Black-box Identity Testing of Noncommutative Rational Formulas of Inversion Height Two

Abhranil Chatterjee
Joint work with V. Arvind and Partha Mukhopadhyay

Workshop on Algebraic Complexity Theory (WACT), 2023

- Polynomial identity testing (PIT): to decide if a given circuit/ABP/formula computes the zero polynomial.

- Polynomial identity testing (PIT): to decide if a given circuit/ABP/formula computes the zero polynomial.

- Equivalently, to decide whether there exists a nonzero evaluation.

- Polynomial identity testing (PIT): to decide if a given circuit/ABP/formula computes the zero polynomial.

- Equivalently, to decide whether there exists a nonzero evaluation.

- PIT is of two types: white-box and black-box.

Polynomial Identity Testing

- Polynomial identity testing (PIT): to decide if a given circuit/ABP/formula computes the zero polynomial.
- Equivalently, to decide whether there exists a nonzero evaluation.
- PIT is of two types: white-box and black-box.
- In black-box PIT, the polynomial is given as an evaluation oracle and the goal is to find a nonzero evaluation querying the oracle.

- Polynomial identity testing (PIT): to decide if a given circuit/ABP/formula computes the zero polynomial.
- Equivalently, to decide whether there exists a nonzero evaluation.
- PIT is of two types: white-box and black-box.
- In black-box PIT, the polynomial is given as an evaluation oracle and the goal is to find a nonzero evaluation querying the oracle.
- The goal is to output a list of evaluations that works for every polynomial.

Definition (Hitting Set)

We say $\mathcal{H} \in \mathbb{Q}^n$ is a hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, if for every nonzero $f \in \mathcal{C}$, there exists some $(a_1, \ldots, a_n) \in \mathcal{H}$ s.t. $f(a_1, \ldots, a_n) \neq 0$.

Definition (Hitting Set)

We say $\mathcal{H} \in \mathbb{Q}^n$ is a hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, if for every nonzero $f \in \mathcal{C}$, there exists some $(a_1, \ldots, a_n) \in \mathcal{H}$ s.t. $f(a_1, \ldots, a_n) \neq 0$.

- Polynomial Identity Lemma : A randomized polynomial time black-box PIT algorithm for commutative circuits. Derandomizing PIT is open.

Definition (Hitting Set)

We say $\mathcal{H} \in \mathbb{Q}^n$ is a hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}[x_1, \ldots, x_n]$, if for every nonzero $f \in \mathcal{C}$, there exists some $(a_1, \ldots, a_n) \in \mathcal{H}$ s.t. $f(a_1, \ldots, a_n) \neq 0$.

- Polynomial Identity Lemma : A randomized polynomial time black-box PIT algorithm for commutative circuits. Derandomizing PIT is open.
- Efficient derandomization is known for some special cases, ROABP is of our particular interest.

- Noncommutative PIT: to decide if a given noncommutative circuit/ABP/formula computes the zero polynomial in the free algebra.

- Noncommutative PIT: to decide if a given noncommutative circuit/ABP/formula computes the zero polynomial in the free algebra.

Example

$(x_1 + x_2)(x_1 - x_2) \neq x_1^2 - x_2^2,$
$(x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2 - x_1x_2 + x_2x_1.$

- Noncommutative PIT: to decide if a given noncommutative circuit/ABP/formula computes the zero polynomial in the free algebra.

Example

$(x_1 + x_2)(x_1 - x_2) \neq x_1^2 - x_2^2,$
$(x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2 - x_1x_2 + x_2x_1.$

- The black-box PIT is to efficiently find a set of matrix evaluations $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ of small size such that for some evaluation $f(p_1, \ldots, p_n) \neq 0$.

- Noncommutative PIT: to decide if a given noncommutative circuit/ABP/formula computes the zero polynomial in the free algebra.

Example

$(x_1 + x_2)(x_1 - x_2) \neq x_1^2 - x_2^2$,
$(x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2 - x_1x_2 + x_2x_1$.

