Natural Proofs in Algebraic Circuit Complexity

Prerona Chatterjee (Tel Aviv University)
Mrinal Kumar (TIFR, Mumbai)
C. Ramya (IMSc, Chennai)
Ramprasad Saptharishi (TIFR, Mumbai)
Anamay Tengse (University of Haifa)

22nd March 2023

- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$?

- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$? Why?

- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$?
  Why?
  Proof: $ax^2 + bxy + cy^2 = (\alpha x + \beta y)^2 \Leftrightarrow b^2 - 4ac = 0$,
  and $5^2 - 4 \cdot 1 \cdot 9 \neq 0$.

- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$? Why?
  Proof: $ax^2 + bxy + cy^2 = (\alpha x + \beta y)^2 \Leftrightarrow b^2 - 4ac = 0$, and $5^2 - 4 \cdot 1 \cdot 9 \neq 0$.

- Is $x^3 + 2x^2y + 3xy^2 + 8y^3 = (\alpha x + \beta y)^3$ for some α, β?

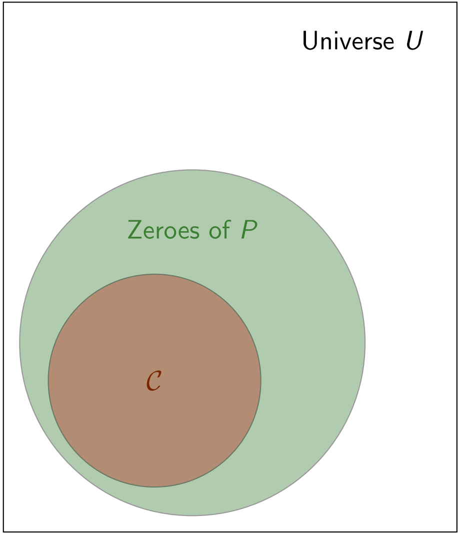
- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$?
  Why?
  Proof: $ax^2 + bxy + cy^2 = (\alpha x + \beta y)^2 \Leftrightarrow b^2 - 4ac = 0$,
  and $5^2 - 4 \cdot 1 \cdot 9 \neq 0$.

- Is $x^3 + 2x^2y + 3xy^2 + 8y^3 = (\alpha x + \beta y)^3$ for some α, β?
  Proof: $ax^3 + bx^2y + cxy^2 + dy^3 = (\alpha x + \beta y)^3 \Rightarrow b^2 - 3ac = 0$,

- Are there any α, β for which $x^2 + 5xy + 9y^2 = (\alpha x + \beta y)^2$?
  Why?
  Proof: $ax^2 + bxy + cy^2 = (\alpha x + \beta y)^2 \Leftrightarrow b^2 - 4ac = 0$,
  and $5^2 - 4 \cdot 1 \cdot 9 \neq 0$.

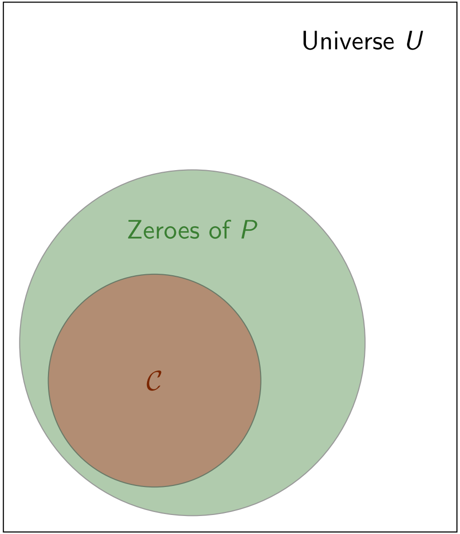
- Is $x^3 + 2x^2y + 3xy^2 + 8y^3 = (\alpha x + \beta y)^3$ for some α, β?
  Proof: $ax^3 + bx^2y + cxy^2 + dy^3 = (\alpha x + \beta y)^3 \Rightarrow b^2 - 3ac = 0$,
  and $2^2 - 3 \cdot 1 \cdot 3 \neq 0$.

Equations for polynomials



Equation for $\mathcal{C}$ is nonzero polynomial P:
P vanishes on coefficients of every $f \in \mathcal{C}$.

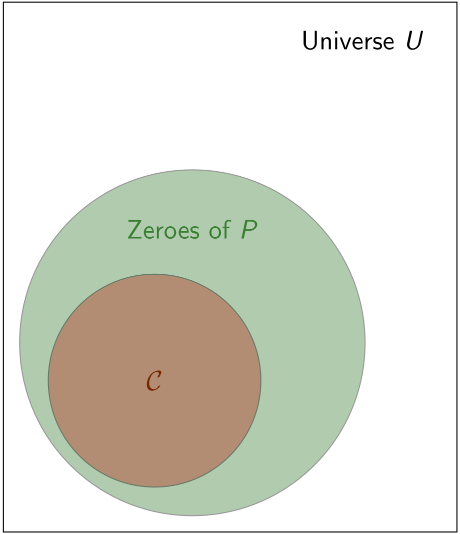
Equations for polynomials



Equation for $\mathcal{C}$ is nonzero polynomial P:
P vanishes on coefficients of every $f \in \mathcal{C}$.

