Can Algebraic Circuit Lower Bounds Have Easy Proofs?

Prerona Chatterjee
TIFR, Mumbai

Mrinal Kumar
IITB, Mumbai

C. Ramya
TIFR, Mumbai

Ramprasad Saptharishi
TIFR, Mumbai

Anamay Tengse
TIFR, Mumbai

Algorithms & Complexity Seminar
University of Waterloo

Part I

The Basics

Polynomials

- Polynomials appear often in computation.
  e.g. Coding theory, complexity theory, combinatorics,...

Polynomials

- Polynomials appear often in computation.
  e.g. Coding theory, complexity theory, combinatorics,...
- Natural to wonder about the cost of computing polynomials

Polynomials

- Polynomials appear often in computation.
  e.g. Coding theory, complexity theory, combinatorics,...

- Natural to wonder about the cost of computing polynomials

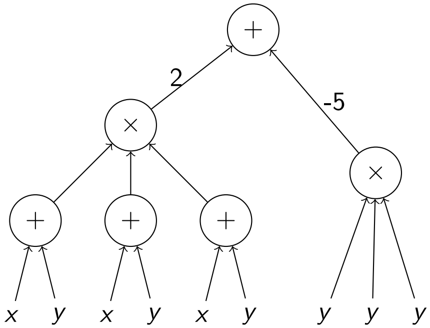
- Variables - $\bar{x} = \{x_1, \ldots, x_n\}$, constants - $\mathbb{F} = \mathbb{C}$
  Operations - Addition $+$ and multiplication $\times$.

Computing Polynomials

$$f(x, y, z) = 2x^3 + 6x^2y + 6xy^2 - 3y^3 \qquad \in \ \mathbb{Q}[x, y, z]$$

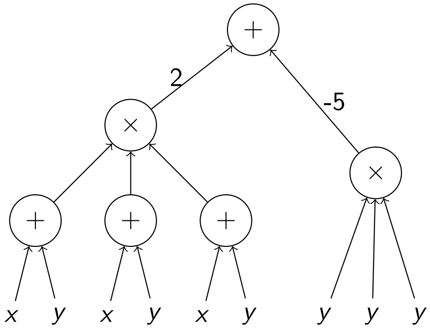
Computing Polynomials

$$f(x,y,z) = 2x^3 + 6x^2y + 6xy^2 - 3y^3 \qquad \in \mathbb{Q}[x,y,z]$$
$$= 2(x+y)^3 - 5y^3$$



Computing Polynomials

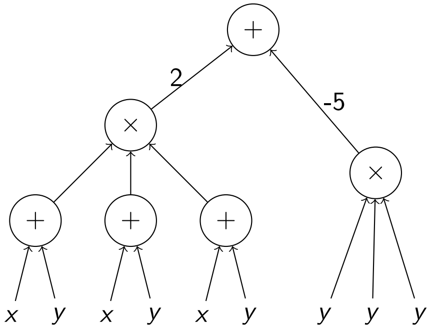
$$f(x,y,z) = 2x^3 + 6x^2y + 6xy^2 - 3y^3 \qquad \in \ \mathbb{Q}[x,y,z]$$
$$= 2(x+y)^3 - 5y^3$$



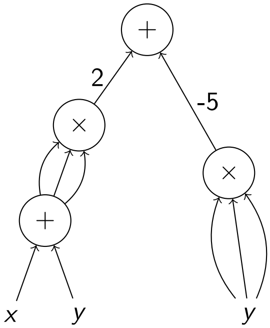
Algebraic Formulas

Computing Polynomials

$$f(x,y,z) = 2x^3 + 6x^2y + 6xy^2 - 3y^3 \qquad \in \ \mathbb{Q}[x,y,z]$$
$$= 2(x+y)^3 - 5y^3$$

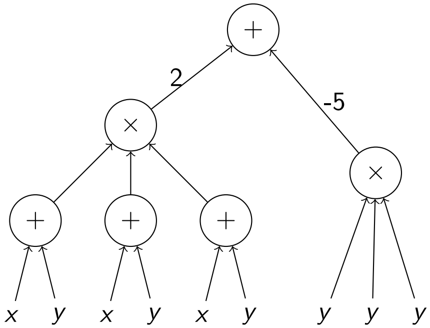


Algebraic Formulas

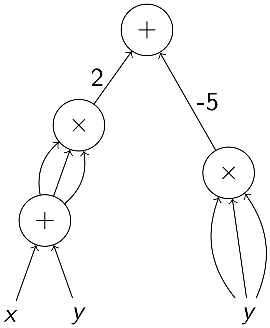


Computing Polynomials

$$f(x,y,z) = 2x^3 + 6x^2y + 6xy^2 - 3y^3 \qquad \in \ \mathbb{Q}[x,y,z]$$
$$= 2(x+y)^3 - 5y^3$$



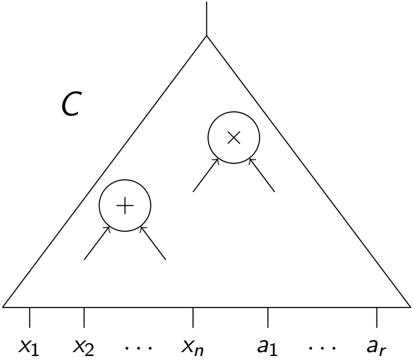
Algebraic Formulas



Algebraic Circuits

Algebraic Circuits

$f(\bar{x}) \in \mathbb{F}[\bar{x}]$

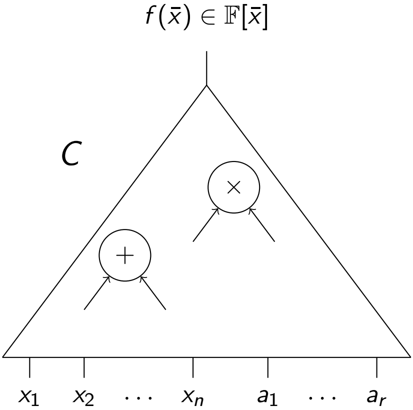


Parameters:

Size(C)
- No. of gates or no. of wires

Depth(C)
- Longest path from root to a leaf

Algebraic Circuits



Parameters:

Size(C)
- No. of gates or no. of wires

Depth(C)
- Longest path from root to a leaf

Q. Can we give tight bounds on size(f) for a certain f?

size(f): Size of the smallest circuit computing $f(\bar{x})$.

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Parameters: Number of variables - n, degree - d
This talk: $d \sim \mathrm{poly}(n)$

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Parameters: Number of variables - n, degree - d
This talk: $d \sim \text{poly}(n)$

Definition (VP - Easy Polynomials):

Class of all n-variate, degree $d = \text{poly}(n)$ polynomials, computable by circuits of size $\text{poly}(n)$.

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Parameters: Number of variables - n, degree - d
This talk: $d \sim \text{poly}(n)$

Definition (VP - Easy Polynomials):

Class of all n-variate, degree $d = \text{poly}(n)$ polynomials, computable by circuits of size $\text{poly}(n)$.

Explicit: Reasonably easy to find coefficient of any monomial.

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Parameters: Number of variables - n, degree - d
This talk: $d \sim \text{poly}(n)$

Definition (VP - Easy Polynomials):

Class of all n-variate, degree $d = \text{poly}(n)$ polynomials, computable by circuits of size $\text{poly}(n)$.

