Matrix coefficient realization theory of noncommutative rational functions

Jurij Volčič (Joint work with Igor Klep)

The University of Auckland

Lens 2015

Jurij Volčič (UoA)

Matrix realizations of nc rational functions

Lens '15 1 / 17

- Theory of skew fields: universal construction
- Theoretical computer science: weighted finite automata
- Free real algebraic geometry: linear matrix inequalities
- Systems/control theory: linear systems evolving on a free group
- Noncommutative symmetric functions: quasi-determinants

Nc rational expressions

 \mathbb{F} a field of characteristic 0, $Z = \{z_1, \dots, z_g\}$, $\mathbb{F} < Z >$ nc polynomials.

Nc rational expressions

 $\mathbb F$ a field of characteristic 0, $Z=\{z_1,\ldots,z_g\},$ $\mathbb F{<}Z{>}$ nc polynomials.

 $\mathcal{R}_{\mathbb{F}}(Z)$ nc rational expressions built from $\mathbb{F} < Z >$ using $+, \cdot, -1, (,)$, e.g. $z_2(1 + z_2^{-1}(z_1 - 3)^{-1})^{-1}, (z_2 - z_2)^{-1}$.

Nc rational expressions

 $\mathbb F$ a field of characteristic 0, $Z=\{z_1,\ldots,z_g\},$ $\mathbb F{<}Z{>}$ nc polynomials.

 $\mathcal{R}_{\mathbb{F}}(Z)$ nc rational expressions built from $\mathbb{F} < Z >$ using $+, \cdot, -1, (,)$, e.g. $z_2(1 + z_2^{-1}(z_1 - 3)^{-1})^{-1}, (z_2 - z_2)^{-1}$.

Evaluations on matrices:

- $\mathcal{M} = \bigcup_{m \in \mathbb{N}} M_m(\mathbb{F})^g$.
- dom r is the subset of \mathcal{M} where $r \in \mathcal{R}_{\mathbb{F}}(Z)$ is defined; dom_m r = dom r $\cap M_m(\mathbb{F})^g$.
- *r* is **degenerate** if dom $r = \emptyset$ and **nondegenerate** otherwise.
- For nondegenerate r_1 and r_2 : $r_1 \sim r_2$ iff $r_1(a) = r_2(a)$ for all $a \in \text{dom } r_1 \cap \text{dom } r_2$.

ヘロト 不得 とくき とくきとうき

Nc rational functions are equivalence classes of nondegenerate expressions, $\mathbb{F} \notin \mathbb{Z}$. This is a skew field (with obvious operations). The class of r is \mathbb{r} , dom $\mathbb{r} = \bigcup_{r \in \mathbb{r}} \text{dom } r$.

Nc rational functions are equivalence classes of nondegenerate expressions, $\mathbb{F}\langle Z \rangle$. This is a skew field (with obvious operations). The class of r is \mathbb{r} , dom $\mathbb{r} = \bigcup_{r \in \mathbb{r}} \operatorname{dom} r$.

This construction is due to Helton, McCullough, Vinnikov.

Nc rational functions are equivalence classes of nondegenerate expressions, $\mathbb{F} \notin \mathbb{Z}$. This is a skew field (with obvious operations). The class of r is \mathbb{r} , dom $\mathbb{r} = \bigcup_{r \in \mathbb{r}} \text{dom } r$.

This construction is due to Helton, McCullough, Vinnikov. We can also describe $\mathbb{F} \not\in Z$ using

- rational expressions over an ∞ -dim skew field (Amitsur, Bergman),
- full matrices over $\mathbb{F} < Z >$ (Cohn),
- Malcev-Neumann construction on a free group (Lewin),
- skew field associated to a free Lie algebra (Lichtman).

(人間) システン イラン

Universal property

 $\mathbb{F}\langle Z \rangle$ is **the universal skew field of fractions** of $\mathbb{F}\langle Z \rangle$, i.e., for every skew field $D \supseteq \mathbb{F}$ and epimorphism $\mathbb{F}\langle Z \rangle \rightarrow D$ we have a commutative diagram



where K is a local ring and $\phi: K \to D$ satisfies $\phi(x) \neq 0 \Rightarrow x^{-1} \in K$.

・聞き くほき くほき 二日

 $\mathbb{F}\langle Z \rangle$ is **the universal skew field of fractions** of $\mathbb{F}\langle Z \rangle$, i.e., for every skew field $D \supseteq \mathbb{F}$ and epimorphism $\mathbb{F}\langle Z \rangle \to D$ we have a commutative diagram



where K is a local ring and $\phi: K \to D$ satisfies $\phi(x) \neq 0 \Rightarrow x^{-1} \in K$.

