Refuting Noncommutative Ideal Membership via Matrix Certificates

Clemens Hofstadler, Peter Krug, Georg Regensburger
Research Institute for Symbolic Computation (RISC), JKU Linz, Austria
Oldenburg, 16 July 2026

JOHANNES KEPLER
UNIVERSITY LINZ

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

$$x \stackrel{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

- Are we sure?

$$x \stackrel{?}{\in} I = \langle x+y+z,\, x^2+y,\, y^2+z,\, z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

- Are we sure?

```
sage: R.<x,y,z> = PolynomialRing(QQ)
sage: I = ideal([x+y+z, x^2+y, y^2+z, z^2+x])
sage: x in I
True
```

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

- Are we sure?
- Are we really sure?

```
sage: R.<x,y,z> = PolynomialRing(QQ)
sage: I = ideal([x+y+z, x^2+y, y^2+z, z^2+x])
sage: x in I
True
```

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

- Are we sure?
- Are we really sure?

```
sage: G = I.groebner_basis()
sage: x.reduce(G)
0
```

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: Yes, $x \in I$.

- Are we sure?
- Are we really sure?
- Are we really really sure?

```
sage: G = I.groebner_basis()
sage: x.reduce(G)
0
```

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x \rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: Yes, $x \in I$.

- Are we sure?
- Are we really sure?
- Are we really really sure?

$$\begin{aligned} x = \ & \frac{1}{6}(z^3 + yz^2 - xz^2 + z^2 + 2yz + 2x + 2y - 2z + 2)\cdot(x+y+z) \\ & + \frac{1}{6}(z^2 - 2)\cdot(x^2+y) \\ & - \frac{1}{6}(z^2 + 2z + 2)\cdot(y^2+z) \\ & - \frac{1}{6}(z^2 + 2yz + 4y - 4)\cdot(z^2+x) \end{aligned}$$

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

- Are we sure?

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x\rangle \subseteq \mathbb{Q}[x,y,z]$$

Answer: No, $x \notin I$.

- Are we sure?

```
sage: R.<x,y,z> = PolynomialRing(QQ)
sage: I = ideal([x^2+y, y^2+z, z^2+x])
sage: x in I
False
```

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x\rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?

```
sage: R.<x,y,z> = PolynomialRing(QQ)
sage: I = ideal([x^2+y, y^2+z, z^2+x])
sage: x in I
False
```

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x\rangle \quad \subseteq \quad \mathbb{Q}[x,y,z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?

```
sage: G = I.groebner_basis()
sage: x.reduce(G)
x
```

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?
- Are we really really sure?

```
sage: G = I.groebner_basis()
sage: x.reduce(G)
x
```

$$x \overset{?}{\in} I = \langle x+y+z,\ x^2+y,\ y^2+z,\ z^2+x\rangle \subseteq \mathbb{Q}[x,y,z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?
- Are we really really sure? – Well, not really.

$$x \overset{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x\rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?
- Are we really really sure? – Well, not really.

Certificate for non-membership

If $\exists a \in V(I) : f(a) \neq 0$ then $f \notin I$.

$$x \stackrel{?}{\in} I = \langle x + y + z,\ x^2 + y,\ y^2 + z,\ z^2 + x \rangle \quad \subseteq \quad \mathbb{Q}[x, y, z]$$

Answer: No, $x \notin I$.

- Are we sure?
- Are we really sure?
- Are we really really sure? – Well, not really.

Certificate for non-membership

If $\exists a \in V(I) : f(a) \neq 0$ then $f \notin I$.

For the example, we can pick $a = (-1, -1, -1)$.

💡 Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.