- The black-box PIT is to efficiently find a set of matrix evaluations $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ of small size such that for some evaluation $f(p_1, \ldots, p_n) \neq 0$.
- [Forbes and Shpilka (2013)] Quasipolynomial-size hitting set for noncommutative formulas (and ABPs) s.t. $f(p_1, \ldots, p_n)$ is nonzero.

- Commutative computation with inverses : admits a canonical representation, each element can be expressed as fg^{-1} for some $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$.

Noncommutative Rational Functions

- Commutative computation with inverses : admits a canonical representation, each element can be expressed as fg^{-1} for some $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$.

- Noncommutative computation with inverses: computes noncommutative rational functions, elements of the universal free skew field.

- Commutative computation with inverses : admits a canonical representation, each element can be expressed as fg^{-1} for some $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$.

- Noncommutative computation with inverses: computes noncommutative rational functions, elements of the universal free skew field.

- Two noncommutative rational expressions compute same rational function in the free skew-field if they agree on evaluations on every matrix tuple whenever defined [Amitsur (1966)].

- Commutative computation with inverses : admits a canonical representation, each element can be expressed as fg^{-1} for some $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$.

- Noncommutative computation with inverses: computes noncommutative rational functions, elements of the universal free skew field.

- Two noncommutative rational expressions compute same rational function in the free skew-field if they agree on evaluations on every matrix tuple whenever defined [Amitsur (1966)].

- Unlike commutative setting, it does not have any canonical representation.

Noncommutative Rational Functions

- Commutative computation with inverses : admits a canonical representation, each element can be expressed as fg^{-1} for some $f, g \in \mathbb{Q}[x_1, \ldots, x_n]$.

- Noncommutative computation with inverses: computes noncommutative rational functions, elements of the universal free skew field.

- Two noncommutative rational expressions compute same rational function in the free skew-field if they agree on evaluations on every matrix tuple whenever defined [Amitsur (1966)].

- Unlike commutative setting, it does not have any canonical representation.

- Inversion height is the maximum number of nested inverses. Bounded by $O(\log s)$ for a size s formula [HW15].

- Rational Identity Testing : Given a noncommutative rational formula, determine if it computes zero in $\mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$.

- Rational Identity Testing : Given a noncommutative rational formula, determine if it computes zero in $\mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$.
- Equivalently, decide whether there exists a nonzero matrix evaluation or not.

- Rational Identity Testing : Given a noncommutative rational formula, determine if it computes zero in $\mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$.
- Equivalently, decide whether there exists a nonzero matrix evaluation or not.

Example

$(x + xy^{-1}x)^{-1} + (x + y)^{-1} - x^{-1}$, known as Hua's identity [Hua (1949)], is zero in the free skew-field.

- RIT for rational formulas can be solved in deterministic polynomial time ([GGOW16], [IQS18], [HH21]) in white-box.

- RIT for rational formulas can be solved in deterministic polynomial time ([GGOW16], [IQS18], [HH21]) in white-box.
- In black-box, randomized polynomial time [DM17].

- RIT for rational formulas can be solved in deterministic polynomial time ([GGOW16], [IQS18], [HH21]) in white-box.
- In black-box, randomized polynomial time [DM17].
- Derandomization of black-box RIT is open.

- RIT for rational formulas can be solved in deterministic polynomial time ([GGOW16], [IQS18], [HH21]) in white-box.
- In black-box, randomized polynomial time [DM17].
- Derandomization of black-box RIT is open.
- Can we derandomize even for rational formulas of bounded inversion height?

Our Result

Theorem (RIT of inversion height two)

We can construct a quasipolynomial-size hitting set for the class of noncommutative rational formulas of inversion height two.

A Toy Example

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \ldots, a_n) \in \mathbb{Q}^n$.

A Toy Example

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \ldots, a_n) \in \mathbb{Q}^n$.

- Consider $r(x_1 + a_1, \ldots, x_n + a_n)$.

A Toy Example

- Let $r(x_1, \dots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \dots, a_n) \in \mathbb{Q}^n$.
- Consider $r(x_1 + a_1, \dots, x_n + a_n)$.
- Inverse to power series transformation using Taylor series: $(f(x+a))^{-1} = (f(a) + rest)^{-1}$.