Informally: if a nc rational expression vanishes on all tuples of matrices over \mathbb{F} , then it vanishes on all tuples of elements in D, where D is an arbitrary skew field containing \mathbb{F} .

Such expressions are called rational identities.

◆□▶ ▲□▶ ▲ヨ▶ ▲ヨ▶ = 目 - のへ⊙

Functions analytic at the origin

It can be hard to distinguish nc rational functions; e.g.

$$(z_1 - (1 + z_2)^{-1}z_1(1 + z_2))((1 + z_2)^{-1}z_1(1 + z_2) - z_2^{-1}z_1z_2^{-1})^{-1} - z_2$$

represents 0, i.e., is a rational identity. Alternative description?

Functions analytic at the origin

It can be hard to distinguish nc rational functions; e.g.

$$(z_1 - (1 + z_2)^{-1}z_1(1 + z_2))((1 + z_2)^{-1}z_1(1 + z_2) - z_2^{-1}z_1z_2^{-1})^{-1} - z_2$$

represents 0, i.e., is a rational identity. Alternative description?

Let $r \in \mathcal{R}_{\mathbb{F}}(Z)$. If $(0, ..., 0) \in \text{dom } r$, then we can expand r into a noncommutative power series $S \in \mathbb{F} \ll Z \gg$. Such a series is **rational**, i.e., it belongs to the rational closure of $\mathbb{F} < Z >$ in $\mathbb{F} \ll Z \gg$.

Functions analytic at the origin

It can be hard to distinguish nc rational functions; e.g.

$$(z_1 - (1 + z_2)^{-1}z_1(1 + z_2))((1 + z_2)^{-1}z_1(1 + z_2) - z_2^{-1}z_1z_2^{-1})^{-1} - z_2$$

represents 0, i.e., is a rational identity. Alternative description?

Let $r \in \mathcal{R}_{\mathbb{F}}(Z)$. If $(0, ..., 0) \in \text{dom } r$, then we can expand r into a noncommutative power series $S \in \mathbb{F} \ll Z \gg$. Such a series is **rational**, i.e., it belongs to the rational closure of $\mathbb{F} < Z >$ in $\mathbb{F} \ll Z \gg$.

Theorem (Schützenberger, '61)

Every rational series *S* has a linear representation, *i.e.*, there exists $n \in \mathbb{N}$ and $\mathbf{c} \in \mathbb{F}^{1 \times n}$, $\mathbf{b} \in \mathbb{F}^{n \times 1}$ and $A_j \in \mathbb{F}^{n \times n}$ for $1 \leq j \leq g$, such that

$$S = \mathbf{c} \left(I_n - \sum_{j=1}^g A_j z_j \right)^{-1} \mathbf{b}.$$

Previous result can be applied to rational expressions defined at some point in \mathbb{F}^g . What about other rational expressions, e.g. $(z_1z_2 - z_2z_1)^{-1}$?

Previous result can be applied to rational expressions defined at some point in \mathbb{F}^g . What about other rational expressions, e.g. $(z_1z_2 - z_2z_1)^{-1}$?

Let $m \in \mathbb{N}$. The algebra of **generalized polynomials over** $M_m(\mathbb{F})$ is defined as

$$M_m(\mathbb{F}) {<} Z {>} := M_m(\mathbb{F}) *_{\mathbb{F}} \mathbb{F} {<} Z {>} .$$

Its (*Z*)-completion is called the algebra of **generalized series over** $M_m(\mathbb{F})$ and denoted $M_m(\mathbb{F}) \ll Z \gg$.

Previous result can be applied to rational expressions defined at some point in \mathbb{F}^g . What about other rational expressions, e.g. $(z_1z_2 - z_2z_1)^{-1}$?

Let $m \in \mathbb{N}$. The algebra of **generalized polynomials over** $M_m(\mathbb{F})$ is defined as

$$M_m(\mathbb{F}) < Z > := M_m(\mathbb{F}) *_{\mathbb{F}} \mathbb{F} < Z > .$$

Its (*Z*)-completion is called the algebra of **generalized series over** $M_m(\mathbb{F})$ and denoted $M_m(\mathbb{F}) \ll Z \gg$.

Assume r is defined at $p \in M_m(\mathbb{F})^g$. Then we can expand r into a generalized series S about the point p. Again, this series belongs to the rational closure of $M_m(\mathbb{F}) < Z >$ in $M_m(\mathbb{F}) \ll Z \gg$.