$$x \notin \langle x^2 - 2 \rangle$$

$$a = \pm\sqrt{2}$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \notin \langle x^2 - 2 \rangle \qquad\qquad x \notin \langle x^2 \rangle$$

$$a = \pm\sqrt{2} \qquad\qquad x^2(\boxed{?}) = 0 \qquad x(\boxed{?}) \neq 0$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \notin \langle x^2 - 2 \rangle \qquad x \notin \langle x^2 \rangle$$

$$a = \pm\sqrt{2} \qquad x^2(\boxed{}) = 0 \qquad x(\boxed{}) \neq 0$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \notin \langle x^2 - 2 \rangle \qquad\qquad x \notin \langle x^2 \rangle$$

$$a = \pm\sqrt{2} \qquad\qquad x^2\left(\boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}}\right) = 0 \qquad\qquad x\left(\boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}}\right) \neq 0$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \;\notin\; \langle x^2 - 2 \rangle$$

$$a = \pm\sqrt{2}$$

$$x \;\notin\; \langle x^2 \rangle$$

$$x^2\left(\boxed{\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}}\right) = 0 \qquad x\left(\boxed{\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}}\right) \neq 0$$

$$A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \notin \langle x^2 - 2 \rangle$$

$$a = \pm\sqrt{2}$$

$$A = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$$

$$x \notin \langle x^2 \rangle$$

$$x^2\left(\boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}}\right) = 0 \qquad x\left(\boxed{\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}}\right) \neq 0$$

$$A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$$

Use point $a \in V(I)$ with $f(a) \neq 0$ to certify non-membership $f \notin I$.

Problems

- Might require field extensions.
- No such point if polynomial lies in the radical.

$$x \notin \langle x^2 - 2 \rangle \qquad\qquad x \notin \langle x^2 \rangle$$

$$a = \pm\sqrt{2} \qquad\qquad x^2\left(\boxed{\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}}\right) = 0 \qquad x\left(\boxed{\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}}\right) \neq 0$$

$$A = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right) \qquad\qquad A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$$

To certify $(x-2)y \notin \langle (x-2)^2 y, y^2 \rangle$, we can use

$$A = \left(\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \right).$$

Perfect Nullstellensatz (Eisenbud, Hochster '79; Salomon, Shalit, Shamovich '18)

Let K be a field and $f, f_1, \dots, f_k \in K[x_1, \dots, x_n]$.
Then $f \notin \langle f_1, \dots, f_k \rangle$ if and only if

$\exists$ commuting square matrices $A = (A_1, \dots, A_n)$ over K:

$$f_1(A) = \cdots = f_k(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

We want non-membership certificates for noncommutative polynomials.

We want non-membership certificates for noncommutative polynomials.

$= \text{free algebra } K\langle x_1, \ldots, x_n \rangle$

We want non-membership certificates for noncommutative polynomials.

$= \text{free algebra } K\langle x_1, \ldots, x_n \rangle$

$$xy^2x - xy^2 \quad \stackrel{?}{\in} \quad I = (xyx - xy) \quad \subseteq \quad \mathbb{Q}\langle x, y \rangle$$

We want non-membership certificates for noncommutative polynomials.

$= \text{free algebra } K\langle x_1, \ldots, x_n \rangle$

$$xy^2x - xy^2 \overset{?}{\in} I = (xyx - xy) \subseteq \mathbb{Q}\langle x, y \rangle$$

✔ $f \in (f_1, \ldots, f_r)$

can always be verified via GBs

$$\begin{aligned} xy^2x - xy^2 &= (xyx - xy) \cdot (y - yx) \\ &\quad + xy \cdot (xyx - xy) \end{aligned}$$

We want non-membership certificates for noncommutative polynomials.

= free algebra $K\langle x_1, \dots, x_n \rangle$

$$xy^2x - yxy \overset{?}{\in} I = (xyx - xy) \subseteq \mathbb{Q}\langle x, y \rangle$$

✓ $f \in (f_1, \dots, f_r)$

can always be verified via GBs

$$\begin{aligned} xy^2x - xy^2 &= (xyx - xy) \cdot (y - yx) \\ &\quad + xy \cdot (xyx - xy) \end{aligned}$$

We want non-membership certificates for noncommutative polynomials.