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \ldots, a_n) \in \mathbb{Q}^n$.

- Consider $r(x_1 + a_1, \ldots, x_n + a_n)$.

- Inverse to power series transformation using Taylor series: $(f(x + a))^{-1} = (f(a) + rest)^{-1}$.

- $r(x_1 + a_1, \ldots, x_n + a_n)$ is a recognizable series of size $2s$.

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \ldots, a_n) \in \mathbb{Q}^n$.
- Consider $r(x_1 + a_1, \ldots, x_n + a_n)$.
- Inverse to power series transformation using Taylor series: $(f(x+a))^{-1} = (f(a) + rest)^{-1}$.
- $r(x_1 + a_1, \ldots, x_n + a_n)$ is a recognizable series of size $2s$.
- RIT of r now reduces to PIT of a noncommutative ABP.

A Toy Example

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(a_1, \ldots, a_n) \in \mathbb{Q}^n$.
- Consider $r(x_1 + a_1, \ldots, x_n + a_n)$.
- Inverse to power series transformation using Taylor series: $(f(x+a))^{-1} = (f(a) + rest)^{-1}$.
- $r(x_1 + a_1, \ldots, x_n + a_n)$ is a recognizable series of size $2s$.
- RIT of r now reduces to PIT of a noncommutative ABP.

r may not be defined at any $(a_1, \ldots a_n) \in \mathbb{Q}^n$, for example, $r = (x_1x_2 - x_2x_1)^{-1}$.

- There exists $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ such that r is defined at that matrix tuple.

- There exists $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ such that r is defined at that matrix tuple.

- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$ and expand.

- There exists $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ such that r is defined at that matrix tuple.

- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$ and expand.

- It produces terms $p_1 x_2 p_3 x_4$, $p_1 x_2 x_3 p_4$ etc where $p_1 x_1 p_2 x_2$ and $p_1 p_2 x_1 x_2$ are two different words.

- There exists $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ such that r is defined at that matrix tuple.
- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$ and expand.
- It produces terms $p_1x_2p_3x_4$, $p_1x_2x_3p_4$ etc where $p_1x_1p_2x_2$ and $p_1p_2x_1x_2$ are two different words.
- These are called generalized monomials and studied by Volčič (2018). Generalized series and generalized polynomial are defined accordingly.

- There exists $(p_1, \ldots, p_n) \in \mathrm{Mat}_d^n(\mathbb{Q})$ such that r is defined at that matrix tuple.
- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$ and expand.
- It produces terms $p_1 x_2 p_3 x_4$, $p_1 x_2 x_3 p_4$ etc where $p_1 x_1 p_2 x_2$ and $p_1 p_2 x_1 x_2$ are two different words.
- These are called generalized monomials and studied by Volčič (2018). Generalized series and generalized polynomial are defined accordingly.
- We can define a generalized ABP (or an automaton) over $\mathrm{Mat}_m(\mathbb{Q})$ where the edge labels are of form $\sum p_i x_i q_i$ for some $p_i, q_i \in \mathrm{Mat}_m(\mathbb{Q})$.

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(p_1, \ldots p_n) \in \mathrm{Mat}_m^n(\mathbb{Q})$.

A Matrix Shift

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(p_1, \ldots p_n) \in \mathrm{Mat}_m^n(\mathbb{Q})$.

- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$.

A Matrix Shift

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(p_1, \ldots p_n) \in \mathrm{Mat}_m^n(\mathbb{Q})$.
- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$.
- $r(x_1 + p_1, \ldots, x_n + p_n)$ is a generalized recognizable series of size at most $2s$ [Volčič].

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(p_1, \ldots p_n) \in \mathrm{Mat}_m^n(\mathbb{Q})$.
- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$.
- $r(x_1 + p_1, \ldots, x_n + p_n)$ is a generalized recognizable series of size at most $2s$ [Volčič].
- RIT of r now reduces to identity testing of a generalized ABP.

