On the non-commutative rank of a symbolic matrix

Gábor Ivanyos[1] K. V. Subrahmanyam[2] *Youming Qiao*[3]

27 Nov 2017 @ Australian Algebra Conference, UTS

[1]Hungarian Academy of Sciences

[2]Chennai Mathematical Institute

[3]Centre for Quantum Software and Information, University of Technology Sydney

Table of Contents

Commutative and non-commutative ranks of symbolic matrices

Two rank concepts of a symbolic matrix

Fix an infinite field $\mathbb{F}$, and a set of variables $X = \{x_1, \ldots, x_m\}$.

Definition

A *symbolic matrix* T over $\mathbb{F}$ and X is a matrix with entries being (possibly zero) linear forms over $\mathbb{F}$.

- The commutative rank of T, $\mathrm{crk}(T)$, is the rank of T over $\mathbb{F}(x_1, \ldots, x_m)$ (the rational function field).
- The non-commutative rank of T, $\mathrm{ncrk}(T)$, is the rank of T over $\mathbb{F}\langle\!\langle x_1, \ldots, x_m \rangle\!\rangle$ (the free skew field).

Example

A 3×3 symbolic matrix over $\mathbb{F}$ and $\{x, y, z\}$:

$$sk_3 = \begin{bmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{bmatrix}.$$

- $\mathrm{crk}(sk_3) = 2$.
- $\mathrm{ncrk}(sk_3) = 3$.

More on the commutative rank

Example

A 3×3 symbolic matrix over $\mathbb{F}$ and $\{x, y, z\}$:

$$sk_3 = \begin{bmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{bmatrix}.$$

- $\mathrm{crk}(sk_3) = 2$.
- $\mathrm{ncrk}(sk_3) = 3$.

Commutative rank

An $n \times n$ symbolic matrix T can be written as

$$T = B_1 x_1 + \cdots + B_m x_m,$$

where B_i's are $n \times n$ matrices over $\mathbb{F}$.

Let $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq M(n, \mathbb{F})$. Define

$$\mathrm{maxrk}(\mathcal{B}) = \max\{\mathrm{rk}(B) : B \in \mathcal{B}\}.$$

Easy to see that $\mathrm{maxrk}(\mathcal{B}) = \mathrm{crk}(T)$.

More on the non-commutative rank

Example

A 3×3 symbolic matrix over $\mathbb{F}$ and $\{x, y, z\}$:

$$sk_3 = \begin{bmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{bmatrix}.$$

- $\mathrm{crk}(sk_3) = 2$.
- $\mathrm{ncrk}(sk_3) = 3$.

Non-commutative rank

Recall that $T = B_1 x_1 + \cdots + B_m x_m$, and $\mathcal{B} = \langle B_1, \ldots, B_m \rangle$. For $U \leq \mathbb{F}^n$,

$$\mathcal{B}(U) := \langle \cup_i B_i(U) \rangle.$$

Define the discrepancy of $\mathcal{B}$, $\mathrm{disc}(\mathcal{B})$, as

$$\max\{\dim(U) - \dim(\mathcal{B}(U)) : U \leq \mathbb{F}^n\}.$$

Then by [Fortin-Reutenauer, 2004],

$$\mathrm{ncrk}(T) = n - \mathrm{disc}(\mathcal{B}).$$

A timeline for crk and ncrk

1966 — Amitsur proposed the concept of the free skew field.

A timeline for crk and ncrk

1966 Amitsur proposed the concept of the free skew field.

1967 Edmonds proposed the problem of computing crk.

A timeline for crk and ncrk

1966 Amitsur proposed the concept of the free skew field.

1967 Edmonds proposed the problem of computing crk.

1973 P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.

A timeline for crk and ncrk

1966	Amitsur proposed the concept of the free skew field.
1967	Edmonds proposed the problem of computing crk.
1973	P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.
1979	Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.

A timeline for crk and ncrk

1966 Amitsur proposed the concept of the free skew field.

1967 Edmonds proposed the problem of computing crk.

1973 P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.

1979 Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.

