 - x_3 \\ 5x_2 + 3x_3 & x_2 - \frac{1}{2}x_3 \end{bmatrix}$$

* From a graph, we can build special matrices of linear forms

- From Tutte and Lovász

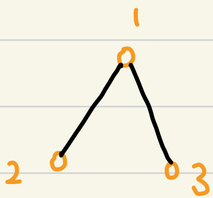
e.g.



$$\Rightarrow \begin{array}{c c} & \begin{array}{cc} 1' & 2' \end{array} \\ \begin{array}{c} 1 \\ 2 \end{array} & \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & 0 \end{bmatrix} \end{array}$$

(1) Bipartite: each variable appears in (at most) one position;

(2) Undirected simple: each variable appears in (at most) two positions.



$$\Rightarrow \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 0 & x_{12} & x_{13} \\ -x_{12} & 0 & 0 \\ -x_{13} & 0 & 0 \end{bmatrix} \end{array}$$

Tensor Isomorphism in cryptography

* Our current Internet security relies on factoring and discrete logarithm

* If a quantum computer was built, they would not be secure (Shor's algorithm)

* NIST started the "post-quantum cryptography competition" in 2017
    * The most recent call for additional digital signature schemes
        - MEDS (meds-pqc.org): 3-tensor isomorphism
        - ALTEQ (pqcalteq.github.io): alternating trilinear form equivalence
        - LESS (less-project.com): code equivalence

* These problems resist current quantum algorithm techniques [Hallgren-Moore-Rotteler-Russell-Sen]

Today's lecture: questions and techniques

* Graph Isomorphism: universality in testing isomorphism of combinatorial structures
    - Directed graph iso, hypergraph iso, line graphs, homeomorphism of 2-complexes...

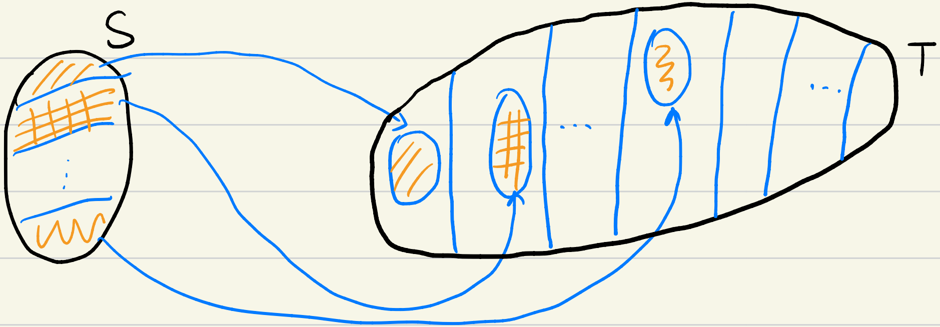
* Tensor Isomorphism: universality in testing isomorphism of algebraic structures?
    - Polynomial isomorphism, group isomorphism, algebra isomorphism...

* Universality: either "containment" of orbit structures [Gelfand and Panomerav] or polynomial-time reductions

Comparing orbit structures of different actions

* Gelfand and Panomerav used the following to compare group actions

* Suppose G acts on S and H acts on T. The latter action contains the former, if there exists a map from S to T that preserves and respects orbits.



* Leads to the tame-wild dichotomy in the representation theory of Drozd.

From group isomorphism to bilinear map isometry

* **Group Isomorphism:** p-groups of class 2 and exponent p via Baer's correspondence

* Skew-symmetric bilinear map isometry: U, V: fin-dim vector spaces over $\mathbb{F}_p$

Input: Bilinear maps $f, g: U \times U \to V$

Output: True if $\exists A \in GL(U)$, $B \in GL(V)$, s.t. $\forall u, u' \in U$, $f(A(u), A(u')) = B(g(u, u'))$

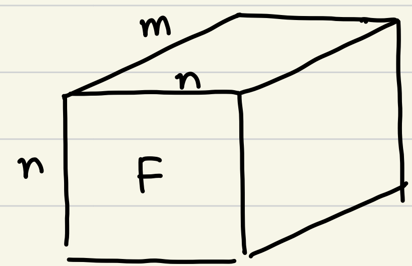
False otherwise

* Suppose $U \cong \mathbb{F}_p^n$, $V \cong \mathbb{F}_p^m$.

$f: U \times U \to V$ is stored as

a 3-way array F

$F(i, j, k) = f(e_i, e_j)_k$



Bilinear map isometry

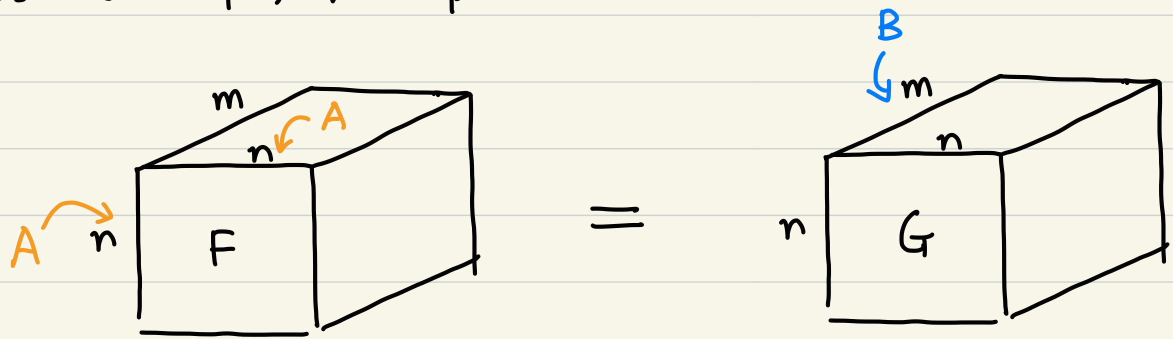
* Skew-symmetric bilinear map isometry: U, V: fin-dim vector spaces over $\mathbb{F}_p$