A Matrix Shift

- Let $r(x_1, \ldots, x_n)$ is the input rational formula of size s and r is defined at $(p_1, \ldots p_n) \in \mathrm{Mat}_m^n(\mathbb{Q})$.
- Consider $r(x_1 + p_1, \ldots, x_n + p_n)$.
- $r(x_1 + p_1, \ldots, x_n + p_n)$ is a generalized recognizable series of size at most $2s$ [Volčič].
- RIT of r now reduces to identity testing of a generalized ABP.
- Identity testing of a generalized ABP over $\mathrm{Mat}_m(\mathbb{Q})$ reduces to PIT of $m \times m$ matrix of noncommutative ABPs.

- Observe that, r is defined on a matrix tuple, if for every inverse gate it evaluates to an invertible matrix.

- Observe that, r is defined on a matrix tuple, if for every inverse gate it evaluates to an invertible matrix.

Definition

$\mathcal{H} \in \mathrm{Mat}_d^n(\mathbb{Q})$ is a strong hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$, if for every nonzero $r \in \mathcal{C}$, there exists some $(p_1, \ldots, p_n) \in \mathcal{H}$ s.t. $r(p_1, \ldots, p_n)$

- Observe that, r is defined on a matrix tuple, if for every inverse gate it evaluates to an invertible matrix.

Definition

$\mathcal{H} \in \mathrm{Mat}_d^n(\mathbb{Q})$ is a strong hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$, if for every nonzero $r \in \mathcal{C}$, there exists some $(p_1, \ldots, p_n) \in \mathcal{H}$ s.t. $r(p_1, \ldots, p_n)$is invertible.

- The existence follows from the result of Ivanyos, Qiao and Subrahmanyam (2018).

- Observe that, r is defined on a matrix tuple, if for every inverse gate it evaluates to an invertible matrix.

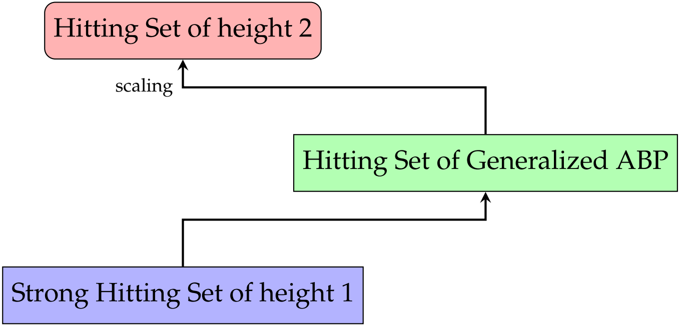
Definition

$\mathcal{H} \in \mathrm{Mat}_d^n(\mathbb{Q})$ is a strong hitting set for a circuit class $\mathcal{C} \subseteq \mathbb{Q}\langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$, if for every nonzero $r \in \mathcal{C}$, there exists some $(p_1, \ldots, p_n) \in \mathcal{H}$ s.t. $r(p_1, \ldots, p_n)$is invertible.

- The existence follows from the result of Ivanyos, Qiao and Subrahmanyam (2018).

- Our refined goal is now to construct a strong hitting set for rational formulas of inversion height one.

Our Approach



Our Approach

- Intuitively, a division algebra is a matrix algebra where we can always do additions, multiplications and divisions.

- Intuitively, a division algebra is a matrix algebra where we can always do additions, multiplications and divisions.

- We can define an ABP (or an automaton) over a division algebra D where the edge labels are of form $\sum p_i x_i q_i$ for some $p_i, q_i \in D$.