E.g.1 $U = \{ax^2 + bxy + cy^2\}$,
$\mathcal{C} = \{(\alpha x + \beta y)^2\}$,
$P = b^2 - 4ac$.
$f \in \mathcal{C}$ if and only if $P(f) = 0$

Equations for polynomials



Equation for $\mathcal{C}$ is nonzero polynomial P:
P vanishes on coefficients of every $f \in \mathcal{C}$.

E.g.1 $U = \{ax^2 + bxy + cy^2\}$,
$\mathcal{C} = \{(\alpha x + \beta y)^2\}$,
$P = b^2 - 4ac$.
$f \in \mathcal{C}$ if and only if $P(f) = 0$

E.g.2 $U = \{ax^3 + bx^2y + cxy^2 + dy^3\}$,
$\mathcal{C} = \{(\alpha x + \beta y)^3\}$,
$P = b^2 - 3ac$.
If $f \in \mathcal{C}$ then $P(f) = 0$

- What happens when a class $\mathcal{C}$ has equations?

- What happens when a class $\mathcal{C}$ has equations?

- Which classes are we interested in?

- What happens when a class $\mathcal{C}$ has equations?

- Which classes are we interested in?

- Does the "complexity" of these equations matter?

- What happens when a class $\mathcal{C}$ has equations?

  "Explicit" polynomials outside the class, sometimes

- Which classes are we interested in?

- Does the "complexity" of these equations matter?

- What happens when a class $\mathcal{C}$ has equations?

  "Explicit" polynomials outside the class, sometimes

- Which classes are we interested in?

  Corresponding to algebraic models

- Does the "complexity" of these equations matter?

- What happens when a class $\mathcal{C}$ has equations?
  "Explicit" polynomials outside the class, sometimes

- Which classes are we interested in?
  Corresponding to algebraic models

- Does the "complexity" of these equations matter?
  Yes, for "explicit" lower bounds

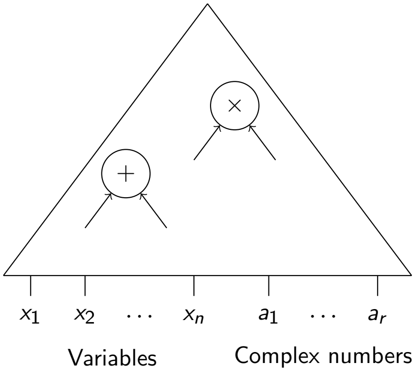
Algebraic Circuits

Algebraic Circuits

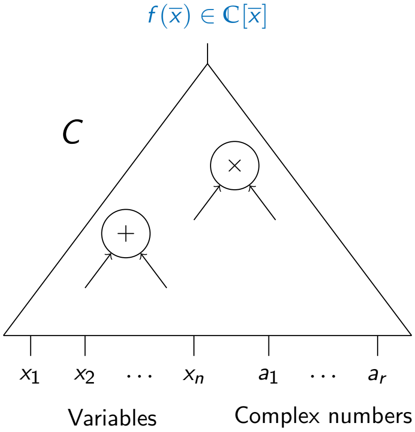
$x_1 \quad x_2 \quad \cdots \quad x_n \qquad a_1 \quad \cdots \quad a_r$