Explicit: Reasonably easy to find coefficient of any monomial.

Definition (Criterion for VNP - Explicit Polynomials):

Suppose f is an n-variate, degree $d = \text{poly}(n)$ polynomial whose coefficients are computable in $\#\text{P}/\text{poly}$; then $f \in \text{VNP}$.

Easy and Hard Polynomials [Val79]

Q. Can we find "explicit" polynomials that are "hard" to compute?

Parameters: Number of variables - n, degree - d
This talk: $d \sim \text{poly}(n)$

Definition (VP - Easy Polynomials):

Class of all n-variate, degree $d = \text{poly}(n)$ polynomials, computable by circuits of size $\text{poly}(n)$.

Explicit: Reasonably easy to find coefficient of any monomial.

Definition (Criterion for VNP - Explicit Polynomials):

Suppose f is an n-variate, degree $d = \text{poly}(n)$ polynomial whose coefficients are computable in $\#\text{P}/\text{poly}$; then $f \in \text{VNP}$.

Q. VP vs VNP $\approx$ Det_n vs Perm_n.

Finding Hard Polynomials

- Best Lower Bounds:
  - Circuits: $\Theta(n \log d)$ for $x_1^d + \ldots + x_n^d$ [BS83,Smo97]
  - Formulas: $\Theta(n^2)$ for $\mathrm{ESym}(n, 0.1n)$ [CKSV20]

Finding Hard Polynomials

- Best Lower Bounds:
  - Circuits: $\Theta(n \log d)$ for $x_1^d + \ldots + x_n^d$ [BS83,Smo97]
  - Formulas: $\Theta(n^2)$ for $\mathrm{ESym}(n, 0.1n)$ [CKSV20]

- Progress in Restricted Models:
  - Constant depth circuits [NW95,KST16,GKKS13,...]
  - Multilinear models [Raz09,DMPY12,...]
  - Non-commutative models [Nis91,LMP16,CILM18,...]
  - Monotone models [Yeh19,Sri19]

Finding Hard Polynomials

- Best Lower Bounds:
  - Circuits: $\Theta(n \log d)$ for $x_1^d + \ldots + x_n^d$ [BS83,Smo97]
  - Formulas: $\Theta(n^2)$ for $\mathrm{ESym}(n, 0.1n)$ [CKSV20]
- Progress in Restricted Models:
  - Constant depth circuits [NW95,KST16,GKKS13,...]
  - Multilinear models [Raz09,DMPY12,...]
  - Non-commutative models [Nis91,LMP16,CILM18,...]
  - Monotone models [Yeh19,Sri19]

Observation: Most of the proofs follow a certain template.

Finding Hard Polynomials

- Best Lower Bounds:
  - Circuits: $\Theta(n \log d)$ for $x_1^d + \ldots + x_n^d$ [BS83,Smo97]
  - Formulas: $\Theta(n^2)$ for $\mathrm{ESym}(n, 0.1n)$ [CKSV20]
- Progress in Restricted Models:
  - Constant depth circuits [NW95,KST16,GKKS13,...]
  - Multilinear models [Raz09,DMPY12,...]
  - Non-commutative models [Nis91,LMP16,CILM18,...]
  - Monotone models [Yeh19,Sri19]

Observation: Most of the proofs follow a certain template.

Are current methods insufficient?

Part II

The Result

Proofs of Hardness/Non-membership

Toy Problem: $\mathcal{C} = \{(\alpha t - \beta)^2 : \alpha, \beta \in \mathbb{C}\}$.

Proofs of Hardness/Non-membership

Toy Problem: $\mathcal{C} = \{(\alpha t - \beta)^2 : \alpha, \beta \in \mathbb{C}\}$.

Finding explicit $h \notin \mathcal{C}$:

Proofs of Hardness/Non-membership

Toy Problem: $\mathcal{C} = \{(\alpha t - \beta)^2 : \alpha, \beta \in \mathbb{C}\}$.

Finding explicit $h \notin \mathcal{C}$:

- "Weakness" of $\mathcal{C}$:
  If $f(t) = at^2 + bt + c \in \mathcal{C}$, then $b^2 - 4ac = 0$.

Proofs of Hardness/Non-membership

Toy Problem: $\mathcal{C} = \{(\alpha t - \beta)^2 : \alpha, \beta \in \mathbb{C}\}$.

<ins>Finding explicit $h \notin \mathcal{C}$</ins>:

- "Weakness" of $\mathcal{C}$:
  If $f(t) = at^2 + bt + c \in \mathcal{C}$, then $b^2 - 4ac = 0$.
- "Hard" Polynomial:
  $h(t) = a't^2 + b't + c'$ such that $b'^2 - 4a'c' \neq 0$.

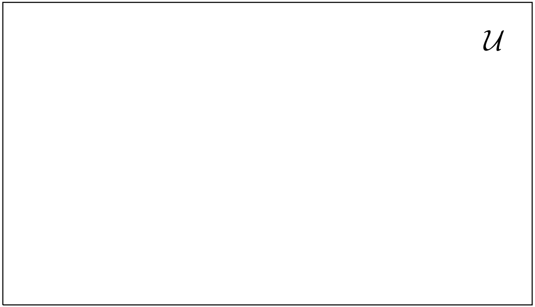
Natural Properties [RR97]

$\mathcal{U}$ - universe, $\mathcal{C}$ - class, $\mathcal{P}$ - property

Natural Properties [RR97]

$\mathcal{U}$ - universe, $\quad \mathcal{C}$ - class, $\quad \mathcal{P}$ - property

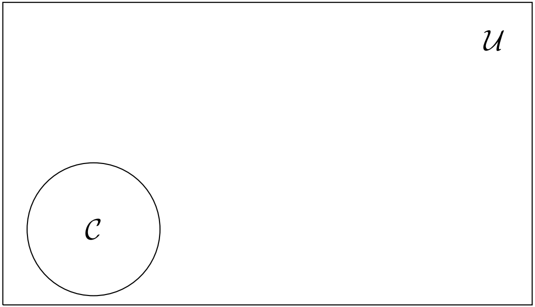
$at^2 + bt + c, \quad (\alpha t - \beta)^2, \quad b^2 - 4ac \neq 0$



Natural Properties [RR97]

$\mathcal{U}$ - universe, $\mathcal{C}$ - class, $\mathcal{P}$ - property

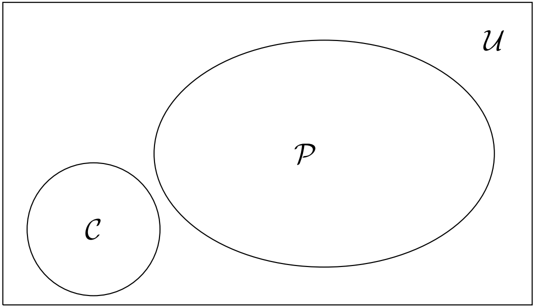
$at^2 + bt + c$, $(\alpha t - \beta)^2$, $b^2 - 4ac \neq 0$



Natural Properties [RR97]

$\mathcal{U}$ - universe, $\quad \mathcal{C}$ - class, $\quad \mathcal{P}$ - property