$= \text{free algebra } K\langle x_1, \ldots, x_n \rangle$

$$xy^2x - yxy \stackrel{?}{\in} I = (xyx - xy) \quad \subseteq \quad \mathbb{Q}\langle x, y \rangle$$

✔ $f \in (f_1, \ldots, f_r)$

can always be verified via GBs

$$xy^2x - xy^2 = (xyx - xy) \cdot (y - yx) + xy \cdot (xyx - xy)$$

✘ $f \notin (f_1, \ldots, f_r)$

may lead to an **infinite GB computation**

$\Rightarrow$ need other methods

We want non-membership certificates for noncommutative polynomials.
$= \text{free algebra } K\langle x_1, \ldots, x_n\rangle$

$$xy^2x - yxy \overset{?}{\in} I = (xyx - xy) \subseteq \mathbb{Q}\langle x, y\rangle$$

✔ $f \in (f_1, \ldots, f_r)$

can always be verified via GBs

$$xy^2x - xy^2 = (xyx - xy) \cdot (y - yx) + xy \cdot (xyx - xy)$$

✘ $f \notin (f_1, \ldots, f_r)$

may lead to an **infinite GB computation**

$\Rightarrow$ need other methods

Matrix certificate $\quad A = \left(\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right)$

$$(xyx - xy)(A) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad (xy^2x - yxy)(A) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Matrix Certificate

Let $f, f_1, \dots, f_r \in K\langle x_1, \dots, x_n \rangle$. A matrix certificate of non-membership for f in $(f_1, \dots, f_r)$ is a tuple of square matrices $A = (A_1, \dots, A_n)$ over K with

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

Matrix Certificate

Let $f, f_1, \ldots, f_r \in K\langle x_1, \ldots, x_n \rangle$. A matrix certificate of non-membership for f in $(f_1, \ldots, f_r)$ is a tuple of square matrices $A = (A_1, \ldots, A_n)$ over K with

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

- Matrix certificates cannot always exist.

Matrix Certificate

Let $f, f_1, \ldots, f_r \in K\langle x_1, \ldots, x_n \rangle$. A matrix certificate of non-membership for f in $(f_1, \ldots, f_r)$ is a tuple of square matrices $A = (A_1, \ldots, A_n)$ over K with

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

- Matrix certificates cannot always exist.
- Square matrices are not enough:

$$yx - 1 \quad \notin \quad (xy - 1) \quad \subseteq \quad \mathbb{Q}\langle x, y \rangle$$

Matrix Certificate

Let $f, f_1, \ldots, f_r \in K\langle x_1, \ldots, x_n\rangle$. A matrix certificate of non-membership for f in $(f_1, \ldots, f_r)$ is a tuple of square matrices $A = (A_1, \ldots, A_n)$ over K with

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

- Matrix certificates cannot always exist.
- Square matrices are not enough:

$$yx - 1 \notin (xy - 1) \subseteq \mathbb{Q}\langle x, y\rangle$$

$$A = \left(\begin{pmatrix} 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)$$

Matrix Certificate

Let $f, f_1, \ldots, f_r \in K\langle x_1, \ldots, x_n \rangle$. A matrix certificate of non-membership for f in $(f_1, \ldots, f_r)$ is a tuple of ~~square~~ matrices $A = (A_1, \ldots, A_n)$ over K with
rectangular

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

- Matrix certificates cannot always exist.
- Square matrices are not enough:

$$yx - 1 \quad \notin \quad (xy - 1) \quad \subseteq \quad \mathbb{Q}\langle x, y \rangle$$

$$A = \left(\begin{pmatrix} 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

Matrix Certificate

Let $f, f_1, \ldots, f_r \in K\langle x_1, \ldots, x_n \rangle$. A matrix certificate of non-membership for f in $(f_1, \ldots, f_r)$ is a tuple of ~~square~~ matrices $A = (A_1, \ldots, A_n)$ over K with rectangular

$$f_1(A) = \cdots = f_r(A) = 0 \quad \text{and} \quad f(A) \neq 0.$$

- Matrix certificates cannot always exist.
- Square matrices are not enough:

$$yx - 1 \notin (xy - 1) \subseteq \mathbb{Q}\langle x, y \rangle$$

$$A = \left(\begin{pmatrix} 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

- With rectangular matrices we must be careful with the dimensions!