Variables Complex numbers

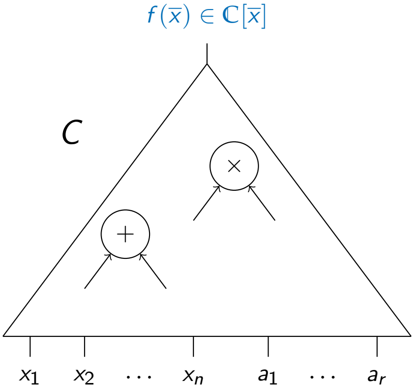
Algebraic Circuits



Algebraic Circuits



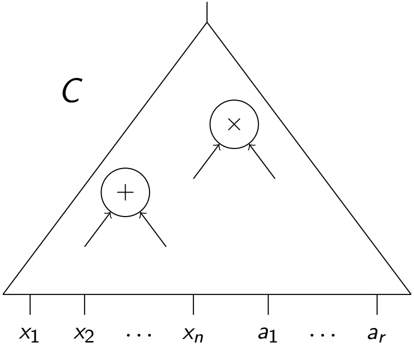
Algebraic Circuits



Algebraic Circuit for $f(\overline{x})$

Algebraic Circuits

$f(\overline{x}) \in \mathbb{C}[\overline{x}]$

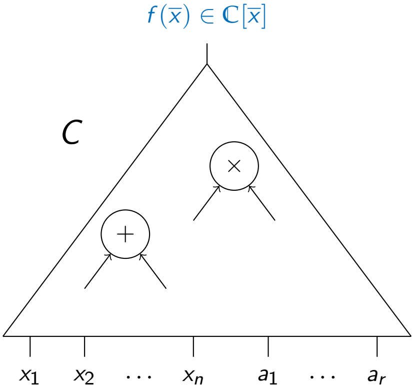


Algebraic Circuit for $f(\overline{x})$

Size(C): Number of *gates*

- $\approx$ No. of operations used by C

Algebraic Circuits



Algebraic Circuit for $f(\overline{x})$

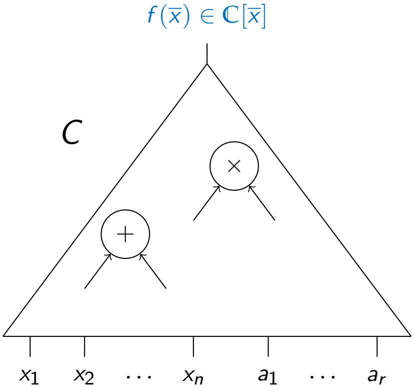
Size(C): Number of *gates*

- $\approx$ No. of operations used by C

Size(f): Size of the smallest circuit for f

- Min operations to compute f

Algebraic Circuits



Algebraic Circuit for $f(\overline{x})$

Size(C): Number of *gates*

- $\approx$ No. of operations used by C

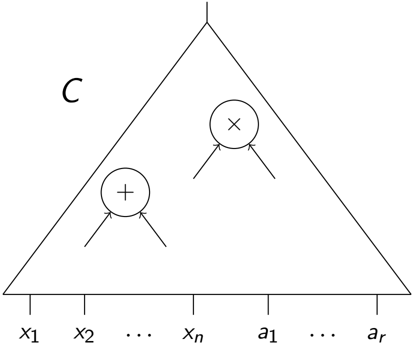
Size(f): Size of the smallest circuit for f

- Min operations to compute f

Formula: Circuit whose graph is a tree

Algebraic Circuits

$f(\overline{x}) \in \mathbb{C}[\overline{x}]$



Algebraic Circuit for $f(\overline{x})$

Size(C): Number of *gates*

- $\approx$ No. of operations used by C

Size(f): Size of the smallest circuit for f

- Min operations to compute f

Formula: Circuit whose graph is a tree

"Low-degree" polynomials.

Variables: n, Degree: d,

Polynomials with $d = \text{poly}(n)$.

Algebraic circuit complexity: Basics

Boolean world

Algebraic world

- P (or P/ poly)
  — E.g. MaxFlow,Matching
- NP (or NP/ poly)
  — 'verifiable' in poly-time
  — E.g. SAT

Algebraic circuit complexity: Basics

Boolean world

- P (or P/ poly)
  — E.g. MaxFlow,Matching
- NP (or NP/ poly)
  — 'verifiable' in poly-time
  — E.g. SAT

Algebraic world

- VP (efficiently computable)
  — E.g. (Symbolic) Determinant

Algebraic circuit complexity: Basics

Boolean world

- P (or P/ poly)
  — E.g. MaxFlow,Matching
- NP (or NP/ poly)
  — 'verifiable' in poly-time
  — E.g. SAT

Algebraic world

- VP (efficiently computable)
  — E.g. (Symbolic) Determinant
- VNP ("explicit")
  — A_f in # P/ poly, $A_f(m) = \text{coeff}_f(m)$
  — E.g. Permanent

Algebraic circuit complexity: Basics

Boolean world

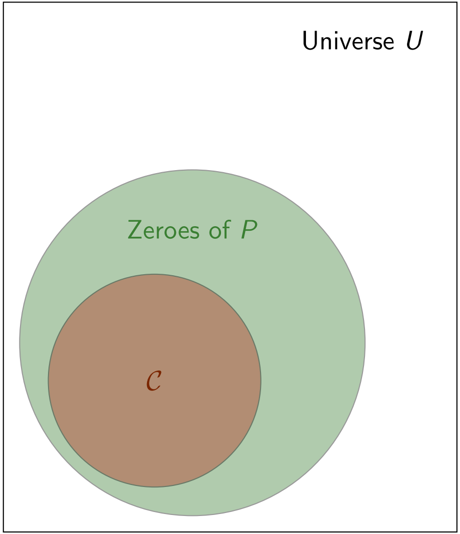
- P (or P/ poly)
  — E.g. MaxFlow,Matching
- NP (or NP/ poly)
  — 'verifiable' in poly-time
  — E.g. SAT

Algebraic world

- VP (efficiently computable)
  — E.g. (Symbolic) Determinant
- VNP ("explicit")
  — A_f in # P/ poly, $A_f(m) = \text{coeff}_f(m)$
  — E.g. Permanent

Big questions: VP vs VNP, Det_n vs Perm_n

Equations for Polynomials: Recap

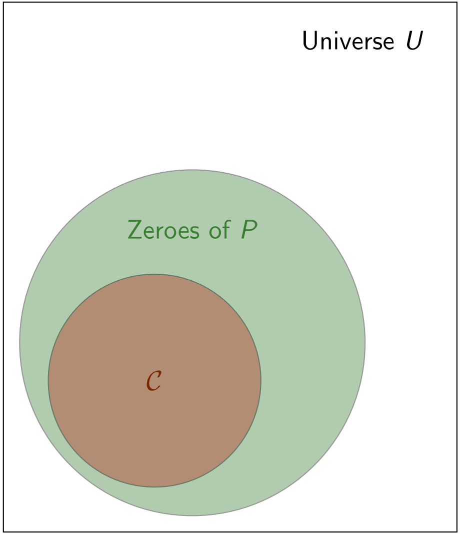


Definition.