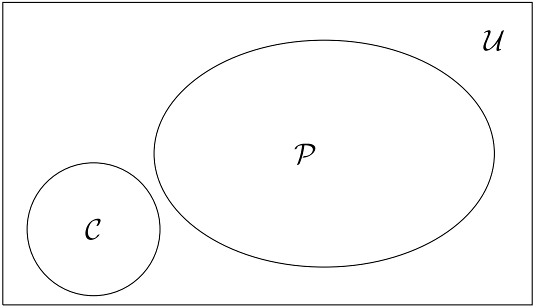
$at^2 + bt + c, \quad (\alpha t - \beta)^2, \quad b^2 - 4ac \neq 0$



Natural Properties [RR97]

$\mathcal{U}$ - universe, $\quad \mathcal{C}$ - class, $\quad \mathcal{P}$ - property

$at^2 + bt + c, \quad (\alpha t - \beta)^2, \quad b^2 - 4ac \neq 0$

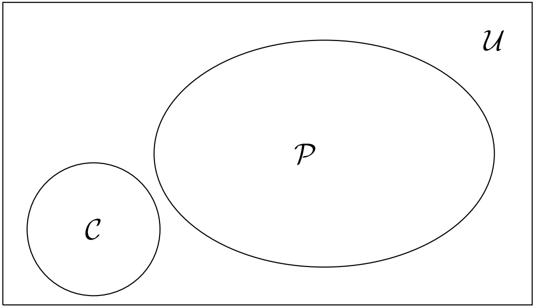


- **Useful** against $\mathcal{C}$: $\mathcal{C} \cap \mathcal{P} = \emptyset$.

Natural Properties [RR97]

$\mathcal{U}$ - universe, $\mathcal{C}$ - class, $\mathcal{P}$ - property

$at^2 + bt + c$, $(\alpha t - \beta)^2$, $b^2 - 4ac \neq 0$

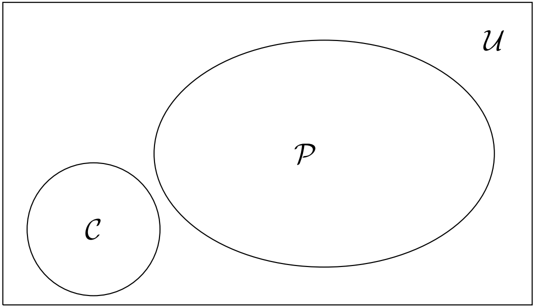


- **Useful** against $\mathcal{C}$: $\mathcal{C} \cap \mathcal{P} = \emptyset$.
- **Constructive**: "Easy" to decide if $f \in \mathcal{P}$, for all f.

Natural Properties [RR97]

$\mathcal{U}$ - universe, $\mathcal{C}$ - class, $\mathcal{P}$ - property

$at^2 + bt + c$, $(\alpha t - \beta)^2$, $b^2 - 4ac \neq 0$

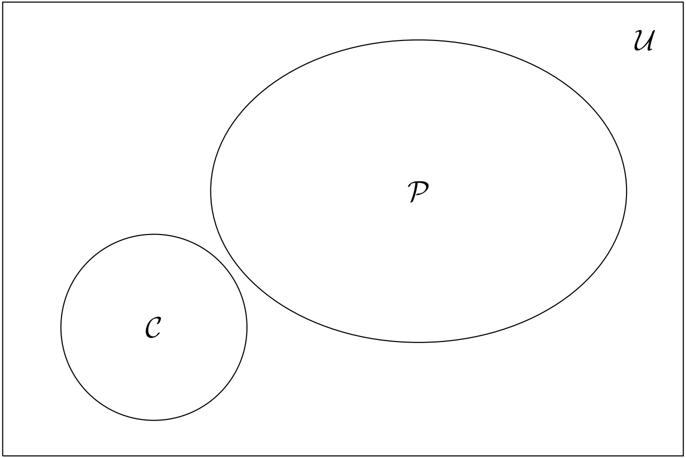


- **Useful** against $\mathcal{C}$: $\mathcal{C} \cap \mathcal{P} = \emptyset$.
- **Constructive**: "Easy" to decide if $f \in \mathcal{P}$, for all f.
- **Large**: "Most" $f \in \mathcal{P}$.

Lower Bounds from Natural Properties

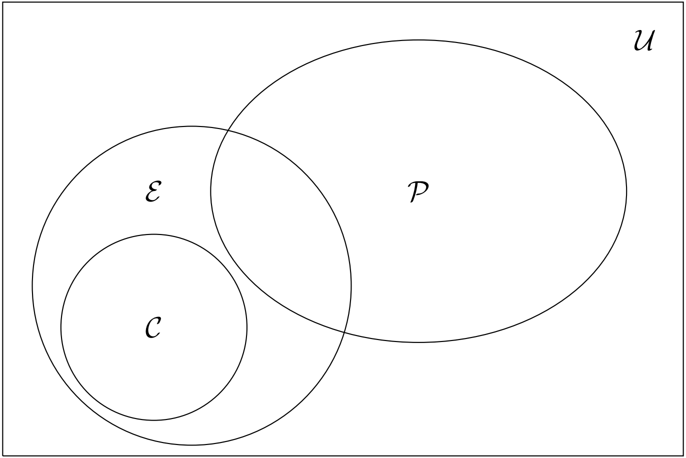
$\mathcal{C}$ - class

$\mathcal{P}$ - property



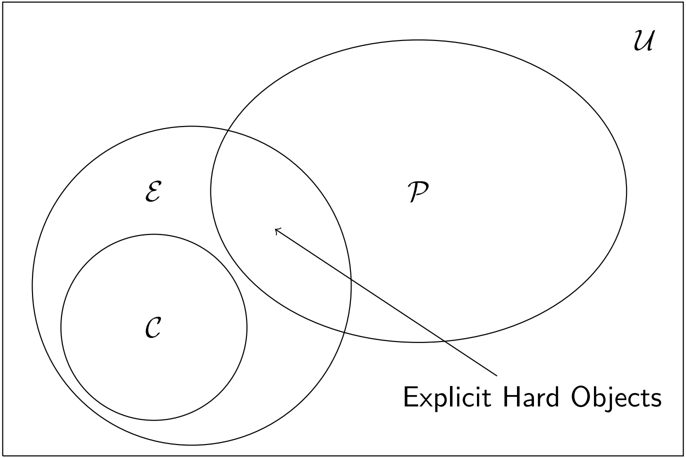
Lower Bounds from Natural Properties

$\mathcal{C}$ - class $\quad$ $\mathcal{E}$ - explicit objects $\quad$ $\mathcal{P}$ - property



Lower Bounds from Natural Properties

$\mathcal{C}$ - class $\qquad$ $\mathcal{E}$ - explicit objects $\qquad$ $\mathcal{P}$ - property



Natural Properties for Polynomials [FSV18,GKSS17]

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

$\mathcal{M}$ - monomials in $\bar{x}$ of degree d, $N = |\mathcal{M}| = \binom{n+d}{n}$.

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

$\mathcal{M}$ - monomials in $\bar{x}$ of degree d, $N = |\mathcal{M}| = \binom{n+d}{n}$.

$$f(x_1, \ldots, x_n) = \sum_{m \in \mathcal{M}} f_m \cdot m \qquad f_m = \mathrm{coeff}_f(m)$$

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

$\mathcal{M}$ - monomials in $\bar{x}$ of degree d, $N = |\mathcal{M}| = \binom{n+d}{n}$.

$$f(x_1, \ldots, x_n) = \sum_{m \in \mathcal{M}} f_m \cdot m \qquad f_m = \mathrm{coeff}_f(m)$$

Let $\mathrm{coeffs}(f) = [f_{m_1}, f_{m_2}, \ldots, f_{m_N}] \in \mathbb{F}^N$.