Input: Bilinear maps $f, g: U \times U \to V$

Output: True if $\exists A \in GL(U), B \in GL(V)$, s.t. $\forall u, u' \in U$, $f(A(u), A(u')) = B(g(u,u'))$

False otherwise

* Suppose $U \cong \mathbb{F}_p^n$, $V \cong \mathbb{F}_p^m$



Algebra isomorphism

* Algebra isomorphism problem: V: fin-dim vector space over $\mathbb{F}$

Input: Bilinear maps $f, g: V \times V \to V$

Output: True if $\exists A \in GL(V)$, s.t. $\forall v, v' \in V$, $f(A(v), A(v')) = A(g(v, v'))$

False otherwise.

* Imposing conditions (alternating, associativity, Jacobi) give associative or Lie algebras

* Studied in theoretical computer science and computer algebra [Agrawal–Saxena, Saxena–Kayal, Grochow, Brooksbank–Wilson]

Algebra isomorphism

* Algebra isomorphism problem: V: fin-dim vector space over $\mathbb{F}$

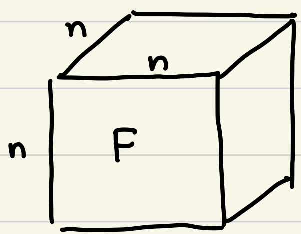
  Input: Bilinear maps $f, g : V \times V \to V$

  Output: True if $\exists\, A \in GL(V)$, s.t. $\forall\, v, v' \in V$, $f(A(v), A(v')) = A(g(v, v'))$

  False otherwise.

* Computing with associative or Lie algebras [Rónyai, Ivanyos, de Graaf]

* Suppose $V \cong \mathbb{F}^n$. Represent f by its structure constants



$$F(i, j, k) = f(e_i, e_j)_k$$

Algebra isomorphism

* Algebra isomorphism problem: V: fin-dim vector space over $\mathbb{F}$

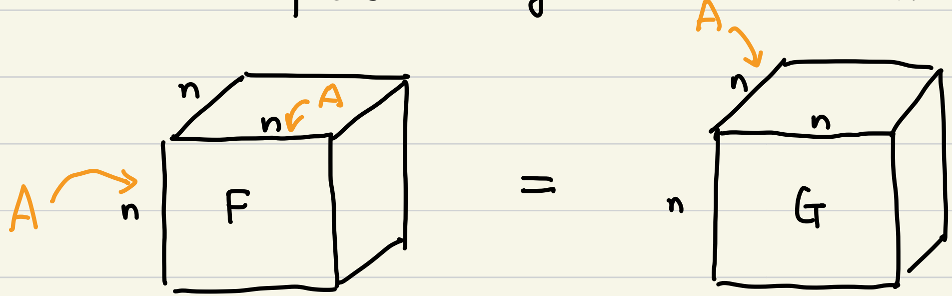
  Input: Bilinear maps $f, g: V \times V \to V$

  Output: True if $\exists\, A \in GL(V)$, s.t. $\forall v, v' \in V$. $f(A(v), A(v')) = A(g(v, v'))$

  False otherwise.

* Computing with associative or Lie algebras [Rónyai, Ivanyos, de Graaf]

* Suppose $V \cong \mathbb{F}^n$. Represent f by its structure constants



Cubic form equivalence

* Cubic form equivalence:

Input: Cubic forms $f, g \in \mathbb{F}[x_1, \cdots, x_n]$

Output: True if $\exists\, A = (a_{ij}) \in GL(n, \mathbb{F})$, $f(x_1, \cdots, x_n) = g(\sum_{i=1}^{n} a_{1i} \cdot x_i, \cdots, \sum_{i=1}^{n} a_{ni} x_i)$

False otherwise

* Studied in multivariate cryptography [Patarin, Bouillaguet—Fouque—Véber, Beullens]

Cubic form equivalence

* Cubic form equivalence:

Input: cubic forms $f, g \in \mathbb{F}[x_1, \cdots, x_n]$

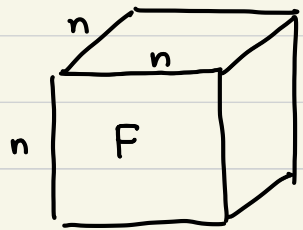
Output: True if $\exists\, A = (a_{ij}) \in GL(n, \mathbb{F})$, $f(x_1, \cdots, x_n) = g(\sum_{i=1}^{n} a_{1i} \cdot x_i, \cdots, \sum_{i=1}^{n} a_{ni} x_i)$

false otherwise.

* Suppose $char(\mathbb{F}) \neq 2$ or 3. $f: \mathbb{F}^n \to \mathbb{F}$.