Equation for $\mathcal{C}$ is nonzero polynomial P:

P vanishes on coefficients of all $f \in \mathcal{C}$.

Equations for Polynomials: Recap



Definition.

Equation for $\mathcal{C}$ is nonzero polynomial P:

P vanishes on coefficients of all $f \in \mathcal{C}$.

Rest of this talk:

Assume degree d = number of variables n.

N = Number of coefficients = $\binom{n+d}{d}$,

$N = 2^{O(n)}$.

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.
  E.g. If $\mathcal{C}$ is VP and $h \in$ VNP, we just proved VP $\neq$ VNP!

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.
  E.g. If $\mathcal{C}$ is VP and $h \in$ VNP, we just proved VP $\neq$ VNP!

- Best known lower bounds in structured models:
  Constant depth formulas [NW95,GKKS13,LST21], multilinear formulas [Raz05,KS23], non-commutative formulas [Nis91,TLS22], multilinear circuits [KV20], ...

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.
  E.g. If $\mathcal{C}$ is VP and $h \in$ VNP, we just proved VP $\neq$ VNP!

- Best known lower bounds in structured models:
  Constant depth formulas [NW95,GKKS13,LST21], multilinear formulas [Raz05,KS23], non-commutative formulas [Nis91,TLS22], multilinear circuits [KV20], ...
- ALL the above use equations! Almost all these equations have poly-sized circuits.

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.
  E.g. If $\mathcal{C}$ is VP and $h \in$ VNP, we just proved VP $\neq$ VNP!

- Best known lower bounds in structured models:
  Constant depth formulas [NW95,GKKS13,LST21], multilinear formulas [Raz05,KS23], non-commutative formulas [Nis91,TLS22], multilinear circuits [KV20], ...
- ALL the above use equations! Almost all these equations have poly-sized circuits.
- Notable omissions:
  Best known lower bounds against circuits [BS83], formulas [Kal85,CKSV22], and determinantal complexity [KV22].

Using equations to prove lower bounds

- P is an equation for the class $\mathcal{C}$: if $P(h) \neq 0$ for some h, then $h \notin \mathcal{C}$.
  E.g. If $\mathcal{C}$ is VP and $h \in$ VNP, we just proved VP $\neq$ VNP!

- Best known lower bounds in structured models:
  Constant depth formulas [NW95,GKKS13,LST21], multilinear formulas [Raz05,KS23], non-commutative formulas [Nis91,TLS22], multilinear circuits [KV20], ...
- ALL the above use equations! Almost all these equations have poly-sized circuits.
- Notable omissions:
  Best known lower bounds against circuits [BS83], formulas [Kal85,CKSV22], and determinantal complexity [KV22].

Q. Are there (poly-sized) equations for general classes?

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

A nonzero, N-variate polynomial P is a $\mathcal{D}$-natural proof for $\mathcal{C} \subset \mathbb{R}[x_1, \ldots, x_n]$, if:

1. (Usefulness) P is an equation for $\mathcal{C}$, and
2. (Constructibility) $P \in \mathcal{D}$.

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

A nonzero, N-variate polynomial P is a $\mathcal{D}$-natural proof for $\mathcal{C} \subset \mathbb{R}[x_1, \ldots, x_n]$, if:

1. (Usefulness) P is an equation for $\mathcal{C}$, and
2. (Constructibility) $P \in \mathcal{D}$.

Summary.

- Equations are useful in proving explicit lower bounds.

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

A nonzero, N-variate polynomial P is a $\mathcal{D}$-natural proof for $\mathcal{C} \subset \mathbb{R}[x_1, \ldots, x_n]$, if:

1. (Usefulness) P is an equation for $\mathcal{C}$, and
2. (Constructibility) $P \in \mathcal{D}$.

Summary.

- Equations are useful in proving explicit lower bounds.
- Known lower bounds against almost all structured models $\mathcal{C}$, give VP-natural proofs for $\mathcal{C}$.

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

A nonzero, N-variate polynomial P is a $\mathcal{D}$-natural proof for $\mathcal{C} \subset \mathbb{R}[x_1, \ldots, x_n]$, if:

1. (Usefulness) P is an equation for $\mathcal{C}$, and
2. (Constructibility) $P \in \mathcal{D}$.

Summary.

- Equations are useful in proving explicit lower bounds.
- Known lower bounds against almost all structured models $\mathcal{C}$, give VP-natural proofs for $\mathcal{C}$.
- !! Most lower bounds against general models do not use VP-natural proofs, or equations.