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

$\mathcal{M}$ - monomials in $\bar{x}$ of degree d, $N = |\mathcal{M}| = \binom{n+d}{n}$.

$$f(x_1, \ldots, x_n) = \sum_{m \in \mathcal{M}} f_m \cdot m \qquad f_m = \mathrm{coeff}_f(m)$$

Let $\mathrm{coeffs}(f) = [f_{m_1}, f_{m_2}, \ldots, f_{m_N}] \in \mathbb{F}^N$.

Definition (Defining Equation)

A polynomial P is said to be a defining equation for a class $\mathcal{C}$, if $P(\mathrm{coeffs}(f)) = 0$ for all $f \in \mathcal{C}$.

Natural Properties for Polynomials [FSV18,GKSS17]

Variables $\bar{x} = \{x_1, \ldots, x_n\}$, Degree - d, Field $\mathbb{F}$.

$\mathcal{M}$ - monomials in $\bar{x}$ of degree d, $N = |\mathcal{M}| = \binom{n+d}{n}$.

$$f(x_1, \ldots, x_n) = \sum_{m \in \mathcal{M}} f_m \cdot m \qquad f_m = \mathrm{coeff}_f(m)$$

Let $\mathrm{coeffs}(f) = [f_{m_1}, f_{m_2}, \ldots, f_{m_N}] \in \mathbb{F}^N$.

Definition (Defining Equation)

A polynomial P is said to be a defining equation for a class $\mathcal{C}$, if $P(\mathrm{coeffs}(f)) = 0$ for all $f \in \mathcal{C}$.

$\mathcal{U} = \mathbb{F}^N$ $\mathcal{C} = \mathrm{VP}(n, d)$ $P_N =$ defining equation

Algebraically Natural Proofs [FSV18,GKSS17]

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$;   let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a *natural proof against* $\mathcal{C}_n$ if:

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a *natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: $P(\text{coeffs}(f)) = 0$ for all $f \in \mathcal{C}_n$.

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a *natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: $P(\text{coeffs}(f)) = 0$ for all $f \in \mathcal{C}_n$.
- **Constructivity**: P is "easy" to compute.

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a *natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: $P(\text{coeffs}(f)) = 0$ for all $f \in \mathcal{C}_n$.
- **Constructivity**: P is "easy" to compute.
- **Largeness**: $P(\text{coeffs}(g)) \neq 0$ for most g.

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a *natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: $P(\text{coeffs}(f)) = 0$ for all $f \in \mathcal{C}_n$.
- **Constructivity**: P is "easy" to compute.
- **Largeness**: $P(\text{coeffs}(g)) \neq 0$ for most g.

Q. Are there natural proofs against VP_n?

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a $\mathcal{D}_N$*-natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: $P(\text{coeffs}(f)) = 0$ for all $f \in \mathcal{C}_n$.
- **Constructivity**: $P \in \mathcal{D}_N$.
- **Largeness**: $P(\text{coeffs}(g)) \neq 0$ for most g.

Q. Are there natural proofs against VP_n?

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a $\mathcal{D}_N$-*natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: P is a defining equation for $\mathcal{C}_n$.
- **Constructivity**: $P \in \mathcal{D}_N$.
- **Largeness**: $P(\text{coeffs}(g)) \neq 0$ for most g.

Q. Are there natural proofs against VP_n?

Algebraically Natural Proofs [FSV18,GKSS17]

For n, d and $N = \binom{n+d}{n}$; let $\mathcal{U} = \mathbb{F}^N$, $\mathcal{C}_n \subset \mathbb{F}^N$.

$P(Z_1, \ldots, Z_N)$ is a $\mathcal{D}_N$-*natural proof against* $\mathcal{C}_n$ if:

- **Usefulness**: P is a defining equation for $\mathcal{C}_n$.
- **Constructivity**: $P \in \mathcal{D}_N$.
- **Largeness**: $P(\text{coeffs}(g)) \neq 0$ for most g.

Q. Are there large VP_N-defining equations for VP_n?

Related Works

- **Natural Proofs** [FSV18]
  - Derandomization statement for $\mathcal{C}$ contradicts existence of natural proofs for $\mathcal{C}$.

Related Works

- **Natural Proofs** [FSV18]
  - Derandomization statement for $\mathcal{C}$ contradicts existence of natural proofs for $\mathcal{C}$.
  - For several restricted classes $\mathcal{C}_n$ and $\mathcal{D}_N$, there are no $\mathcal{D}_N$-natural proofs against $\mathcal{C}_n$.

Related Works

- **Natural Proofs** [FSV18]
  - Derandomization statement for $\mathcal{C}$ contradicts existence of natural proofs for $\mathcal{C}$.
  - For several restricted classes $\mathcal{C}_n$ and $\mathcal{D}_N$, there are no $\mathcal{D}_N$-natural proofs against $\mathcal{C}_n$.
- **Variety Membership** [BIJL18,BIL+19]
  - Hardness of membership testing rules out efficient defining equations for certain classes.

Related Works

- **Natural Proofs** [FSV18]
  - Derandomization statement for $\mathcal{C}$ contradicts existence of natural proofs for $\mathcal{C}$.
  - For several restricted classes $\mathcal{C}_n$ and $\mathcal{D}_N$, there are no $\mathcal{D}_N$-natural proofs against $\mathcal{C}_n$.
- **Variety Membership** [BIJL18,BIL+19]
  - Hardness of membership testing rules out efficient defining equations for certain classes.
- **Rank Methods** [EGOW18,GMOW19]
  - *Rank-based methods* will not show optimal lower bounds.
  - Tensor rank lower bounds do not lift to higher dimensions.

Related Works

- **Natural Proofs** [FSV18]
  - Derandomization statement for $\mathcal{C}$ contradicts existence of natural proofs for $\mathcal{C}$.
  - For several restricted classes $\mathcal{C}_n$ and $\mathcal{D}_N$, there are no $\mathcal{D}_N$-natural proofs against $\mathcal{C}_n$.
- **Variety Membership** [BIJL18,BIL+19]
  - Hardness of membership testing rules out efficient defining equations for certain classes.
- **Rank Methods** [EGOW18,GMOW19]
  - *Rank-based methods* will not show optimal lower bounds.
  - Tensor rank lower bounds do not lift to higher dimensions.

Q. What about natural proofs for VP?

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

A. *Almost* yes, for *natural* polynomials.

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

A. *Almost* yes, for *natural* polynomials.

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}'_{\mathbb{C}}$):

For n,d and $N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that

for all $f \in \mathrm{VP}(n, d)$ *with small integer coefficients*,

$P(\mathrm{coeffs}(f)) = 0$.

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

A. *Almost* yes, for *natural* polynomials.

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}'_{\mathbb{C}}$):

For n,d and $N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that

for all $f \in \mathrm{VP}(n, d)$ *with small integer coefficients*,

$P(\mathrm{coeffs}(f)) = 0$.

Restriction **not on circuits** computing the polynomials.

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

A. *Almost* yes, for *natural* polynomials.

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}'_{\mathbb{C}}$):

For n,d and $N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that

for all $f \in \mathrm{VP}(n, d)$ *with small integer coefficients*,

$P(\mathrm{coeffs}(f)) = 0$.