1999 Cohn and Reutenauer showed $\mathrm{ncrk} \in \mathrm{PSPACE}$.

A timeline for crk and ncrk

1966	Amitsur proposed the concept of the free skew field.
1967	Edmonds proposed the problem of computing crk.
1973	P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.
1979	Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.
1999	Cohn and Reutenauer showed $\mathrm{ncrk} \in \mathrm{PSPACE}$.
2003	Kabanets and Impagliazzo showed that derandomising crk implies strong arithmetic circuit lower bounds.

A timeline for crk and ncrk

1966 Amitsur proposed the concept of the free skew field.

1967 Edmonds proposed the problem of computing crk.

1973 P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.

1979 Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.

1999 Cohn and Reutenauer showed $\mathrm{ncrk} \in \mathrm{PSPACE}$.

2003 Kabanets and Impagliazzo showed that derandomising crk implies strong arithmetic circuit lower bounds.

crk *and* ncrk *intertwined.*

A timeline for crk and ncrk

1966 Amitsur proposed the concept of the free skew field.

1967 Edmonds proposed the problem of computing crk.

1973 P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.

1979 Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.

1999 Cohn and Reutenauer showed ncrk $\in$ PSPACE.

2003 Kabanets and Impagliazzo showed that derandomising crk implies strong arithmetic circuit lower bounds.

crk *and* ncrk *intertwined.*

2003 Gurvits presented a deterministic efficient algorithm to test whether crk is full when crk $=$ ncrk.

A timeline for crk and ncrk

- 1966 Amitsur proposed the concept of the free skew field.
- 1967 Edmonds proposed the problem of computing crk.
- 1973 P. M. Cohn proposed the problem of computing ncrk, and showed that it is decidable.
- 1979 Lovász observed a randomised efficient algorithm for crk, and several connections to combinatorics.
- 1999 Cohn and Reutenauer showed $\mathrm{ncrk} \in \mathrm{PSPACE}$.
- 2003 Kabanets and Impagliazzo showed that derandomising crk implies strong arithmetic circuit lower bounds.
- # crk *and* ncrk *intertwined.*
- 2003 Gurvits presented a deterministic efficient algorithm to test whether crk is full when $\mathrm{crk} = \mathrm{ncrk}$.
- 2004 Fortin and Reutenauer showed $\mathrm{crk} \leq \mathrm{ncrk} \leq 2 \cdot \mathrm{crk}$.

Progress on ncrk in 2015

Theorem

ncrk *can be computed in deterministic polynomial time.*

- *Over $\mathbb{Q}$ [Garg-Gurvits-Oliveira-Wigderson, 2015].*
- *Over any field [Ivanyos-Q-Subrahmanyam, 2015].*

Progress on ncrk in 2015

Theorem

ncrk *can be computed in deterministic polynomial time.*

- *Over $\mathbb{Q}$ [Garg-Gurvits-Oliveira-Wigderson, 2015].*
- *Over any field [Ivanyos-Q-Subrahmanyam, 2015].*

- The previous record is PSPACE [Cohn-Reutenauer 1999].
- Algorithm techniques are completely different.
- The analyses of both algorithms rely on an invariant-theoretic quantity.

Progress on ncrk in 2015

Theorem

ncrk *can be computed in deterministic polynomial time.*

- *Over $\mathbb{Q}$ [Garg-Gurvits-Oliveira-Wigderson, 2015].*
- *Over any field [Ivanyos-Q-Subrahmanyam, 2015].*

- The previous record is PSPACE [Cohn-Reutenauer 1999].
- Algorithm techniques are completely different.
- The analyses of both algorithms rely on an invariant-theoretic quantity.

In this talk, we focus on a result in invariant theory, which implies that $\mathrm{ncrk} \in \mathrm{NP} \cap \mathrm{coNP}$, and is a key to the algorithm in [IQS].

Non-commutative rank and matrix semi-invariants

Matrix invariants and semi-invariants

$M(n, \mathbb{F})^{\oplus m}$: the linear space of m-tuples of $n \times n$ matrices over $\mathbb{F}$.