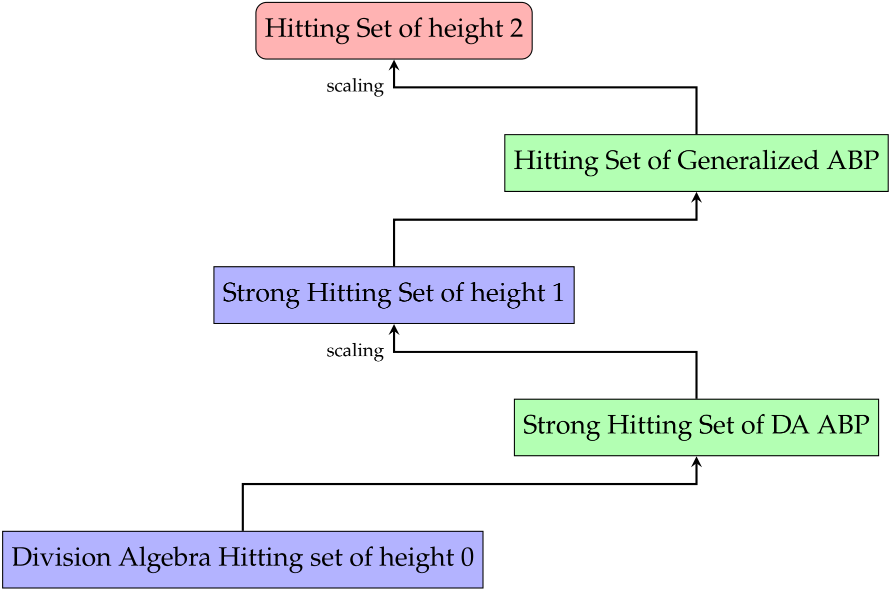
Our Approach

- Intuitively, a division algebra is a matrix algebra where we can always do additions, multiplications and divisions.
- We can define an ABP (or an automaton) over a division algebra D where the edge labels are of form $\sum p_i x_i q_i$ for some $p_i, q_i \in D$.
- Constructing a strong hitting set for a division algebra ABP reduces to PIT of a product of ROABPs.

- Intuitively, a division algebra is a matrix algebra where we can always do additions, multiplications and divisions.
- We can define an ABP (or an automaton) over a division algebra D where the edge labels are of form $\sum p_i x_i q_i$ for some $p_i, q_i \in D$.
- Constructing a strong hitting set for a division algebra ABP reduces to PIT of a product of ROABPs.
- A hitting set $\mathcal{H}$ is a division algebra hitting set if $\mathcal{H} \in D^n$ for some division algebra D. Any division algebra hitting set is a strong hitting set.

Our Approach

- Intuitively, a division algebra is a matrix algebra where we can always do additions, multiplications and divisions.
- We can define an ABP (or an automaton) over a division algebra D where the edge labels are of form $\sum p_i x_i q_i$ for some $p_i, q_i \in D$.
- Constructing a strong hitting set for a division algebra ABP reduces to PIT of a product of ROABPs.
- A hitting set $\mathcal{H}$ is a division algebra hitting set if $\mathcal{H} \in D^n$ for some division algebra D. Any division algebra hitting set is a strong hitting set.
- Refined goal is to compute a division algebra hitting set for noncommutative formulas.


Hitting Set of height 2
scaling
Hitting Set of Generalized ABP
Strong Hitting Set of height 1
scaling
Strong Hitting Set of DA ABP
Division Algebra Hitting set of height 0

ROABP :

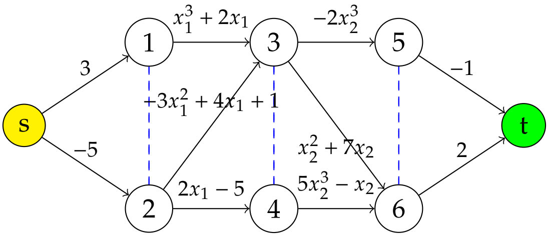


Figure: a bivariate ROABP

ROABP :

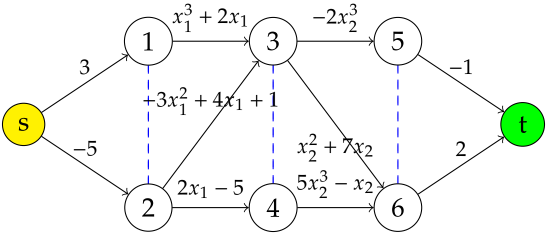


Figure: a bivariate ROABP

- Hitting set generator : A polynomial map $\mathcal{G} : \mathbb{F}^t \longrightarrow \mathbb{F}^n$ is a generator for a circuit class $\mathcal{C}$ if for every n-variate polynomial f in $\mathcal{C}$, $f \equiv 0$ if and only if the t-variate polynomial $f \circ \mathcal{G} \equiv 0$.