Restriction **not on circuits** computing the polynomials.

P is nonzero on sizeable fraction of polynomials with small integer coefficients.

Main Theorem

Q. Are there VP(N)-natural proofs against VP(n)?

A. *Almost* yes, for *natural* polynomials.

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}'_{\mathbb{C}}$):

For n,d and $N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that

for all $f \in \mathrm{VP}(n, d)$ *with small integer coefficients*,

$P(\mathrm{coeffs}(f)) = 0$.

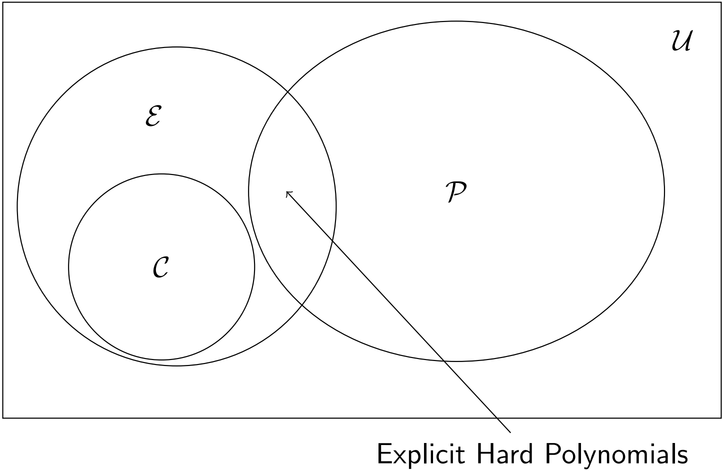
Restriction **not on circuits** computing the polynomials.

P is nonzero on sizeable fraction of polynomials with small integer coefficients.

Q. How is this different from natural proofs?

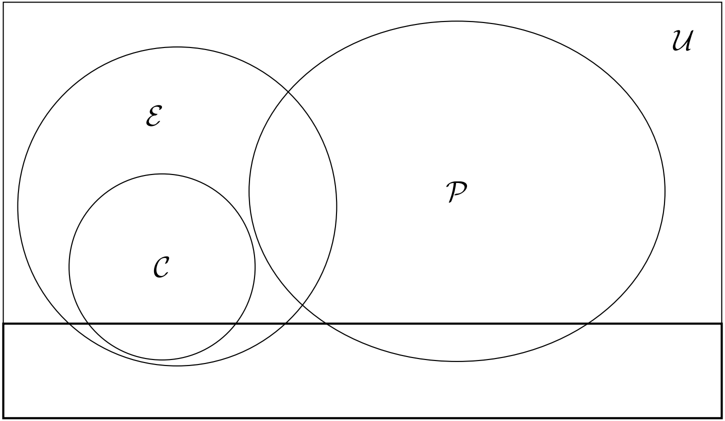
Our Result and Natural Proofs

$\mathcal{C}$ - class, $\mathcal{P}$ - property, $\mathcal{E}$ - explicit polynomials



Our Result and Natural Proofs

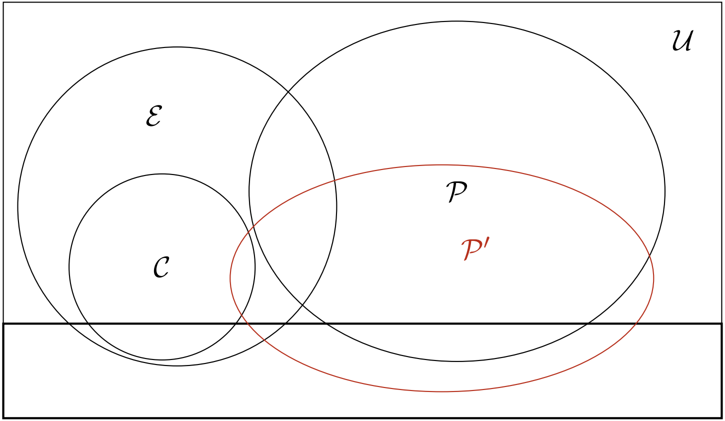
$\mathcal{C}$ - class, $\mathcal{P}$ - property, $\mathcal{E}$ - explicit polynomials



Our Result and Natural Proofs

$\mathcal{C}$ - class, $\mathcal{P}$ - property, $\mathcal{E}$ - explicit polynomials

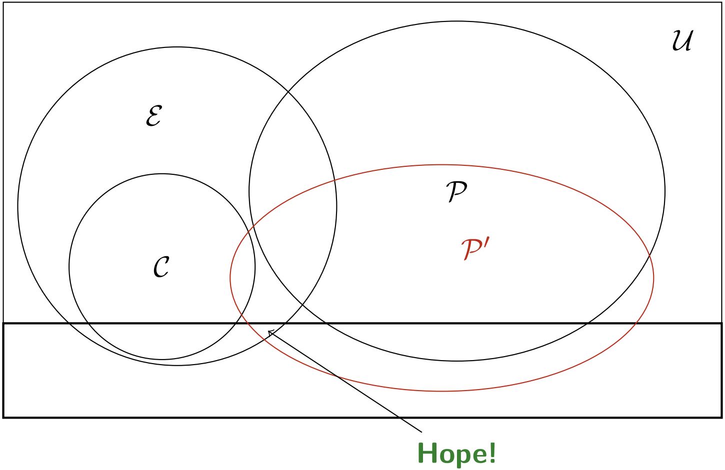
$\mathcal{P}'$ - our property



Our Result and Natural Proofs

$\mathcal{C}$ - class, $\mathcal{P}$ - property, $\mathcal{E}$ - explicit polynomials

$\mathcal{P}'$ - our property



Part III

Proofs and Discussion

Defining Property of VP

Defining Property of VP

Want: A property of VP that can be expressed succinctly.

Defining Property of VP

Want: A property of VP that can be expressed succinctly.

Definition (Hitting Set)

$\mathcal{H} \subset \mathbb{F}^n$ is a *hitting set* for a class $\mathcal{C}$ of n-variate polynomials, if for all $0 \neq f \in \mathcal{C}$, there exists an $h \in \mathcal{H}$ such that $f(h) \neq 0$.

Defining Property of VP

Want: A property of VP that can be expressed succinctly.

Definition (Hitting Set)

$\mathcal{H} \subset \mathbb{F}^n$ is a *hitting set* for a class $\mathcal{C}$ of n-variate polynomials, if for all $0 \neq f \in \mathcal{C}$, there exists an $h \in \mathcal{H}$ such that $f(h) \neq 0$.

Theorem [HS80,For14]

There *exist* hitting sets of size $\mathrm{poly}(n, d, s)$ for the class of n-variate, degree d polynomials that have circuits of size s.

Defining Property of VP

Want: A property of VP that can be expressed succinctly.

Definition (Hitting Set)

$\mathcal{H} \subset \mathbb{F}^n$ is a *hitting set* for a class $\mathcal{C}$ of n-variate polynomials, if for all $0 \neq f \in \mathcal{C}$, there exists an $h \in \mathcal{H}$ such that $f(h) \neq 0$.

Theorem [HS80,For14]

There *exist* hitting sets of size $\mathrm{poly}(n, d, s)$ for the class of n-variate, degree d polynomials that have circuits of size s.

Hitting sets with small integers in the small coefficient setting.

Defining Property of VP

Want: A property of VP that can be expressed succinctly.