$P = \mathbb{F}[x_{i,j,k} : i \in [m], j, k \in [n]]$: the ring of polynomial functions on $M(n, \mathbb{F})^{\oplus m}$.

Matrix invariants and semi-invariants

$M(n,\mathbb{F})^{\oplus m}$**:** the linear space of m-tuples of $n \times n$ matrices over $\mathbb{F}$.

$P = \mathbb{F}[x_{i,j,k} : i \in [m], j, k \in [n]]$**:** the ring of polynomial functions on $M(n,\mathbb{F})^{\oplus m}$.

Two actions and two invariant rings

Simul. conjugation $A \in \mathrm{SL}(n,\mathbb{F})$ sends

$$(B_1, \ldots, B_m) \in M(n,\mathbb{F})^{\oplus m} \to (AB_1A^{-1}, \ldots, AB_mA^{-1}).$$

Simul. left-right mult. $(A, D) \in \mathrm{SL}(n,\mathbb{F}) \times \mathrm{SL}(n,\mathbb{F})$ sends

$$(B_1, \ldots, B_m) \in M(n,\mathbb{F})^{\oplus m} \to (AB_1D^{-1}, \ldots, AB_mD^{-1}).$$

Matrix invariants and semi-invariants

$M(n,\mathbb{F})^{\oplus m}$**:** the linear space of m-tuples of $n \times n$ matrices over $\mathbb{F}$.

$P = \mathbb{F}[x_{i,j,k} : i \in [m], j, k \in [n]]$**:** the ring of polynomial functions on $M(n,\mathbb{F})^{\oplus m}$.

Two actions and two invariant rings

Simul. conjugation $A \in \mathrm{SL}(n,\mathbb{F})$ sends

$$(B_1, \dots, B_m) \in M(n,\mathbb{F})^{\oplus m} \to (AB_1A^{-1}, \dots, AB_mA^{-1}).$$

Simul. left-right mult. $(A, D) \in \mathrm{SL}(n,\mathbb{F}) \times \mathrm{SL}(n,\mathbb{F})$ sends

$$(B_1, \dots, B_m) \in M(n,\mathbb{F})^{\oplus m} \to (AB_1D^{-1}, \dots, AB_mD^{-1}).$$

The ring of matrix invariants

$MI(n, m) = \{f \in P : f \text{ invariant under simul. conjugation action}\}$.

The ring of matrix semi-invariants

$MSI(n, m) = \{f \in P : f \text{ invariant under simul. left-right action}\}$.

Matrix semi-invariants and the non-commutative rank

For an invariant ring R, let the *nullcone* of R, $N(R)$, be the set of common zeros of those $f \in R$ w/o constant term [Hilbert, 1893].

Theorem ([Fortin-Reutenauer, 2004 & Bürgin-Draisma, 2006])

Let $T = B_1x_1 + \cdots + B_mx_m$, *and* $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m}$. $\mathrm{ncrk}(T) < n \iff \mathbf{B} \in N(MSI(n, m))$.

Matrix semi-invariants and the non-commutative rank

For an invariant ring R, let the *nullcone* of R, $N(R)$, be the set of common zeros of those $f \in R$ w/o constant term [Hilbert, 1893].

Theorem ([Fortin-Reutenauer, 2004 & Bürgin-Draisma, 2006])

Let $T = B_1x_1 + \cdots + B_mx_m$, and $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m}$.
$\mathrm{ncrk}(T) < n \iff \mathbf{B} \in N(MSI(n, m))$.

- Suppose $\mathrm{ncrk}(T) = n$. Then $\mathbf{B} \notin N(MSI(n, m))$, so $\exists f \in MSI(n, m)$ w/o constant term, s.t. $f(\mathbf{B}) \neq 0$.
- *If furthermore* $\deg(f) \leq \mathrm{poly}(n)$, then $\mathrm{ncrk} \in \mathrm{NP} \cap \mathrm{coNP}$.