Let $\hat{f}(u,v,w) = f(u+v+w) - f(u+v) - f(u+w) - f(v+w) + f(u) + f(v) + f(w)$

$\hat{f}: \mathbb{F}^n \times \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ is a symmetric trilinear form



$F(i,j,k) = \hat{f}(e_i, e_j, e_k)$

Cubic form equivalence

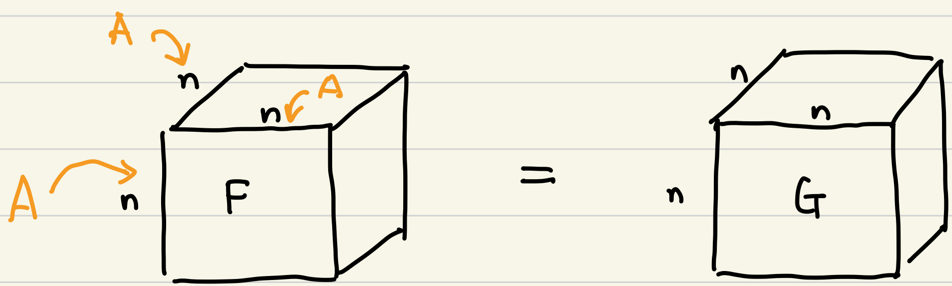
* Cubic form equivalence:

Input : cubic forms $f, g \in \mathbb{F}[x_1, \cdots, x_n]$

Output : True if $\exists\ A = (a_{ij}) \in GL(n, \mathbb{F})$, $f(x_1, \cdots, x_n) = g(\sum_{i=1}^{n} a_{1i} \cdot x_i, \cdots, \sum_{i=1}^{n} a_{ni} x_i)$

false otherwise.

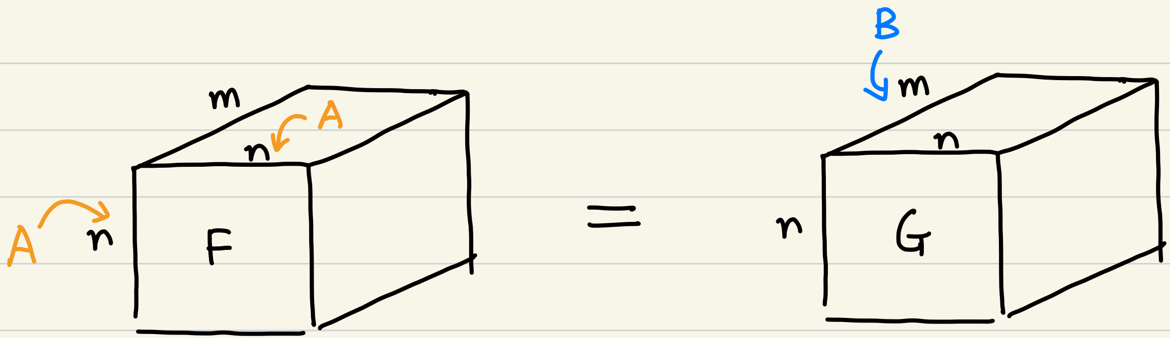
* Suppose $\text{char}(\mathbb{F}) \neq 2$ or 3. By examining symmetric trilinear forms



A brief recap...

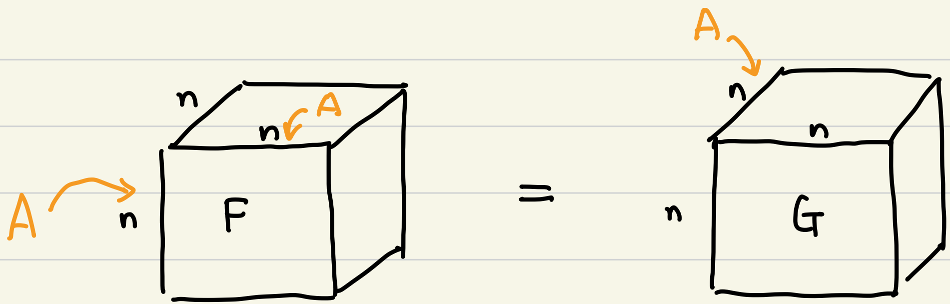
* class-2 exp-p p-group iso:

$f, g : U \times U \to V$



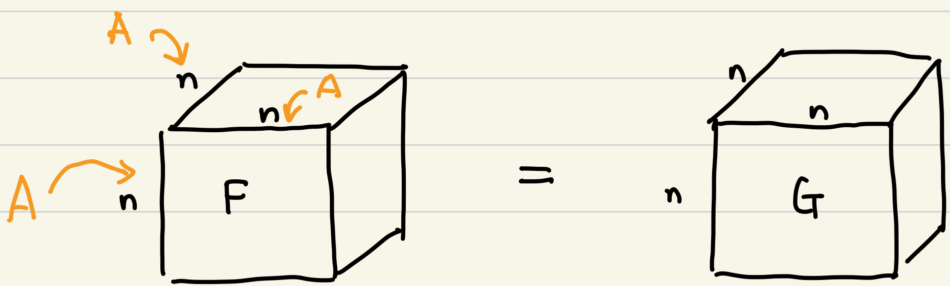
* Algebra iso:

$f, g : U \times U \to U$



* Cubic form iso:

$f, g : U \times U \times U \to \mathbb{F}$



Relations between group/algebra/cubic form iso?

* Can we compare group/algebra/cubic form iso?

* Warm up: can we compare the following matrix problems?

* Matrix equivalence:

  $f, g : U \to V$

* Matrix conjugacy:

  $f, g : U \to U$

- Suppose dim(U)=dim(V)=n, over alg. closed fields

- Matrix equivalence: n+1 orbits (by ranks)

- Matrix conjugacy: infinitely many orbits (by Jordan n.f.)

- Matrix conjugacy is more complicated than equivalence

Main result I

Theorem. [Futorny-Grochow-Sergeichuk, Grochow-Q, Grochow-Q-Tang] The following actions on 3-way arrays are equivalent under containment:

* Tensor isomorphism ($U \times V \times W \to F$).
* (Symmetric or skew-symmetric) bilinear map isomorphism ($U \times U \to V$).
* (Symmetric or skew-symmetric) trilinear form isomorphism ($U \times U \times U \to F$).
* (Lie or associative) algebra isomorphism ($U \times U \to U$).

