Some algebraic algorithms and complexity classes inspired by connections between matrix spaces and graphs

> Youming Qiao University of Technology Sydney

@ Workshop on Algebraic Complexity Theory (WACT) 202330 March, 2023

Some typos corvected, N.B. added, on 5 April. 1. Some connections between graphs and matrix spaces

2. Algorithm: alternating paths and Wong sequences

3. Complexity: graph isomorphism and matrix space equivalence

4. More connections, more problems

- * Based on the following joint works:
- Yinan Li, Youming Qiao, Avi Wigderson, Yuval Wigderson, Chuanqi Zhang: Connections between graphs and matrix spaces. CoRR abs/2206.04815 (2022). To appear in Israel J Maths
- Joshua A. Grochow, Youming Qiao: On the complexity of isomorphism problems for tensors, groups, and polynomials I: Tensor Isomorphism-completeness. ITCS 2021: 31:1-31:19.
- Gábor Ivanyos, Youming Qiao, K. V. Subrahmanyam: Constructive non-commutative rank computation is in deterministic polynomial time. Comput. Complex. 27(4): 561–593 (2018).
- Yinan Li, Youming Qiao: Linear algebraic analogues of the graph isomorphism problem and the Erdős-Rényi model. FOCS 2017: 463–474.

From graphs to matrix spaces

* For $n \in \mathbb{N}$, $[n] := \{1, 2, \dots, n\}$. \mathbb{F} : a field

* M(n, F): the linear space of n×n matrices over F

* For $i, j \in [n]$, $E_{i,j} \in M(n, \mathbb{F})$ is the (i, j)th elementary matrix

$$E_{i,j} = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{bmatrix}$$

From graphs to matrix spaces

* For $n \in \mathbb{N}$, $[n] := \{1, 2, \dots, n\}$. \mathbb{F} : a field

* M(n, F): the linear space of n×n matrices over F

* For $i, j \in [n]$, $E_{i,j} \in M(n, \mathbb{F})$ is the (i, j)th elementary matrix

* A bipartite graph G = (LUR, F) A matrix space $B_G \subseteq M(n, F)$ $L = R = [n], F \subseteq L \times R$ $B_G = span \{E_{i,j} \mid (i,j) \in F\}$

From graphs to matrix spaces

* For $n \in \mathbb{N}$, $[n] := \{1, 2, \dots, n\}$. \mathbb{H} : a field

* M(n, F): the linear space of n×n matrices over F

* For $i, j \in [n]$, $E_{i,j} \in M(n, \mathbb{F})$ is the (i, j)th elementary matrix

* A bipartite graph G = (LUR, F) A matrix space $B_G \subseteq M(n, \mathbb{F})$ $L = R = [n], F \subseteq L \times R$ $B_G = span \{E_{i,j} \mid (i,j) \in F\}$

Observation. (Tutte, Edmonds, Lovász) (T has a perfect matching (=> BG contains a full-rank matrix

Connections between graphs and matrix spaces

Observation. (Tutte, Edmonds, Lovász) G has a perfect matching (=> BG contains a full-rank matrix

* A classical result of the type: G has property P iff B_G has property Q

Connections between graphs and matrix spaces Observation. (Tutte, Edmonds, Lovász) (T has a perfect matching (=> BG contains a full-rank matrix

* A classical result of the type: G has property P iff B_G has property Q

* Symbolic determinant identity testing (SDIT) essentially asks to test if a general matrix space contains a full-rank matrix: a problem of key importance in algebraic complexity [Kabanets-Impagliazzo]

* Quasi-NC algorithm for perfect matching [Fenner-Gurjar-Thierauf]

* We now examine another side of the above observation

Another correspondence between graph and matrix space structures * $(f = (LUR, F)) \xrightarrow{B_{g}} B_{g} = span \{E_{i,j} \mid (i,j) \in F\} \subseteq M(n, F)$ L = R = [n]

Obs. G has a perfect matching (=) BG contains a full-rank matrix

Prop. (Hall) (f has a shrunk subset (=) Bg has a shrunk subspace $S \subseteq L$, |S| > |N(S)| $S \subseteq H^n$, dim(S) > dim(Bg(S)) $N(S) \subseteq R$ is the setBg(S) = Span(UB(S))f neighbours of S