ROABP :

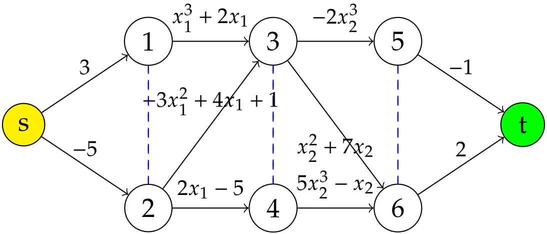


Figure: a bivariate ROABP

- Hitting set generator : A polynomial map $\mathcal{G} : \mathbb{F}^t \longrightarrow \mathbb{F}^n$ is a generator for a circuit class $\mathcal{C}$ if for every n-variate polynomial f in $\mathcal{C}$, $f \equiv 0$ if and only if the t-variate polynomial $f \circ \mathcal{G} \equiv 0$.

- [Forbes and Shpilka (2013)] For a D-variate ROABP, we can construct a hitting set generator $\mathcal{G} : \mathbb{F}^{\log D} \to \mathbb{F}^{D}$, therefore a hitting set of quasi-polynomial size.

- [Forbes and Shpilka (2013)] For a D-variate ROABP, we can construct a hitting set generator $\mathcal{G} : \mathbb{F}^{\log D} \to \mathbb{F}^{D}$, therefore a hitting set of quasi-polynomial size.

- The main idea is to merge the adjacent layers and reduce the number of variables.

- [Forbes and Shpilka (2013)] For a D-variate ROABP, we can construct a hitting set generator $\mathcal{G} : \mathbb{F}^{\log D} \to \mathbb{F}^{D}$, therefore a hitting set of quasi-polynomial size.
- The main idea is to merge the adjacent layers and reduce the number of variables.
- Noncommutative ABP PIT via commutative ROABP PIT by the following matrix substitutions.

$$M_i = \begin{bmatrix} 0 & z_1^i & 0 & \cdots & 0 \\ 0 & 0 & z_2^i & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & z_d^i \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

- [Forbes and Shpilka (2013)] For a D-variate ROABP, we can construct a hitting set generator $\mathcal{G} : \mathbb{F}^{\log D} \to \mathbb{F}^{D}$, therefore a hitting set of quasi-polynomial size.

- The main idea is to merge the adjacent layers and reduce the number of variables.

- Noncommutative ABP PIT via commutative ROABP PIT by the following matrix substitutions.

$$M_i = \begin{bmatrix} 0 & z_1^i & 0 & \cdots & 0 \\ 0 & 0 & z_2^i & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & z_d^i \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}, \qquad f(M_1, \ldots, M_n) = \begin{bmatrix} & & \star \\ & & \\ & & \end{bmatrix}.$$

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.
$K : F(\omega)$ where $\omega : \ell^{th}$ primitive roots of unity ($\omega^{\ell} = 1$).

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.
$K : F(\omega)$ where $\omega : \ell^{th}$ primitive roots of unity ($\omega^\ell = 1$).
$\sigma(\omega) = \omega^k$ where k is relatively prime to ℓ ($\sigma : K \longrightarrow K$ is an automorphism that fixes F).

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.
$K : F(\omega)$ where $\omega : \ell^{th}$ primitive roots of unity ($\omega^{\ell} = 1$).
$\sigma(\omega) = \omega^k$ where k is relatively prime to ℓ ($\sigma : K \longrightarrow K$ is an automorphism that fixes F).

$$M = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ z & 0 & \cdots & 0 & 0 \end{bmatrix},$$

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.
$K : F(\omega)$ where $\omega : \ell^{th}$ primitive roots of unity ($\omega^\ell = 1$).
$\sigma(\omega) = \omega^k$ where k is relatively prime to ℓ ($\sigma : K \longrightarrow K$ is an automorphism that fixes F).