Main result I

Theorem. [Futorny-Grochow-Sergeichuk, Grochow-Q, Grochow-Q-Tang] The following actions on 3-way arrays are equivalent under containment:

* Tensor isomorphism (UxVxW->F).
* (Symmetric or skew-symmetric) bilinear map isomorphism (UxU->V).
* (Symmetric or skew-symmetric) trilinear form isomorphism (UxUxU->F).
* (Lie or associative) algebra isomorphism (UxU->U).

* The constructions are efficient, i.e. the dimension increase is only polynomial, and the procedures can be carried out by polynomial-time algorithms

* So classifying cubic forms and Lie algebras are "equally difficult".
  - This is in contrast to the matrix case!

Main result II

* It is also natural to study k-way arrays, and to start with, consider $U_1, U_2, \cdots, U_k$ vector spaces over $\mathbb{F}$. $GL(U_1) \times GL(U_2) \times \cdots \times GL(U_k)$ naturally acts on $U_1 \otimes U_2 \otimes \cdots \otimes U_k$

Theorem. [Grochow-Q] The 3-tensor action contains the k-tensor action for k>3.

Main result II

* It is also natural to study k-way arrays, and to start with, consider $U_1, U_2, \cdots, U_k$ vector spaces over $\mathbb{F}$. $GL(U_1) \times GL(U_2) \times \cdots \times GL(U_k)$ naturally acts on $U_1 \otimes U_2 \otimes \cdots \otimes U_k$

Theorem. [Grochow-Q] The 3-tensor action contains the k-tensor action for k>3.

* 3-tensors are more difficult than 2-tensors (matrices)

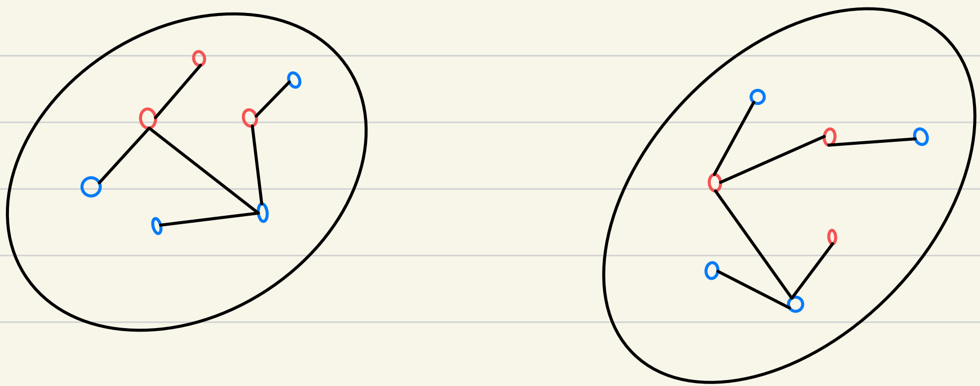
* But when k>3, the orbit structures "do not become more difficult".

* Proof makes use of path algebras from representation theory.

Methods for relating the problems

* Two techniques for relating 3-way arrays under different actions: Gelfand-Panomerav and gadget methods

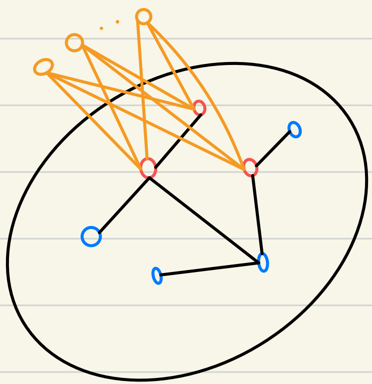
* The gadgets are reminiscent of those used for colored graph isomorphism

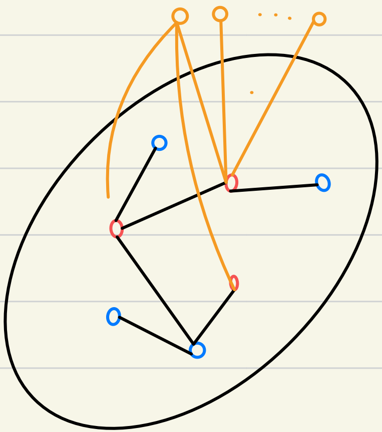


Methods for relating the problems

* Two techniques for relating 3-way arrays under different actions: Gelfand-Panomerav and gadget methods

* The gadgets are reminiscent of those used for colored graph isomorphism





- Star gadgets:
Degrees of red vertices are large enough so blue vertices cannot be mapped to them

One example of the reductions

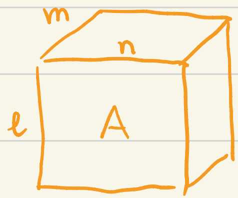
Goal. Given $f, g : U \times V \times W \to \mathbb{F}$, construct $\hat{f}, \hat{g} : S \times S \to T$, skew-symmetric such that $f \sim g$ under $GL(U) \times GL(V) \times GL(W)$ iff $\hat{f} \sim \hat{g}$ under $GL(S) \times GL(T)$

Construction.

$\dim(U) = \ell$

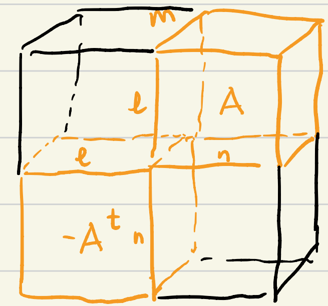
$\dim(V) = n$

$\dim(W) = m$



$\Rightarrow$ $S = U \oplus V$

$T = W$



(Entries outside the orange region are 0).

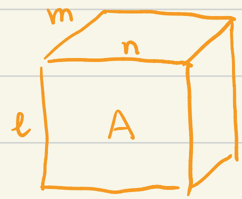
From tensors to bilinear maps

Construction.