Definition (Hitting Set)

$\mathcal{H} \subset \mathbb{F}^n$ is a *hitting set* for a class $\mathcal{C}$ of n-variate polynomials, if for all $0 \neq f \in \mathcal{C}$, there exists an $h \in \mathcal{H}$ such that $f(h) \neq 0$.

Theorem [HS80,For14]

There *exist* hitting sets of size poly(n, d, s) for the class of n-variate, degree d polynomials that have circuits of size s.

Hitting sets with small integers in the small coefficient setting.

Idea: For a nonzero g, $g(\mathcal{H}) = 0$ is a proof that $g \notin \mathcal{C}$.

Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.

Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\qquad 0 \neq g(\bar{x})$ input polynomial.

coeffs(g)

Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.

$\boxed{g(h_1)}$

coeffs(g)

Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\qquad 0 \neq g(\bar{x})$ input polynomial.

$\boxed{g(h_1)}$ $\qquad$ $\boxed{g(h_2)}$

$\mathsf{coeffs}(g)$

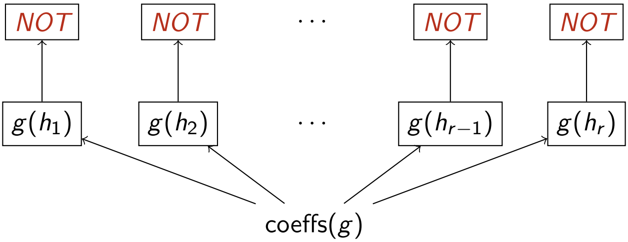
Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\qquad 0 \neq g(\bar{x})$ input polynomial.

$$
\begin{tikzcd}
\boxed{g(h_1)} & \boxed{g(h_2)} & \cdots & \boxed{g(h_{r-1})} & \boxed{g(h_r)} \\
 & & \text{coeffs}(g) \arrow[ull] \arrow[ul] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

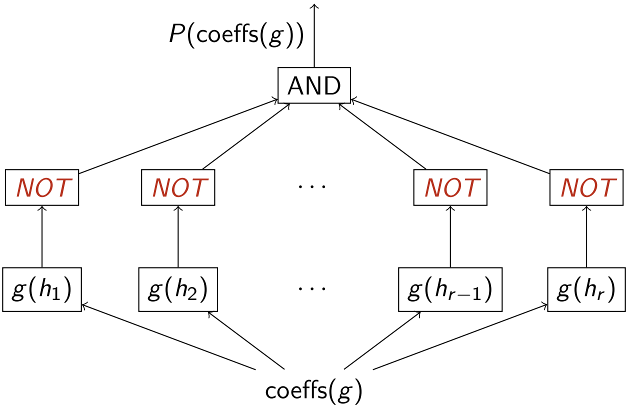
Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.



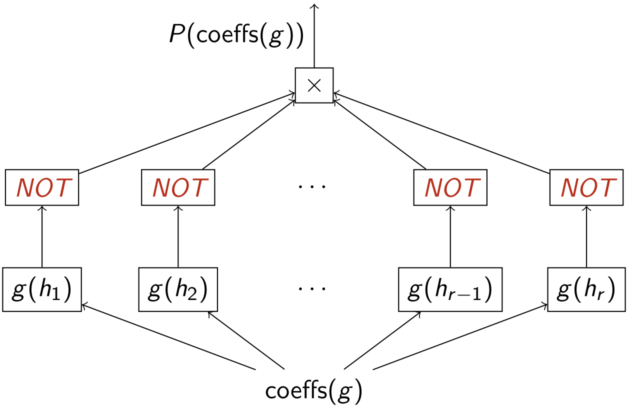
Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.



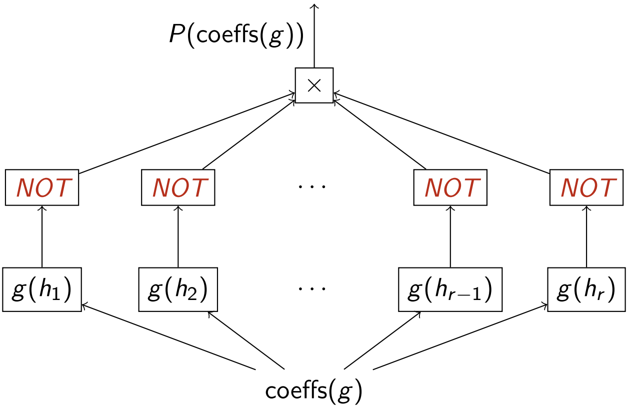
Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\qquad 0 \neq g(\bar{x})$ input polynomial.



Hitting Set as a Defining Property

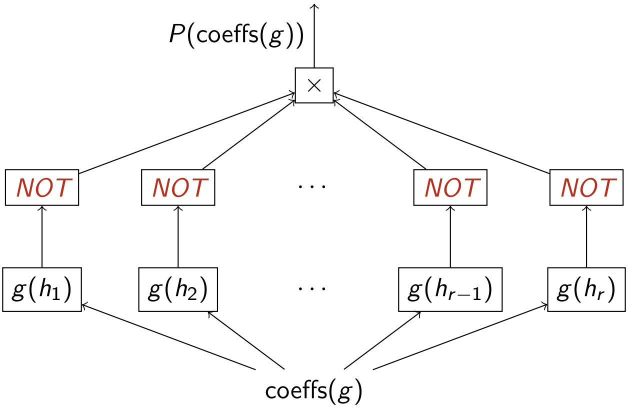
$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.



NOT(0) =nonzero

Hitting Set as a Defining Property

$\mathcal{H} = \{h_1, \ldots, h_r\}$ hitting set for $\mathcal{C}$, $\quad 0 \neq g(\bar{x})$ input polynomial.



$NOT(0) =$nonzero $\quad NOT(\text{nonzero}) = 0$

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

$\text{coeffs}(g) = [g_{m_1}, g_{m_2}, \ldots, g_{m_N}]$, $\{m_1, \ldots, m_N\} = \mathcal{M}$.

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

$\text{coeffs}(g) = [g_{m_1}, g_{m_2}, \ldots, g_{m_N}]$, $\{m_1, \ldots, m_N\} = \mathcal{M}$.

Let $\text{eval}(h) = [m_1(h), m_2(h), \ldots, m_N(h)]$.

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

$\text{coeffs}(g) = [g_{m_1}, g_{m_2}, \ldots, g_{m_N}]$, $\{m_1, \ldots, m_N\} = \mathcal{M}$.

Let $\text{eval}(h) = [m_1(h), m_2(h), \ldots, m_N(h)]$.

Now $g(h) = \langle \text{coeffs}(g), \text{eval}(h) \rangle = \sum_{m \in \mathcal{M}} g_m m(h)$.

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

$\text{coeffs}(g) = [g_{m_1}, g_{m_2}, \ldots, g_{m_N}]$, $\{m_1, \ldots, m_N\} = \mathcal{M}$.

Let $\text{eval}(h) = [m_1(h), m_2(h), \ldots, m_N(h)]$.

Now $g(h) = \langle \text{coeffs}(g), \text{eval}(h) \rangle = \sum_{m \in \mathcal{M}} g_m m(h)$.

Note:

- Linear polynomial in $\text{coeffs}(g)$.