Realizations

If $S \in M_m(\mathbb{F}) \ll Z \gg$ is a rational series, then there exists $n \in \mathbb{N}$ and $\mathbf{c} \in M_m(\mathbb{F})^{1 \times n}$, $\mathbf{b} \in M_m(\mathbb{F})^{n \times 1}$, $A_j \in \sum M_m(\mathbb{F})^{n \times n} z_j M_m(\mathbb{F})^{n \times n}$

for $1 \leq j \leq g$, such that

$$S = \mathbf{c} \left(I_n - \sum_{j=1}^g A_j \right)^{-1} \mathbf{b}.$$

 $(\mathbf{b}, A, \mathbf{c})$ is called a **(linear) representation** of S of dimension n.

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 善臣 - のへで

Realizations

If $S \in M_m(\mathbb{F}) \ll Z \gg$ is a rational series, then there exists $n \in \mathbb{N}$ and $\mathbf{c} \in M_m(\mathbb{F})^{1 \times n}$, $\mathbf{b} \in M_m(\mathbb{F})^{n \times 1}$, $A_j \in \sum M_m(\mathbb{F})^{n \times n} z_j M_m(\mathbb{F})^{n \times n}$

for $1 \leq j \leq g$, such that

$$S = \mathbf{c} \left(I_n - \sum_{j=1}^{g} A_j \right)^{-1} \mathbf{b}.$$

 $(\mathbf{b}, A, \mathbf{c})$ is called a **(linear) representation** of S of dimension n.

If $r \in \mathcal{R}_{\mathbb{F}}(Z)$ is defined at $p \in M_m(\mathbb{F})^g$ and S is its expansion about p, then $(\mathbf{b}, A, \mathbf{c})$ is called a **realization of** r **about** p of dimension n.

Interpretation

Let $(\mathbf{b}, A, \mathbf{c})$ be a realization of r about p and let $s \in \mathbb{N}$. With some abuse of the notation we can write

$$\mathbf{c}\left(I_{nms}-\sum_{j=1}^{g}A_{j}(q_{j}-p_{j})
ight)^{-1}\mathbf{b}=r(q)\in M_{ms}(\mathbb{F})$$

for $q \in M_{ms}(\mathbb{F})^g$, where the entries of **c**, **b** and A_j are considered as elements in $M_{ms}(\mathbb{F})$ using the embedding

$$M_m(\mathbb{F}) \hookrightarrow M_{ms}(\mathbb{F}), \qquad a \mapsto \begin{pmatrix} a & & \\ & \ddots & \\ & & a \end{pmatrix}$$

Two examples

Realization of $((1 - z_1 - z_2(1 - z_1)^{-1}z_2)^{-1}$ about (0, 0):

$$\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} I_2 - \begin{pmatrix} z_1 & 0 \\ 0 & z_1 \end{pmatrix} - \begin{pmatrix} 0 & z_2 \\ z_2 & 0 \end{pmatrix} \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Realization of $(z_1z_2 - z_2z_1)^{-1}$ about $(p_1, p_2) \in M_2(\mathbb{F})^2$ assuming that $p_1p_2 - p_2p_1$ is invertible with inverse q:

$$\mathbf{c} \left(l_3 - A_1(z_1 - p_1) - A_2(z_2 - p_2) \right)^{-1} \mathbf{b}, \text{ where}$$

$$\mathbf{c} = \left(q \quad 0 \quad 0 \right), \quad A_1 = \begin{pmatrix} -z_1 p_2 q + p_2 z_1 q & z_1 & 0 \\ 0 & 0 & 0 \\ -z_1 q & 0 & 0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} z_2 p_1 q - p_1 z_2 q & 0 & -z_2 \\ -z_2 q & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mathbf{b} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Jurij Volčič (UoA)

Matrix realizations of nc rational functions

Let $(\mathbf{b}, A, \mathbf{c})$ be a representation over $M_m(\mathbb{F})$ of dimension *n* of series *S*. Its **obstruction modules** are

$$\mathcal{U}_L = \{ \mathbf{u} \in M_m(\mathbb{F})^{1 \times n} : \mathbf{u} A_{i_1} \dots A_{i_\ell} \mathbf{b} = 0 \ \forall i_j, \ell \}, \\ \mathcal{U}_R = \{ \mathbf{u} \in M_m(\mathbb{F})^{n \times 1} : \mathbf{c} A_{i_1} \dots A_{i_\ell} \mathbf{u} = 0 \ \forall i_j, \ell \}.$$