$\dim(U) = \ell$

$\dim(V) = n$

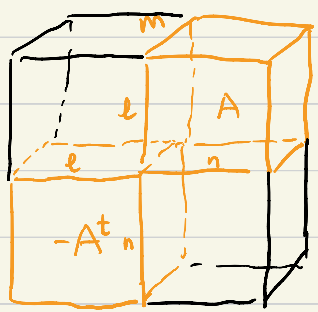
$\dim(W) = m$



$\Downarrow$

$S = U \oplus V$

$T = W$



(Entries outside the orange region are 0).

* This construction does not work because GL(S) may mix U with V. So we need:

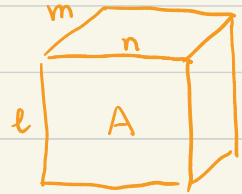
From tensors to bilinear maps

Construction.

dim(U) = ℓ

dim(V) = n

dim(W) = m



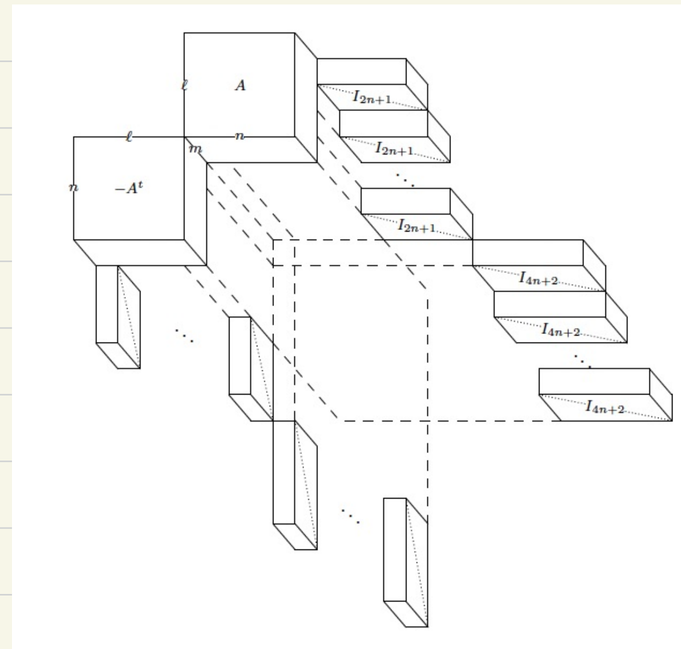
$\Downarrow$

S = U ⊕ V

T = W

(Entries outside the orange region are 0).

* This construction does not work because GL(S) may mix U with V. So we need:



Perfect matchings and non-zero determinant

Bip graph $G = ([n] \uplus [n'], E)$, $|E| = \ell$

$\Rightarrow$ Matrix of linear forms $M_G = B_1 x_1 + \cdots + B_\ell x_\ell$, $B_i \in M(n, \mathbb{F})$

Obs. G has a perfect matching $\Leftrightarrow$ $\mathrm{Det}(M_G) \not\equiv 0$

Hall's marriage theorem

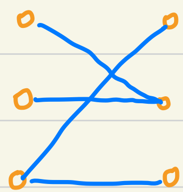
Bip graph $G = ([n] \uplus [n'], E)$, $|E| = \ell$

$\Rightarrow$ Matrix of linear forms $M_G = B_1 x_1 + \cdots + B_\ell x_\ell$, $B_i \in M(n, \mathbb{F})$

Obs. G has a perfect matching $\Leftrightarrow$ $\mathrm{Det}(M_G) \not\equiv 0$

Thm. [Hall] G has a perfect matching $\Leftrightarrow$ G has no shrunk subset

Def. Given $G = (L \uplus R, E)$, $S \subseteq L$ is a shrunk subset of G, if $|S| > |N(S)|$, where $N(S) \subseteq R$ is the set of neighbours of S.



Another correspondence between graph and matrix space structures

Bip graph $G = ([n] \uplus [n'], E)$, $|E| = \ell$

$\Rightarrow$ Matrix of linear forms $M_G = B_1 x_1 + \cdots + B_\ell x_\ell$, $B_i \in M(n, \mathbb{F})$

Obs. G has a perfect matching $\Leftrightarrow$ $\mathrm{Det}(M_G) \not\equiv 0$

Thm. [Hall] G has a perfect matching $\Leftrightarrow$ G has no shrunk subset

Prop. G has a shrunk subset $\Leftrightarrow$ M_G has a shrunk subspace

$S \subseteq L$, $|S| > |N(S)|$

$N(S) \subseteq R$ is the set of neighbours of S

$S \subseteq \mathbb{F}^n$, $\dim(S) > \dim(M_G(S))$

$M_G(S) = \mathrm{span}\left(\bigcup_{i=1}^{\ell} B_i(S) \right)$

A new question about matrices of linear forms

Bip graph $G = ([n] \uplus [n'], E)$, $|E| = \ell$

$\Rightarrow$ Matrix of linear forms $M_G = B_1 x_1 + \cdots + B_\ell x_\ell$, $B_i \in M(n, \mathbb{F})$