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \ \wedge \ f(A) \neq 0$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

$\big\downarrow$ compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

$\big\downarrow$ make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

$\big\downarrow$ plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \;\wedge\; f(A) \neq 0$$

$\big\downarrow$ equations for entries form commutative system

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \ \wedge \ f(A) \neq 0$$

equations for entries form commutative system

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

solve commutative system

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \ \wedge \ f(A) \neq 0$$

equations for entries form commutative system

$$h_1, \ldots, h_k \in \mathbb{Q}[Y]$$

solve commutative system

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \ \wedge \ f(A) \neq 0$$

equations for entries form commutative system

$$h_1, \ldots, h_k \in \mathbb{Q}[Y]$$

solve commutative system $\longrightarrow$ GB (MSOLVE), SMT (CVC5)

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

plug ansatz into polynomials

$$f_1(A) = \cdots = f_r(A) = 0 \ \wedge \ f(A) \neq 0$$

equations for entries form commutative system

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

solve commutative system → GB (MSOLVE)

solve commutative system → SMT (CVC5)

solve commutative system → SAT + Hensel

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

Idea Compute solution over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^{2^N}} \longrightarrow \mathbb{Q}$$

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

solve commutative system

- GB (MSOLVE)
- SMT (CVC5)
- SAT + Hensel

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \ldots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

Idea Compute solution over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^{2^N}} \longrightarrow \mathbb{Q}$$

$$h_1, \ldots, h_k \in \mathbb{Q}[Y]$$

solve commutative system → GB (MSOLVE), SMT (CVC5), SAT + Hensel

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X\rangle$$

$\downarrow$ compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

$\downarrow$ make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

Idea Compute solution over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^{2^N}} \longrightarrow \mathbb{Q}$$

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

$\downarrow$ solve commutative system $\rightarrow$ GB (MSOLVE) / SMT (CVC5) / SAT + Hensel

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

$$f \overset{?}{\notin} (f_1, \dots, f_r) \quad \subseteq \mathbb{Q}\langle X \rangle$$

compute restrictions on dimensions

$$\begin{tikzcd} \bullet \arrow[r, bend left, "x"] & \bullet \arrow[l, bend left, "y"] \arrow[r, "z"] & \bullet \end{tikzcd}$$

make ansatz with fixed matrix dimensions

$$A = \left(\begin{pmatrix} ? \\ ? \end{pmatrix}, \begin{pmatrix} ? & ? \end{pmatrix}, \begin{pmatrix} ? & ? \\ ? & ? \\ ? & ? \end{pmatrix} \right)$$

Idea Compute solution over

$$\mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8 \longrightarrow \cdots \longrightarrow \mathbb{Z}_{2^{2^N}} \longrightarrow \mathbb{Q}$$

$$h_1, \dots, h_k \in \mathbb{Q}[Y]$$

solve commutative system

- GB (MSOLVE)
- SMT (CVC5)
- SAT + Hensel

$$A = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & -1 \end{pmatrix} \right)$$

Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

[1]Department of Mathematics, Faculty of Sciences and Mathematics, University of Niš, Serbia
[2]Institute for Algebra, Johannes Kepler University Linz, Austria

Theorem 2.1. [34] *Let A, B, C be complex matrices such that ABC is defined and let $P = A^\dagger ABCC^\dagger$, $Q = CC^\dagger B^\dagger A^\dagger A$. The following conditions are equivalent:*

(i) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;

$\subseteq$ $\subseteq$?

(ii) $Q \in P\{1,2\}$ *and both of* A^*A $QPCC^*$ *are* E

(iii) $Q \in P\{1,2\}$ *and both of* A^*A *and* $QPCC^*$ *are* EP

(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($ $)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($ $)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

[1]Department of Mathematics, Faculty of Sciences and Mathematics, University of Niš, Serbia
[2]Institute for Algebra, Johannes Kepler University Linz, Austria

Theorem 2.1. [34] *Let A, B, C be complex matrices such that ABC is defined and let $P = A^\dagger ABCC^\dagger$, $Q = CC^\dagger B^\dagger A^\dagger A$. The following conditions are equivalent:*

(i) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;

(ii) $Q \in P\{1,2\}$ *and both of* A^*A ... $QPCC^*$ *are* ...

(iii) $Q \in P\{1,2\}$ *and both of* A^*A ... *and* $QPCC^*$ *are EP* ...