Matrix semi-invariants and the non-commutative rank

For an invariant ring R, let the *nullcone* of R, $N(R)$, be the set of common zeros of those $f \in R$ w/o constant term [Hilbert, 1893].

Theorem ([Fortin-Reutenauer, 2004 & Bürgin-Draisma, 2006])

Let $T = B_1 x_1 + \cdots + B_m x_m$, *and* $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m}$. $\mathrm{ncrk}(T) < n \iff \mathbf{B} \in N(MSI(n, m))$.

- Suppose $\mathrm{ncrk}(T) = n$. Then $\mathbf{B} \notin N(MSI(n, m))$, so $\exists f \in MSI(n, m)$ w/o constant term, s.t. $f(\mathbf{B}) \neq 0$.
- *If furthermore* $\deg(f) \leq \mathrm{poly}(n)$, then $\mathrm{ncrk} \in \mathrm{NP} \cap \mathrm{coNP}$.

Definition

Let $R_{\leq d} = \{f \in R : \deg(f) \leq d\}$. Define

$$\beta(R) = \min\{d \in \mathbb{N} : R \text{ is generated by } R_{\leq d}\}.$$

$$\sigma(R) = \min\{d \in \mathbb{N} : N(R) \text{ is defined by } R_{\leq d}\}.$$

A timeline for $\beta(MI(n,m))$, $\beta(MSI(n,m))$, $\sigma(MSI(n,m))$

♠ general results not limited to *MI* and *MSI*.

♣ for *MI* or *MSI*.

1893, ♠ | Hilbert showed that all of them are finite.

A timeline for $\beta(MI(n,m))$, $\beta(MSI(n,m))$, $\sigma(MSI(n,m))$

♠ general results not limited to *MI* and *MSI*.

♣ for *MI* or *MSI*.

1893, ♠ Hilbert showed that all of them are finite.

1976, ♣ Procesi, Razmyslov: $\beta(MI(n,m)) \leq n^2$.

A timeline for $\beta(MI(n,m))$, $\beta(MSI(n,m))$, $\sigma(MSI(n,m))$

♠ general results not limited to *MI* and *MSI*.

♣ for *MI* or *MSI*.

- 1893, ♠ — Hilbert showed that all of them are finite.
- 1976, ♣ — Procesi, Razmyslov: $\beta(MI(n,m)) \leq n^2$.
- 1982, ♠ — Popov gave the first effective bounds.

A timeline for $\beta(MI(n, m))$, $\beta(MSI(n, m))$, $\sigma(MSI(n, m))$

- ♠ general results not limited to *MI* and *MSI*.
- ♣ for *MI* or *MSI*.

1893, ♠	Hilbert showed that all of them are finite.
1976, ♣	Procesi, Razmyslov: $\beta(MI(n, m)) \leq n^2$.
1982, ♠	Popov gave the first effective bounds.
2001, ♠	Derksen substantially improved Popov's bound. From there, $\beta(MSI(n, m))$ and $\sigma(MSI(n, m))$ are polynomially related, and $\sigma(MSI(n, m)) \leq 2^{O(n^2)}$.

A timeline for $\beta(MI(n,m))$, $\beta(MSI(n,m))$, $\sigma(MSI(n,m))$

- ♠ general results not limited to *MI* and *MSI*.
- ♣ for *MI* or *MSI*.

1893, ♠ Hilbert showed that all of them are finite.

1976, ♣ Procesi, Razmyslov: $\beta(MI(n,m)) \leq n^2$.

1982, ♠ Popov gave the first effective bounds.

2001, ♠ Derksen substantially improved Popov's bound. From there, $\beta(MSI(n,m))$ and $\sigma(MSI(n,m))$ are polynomially related, and $\sigma(MSI(n,m)) \leq 2^{O(n^2)}$.

2015, ♣ Derksen-Makam, Ivanyos-Q-Subrahmanyam: $\sigma(MSI(n,m)) \leq n^2 \pm n$.

The $n^2 + n$ bound on $\sigma(MSI(n, m))$, I

Two components of the proof: regularity lemma [IQSa], and a reduction procedure [DM, IQSb].