Let $(\mathbf{b}, A, \mathbf{c})$ be a representation over $M_m(\mathbb{F})$ of dimension *n* of series *S*. Its **obstruction modules** are

$$\mathcal{U}_L = \{ \mathbf{u} \in M_m(\mathbb{F})^{1 \times n} : \mathbf{u} A_{i_1} \dots A_{i_\ell} \mathbf{b} = 0 \ \forall i_j, \ell \}, \\ \mathcal{U}_R = \{ \mathbf{u} \in M_m(\mathbb{F})^{n \times 1} : \mathbf{c} A_{i_1} \dots A_{i_\ell} \mathbf{u} = 0 \ \forall i_j, \ell \}.$$

We say that $(\mathbf{b}, A, \mathbf{c})$ is

- reduced if \mathcal{U}_L and \mathcal{U}_R are torsion $M_m(\mathbb{F})$ -modules;
- minimal if its dimension is minimal amongst all representations of S;
- totally reduced if if U_L and U_R are trivial.

1 totally reduced \Rightarrow minimal \Rightarrow reduced.

- **1** totally reduced \Rightarrow minimal \Rightarrow reduced.
- We have an algorithm that transforms any representation into a reduced one.

- **1** totally reduced \Rightarrow minimal \Rightarrow reduced.
- We have an algorithm that transforms any representation into a reduced one.
- If dim_𝔅 U_L + dim_𝔅 U_R < m² holds for a reduced representation, then it is minimal.

- totally reduced \Rightarrow minimal \Rightarrow reduced.
- We have an algorithm that transforms any representation into a reduced one.
- If dim_𝔅 U_L + dim_𝔅 U_R < m² holds for a reduced representation, then it is minimal.
- The dimension of a reduced representation is greater than the minimal one for at most 1.

- totally reduced \Rightarrow minimal \Rightarrow reduced.
- We have an algorithm that transforms any representation into a reduced one.
- If dim_𝔅 U_L + dim_𝔅 U_R < m² holds for a reduced representation, then it is minimal.
- The dimension of a reduced representation is greater than the minimal one for at most 1.
- S A totally reduced representation is unique up to a basis change.

- totally reduced \Rightarrow minimal \Rightarrow reduced.
- We have an algorithm that transforms any representation into a reduced one.
- If dim_𝔅 U_L + dim_𝔅 U_R < m² holds for a reduced representation, then it is minimal.
- The dimension of a reduced representation is greater than the minimal one for at most 1.
- **(3)** A totally reduced representation is unique up to a basis change.
- For a rational expression and "almost every" point in its domain, we can find its totally reduced realization using the previously mentioned algorithm.

Can we get a smaller realization about a different $p' \in M_m(\mathbb{F})^g$?

Can we get a smaller realization about a different $p' \in M_m(\mathbb{F})^g$?

Or about $p' \in M_{m'}(\mathbb{F})^g$ for some $m' \neq m$?

Can we get a smaller realization about a different $p' \in M_m(\mathbb{F})^g$?

Or about $p' \in M_{m'}(\mathbb{F})^g$ for some $m' \neq m$?

The answer is **no**.

Can we get a smaller realization about a different $p' \in M_m(\mathbb{F})^g$?

Or about
$$p' \in M_{m'}(\mathbb{F})^g$$
 for some $m' \neq m$?

The answer is **no**.

Therefore we can define **the degree** of a nc rational function. It is independent of the choice of a representing expression $r \in \mathbf{r}$, point of expansion p, and even the size of the matrices in p.

Domain of a nc rational function

$$\begin{split} r_1 &= (1 - z_1 - z_2(1 - z_1)^{-1}z_2)^{-1}, \\ r_2 &= -z_2^{-1}(1 - z_1)(z_2 - (1 - z_1)z_2^{-1}(1 - z_1))^{-1}, \\ r_3 &= (1 \quad 0) \left(I_2 - \begin{pmatrix} z_1 & 0 \\ 0 & z_1 \end{pmatrix} - \begin{pmatrix} 0 & z_2 \\ z_2 & 0 \end{pmatrix} \right)^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{split}$$

▲ 重 ト 重 つへの Lens '15 14 / 17

Domain of a nc rational function

$$\begin{split} r_1 &= (1 - z_1 - z_2 (1 - z_1)^{-1} z_2)^{-1}, \\ r_2 &= -z_2^{-1} (1 - z_1) (z_2 - (1 - z_1) z_2^{-1} (1 - z_1))^{-1}, \\ r_3 &= (1 \quad 0) \left(l_2 - \begin{pmatrix} z_1 & 0 \\ 0 & z_1 \end{pmatrix} - \begin{pmatrix} 0 & z_2 \\ z_2 & 0 \end{pmatrix} \right)^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{split}$$

It can be shown: $\mathbb{r}_1 = \mathbb{r}_2 = \mathbb{r}_3$, $(1, 1) \in \text{dom } r_2 \setminus \text{dom } r_1$, $(0, 0) \in \text{dom } r_1 \setminus \text{dom } r_2$ and dom $r_3 \supsetneq \text{dom } r_1 \cup \text{dom } r_2$.