Another correspondence between graph and matrix space structures * $(f = (LUR, F)) \xrightarrow{B_G} B_G = span \{E_{i,j} | (i,j) \in F\} \subseteq M(n, F)$ L = R = [n]

Obs. G has a perfect matching (=) BG contains a full-rank matrix

Prop. (Hall) (T has a shrunk subset (=) BG has a shrunk subspace

* Non-commutative rational identity testing (NC-RIT) essentially asks to test if a general matrix space admits a shrunk subspace [Hrubeš—Wigderson]

* Geometric complexity theory [Mulmuley], polynomial identity testing [Derksen— Makam], non-commutative algebra [Cohn], analysis [Garg-Gurvits-Oliveira-Wigderson]...

SDIT versus NC-RIT





* SDIT: in coRP over large fields. A major open problem to derandomise it.

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

* The Ivanyos-Q-Subrahmanyam algorithm for NC-RIT:

- 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:



Review of alternating paths on bipartite graphs

So
$$\subseteq$$
 L : unmatched vertices $\bigvee_{T_1} \subseteq R$: neighbours of So via unmatched edges
Si \subseteq L : n.b. of T₁ via matched \swarrow_{edges}

Review of alternating paths on bipartite graphs



Review of alternating paths on bipartite graphs



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

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

"unmatched vertices"

*
$$\mathcal{B} = \operatorname{span}\{B_1, \dots, B_m\} \subseteq \mathcal{M}(n, \mathbb{F})$$
. $C \in \mathcal{B}$
"neighbors of So via unmatched edges"
 $S_0 = \ker(C) \subseteq \mathbb{F}^n \xrightarrow{\mathcal{B}} T_1 = \mathcal{B}(S_0) := \operatorname{span}\{B_1(S_0) \cup \dots \cup B_m(S_n)\} \subseteq \mathbb{F}^n$

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

$$S_{o} = \ker(C) \subseteq \mathbb{F}^{n} \xrightarrow{\mathcal{B}} T_{i} = \mathcal{B}(S_{o}) := \operatorname{span} \{B_{i}(S_{o}) \cup \cdots \cup B_{m}(S_{o})\} \subseteq \mathbb{F}^{n}$$

$$- \operatorname{If} T_{i} \notin \operatorname{im}(C), \operatorname{can} \operatorname{compute} D \in \mathcal{B} \text{ of larger rank}$$

$$- \operatorname{Otherwise} \cdots \qquad \forall "T_{i} \operatorname{contains} an unmatched vector"$$

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

$$S_{0} = \ker(C) \subseteq \mathbb{F}^{n} \xrightarrow{B} T_{1} = B(S_{0}) := \operatorname{span} \{B_{1}(S_{0}) \cup \cdots \cup B_{m}(S_{n})\} \subseteq \operatorname{Im}(C)$$

$$S_{1} = C^{-1}(T_{1}) := \{ \cup \in \mathbb{F}^{n} \mid C(\cup) \in T_{1} \}$$

•

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

$$S_{o} = \ker(C) \subseteq \mathbb{F}^{n} \xrightarrow{B} T_{i} = B(S_{o}) := \operatorname{span} \{B_{i}(S_{o}) \cup \cdots \cup B_{m}(S_{o})\} \subseteq \operatorname{Im}(C)$$

$$S_{i} = C^{-1}(T_{i}) := \{ \cup \in \mathbb{F}^{n} \mid C(\cup) \in T_{i} \}$$

$$T_{2} = B(S_{i})$$

$$- \operatorname{Check} if T_{2} \notin \operatorname{im}(C).$$

$$- \operatorname{Yes} : \operatorname{cannot} \operatorname{find} D \text{ of larger rank in } B$$

$$\operatorname{but}^{n} \operatorname{clo} \operatorname{sp} \operatorname{in} (B \otimes M(n, \mathbb{F})^{n})$$

$$- \operatorname{Np} : \operatorname{continue}$$

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

$$S_{0} = \ker(C) \subseteq \mathbb{F}^{n} \qquad T_{1} = \mathscr{B}(S_{0}) := \operatorname{span} \{B_{1}(S_{0}) \cup \cdots \cup B_{m}(S_{0})\} \subseteq \mathbb{F}^{n}$$

$$C_{-}^{-1}$$

$$S_{1} = C^{-1}(T_{1}) := \{ \forall \in \mathbb{F}^{n} \mid C(\forall) \in T_{1} \}$$

$$T_{2} = \mathscr{B}(S_{1})$$

$$S_{1} = T_{1} \subseteq \operatorname{im}(C)$$

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

Recap for the NC-RIT story

* Start with "G has property P iff B_G has property Q"