Prop. G has a shrunk subset $\Leftrightarrow$ M_G has a shrunk subspace

$S \subseteq L$, $|S| > |N(S)|$

$N(S) \subseteq R$ is the set of neighbours of S

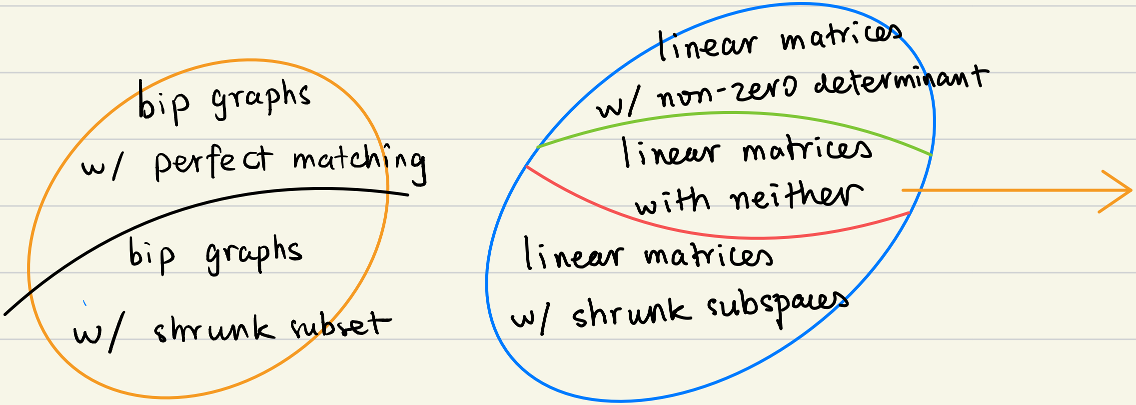
$S \subseteq \mathbb{F}^n$, $\dim(S) > \dim(M_G(S))$

$M_G(S) = \mathrm{span}\left(\bigcup_{i=1}^{\ell} B_i(S) \right)$

Question. Decide if a general matrix of linear forms has a shrunk subspace.

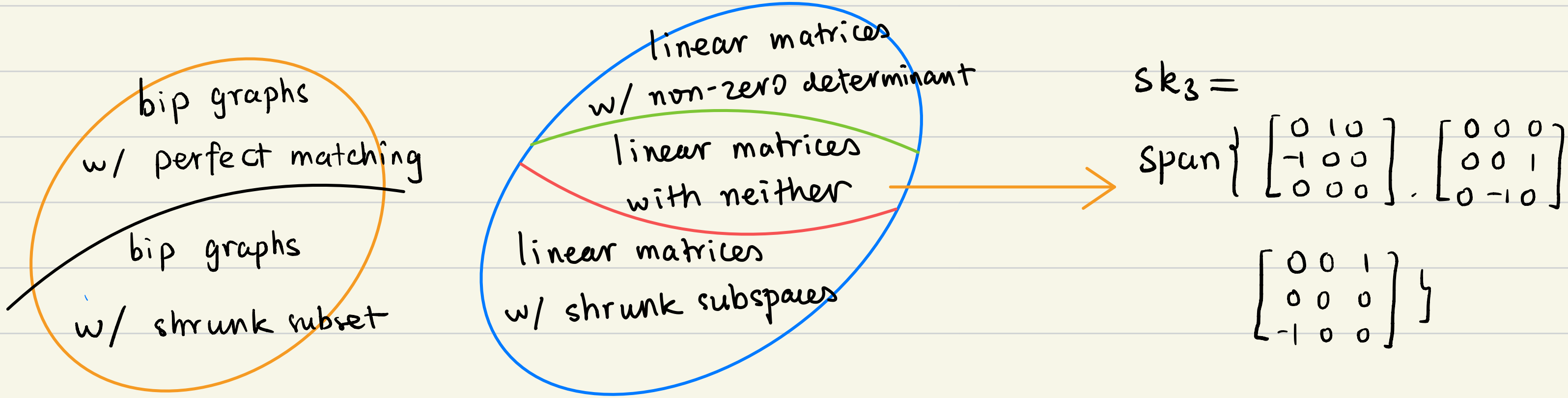
* Invariant theory [King, Bürgin-Draisma, Derksen-Makam], non-commutative algebra [Cohn], analysis [Garg-Gurvits-Oliveira-Wigderson]...

Discrepancy when moving from graphs to tensors I



$$sk_3 = \text{span}\left\{ \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \right\}$$

Discrepancy when moving from graphs to tensors I



* Non-zero det: efficient randomised algorithm. Open: a deterministic efficient one.

* Shrunk subspace: in P by [Garg-Gurvits-Oliveira-Wigderson], [Ivanyos-Q-Subrahmanyam], [Hadama-Hirai]

  - Useful in the Tensor Isomorphism algorithm by Xiaorui Sun

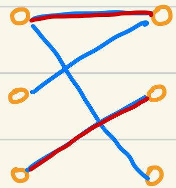
Linear algebraic alternating path method

* The Ivanyos-Q-Subrahmanyam algorithm for deciding shrunk subspaces:
  - A linear algebraic alternating path method [Ivanyos-Karpinski-Q-Santha]
  - A "regularity lemma" for matrix space blow-ups (via division algebras)

Linear algebraic alternating path method

* The Ivanyos-Q-Subrahmanyam algorithm for deciding shrunk subspaces:
  - A linear algebraic alternating path method [Ivanyos-Karpinski-Q-Santha]
  - A "regularity lemma" for matrix space blow-ups (via division algebras)

* Alternating path method on bipartite graphs:
  - Suppose $G=(L \cup R, E)$ is a bipartite graph
  - $M \subseteq E$ is a matching.
  - Can we find a larger matching?
  - Alternating path: a path that alternates between matched and unmatched vertices
  - If an alternating path starts and ends at unmatched vertices... we can find a larger matching!