Domain of a nc rational function

$$\begin{aligned} r_1 &= (1 - z_1 - z_2(1 - z_1)^{-1} z_2)^{-1}, \\ r_2 &= -z_2^{-1}(1 - z_1)(z_2 - (1 - z_1)z_2^{-1}(1 - z_1))^{-1}, \\ r_3 &= (1 \quad 0) \left(I_2 - \begin{pmatrix} z_1 & 0 \\ 0 & z_1 \end{pmatrix} - \begin{pmatrix} 0 & z_2 \\ z_2 & 0 \end{pmatrix} \right)^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

It can be shown: $\mathbb{r}_1 = \mathbb{r}_2 = \mathbb{r}_3$, $(1, 1) \in \text{dom } r_2 \setminus \text{dom } r_1$, $(0, 0) \in \text{dom } r_1 \setminus \text{dom } r_2$ and dom $r_3 \supsetneq \text{dom } r_1 \cup \text{dom } r_2$.

Theorem

If $(\mathbf{c}, A, \mathbf{b})$ is a totally reduced realization of \mathbb{r} about $p \in M_m(\mathbb{F})^g$, then

$$\operatorname{\mathsf{dom}}_{ms} \mathbb{r} = \left\{ q \in M^g_{ms}(\mathbb{F}) \colon \det \left(I_{nms} - \sum_{j=1}^g A_j(q_j - p_j) \right)
eq 0
ight\}.$$

The rational identity testing problem

Denote

 $\kappa(r) = \# \text{constant_terms_in_}r + 2 \cdot \# \text{letters_in_}r + \# \text{inversions_in_}r.$

Example: for

$$r = 2(z_2z_1 - 1)^{-1} - (z_1z_2^{-1} - z_2^{-1}z_1)^{-1} - 1)$$

we have $\kappa(r) = 2 + 2 \cdot 6 + 4 = 18$.

- 4 同 6 4 日 6 4 日 6

The rational identity testing problem

Denote

 $\kappa(r) = #constant_terms_in_r + 2 \cdot #letters_in_r + #inversions_in_r.$

Example: for

$$r = 2(z_2z_1 - 1)^{-1} - (z_1z_2^{-1} - z_2^{-1}z_1)^{-1} - 1)$$

we have $\kappa(r) = 2 + 2 \cdot 6 + 4 = 18$.

Theorem

Let $r \in \mathcal{R}_{\mathbb{F}}(Z)$ and assume dom_m $r \neq \emptyset$. Then r is a rational identity if and only if r vanishes on dom_N r, where

$$N=m\left\lceil \frac{m}{2}\kappa(r)\right\rceil.$$

< 回 ト < 三 ト < 三 ト

Well known: if $p \in \mathbb{F} < Z > \setminus \{0\}$ vanishes on $M_N(\mathbb{F})^g$, then the (polynomial) degree of p is at least 2N.

< 3 × 1

Well known: if $p \in \mathbb{F} < Z > \setminus \{0\}$ vanishes on $M_N(\mathbb{F})^g$, then the (polynomial) degree of p is at least 2N.

Theorem

Let $r \in \mathbb{F} \langle Z \rangle \setminus \{0\}$ and assume dom_m $r \neq \emptyset$. If r vanishes on dom_N r, then the degree of r is strictly greater than $\frac{2N}{m^2} + 1$.

References



💊 J. Berstel, C. Reutenauer:

Noncommutative rational series with applications, Encyclopedia of Mathematics and its Applications **137**, Cambridge, 2011.



P. M. Cohn: Skew fields. Theory of general division rings, Encyclopedia of Mathematics and its Applications 57, Cambridge, 1995.



J. W. Helton, S. A. McCullough, V. Vinnikov: Noncommutative convexity arises from linear matrix inequalities, Journal of Functional Analysis **240.1** (2006) 105–191.

IV:

Matrix coefficient realization theory of noncommutative rational functions, arXiv: 1505.07472.

Jurij Volčič (UoA)