Algebraic Natural Proofs

Definition (Algebraic Natural Proofs [FSV18,GKSS17])

A nonzero, N-variate polynomial P is a $\mathcal{D}$-natural proof for $\mathcal{C} \subset \mathbb{R}[x_1, \ldots, x_n]$, if:

1. (Usefulness) P is an equation for $\mathcal{C}$, and
2. (Constructibility) $P \in \mathcal{D}$.

Summary.

- Equations are useful in proving explicit lower bounds.
- Known lower bounds against almost all structured models $\mathcal{C}$, give VP-natural proofs for $\mathcal{C}$.
- !! Most lower bounds against general models do not use VP-natural proofs, or equations.

Q. Are there VP-natural proofs for general classes like VP?

Two (types of) Questions

Does VP have VP-natural proofs?

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*

   — Find smallest class $\mathcal{D}$ such that VP has $\mathcal{D}$-natural proofs.

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*
   — Find smallest class $\mathcal{D}$ such that VP has $\mathcal{D}$-natural proofs.
   — [FSV18]: "Polynomials in $\mathcal{D}$ can't be equations for depth-3-formulas, and hence VP".
   (where $\mathcal{D}$ is e.g. depth-3-powering, depth-2-formulas).

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*
   — Find smallest class $\mathcal{D}$ such that VP has $\mathcal{D}$-natural proofs.
   — [FSV18]: "Polynomials in $\mathcal{D}$ can't be equations for depth-3-formulas, and hence VP".
   (where $\mathcal{D}$ is e.g. depth-3-powering, depth-2-formulas).

2. *What is the best lower bound we can prove using 'natural' methods*?

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*
   — Find smallest class $\mathcal{D}$ such that VP has $\mathcal{D}$-natural proofs.
   — [FSV18]: "Polynomials in $\mathcal{D}$ can't be equations for depth-3-formulas, and hence VP".
   (where $\mathcal{D}$ is e.g. depth-3-powering, depth-2-formulas).

2. *What is the best lower bound we can prove using 'natural' methods*?
   — Find largest class $\mathcal{C}$ such that $\mathcal{C}$ has VP-natural proofs.

Two (types of) Questions

Does VP have VP-natural proofs?

1. *How 'complex' does a lower bound against* VP *need to be?*
   — Find smallest class $\mathcal{D}$ such that VP has $\mathcal{D}$-natural proofs.
   — [FSV18]: "Polynomials in $\mathcal{D}$ can't be equations for depth-3-formulas, and hence VP".
   (where $\mathcal{D}$ is e.g. depth-3-powering, depth-2-formulas).

2. *What is the best lower bound we can prove using 'natural' methods*?
   — Find largest class $\mathcal{C}$ such that $\mathcal{C}$ has VP-natural proofs.
   — [CKRST20,KRST21]: Bounds on $\mathcal{C}$ using 'hardness-randomness connections'.

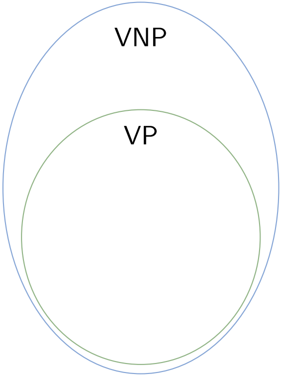
Current Status

Equations for VP in $\mathcal{D}$

Equations for $\mathcal{C}$ in VP

Current Status

Equations for VP in $\mathcal{D}$

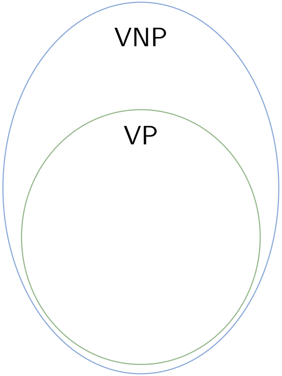


Equations for $\mathcal{C}$ in VP

Current Status

$\mathcal{D} \overset{?}{\subseteq} \mathrm{VP}$

Equations for VP in $\mathcal{D}$



$\mathrm{VP} \overset{?}{\subseteq} \mathcal{C}$

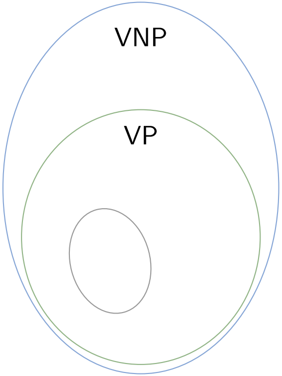
Equations for $\mathcal{C}$ in VP

Current Status

$\mathcal{D} \overset{?}{\subseteq} \mathsf{VP}$

[FSV18]: e.g. $\mathcal{D} \not\subseteq$ powering

Equations for VP in $\mathcal{D}$



$\mathsf{VP} \overset{?}{\subseteq} \mathcal{C}$

Equations for $\mathcal{C}$ in VP

Current Status

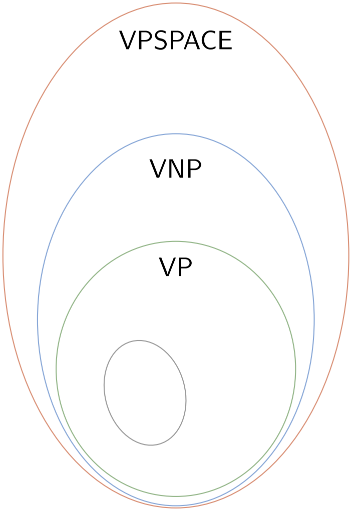
(Easy) $\mathcal{D} \subseteq \mathrm{VPSPACE}$