The $n^2 + n$ bound on $\sigma(MSI(n, m))$, I

Two components of the proof: regularity lemma [IQSa], and a reduction procedure [DM, IQSb].

Recall that for $\mathcal{B} \leq M(n, \mathbb{F})$, $\mathrm{maxrk}(\mathcal{B}) = \max\{\mathrm{rk}(B) : B \in \mathcal{B}\}$.

Lemma (Regularity lemma, [IQSa])

Let $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq M(n, \mathbb{F})$. $\mathcal{B} \otimes M(d, \mathbb{F}) \leq M(nd, \mathbb{F})$. Then d divides $\mathrm{maxrk}(\mathcal{B} \otimes M(d, \mathbb{F}))$.

The $n^2 + n$ bound on $\sigma(MSI(n,m))$, I

Two components of the proof: regularity lemma [IQSa], and a reduction procedure [DM, IQSb].

Recall that for $\mathcal{B} \leq M(n, \mathbb{F})$, $\mathrm{maxrk}(\mathcal{B}) = \max\{\mathrm{rk}(B) : B \in \mathcal{B}\}$.

Lemma (Regularity lemma, [IQSa])

Let $\mathcal{B} = \langle B_1, \ldots, B_m \rangle \leq M(n, \mathbb{F})$. $\mathcal{B} \otimes M(d, \mathbb{F}) \leq M(nd, \mathbb{F})$. Then d divides $\mathrm{maxrk}(\mathcal{B} \otimes M(d, \mathbb{F}))$.

Proof idea

1. $M(d, \mathbb{F})$ can be "replaced" w/ a division algebra $D \subseteq M(d, \mathbb{K})$.
   - Based on classical results by Kummer, Artin-Schreier-Witt, Wedderburn.
2. Every $A \in \mathcal{B} \otimes D$ has rank divisible by d.
3. Transfer between $\otimes M(n, \mathbb{F})$ and $\otimes D$.

The $n^2 + n$ bound on $\sigma(MSI(n,m))$, II

1. If $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m} \notin N(MSI(n,m))$, then $\exists (A_1, \ldots, A_m) \in M(d, \mathbb{F})^{\oplus m}$, such that $C = B_1 \otimes A_1 + \cdots + B_m \otimes A_m$ is of full rank ($= nd$).
    - The first fundamental theorem for MSI [Derksen-Weyman; Domokos-Zubkov; Schofield-Van der Bergh].

The $n^2 + n$ bound on $\sigma(MSI(n,m))$, II

1. If $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m} \notin N(MSI(n,m))$, then $\exists (A_1, \ldots, A_m) \in M(d, \mathbb{F})^{\oplus m}$, such that $C = B_1 \otimes A_1 + \cdots + B_m \otimes A_m$ is of full rank ($= nd$).
   - The first fundamental theorem for MSI [Derksen-Weyman; Domokos-Zubkov; Schofield-Van der Bergh].
2. If $d > n + 1$, we can delete n rows and n columns from C to obtain $C' = B_1 \otimes A'_1 + \cdots + B_m \otimes A'_m \in \mathcal{B} \otimes M(d-1, \mathbb{F})$ of rank $\geq nd - 2n$.
   - When $d > n + 1$, $nd - 2n > (d-1)(n-1)$.

The $n^2 + n$ bound on $\sigma(MSI(n, m))$, II

1. If $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m} \notin N(MSI(n, m))$, then $\exists (A_1, \ldots, A_m) \in M(d, \mathbb{F})^{\oplus m}$, such that $C = B_1 \otimes A_1 + \cdots + B_m \otimes A_m$ is of full rank ($= nd$).
   - The first fundamental theorem for MSI [Derksen-Weyman; Domokos-Zubkov; Schofield-Van der Bergh].
2. If $d > n + 1$, we can delete n rows and n columns from C to obtain $C' = B_1 \otimes A_1' + \cdots + B_m \otimes A_m' \in \mathcal{B} \otimes M(d-1, \mathbb{F})$ of rank $\geq nd - 2n$.
   - When $d > n + 1$, $nd - 2n > (d-1)(n-1)$.
3. Use the regularity lemma to obtain a full-rank ($= (d-1)n$) $C'' = B_1 \otimes A_1'' + \cdots + B_m \otimes A_m'' \in \mathcal{B} \otimes M(d-1, \mathbb{F})$.