* Go on to examine the problem of testing "B has property Q" N.B. This is just one way of arriving at NC-RIT

Recap for the NC-RIT story

* Start with "G has property P iff B_G has property Q"

* Go on to examine the problem of testing "B has property Q"

- * Inspired by techniques for solving the problem of testing "G has property P"
 - 1. [Garg-Gurvits-Oliveira-Wigderson] Sinkhorn's scaling algorithm
 - 2. [Ivanyos-Q-Subrahmanyam] the augmenting path algorithm
 - 3. [Hamada-Hirai] submodular optimisation

Recap for the NC-RIT story

* Start with "G has property P iff B_G has property Q"

* Go on to examine the problem of testing "B has property Q''

- * Inspired by techniques for solving the problem of testing "G has property P"
 - 1. [Garg-Gurvits-Oliveira-Wigderson] Sinkhorn's scaling algorithm
 - 2. [Ivanyos-Q-Subrahmanyam] the augmenting path algorithm
 - 3. [Hamada-Hirai] submodular optimisation

* The situation is usually more complicated for testing "B has property Q''

- The discrepancy between "full-rank matrices" and "shrunk subspaces"

not having

Graph isomorphism versus matrix space equivalence

Def. $G_1 = (LUR, F_1)$ and $G_2 = (LUR, F_2)$, L = R = [n], $F_1, F_2 \subseteq L \times R$ we isomorphic, if $\exists \sigma, \pi \in S_n$, such that $(i, j) \in F_1 \iff (\sigma(i), \pi(j)) \in \hat{f}_2$

* Bipartite graph iso is as hard as general graph iso

Graph isomorphism versus matrix space equivalence

Def. $G_1 = (LUR, F_1)$ and $G_2 = (LUR, F_2)$, L = R = [n], $F_1, F_2 \subseteq L \times R$ we isomorphic, if $\exists \sigma, \pi \in S_n$, such that $(i, j) \in F_1 \iff (\sigma(i), \pi(j)) \in \hat{f}_2$

* A_1 , $A_2 \in M(n, \mathbb{F})$ are equivalent, if $\exists L, R \in GL(n, \mathbb{F})$, $A_1 = LA_2R$

Def. Matrix spaces B_1 , $B_2 \subseteq M(n, F)$ are equivalent, if $\exists L, R \in GL(n, F)$ such that $B_1 = LB_2R := \{LBR \mid B \in B_2\}$

Graph isomorphism versus matrix space equivalence

Def. $G_1 = (LUR, F_1)$ and $G_2 = (LUR, F_2)$, L = R = [n], $F_1, F_2 \subseteq L \times R$ we isomorphic, if $\exists \sigma, \pi \in S_n$, such that $(i, j) \in F_1 \iff (\sigma(i), \pi(j)) \in \hat{f}_2$

* A_1 , $A_2 \in M(n, \mathbb{F})$ are equivalent, if $\exists L, R \in GL(n, \mathbb{F})$, $A_1 = LA_2R$

Def. Matrix spaces B_1 , $B_2 \subseteq M(n, \mathbb{F})$ are equivalent, if $\exists L, R \in GL(n, \mathbb{F})$ such that $B_1 = LB_2R := \{LBR \mid B \in B_2\}$

Prop. [Li-Q-Wigderson-Wigderson-Zhang] Grand Have isomorphic (=> BG and BH are equivalent

Matrix space equivalence Prop. [Li-Q-Wigderson-Wigderson-Zhang] Gr and H are isomorphic (=> BG and BH are equivalent Tensorloo

* Matrix space equivalence as a proper generalisation of graph isomorphism

* Next step: matrix space equivalence for general matrix spaces

Matrix space equivalence

* Matrix space equivalence as a proper generalisation of graph isomorphism

* Next step: matrix space equivalence for general matrix spaces

- * Results inspired by the study of graph isomorphism?
 - [Li-Q]: individualisation and refinement as used in [Babai-Erdős-Selkow]