'coeffs in PSPACE'

$\mathcal{D} \overset{?}{\subseteq} \mathrm{VP}$

[FSV18]: e.g. $\mathcal{D} \not\subseteq$ powering

Equations for VP in $\mathcal{D}$



$\mathrm{VP} \overset{?}{\subseteq} \mathcal{C}$

Equations for $\mathcal{C}$ in VP

Current Status

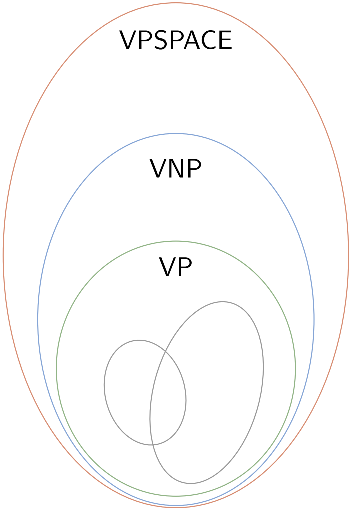
(Easy) $\mathcal{D} \subseteq$ VPSPACE

'coeffs in PSPACE'

$\mathcal{D} \overset{?}{\subseteq}$ VP

[FSV18]: e.g. $\mathcal{D} \not\subseteq$ powering

Equations for VP in $\mathcal{D}$



VP $\overset{?}{\subseteq} \mathcal{C}$

[CKRST20]: VP$' \subseteq \mathcal{C}$

VP $\cap \{-1, 0, 1\}$ coeffs

Equations for $\mathcal{C}$ in VP

Current Status

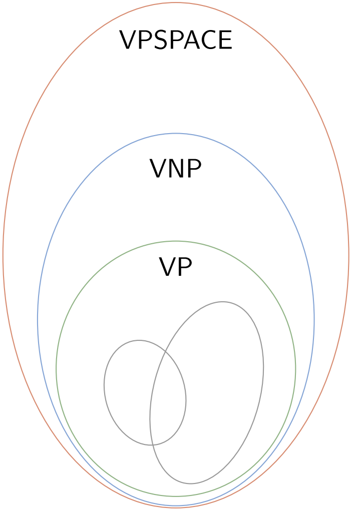
(Easy) $\mathcal{D} \subseteq$ VPSPACE

'coeffs in PSPACE'

$\mathcal{D} \overset{?}{\subseteq}$ VP

[FSV18]: e.g. $\mathcal{D} \not\subseteq$ powering

Equations for VP in $\mathcal{D}$



[KRST21]: VNP $\not\subseteq \mathcal{C}$

If Perm is $\exp(n^{\epsilon})$-hard

VP $\overset{?}{\subseteq} \mathcal{C}$

[CKRST20]: VP$'$ $\subseteq \mathcal{C}$

VP $\cap$ $\{-1, 0, 1\}$ coeffs

Equations for $\mathcal{C}$ in VP

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathsf{VP}'_n = \mathsf{VP}_n \cap \{-1, 0, 1\}^N$.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathsf{VP}'_n = \mathsf{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.
- [HS80]: There *exist* efficient hitting sets S, for VP.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.
- [HS80]: There *exist* <u>efficient</u> hitting sets S, for VP.
- Key Idea: Equations from hitting sets.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.
- [HS80]: There *exist* efficient hitting sets S, for VP.

- Key Idea: Equations from hitting sets.
  - Construct P: $P(f) = 0$ if and only if $f(a) \neq 0$ for some $a \in S$.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.
- [HS80]: There *exist* efficient hitting sets S, for VP.

- Key Idea: Equations from hitting sets.
  - Construct P: $P(f) = 0$ if and only if $f(a) \neq 0$ for some $a \in S$.
  - (Issue): Requires "algebraic-NOT-gate" of degree $\approx$ size-of-domain.

Equations for VP': Ideas

Theorem [CKRST20]: VP_N contains (non-trivial) equations for $\mathrm{VP}'_n = \mathrm{VP}_n \cap \{-1, 0, 1\}^N$.

- Defn (Hitting Set) Set $S \subset \mathbb{Z}^n$ is a *hitting set* for a class $\mathcal{C}$, if for all $f \in \mathcal{C}$ there is some $a \in S$: $f(a) \neq 0$.
- "Diagonalisation using hitting sets" [HS80,Agr05]: If $h(a) = 0$ for all $a \in S$, then $h \notin \mathcal{C}$.
- [HS80]: There *exist* <u>efficient</u> hitting sets S, for VP.