The $n^2 + n$ bound on $\sigma(MSI(n,m))$, II

1. If $\mathbf{B} = (B_1, \ldots, B_m) \in M(n, \mathbb{F})^{\oplus m} \notin N(MSI(n,m))$, then $\exists (A_1, \ldots, A_m) \in M(d, \mathbb{F})^{\oplus m}$, such that $C = B_1 \otimes A_1 + \cdots + B_m \otimes A_m$ is of full rank ($= nd$).
   - The first fundamental theorem for MSI [Derksen-Weyman; Domokos-Zubkov; Schofield-Van der Bergh].
2. If $d > n + 1$, we can delete n rows and n columns from C to obtain $C' = B_1 \otimes A_1' + \cdots + B_m \otimes A_m' \in \mathcal{B} \otimes M(d-1, \mathbb{F})$ of rank $\geq nd - 2n$.
   - When $d > n+1$, $nd - 2n > (d-1)(n-1)$.
3. Use the regularity lemma to obtain a full-rank ($= (d-1)n$) $C'' = B_1 \otimes A_1'' + \cdots + B_m \otimes A_m'' \in \mathcal{B} \otimes M(d-1, \mathbb{F})$.

Remark

This was the second reduction procedure as in [IQSb]. The first reduction procedure was discovered by Derksen and Makam.

Some concluding remarks

A remark on $\mathrm{ncrk} \in \mathrm{P}$

An analogy between bipartite graphs and matrix spaces.

Bipartite graphs	
Vertex set	Sets L and R.
Edge set	Subsets of $L \times R$.
Isomorphism	$\mathrm{Sym}(L) \times \mathrm{Sym}(R)$.

Matrix spaces	
Vertices	Vector spaces V and U.
Edges	Subspaces of $V \otimes U$.
Isomorphism	$\mathrm{GL}(V) \times \mathrm{GL}(U)$.

A remark on $\mathrm{ncrk} \in \mathrm{P}$

An analogy between bipartite graphs and matrix spaces.

Bipartite graphs

Vertex set Sets L and R.

Edge set Subsets of $L \times R$.

Isomorphism $\mathrm{Sym}(L) \times \mathrm{Sym}(R)$.

Matrix spaces

Vertices Vector spaces V and U.

Edges Subspaces of $V \otimes U$.

Isomorphism $\mathrm{GL}(V) \times \mathrm{GL}(U)$.

This analogy motivates to adapt algorithmic techniques on bipartite graphs to tackle ncrk.

Ivanyos-Q-Subrahmanyam resorts to the augmenting path idea, and uses that $\sigma(MSI(n, m)) \leq n^2 + n$.

Garg-Gurvits-Oliveira-Wigderson resorts to the alternating scaling idea, and uses that $\sigma(MSI(n, m)) \leq 2^{O(n^2)}$.

Some further remarks

- The resolutions of the ncrk problem rely a nice combination of invariant theory, non-commutative algebra, combinatorics and optimisation, quantum theory, and algorithm design and analysis.

Some further remarks

- The resolutions of the ncrk problem rely a nice combination of invariant theory, non-commutative algebra, combinatorics and optimisation, quantum theory, and algorithm design and analysis.
- It opens up a new line of thoughts on the crk problem, which is of fundamental importance in computational complexity.

Some further remarks

- The resolutions of the ncrk problem rely a nice combination of invariant theory, non-commutative algebra, combinatorics and optimisation, quantum theory, and algorithm design and analysis.
- It opens up a new line of thoughts on the crk problem, which is of fundamental importance in computational complexity.
- The analogy between bipartite graphs and matrix spaces seems to have further potential. The next talk will serve as another example on how a similar analogy can be useful in computing with finite groups.

Thank you for your attention.

Questions please?