(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($...$)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}($...$)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ *and* $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$\subseteq$

$\subseteq$?

```
sage: from operator_gb import *
sage: F.<a,b,c,...> = FreeAlgebra(QQ)
sage: assumptions = [a*b*a - a,...]
sage: claim = abc_dag - c_dag*b_dag*a_dag
sage: counterexample(assumptions, claim)
```

$$A = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law

Dragana S. Cvetković-Ilić[1], Clemens Hofstadler[2], Jamal Hossein Poor[2], Jovana Milošević[1], Clemens G. Raab[2], and Georg Regensburger[2]

[1]Department of Mathematics, Faculty of Sciences and Mathematics, University of Niš, Serbia
[2]Institute for Algebra, Johannes Kepler University Linz, Austria

Theorem 2.1. [34] *Let A, B, C be complex matrices such that ABC is defined and let $P = A^\dagger ABCC^\dagger$, $Q = CC^\dagger B^\dagger A^\dagger A$. The following conditions are equivalent:*

(i) $(ABC)^\dagger = C^\dagger B^\dagger A^\dagger$;

(ii) $Q \in P\{1,2\}$ and both of A^*A ... $QPCC^*$ are E...

(iii) $Q \in P\{1,2\}$ and both of A^*A ... and $QPCC^*$ are EP...

(iv) $Q \in P\{1\}$, $\mathcal{R}(A^*AP) = \mathcal{R}($...$)$ and $\mathcal{R}(CC^*P^*) = \mathcal{R}($...$)$;

(v) $PQ = (PQ)^2$, $\mathcal{R}(A^*AP) = \mathcal{R}(Q^*)$ and $\mathcal{R}(CC^*P^*) = \mathcal{R}(Q)$.

$\subseteq$

$\subseteq$?

Example 2.5. *Let*

$$A = \begin{bmatrix} -3 & 2 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad C = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Then

$$A^\dagger = \frac{1}{17}\begin{bmatrix} -3 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}, \quad B^\dagger = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 1 & 0 & -1 \end{bmatrix}, \quad C^\dagger = C.$$

If we define P and Q as in Theorem 2.1, we get that $PQ = 0$ is idempotent and $\mathcal{R}(A^*AP) \subseteq \mathcal{R}(Q^*)$ and $\mathcal{R}(CC^*P^*) \subseteq \mathcal{R}(Q)$ but $(ABC)^\dagger \neq C^\dagger B^\dagger A^\dagger$.

```
sage: from operator_gb import *
sage: F.<a,b,c,...> = FreeAlgebra(QQ)
sage: assumptions = [a*b*a - a,...]
sage: claim = abc_dag - c_dag*b_dag*a_dag
sage: counterexample(assumptions, claim)
```

$$A = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \quad C = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Theorem (Tseitin '58)

The ideal in $K\langle a, b, c, d, e\rangle$ generated by

$$\begin{array}{llll} ac - ca, & ad - da, & bc - cb, & bd - db, \\ ce - eca, & de - edb, & cca - ccae & \end{array}$$

has undecidable membership problem.

Theorem (Tseitin '58)

The ideal in $K\langle a, b, c, d, e\rangle$ generated by

$$\begin{array}{llll} ac - ca, & ad - da, & bc - cb, & bd - db, \\ ce - eca, & de - edb, & cca - ccae & \end{array}$$

has undecidable membership problem.

- We generate 5000 random binomials $v - w$.
- We test membership via quick GB computation (one is in the ideal).

Theorem (Tseitin '58)

The ideal in $K\langle a, b, c, d, e\rangle$ generated by

$$\begin{array}{llll} ac - ca, & ad - da, & bc - cb, & bd - db, \\ ce - eca, & de - edb, & cca - ccae & \end{array}$$

has undecidable membership problem.

- We generate 5000 random binomials $v - w$.
- We test membership via quick GB computation (one is in the ideal).
- For the rest, we try to construct matrix certificates.
- We find certificates for all 4999 binomials in < 90 sec.

Theorem (Tseitin '58)

The ideal in $K\langle a, b, c, d, e\rangle$ generated by

$$ac - ca, \quad ad - da, \quad bc - cb, \quad bd - db,$$
$$ce - eca, \quad de - edb, \quad cca - ccae$$

has undecidable membership problem.

- We generate 5000 random binomials $v - w$.
- We test membership via quick GB computation (one is in the ideal).
- For the rest, we try to construct matrix certificates.
- We find certificates for all 4999 binomials in < 90 sec.

$$A = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 1 & 1 & 1 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 0 \end{pmatrix} \qquad E = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 1 \end{pmatrix}$$