- Key Idea: Equations from hitting sets.
  - Construct P: $P(f) = 0$ if and only if $f(a) \neq 0$ for some $a \in S$.
  - (Issue): Requires "algebraic-NOT-gate" of degree $\approx$ size-of-domain. (*jugāṛ*): Restrict coefficients (hence VP'), simulate "Chinese remaindering" using non-uniformity.

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.
  — Does not affect computability, e.g. $\mathsf{Perm} \in \mathsf{VP}' \Leftrightarrow \mathsf{VP} = \mathsf{VNP}$.

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.
  — Does not affect computability, e.g. $\mathsf{Perm} \in \mathsf{VP}' \Leftrightarrow \mathsf{VP} = \mathsf{VNP}$.
  — Result also holds for integer coefficients with absolute value $\sim 2^n$.

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.
  — Does not affect computability, e.g. $\mathsf{Perm} \in \mathsf{VP}' \Leftrightarrow \mathsf{VP} = \mathsf{VNP}$.
  — Result also holds for integer coefficients with absolute value $\sim 2^n$.
  — Making this work for $2^{n^{\omega(1)}}$ would imply VP-natural proofs for VP!

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.
  - — Does not affect computability, e.g. $\mathsf{Perm} \in \mathsf{VP}' \Leftrightarrow \mathsf{VP} = \mathsf{VNP}$.
  - — Result also holds for integer coefficients with absolute value $\sim 2^n$.
  - — Making this work for $2^{n^{\omega(1)}}$ would imply VP-natural proofs for VP!
- Efficient hitting sets also exist for VNP,
  - [?!] The same result holds for the analogous class VNP'.

Equations for VP': Comments

- Bounded coefficients: Almost all well-studied polynomials have small coefficients.
  — Does not affect computability, e.g. $\mathsf{Perm} \in \mathsf{VP}' \Leftrightarrow \mathsf{VP} = \mathsf{VNP}$.
  — Result also holds for integer coefficients with absolute value $\sim 2^n$.
  — Making this work for $2^{n^{\omega(1)}}$ would imply VP-natural proofs for VP!

- Efficient hitting sets also exist for VNP,
  [?!] The same result holds for the analogous class VNP'.
  — BUT if some $h \in \mathsf{VNP}'$ (say Perm) vanishes on a hitting set for VP,
  then that hitting set gives a "VP-natural proof for $\mathsf{VP} \neq \mathsf{VNP}$"!!

No* VP-equations for VNP: Ideas

No* VP-equations for VNP: Ideas

Hardness $\longrightarrow$ Psuedorandomness
[KI03]

No* VP-equations for VNP: Ideas

$\exp(\sqrt{n})$-hard poly h

Hardness $\longrightarrow$ Psuedorandomness

[KI03]

No* VP-equations for VNP: Ideas

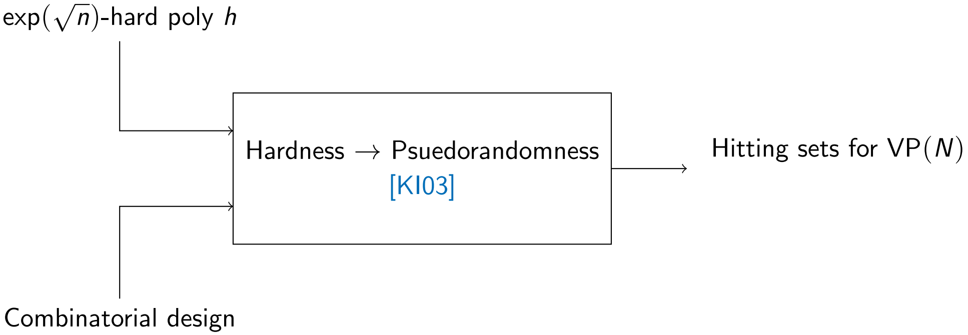
$\exp(\sqrt{n})$-hard poly h

Hardness $\rightarrow$ Psuedorandomness

[KI03]

Combinatorial design

No* VP-equations for VNP: Ideas



Recall: S hitting set for VP $\Rightarrow$ no $f \in$ VP vanishes on all of S.

No* VP-equations for VNP: Ideas

■ Our contribution [KRST21]

$\exp(\sqrt{n})$-hard poly h

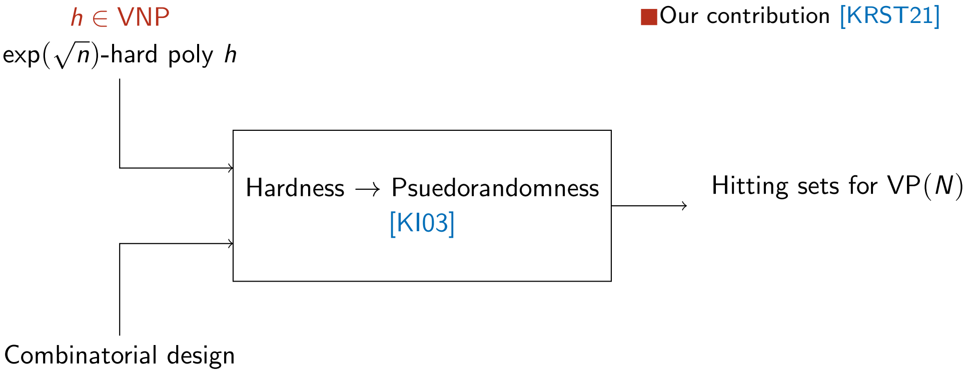
Hardness $\rightarrow$ Psuedorandomness
[KI03]

Hitting sets for VP(N)

Combinatorial design

Recall: S hitting set for VP $\Rightarrow$ no $f \in$ VP vanishes on all of S.