Alternating path method: from graphs to tensors

$G_T = ([n] \uplus [n'], E)$

$M = B_1 x_1 + \cdots + B_\ell x_\ell$

$B_i \in M(n, \mathbb{F})$

Alternating path method: from graphs to tensors

$G = ([n] \uplus [n'], E)$	$F \subseteq E$: a matching
$M = B_1 x_1 + \cdots + B_\ell x_\ell$ $B_i \in M(n, \mathbb{F})$	$B = a_1 B_1 + \cdots + a_\ell B_\ell$

Alternating path method: from graphs to tensors

$G = ([n] \uplus [n'], E)$	$F \subseteq E$: a matching	$S \subseteq [n]$: unmatched left vertices
$M = B_1 x_1 + \cdots + B_\ell x_\ell$ $B_i \in M(n, \mathbb{F})$	$B = a_1 B_1 + \cdots + a_\ell B_\ell$	$\ker(B)$

Alternating path method: from graphs to tensors

$G = ([n] \uplus [n'], E)$	$F \subseteq E$: a matching	$S \subseteq [n]$: unmatched left vertices
$M = B_1 x_1 + \cdots + B_\ell x_\ell$ $B_i \in M(n, \mathbb{F})$	$B = a_1 B_1 + \cdots + a_\ell B_\ell$	$\ker(B)$

$T \subseteq [n']$: matched right vertices
$\mathrm{im}(B)$

Alternating path method: from graphs to tensors

$G = ([n] \uplus [n'], E)$	$F \subseteq E$: a matching	$S \subseteq [n]$: unmatched left vertices
$M = B_1 x_1 + \cdots + B_\ell x_\ell$ $B_i \in M(n, \mathbb{F})$	$B = a_1 B_1 + \cdots + a_\ell B_\ell$	$\ker(B)$

$T \subseteq [n']$: matched right vertices	A walk from left to right via unmatched edges	
$\mathrm{im}(B)$	$V \subseteq \mathbb{F}^n \to M(V)$ $= \mathrm{span}\left(\bigcup_{i=1}^{\ell} B_i(V)\right)$	

Alternating path method: from graphs to tensors

$G = ([n] \uplus [n'], E)$	$F \subseteq E$: a matching	$S \subseteq [n]$: unmatched left vertices
$M = B_1 x_1 + \cdots + B_\ell x_\ell$, $B_i \in M(n, \mathbb{F})$	$B = a_1 B_1 + \cdots + a_\ell B_\ell$	$\ker(B)$

$T \subseteq [n']$: matched right vertices	A walk from left to right via unmatched edges	A walk from right to left via matched edges
$\mathrm{im}(B)$	$V \subseteq \mathbb{F}^n \to M(V) = \mathrm{span}\left(\bigcup_{i=1}^{\ell} B_i(V)\right)$	$W \subseteq \mathbb{F}^n \to B^{-1}(W) = \{ v \in V \mid B(v) \in W \}$

Linear algebraic alternating path method

* $M = B_1 x_1 + \cdots + B_\ell x_\ell$ $\quad B = a_1 B_1 + \cdots + a_\ell B_\ell$

$V_0 = \ker(B) \Rightarrow W_1 = M(V_0) \Rightarrow V_1 = B^{-1}(W_1) \Rightarrow W_2 = M(V_1) \Rightarrow \cdots$

Linear algebraic alternating path method

* $M = B_1 x_1 + \cdots + B_\ell x_\ell$ $\quad B = a_1 B_1 + \cdots + a_\ell B_\ell$

$V_0 = \ker(B) \Rightarrow W_1 = M(V_0) \Rightarrow V_1 = B^{-1}(W_1) \Rightarrow W_2 = M(V_1) \Rightarrow \cdots$

* $W_1 \subsetneq W_2 \subsetneq W_3 \subsetneq \cdots \subsetneq W_k = W_{k+1} = \cdots$

Lemma. $W_k \subseteq \mathrm{Im}(B) \Leftrightarrow \exists$ a shrunk subspace U s.t. $\dim(U) - \dim(M(U)) = \mathrm{corank}(B)$

– [Ivanyos–Karpinski–Q–Santha]

Summary

* Graph isomorphism to tensor isomorphism
  - The question of equivalences between iso problems for algebraic structures
  - Star gadget for graphs vs Identity matrix gadget for tensors

Summary

* Graph isomorphism to tensor isomorphism
  - The question of equivalences between iso problems for algebraic structures
  - Star gadget for graphs vs Identity matrix gadget for tensors

* Graph perfect matching to tensor non-zero det
  - The breakdown of Hall's marriage theorem, and the shrunk subspace question
  - Alternating path method and its linear algebraic counterpart

Summary

* Graph isomorphism to tensor isomorphism
  - The question of equivalences between iso problems for algebraic structures
  - Star gadget for graphs vs Identity matrix gadget for tensors

* Graph perfect matching to tensor non-zero det
  - The breakdown of Hall's marriage theorem, and the shrunk subspace question
  - Alternating path method and its linear algebraic counterpart

* More structure correspondences?
* More graph-theoretic type questions for tensors?
* More linear algebraic counterparts of graph-theoretic techniques?
  - Keep in mind that new phenomena and complications are there for tensors :)

Thank you!

And questions please :)

Linear algebraic alternating path method

* The Ivanyos-Q-Subrahmanyam algorithm for deciding shrunk subspaces:
  - A linear algebraic alternating path method [Ivanyos-Karpinski-Q-Santha]
  - A "regularity lemma" for matrix space blow-ups (via division algebras)

* Alternating path method on bipartite graphs:

* $G = (L \cup R, E)$, $M \subseteq E$ is a given matching, $U = E \setminus M$: edges not in M

$S_0 \subseteq L$: unmatched vertices $\overset{U}{\Longrightarrow}$ $T_1 \subseteq R$: neighbours of S_0 via unmatched edges

- if T_1 contains an unmatched vertex, an augmenting path is found
- otherwise ...