Evaluating at a point

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}^N$, point $h \in \mathbb{F}^n$

$\text{coeffs}(g) = [g_{m_1}, g_{m_2}, \ldots, g_{m_N}]$, $\{m_1, \ldots, m_N\} = \mathcal{M}$.

Let $\text{eval}(h) = [m_1(h), m_2(h), \ldots, m_N(h)]$.

Now $g(h) = \langle \text{coeffs}(g), \text{eval}(h) \rangle = \sum_{m \in \mathcal{M}} g_m m(h)$.

Note:

- Linear polynomial in $\text{coeffs}(g)$.
- We can "hardwire" $\text{eval}(h)$ in our circuit, for all $h \in \mathcal{H}$.

Algebraic NOT - Finite Fields

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Algebraic NOT - Finite Fields

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Algebraic NOT - Finite Fields

Given: Vector coeffs$(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: For all $x \in \mathbb{F}_q$, $x^q - x = 0$

Algebraic NOT - Finite Fields

Given: Vector coeffs$(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: For all $x \in \mathbb{F}_q$, $x^q - x = 0$

$\Rightarrow$ For all $0 \neq x \in \mathbb{F}_q$, $x^{q-1} - 1 = 0$

Algebraic NOT - Finite Fields

Given: Vector coeffs$(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: For all $x \in \mathbb{F}_q$, $x^q - x = 0$

$\Rightarrow$ For all $0 \neq x \in \mathbb{F}_q$, $x^{q-1} - 1 = 0$

Output: $(\langle \mathrm{coeffs}(g), \mathrm{eval}(h) \rangle)^{q-1} - 1$.

Algebraic NOT - Finite Fields

Given: Vector $\text{coeffs}(g_n) \in \mathbb{F}_q^N$, point $h \in \mathbb{F}_q^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: For all $x \in \mathbb{F}_q$, $x^q - x = 0$

$\Rightarrow$ For all $0 \neq x \in \mathbb{F}_q$, $x^{q-1} - 1 = 0$

Output: $(\langle \text{coeffs}(g), \text{eval}(h) \rangle)^{q-1} - 1$.

$$P(\text{coeffs}(g)) \approx \prod_{h \in \mathcal{H}} \left((\langle \text{coeffs}(g), \text{eval}(h) \rangle)^{q-1} - 1 \right)$$

$\text{Degree}(P) \leq |\mathcal{H}| q \leq \text{poly}(N)$, $\text{Size}(P) \leq \text{poly}(N)$.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree$(q) \approx$ domain$(q) \approx$ range$(g_n(h))$.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree$(q) \approx$ domain$(q) \approx$ range$(g_n(h))$.

Need to restrict range$(g_n(h))$.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree$(q) \approx$ domain$(q) \approx$ range$(g_n(h))$.

Need to restrict range$(g_n(h))$.

Rough Estimate:

Suppose $|\text{coeffs}(g)| \leq L$, $deg(g_n) = \text{poly}(n)$, and $|h| \leq k$.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree$(q) \approx$ domain$(q) \approx$ range$(g_n(h))$.

Need to restrict range$(g_n(h))$.

Rough Estimate:

Suppose $|\text{coeffs}(g)| \leq L$, $deg(g_n) = \text{poly}(n)$, and $|h| \leq k$.

Then $|\text{eval}(h)| \leq k^d$, $|g_n(h)| \approx L \cdot N \cdot k^d$

Algebraic NOT - Integers

Given: Vector coeffs(g_n) $\in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree(q) $\approx$ domain(q) $\approx$ range($g_n(h)$).

Need to restrict range($g_n(h)$).

Rough Estimate:

Suppose $|\,\text{coeffs}(g)| \leq L$, $deg(g_n) = \text{poly}(n)$, and $|h| \leq k$.

Then $|\,\text{eval}(h)| \leq k^d$, $|g_n(h)| \approx L \cdot N \cdot k^d$

For $d \sim n^3$, $N \sim \exp(n \log d)$ and $LNk^d = N^{\omega(1)}$.

Algebraic NOT - Integers

Given: Vector coeffs$(g_n) \in \mathbb{C}^N$, point $h \in \mathbb{C}^n$

Goal: Output zero iff $g_n(h) \neq 0$, using a polynomial.

Fact: Univariate $q(x)$ of degree d has $\leq d$ roots.

$\Rightarrow$ degree$(q) \approx$ domain$(q) \approx$ range$(g_n(h))$.

Need to restrict range$(g_n(h))$.

Rough Estimate:

Suppose $|\text{coeffs}(g)| \leq L$, $deg(g_n) = \text{poly}(n)$, and $|h| \leq k$.

Then $|\text{eval}(h)| \leq k^d$, $|g_n(h)| \approx L \cdot N \cdot k^d$

For $d \sim n^3$, $N \sim \exp(n \log d)$ and $LNk^d = N^{\omega(1)}$.

Cannot directly work with eval(h).

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Chinese Remainder Theorem
For an integer $-2^\ell \leq M \leq 2^\ell$,
if $M \bmod p_i = 0$ for *distinct* primes $p_1, \ldots, p_{2\ell}$; then $M = 0$.

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Chinese Remainder Theorem
For an integer $-2^\ell \leq M \leq 2^\ell$,
if $M \bmod p_i = 0$ for *distinct* primes $p_1, \ldots, p_{2\ell}$; then $M = 0$.

For large enough $\ell = \text{poly}(d, \log N)$ and primes $p_1, \ldots, p_\ell$,
let $\text{eval}_i(h) = \text{eval}(h) \bmod p_i$

$$= [m_1(h) \bmod p_i, \ldots, m_r(h) \bmod p_i] \in \mathbb{C}^N$$

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Chinese Remainder Theorem
For an integer $-2^\ell \leq M \leq 2^\ell$,
if M mod $p_i = 0$ for *distinct* primes $p_1, \ldots, p_{2\ell}$; then $M = 0$.

For large enough $\ell = \text{poly}(d, \log N)$ and primes $p_1, \ldots, p_\ell$,
let $\text{eval}_i(h) = \text{eval}(h) \bmod p_i$
$= [m_1(h) \bmod p_i, \ldots, m_r(h) \bmod p_i] \in \mathbb{C}^N$
$|\text{eval}_i(h)| = \text{poly}(\ell) = \text{poly}(d, \log N)$.

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Chinese Remainder Theorem
For an integer $-2^\ell \leq M \leq 2^\ell$,
if $M \bmod p_i = 0$ for *distinct* primes $p_1, \ldots, p_{2\ell}$; then $M = 0$.

For large enough $\ell = \mathrm{poly}(d, \log N)$ and primes $p_1, \ldots, p_\ell$,
let $\mathrm{eval}_i(h) = \mathrm{eval}(h) \bmod p_i$
$= [m_1(h) \bmod p_i, \ldots, m_r(h) \bmod p_i] \in \mathbb{C}^N$
$|\,\mathrm{eval}_i(h)| = \mathrm{poly}(\ell) = \mathrm{poly}(d, \log N)$.

For $|\,\mathrm{coeffs}(g)| \leq L$, $\;|\langle \mathrm{coeffs}(g), \mathrm{eval}_i(h)\rangle| \leq \mathrm{poly}(N, L, d)$.

Algebraic NOT - Integers

Goal: Check if $g_n(h) = 0$ using a small range.

Chinese Remainder Theorem

For an integer $-2^\ell \leq M \leq 2^\ell$,
if M mod $p_i = 0$ for *distinct* primes $p_1, \ldots, p_{2\ell}$; then $M = 0$.