No* VP-equations for VNP: Ideas



<u>Recall</u>: S hitting set for VP $\Rightarrow$ no $f \in$ VP vanishes on all of S.

No* VP-equations for VNP: Ideas

■Our contribution [KRST21]

$h \in \mathsf{VNP}$

$\exp(\sqrt{n})$-hard poly h

Hardness $\rightarrow$ Psuedorandomness [KI03]

Hitting sets for $\mathsf{VP}(N)$

Combinatorial design

based on RS-codes

Recall: S hitting set for VP $\Rightarrow$ no $f \in$ VP vanishes on all of S.

No* VP-equations for VNP: Ideas

■ Our contribution [KRST21]

$h \in \mathsf{VNP}$

$\exp(\sqrt{n})$-hard poly h

Hardness $\longrightarrow$ Psuedorandomness

[KI03]

"VNP-succinct"

Hitting sets for $\mathsf{VP}(N)$

Combinatorial design

based on RS-codes

Recall: S hitting set for VP $\Rightarrow$ no $f \in \mathsf{VP}$ vanishes on all of S.

No* VP-equations for VNP: Ideas

■Our contribution [KRST21]

$h \in \mathsf{VNP}$

$\exp(\sqrt{n})$-hard poly h

Hardness $\rightarrow$ Psuedorandomness

[KI03]

"VNP-succinct"

Hitting sets for $\mathsf{VP}(N)$

coefficient vectors from $\mathsf{VNP}(n)$

Combinatorial design

based on RS-codes

Recall: S hitting set for VP $\Rightarrow$ no $f \in$ VP vanishes on all of S.

No* VP-equations for VNP: Comments

- Any VP-equation for VP, is a natural proof for VP $\neq$ VNP!

  "If VP, VNP are sufficiently separated, then there is a natural proof for it".

No* VP-equations for VNP: Comments

- Any VP-equation for VP, is a natural proof for VP $\neq$ VNP!

  "If VP, VNP are sufficiently separated, then there is a natural proof for it".

- Note: Coefficient vectors generated here have integers of absolute value $2^{\mathrm{poly}(n)}$, therefore not in VNP$'$. We do not get sub-exponential sized circuits for Perm. :)

No* VP-equations for VNP: Comments

- Any VP-equation for VP, is a natural proof for VP $\neq$ VNP!

  "If VP, VNP are sufficiently separated, then there is a natural proof for it".

- Note: Coefficient vectors generated here have integers of absolute value $2^{\mathrm{poly}(n)}$, therefore not in VNP$'$. We do not get sub-exponential sized circuits for Perm. :)

- "Efficient equations give explicit lower bounds".

  Subject to Perm being $2^{n^{\epsilon}}$ hard.

Open Directions

- “There is a naturalisation barrier”

Open Directions

- "There is a naturalisation barrier"
  - Extend [KRST21] to get VP-succinct hitting sets for VP ...?

Open Directions

- "There is a naturalisation barrier"
  - Extend [KRST21] to get VP-succinct hitting sets for VP ...?
  - Requires a VP-succinct analogue of [KI03], that works even with poly(n)-hardness, highly interesting in its own right.

Open Directions

- “There is a naturalisation barrier”
  - Extend [KRST21] to get VP-succinct hitting sets for VP . . . ?
  - Requires a VP-succinct analogue of [KI03], that works even with poly(n)-hardness, highly interesting in its own right.

- “Natural methods are sufficient”

Open Directions

- "There is a naturalisation barrier"
  - Extend [KRST21] to get VP-succinct hitting sets for VP ...?
  - Requires a VP-succinct analogue of [KI03], that works even with $\mathrm{poly}(n)$-hardness, highly interesting in its own right.

- "Natural methods are sufficient"
  - (Conditionally) extend [CKRST20] to work for VP with coefficients of size $2^{n^{\omega(1)}}$ ...?

Open Directions

- "There is a naturalisation barrier"
  - Extend [KRST21] to get VP-succinct hitting sets for VP ...?
  - Requires a VP-succinct analogue of [KI03], that works even with poly(n)-hardness, highly interesting in its own right.
- "Natural methods are sufficient"
  - (Conditionally) extend [CKRST20] to work for VP with coefficients of size $2^{n^{\omega(1)}}$ ...?
  - Due to [KRST21], equations for coefficients of size $2^{\mathrm{poly}(n)}$ would essentially guarantee a "natural separation" of VP and VNP.

Thank You

Questions?