$$M = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ z & 0 & \cdots & 0 & 0 \end{bmatrix}, \qquad N = \begin{bmatrix} \omega & 0 & 0 & 0 & 0 \\ 0 & \sigma(\omega) & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \sigma^{\ell-2}(\omega) & 0 \\ 0 & 0 & 0 & 0 & \sigma^{\ell-1}(\omega) \end{bmatrix}.$$

$F : \mathbb{Q}(z)$ where z is a new commuting indeterminate.
$K : F(\omega)$ where $\omega : \ell^{th}$ primitive roots of unity ($\omega^{\ell} = 1$).
$\sigma(\omega) = \omega^k$ where k is relatively prime to ℓ ($\sigma : K \longrightarrow K$ is an automorphism that fixes F).

$$M = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ z & 0 & \cdots & 0 & 0 \end{bmatrix}, \qquad N = \begin{bmatrix} \omega & 0 & 0 & 0 & 0 \\ 0 & \sigma(\omega) & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \sigma^{\ell-2}(\omega) & 0 \\ 0 & 0 & 0 & 0 & \sigma^{\ell-1}(\omega) \end{bmatrix}.$$

D : F-linear combination of $M^i N^j$ (wlog $0 \leq i, j \leq \ell - 1$).
$D = (K/F, \sigma, z)$: Cyclic division algebra of index ℓ.

Division Algebra HS for noncommutative formulas

Matrix representation of a division algebra element:

$$\begin{bmatrix} 0 & b & 0 & \cdots & 0 \\ 0 & 0 & \sigma(b) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \sigma^{\ell-2}(b) \\ z\sigma^{\ell-1}(b) & 0 & \cdots & 0 & 0 \end{bmatrix}$$

Matrix representation of Forbes-Shpilka hitting set:

$$\begin{bmatrix} 0 & f_1^i(\bar{\alpha}) & 0 & \cdots & 0 \\ 0 & 0 & f_2^i(\bar{\alpha}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_D^i(\bar{\alpha}) \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

Division Algebra HS for noncommutative formulas

Matrix representation of a division algebra element:

$$\begin{bmatrix} 0 & b & 0 & \cdots & 0 \\ 0 & 0 & \sigma(b) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \sigma^{\ell-2}(b) \\ z\sigma^{\ell-1}(b) & 0 & \cdots & 0 & 0 \end{bmatrix}$$

Matrix representation of Forbes-Shpilka hitting set:

$$\begin{bmatrix} 0 & f_1^i(\bar{\alpha}) & 0 & \cdots & 0 \\ 0 & 0 & f_2^i(\bar{\alpha}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_D^i(\bar{\alpha}) \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

The goal is to find ω and σ such that each $f_j(\bar{\alpha})$ is in $K = F(\omega)$ and $\sigma(f_j(\bar{\alpha})) = f_{j+1}(\bar{\alpha})$.

Division Algebra HS for noncommutative formulas

Matrix representation of our hitting set over $\mathbb{Q}(\omega, z)$:

$$M(x_i) = \left[\begin{array}{ccccc|ccc} 0 & f_0^i(\bar{\alpha}) & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & f_1^i(\bar{\alpha}) & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & f_{D-1}^i(\bar{\alpha}) & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & f_D^i(\bar{\alpha}) & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & f_{\ell-2}^i(\bar{\alpha}) \\ z f_{\ell-1}^i(\bar{\alpha}) & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right].$$

Strong HS for a division algebra ABP

- Every nonzero generalized ABP over a division algebra has a witness of form:

$$M(x_k) = \begin{bmatrix} 0 & p_{k1} & 0 & \cdots & 0 \\ 0 & 0 & p_{k2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & p_{k(d-1)} \\ p_{kd} & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

- Write each $p_{kl} = \sum y_{ijkl} C_{ij}$ where C_{ij}s are the division algebra basis.