Review of alternating paths on bipartite graphs

* $G = (L \cup R, E)$, $M \subseteq E$ is a given matching, $U = E \setminus M$: edges not in M

$S_0 \subseteq L$: unmatched vertices $\overset{U}{\Rightarrow}$ $T_1 \subseteq R$: neighbours of S_0 via unmatched edges

$S_1 \subseteq L$: n.b. of T_1 via matched edges $\overset{M}{\Leftarrow}$

Review of alternating paths on bipartite graphs

* $G = (L \cup R, E)$, $M \subseteq E$ is a given matching , $U = E \setminus M$: edges not in M

$S_0 \subseteq L$: unmatched vertices $\overset{U}{\Longrightarrow}$ $T_1 \subseteq R$: neighbours of S_0 via unmatched edges

$\overset{M}{\Longleftarrow}$

$S_1 \subseteq L$: n.b. of T_1 via matched edges $\overset{U}{\Longrightarrow}$ $T_2 \subseteq R$: n.b. of S_1 via unmatched edges

- Check if T_2 contains an unmatched vertex
- Yes : augmenting path. No : continue

Review of alternating paths on bipartite graphs

* $G = (L \cup R, E)$, $M \subseteq E$ is a given matching, $U = E \setminus M$: edges not in M

$S_0 \subseteq L$: unmatched vertices $\overset{U}{\Longrightarrow}$ $T_1 \subseteq R$: neighbours of S_0 via unmatched edges

$\overset{M}{\Longleftarrow}$

$S_1 \subseteq L$: n.b. of T_1 via matched edges

$\overset{U}{\Longrightarrow}$ $T_2 \subseteq R$: n.b. of S_1 via unmatched edges

- Check if T_2 contains an unmatched vertex
- Yes : augmenting path. No : continue

⋮

STOP if T_i consists of matched vertices and $T_i \subseteq T_1 \cup T_2 \cup \cdots \cup T_{i-1}$

Linear algebraic alternating path method

* $\mathcal{B} = \text{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$S_0 = \ker(C) \subseteq \mathbb{F}^n$

S_0 → "unmatched vertices"

Linear algebraic alternating path method

* $\mathcal{B} = \text{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$S_0 = \ker(C) \subseteq \mathbb{F}^n \overset{\mathcal{B}}{\Longrightarrow} T_1 = \mathcal{B}(S_0) := \text{span}\{B_1(S_0) \cup \cdots \cup B_m(S_0)\} \subseteq \mathbb{F}^n$

T_1 → "neighbors of S_0 via unmatched edges"

Linear algebraic alternating path method

* $\mathcal{B} = \text{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$S_0 = \ker(C) \subseteq \mathbb{F}^n \overset{\mathcal{B}}{\Longrightarrow} T_1 = \mathcal{B}(S_0) := \text{span}\{B_1(S_0) \cup \cdots \cup B_m(S_0)\} \subseteq \mathbb{F}^n$

- If $T_1 \nsubseteq \text{im}(C)$, can compute $D \in \mathcal{B}$ of larger rank
- Otherwise ... ↘ "T_1 contains an unmatched vector"

Linear algebraic alternating path method

* $\mathcal{B} = \mathrm{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$S_0 = \ker(C) \subseteq \mathbb{F}^n \xrightarrow{\mathcal{B}} T_1 = \mathcal{B}(S_0) := \mathrm{span}\{B_1(S_0) \cup \cdots \cup B_m(S_0)\} \subseteq \mathrm{Im}(C)$

$\xleftarrow{C^{-1}}$

$S_1 = C^{-1}(T_1) := \{v \in \mathbb{F}^n \mid C(v) \in T_1\}$

Linear algebraic alternating path method

* $\mathcal{B} = \text{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$$S_0 = \ker(C) \subseteq \mathbb{F}^n \overset{\mathcal{B}}{\Longrightarrow} T_1 = \mathcal{B}(S_0) := \text{span}\{B_1(S_0) \cup \cdots \cup B_m(S_0)\} \subseteq \text{Im}(C)$$

$$\overset{C^{-1}}{\Longleftarrow}$$

$$S_1 = C^{-1}(T_1) := \{v \in \mathbb{F}^n \mid C(v) \in T_1\}$$

$$\overset{\mathcal{B}}{\Longrightarrow} T_2 = \mathcal{B}(S_1)$$

- Check if $T_2 \nsubseteq \text{im}(C)$.
- Yes : cannot find D of larger rank in $\mathcal{B}$
  but "do so in $\mathcal{B} \otimes M(n, \mathbb{F})$"
- No : continue

Linear algebraic alternating path method

* $\mathcal{B} = \mathrm{span}\{B_1, \cdots, B_m\} \subseteq M(n, \mathbb{F})$. $C \in \mathcal{B}$

$S_0 = \ker(C) \subseteq \mathbb{F}^n \xrightarrow{\mathcal{B}} T_1 = \mathcal{B}(S_0) := \mathrm{span}\{B_1(S_0) \cup \cdots \cup B_m(S_0)\} \subseteq \mathbb{F}^n$

$\xleftarrow{C^{-1}}$

$S_1 = C^{-1}(T_1) := \{v \in \mathbb{F}^n \mid C(v) \in T_1\}$

$\xrightarrow{\mathcal{B}} T_2 = \mathcal{B}(S_1)$

$\vdots$ STOP if $T_{i+1} = T_i \leq \mathrm{im}(C)$

Lemma. [Ivanyos–Karpinski–Q–Santha] $\mathcal{B}$ has a shrunk subspace of gap corank(C) iff $\exists i$, $T_{i+1} = T_i \leq \mathrm{im}(C)$