* [Grochow-Q]: a complexity class called Tensor Isomorphism (TI) in analogy with GI - A gadget design in analogy with some method from colored graph isomorphism Matrix space equivalence as tensor isomorphism

* [Grochow-Q]: a complexity class called Tensor Isomorphism (TI) in analogy with GI



Matrix space equivalence as tensor isomorphism

* [Grochow-Q]: a complexity class called Tensor Isomorphism (TI) in analogy with GI



Matrix space equivalence as tensor isomorphism



Def. [Grochow-Q] The complexity class **TI** consists of problems polynomial-time reducible to the matrix space equivalence = 3-tensor isomorphism problem.

* Wishful thinking: just as GI captures isomorphism problems for combinatorial structures, TI captures isomorphism problems for algebraic structures













3-way arrays are versatile

* Under different actions, 3-way arrays encode tensors, bilinear maps, algebras, and trilinear forms

* Putting some structural restrictions we get more

1. Symmetric bilinear maps f:UxU->V: systems of quadratic forms

2. Skew-symmetric bilinear maps over GF(p): p-groups of class 2 and exponent p

3. Symmetric trilinear forms over F, char(F) not 2 or 3: cubic forms

4. Associativity, Jacobi conditions...: associative algebras or Lie algebras

TI-complete problems

Theorem. [Futorny-Grochow-Sergeichuk, Grochow-Q]

The following problems are TI-complete:

- Isomorphism of p-groups of class 2 and exponent p, given by matrix groups
- Isomorphism of systems of quadratic forms, cubic forms
- Isomorphism of associative and Lie algebras

TI-complete problems

Theorem. [Futorny-Grochow-Sergeichuk, Grochow-Q]

The following problems are TI-complete:

- Isomorphism of p-groups of class 2 and exponent p, given by matrix groups
- Isomorphism of systems of quadratic forms, cubic forms
- Isomorphism of associative and Lie algebras

* How about d-tensors for d>3? Note that 2-tensor isomorphism (matrix equivalence) is easy.

d, d > 3

Theorem. [Grochow-Q] k-tensor isomorphism reduces to 3-tensor isomorphism.

* In the spirit that 3SAT is NP-complete, and 2SAT is in P.

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



One example of the reductions

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



From tensors to bilinear maps



From tensors to bilinear maps



More correspondences, more questions

* A directed graph
$$G = (V, F) \Rightarrow B_G = \text{span}\{E_{i,j}|(i,j)\in F\} \subseteq M(n, \mathbb{F}).$$

 $V = [n], F \subseteq V \times V$

Prop.[Li-Q-Wigderson-Wigderson-Zhang] G is acyclic <=> BG contains only nilpotent matrices

* Not so surprising, but ..

More correspondences, more questions

* A directed graph
$$G = (V, F) \Rightarrow B_G = \text{span}\{E_{i,j}|(i,j)\in F\} \subseteq M(n, \mathbb{F}).$$

 $V = [n], F \subseteq V \times V$

Prop. [ibid.] Max size over acyclic subgraphs in G = Max dim over nilpotent subspaces in BG

* Generalise Gerstenhaber's result:

max dim of nilpotent matrix spaces in
$$M(n, FF) = \binom{n}{2}$$

Def. (Matrix space nilpotency testing) Given a linear basis of a matrix space **B**, decide if B contains only nilpotent matrices.

* Given a symbolic matrix S of size n, decide if Sⁿ is the zero matrix.

* Reduces to SDIT, which is equivalent to asking whether the (1, 1) entry of Sⁿ is O

* The naturally associated group action is matrix conjugation (instead of left-right) on matrix tuples. The nullcone problem, rank-1 spanned setting, etc. are easier.

* SDIT reduces to computing the nilpotency index [Li-Q-Wigderson-Wigderson-Zhang]

Brief summary

- * A pattern of the stories:
- 1. Start with "G has property P iff B_G has property Q"
- 2. Ask the question "B has property Q''
- 3. Devise linear algebraic analogues of graph-theoretic methods
- * Shrunk subset vs shrunk subspace, graph isomorphism vs tensor isomorphism
- * Alternating paths vs Wong sequences, graph coloring gadgets vs rank gadgets
- * Will matrix space nilpotency test be the next target?

Thank you!

And questions please :)