Strong HS for a division algebra ABP

- Every nonzero generalized ABP over a division algebra has a witness of form:

$$M(x_k) = \begin{bmatrix} 0 & p_{k1} & 0 & \cdots & 0 \\ 0 & 0 & p_{k2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & p_{k(d-1)} \\ p_{kd} & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

- Write each $p_{kl} = \sum y_{ijkl} C_{ij}$ where C_{ij}s are the division algebra basis.

- Image will be a block diagonal matrix and for each block, the matrix entry will be an ROABP over same partition.

Strong HS for a division algebra ABP

- Every nonzero generalized ABP over a division algebra has a witness of form:

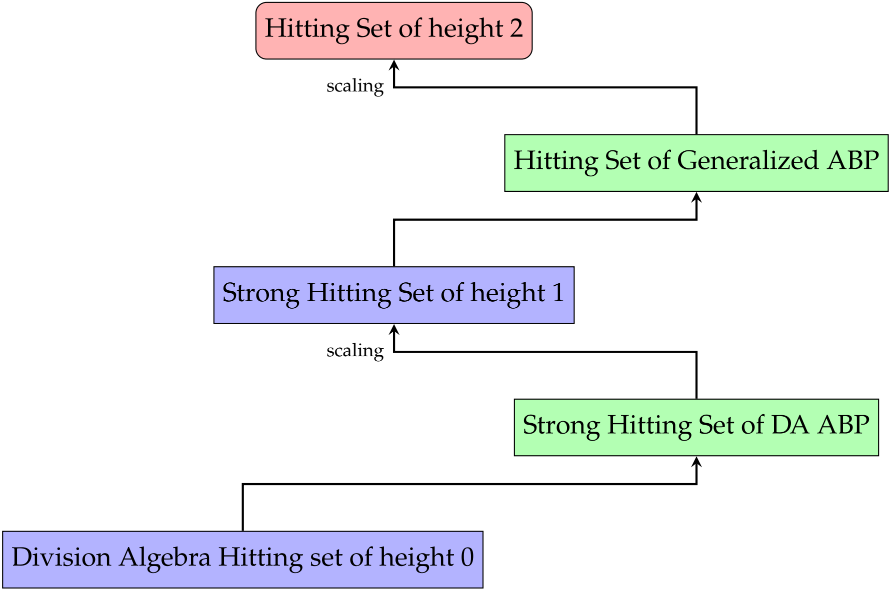
$$M(x_k) = \begin{bmatrix} 0 & p_{k1} & 0 & \cdots & 0 \\ 0 & 0 & p_{k2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & p_{k(d-1)} \\ p_{kd} & 0 & \cdots & 0 & 0 \end{bmatrix}.$$

- Write each $p_{kl} = \sum y_{ijkl} C_{ij}$ where C_{ij}s are the division algebra basis.

- Image will be a block diagonal matrix and for each block, the matrix entry will be an ROABP over same partition.

- Finding invertible image reduces to ROABP PIT.

Our Approach



Why do we stop at height two?

- Inductively build a hitting set for formulas of height h for every h (need more).

Why do we stop at height two?

- Inductively build a hitting set for formulas of height h for every h (need more).
- Inductively build a strong hitting set for formulas of height h for every h (don't know).

Why do we stop at height two?

- Inductively build a hitting set for formulas of height h for every h (need more).

- Inductively build a strong hitting set for formulas of height h for every h (don't know).

- Inductively build a division algebra hitting set for formulas of height h for every h (don't know).

Why do we stop at height two?

- Inductively build a hitting set for formulas of height h for every h (need more).
- Inductively build a strong hitting set for formulas of height h for every h (don't know).
- Inductively build a division algebra hitting set for formulas of height h for every h (don't know).
- Suffices to find a division algebra hitting set for a division algebra ABP.

Why do we stop at height two?

- Inductively build a hitting set for formulas of height h for every h (need more).
- Inductively build a strong hitting set for formulas of height h for every h (don't know).
- Inductively build a division algebra hitting set for formulas of height h for every h (don't know).
- Suffices to find a division algebra hitting set for a division algebra ABP.

Can we embed the strong hitting set inside a larger dimensional division algebra and continue the induction?

Thank You