For large enough $\ell = \mathrm{poly}(d, \log N)$ and primes $p_1, \ldots, p_\ell$,
let $\mathrm{eval}_i(h) = \mathrm{eval}(h) \bmod p_i$
$= [m_1(h) \bmod p_i, \ldots, m_r(h) \bmod p_i] \in \mathbb{C}^N$
$|\mathrm{eval}_i(h)| = \mathrm{poly}(\ell) = \mathrm{poly}(d, \log N)$.

For $|\mathrm{coeffs}(g)| \leq L$, $|\langle \mathrm{coeffs}(g), \mathrm{eval}_i(h) \rangle| \leq \mathrm{poly}(N, L, d)$.

$$[g_n(h) = 0] \equiv \bigwedge_{i \in [\ell]} [\langle \mathrm{coeffs}(g), \mathrm{eval}_i(h) \rangle =_{p_i} 0]$$

Note: Can "hardwire" $\mathrm{eval}_i(h)$ for all $i \in [\ell]$ and $h \in \mathcal{H}$.

Algebraic NOT - Integers

$$[x =_{p_i} 0] \approx \prod_{\substack{-M \leq a \leq M \\ p_i \nmid a}} (x - a)$$

For $M = \text{poly}(L, N, d) = \text{poly}(N)$.

Algebraic NOT - Integers

$$[x =_{p_i} 0] \approx \prod_{\substack{-M \le a \le M \\ p_i \nmid a}} (x - a)$$

For $M = \mathrm{poly}(L, N, d) = \mathrm{poly}(N)$.

Defining Equation for $\mathrm{VP}_{\mathbb{C}}$

$$P(\mathrm{coeffs}(g)) \approx \prod_{h \in \mathcal{H}} \prod_{i \in [\ell]} \prod_{\substack{-M \le a \le M \\ p_i \nmid a}} (\langle \mathrm{coeffs}(g), \mathrm{eval}_i(h) \rangle - a)$$

$\mathrm{Deg}(P) \le |\mathcal{H}|\, \mathrm{poly}(n)\, \mathrm{poly}(N) \le \mathrm{poly}(N)$

$\mathrm{Size}(P) \le \mathrm{poly}(N)$.

Results for VP

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}'_{\mathbb{C}}$)

For n,d and $N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that

for all $f \in \mathrm{VP}_{\mathbb{C}}(n, d)$ with coefficients in $\{-N, \ldots, N\}$,

$P(\mathrm{coeffs}(f)) = 0$.

Theorem [CKRST20] (Defining Equations for $\mathrm{VP}_{\mathbb{F}}$)

For any fixed finite field $\mathbb{F}$, and n,d,$N = \binom{n+d}{n}$,

There exists a nonzero $P(Z_1, \ldots, Z_N) \in \mathrm{VP}_{\mathbb{F}}(N)$ such that

for all $f \in \mathrm{VP}_{\mathbb{F}}(n, d)$, $P(\mathrm{coeffs}(f)) = 0$.

Results for VNP

Theorem [CKRST20] (Defining Equations for $\mathrm{VNP}'_{\mathbb{C}}$)
For n,d and $N = \binom{n+d}{n}$,
There exists a nonzero $Q(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ such that
for all $f \in \mathrm{VNP}_{\mathbb{C}}(n, d)$ with coefficients in $\{-N, \ldots, N\}$,
$Q(\mathrm{coeffs}(f)) = 0$.

Theorem [CKRST20] (Defining Equations for $\mathrm{VNP}_{\mathbb{F}}$)
For any fixed finite field $\mathbb{F}$, and n,d,$N = \binom{n+d}{n}$,
There exists a nonzero $Q(Z_1, \ldots, Z_N) \in \mathrm{VP}_{\mathbb{F}}(N)$ such that
for all $f \in \mathrm{VNP}_{\mathbb{F}}(n, d)$, $Q(\mathrm{coeffs}(f)) = 0$.

Summary

- Existence of small hitting sets gives efficient defining equations in interesting restricted settings.

Summary

- Existence of small hitting sets gives efficient defining equations in interesting restricted settings.

- Efficient defining exist for polynomials with "small" coefficients, in both VP and VNP.

Summary

- Existence of small hitting sets gives efficient defining equations in interesting restricted settings.
- Efficient defining exist for polynomials with "small" coefficients, in both VP and VNP.
- Existence of defining equations cannot separate VP and VNP.

  The hitting sets and the defining equations are different.

About the Results

- The restriction is only on the polynomials, circuits can use any constants.

  Well-studied natural polynomials have small coefficients.

  e.g. Determinant, Permanent, Clique polynomial, . . .

About the Results

- The restriction is only on the polynomials, circuits can use any constants.

  Well-studied natural polynomials have small coefficients.

  e.g. Determinant, Permanent, Clique polynomial, ...

- Defining equations are not large in the usual sense.

  Finding “non-roots” of equations is usually not hard.

About the Results

- The restriction is only on the polynomials, circuits can use any constants.

  Well-studied natural polynomials have small coefficients.

  e.g. Determinant, Permanent, Clique polynomial, ...

- Defining equations are not large in the usual sense.

  Finding "non-roots" of equations is usually not hard.

- Non-explicitness of defining equations comes from the non-explicitness of the hitting sets used.

Questions

- Does all of VP (or VNP) have efficient defining equations?
  - Unlikely that our proof extends. Do the results imply something stronger?
  - Constant free VP and VNP.

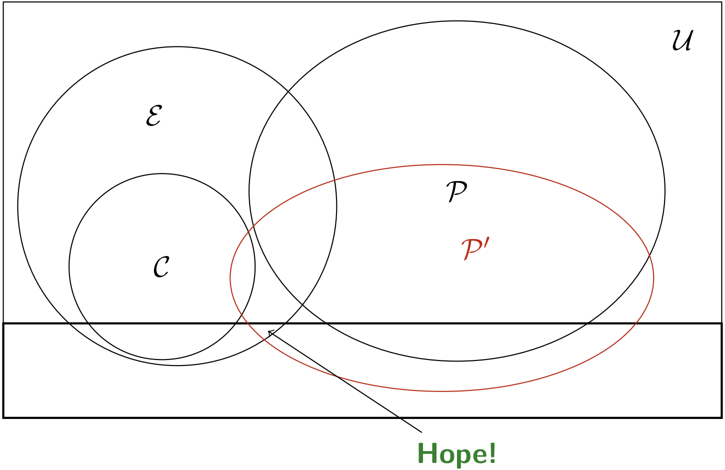
Questions

- Does all of VP (or VNP) have efficient defining equations?
  - Unlikely that our proof extends. Do the results imply something stronger?
  - Constant free VP and VNP.

- Are there small explicit hitting sets for small circuits?
  - *Bootstrapping*: Constructions from low variate hitting sets and hardness [AGS18,KST19,GKSS19,And20].

Questions

- Does all of VP (or VNP) have efficient defining equations?
  - Unlikely that our proof extends. Do the results imply something stronger?
  - Constant free VP and VNP.
- Are there small explicit hitting sets for small circuits?
  - *Bootstrapping*: Constructions from low variate hitting sets and hardness [AGS18,KST19,GKSS19,And20].
- Defining equations for other models not covered by [FSV18]?
  - Our proof technique will need small coefficients.



Thank You