Is there an Algebraic Natural Proofs Barrier?

Anamay Tengse

Prerona Chatterjee, Mrinal Kumar, C. Ramya, Ramprasad Saptharishi

STCS Symposium

March 2021

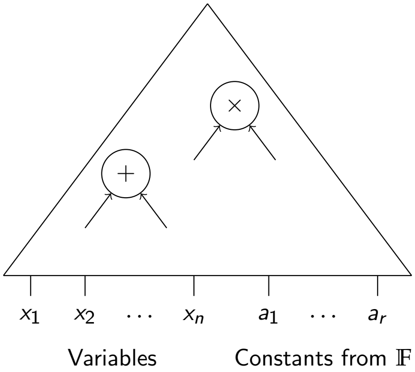
Computing Polynomials

Computing Polynomials

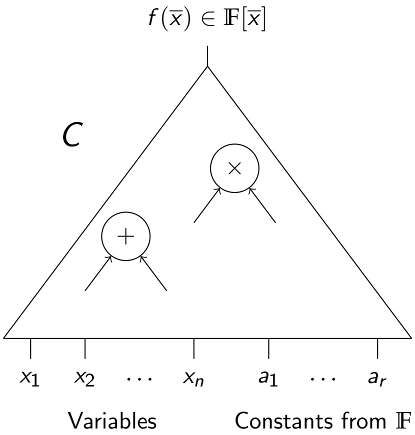
$x_1 \quad x_2 \quad \cdots \quad x_n \qquad a_1 \quad \cdots \quad a_r$

Variables — Constants from $\mathbb{F}$

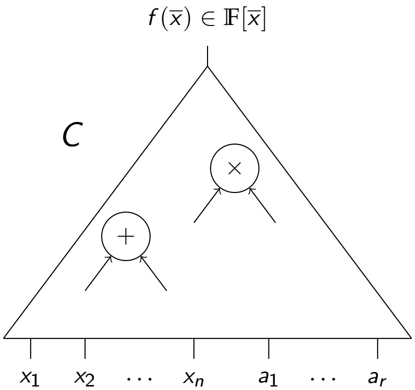
Computing Polynomials



Computing Polynomials

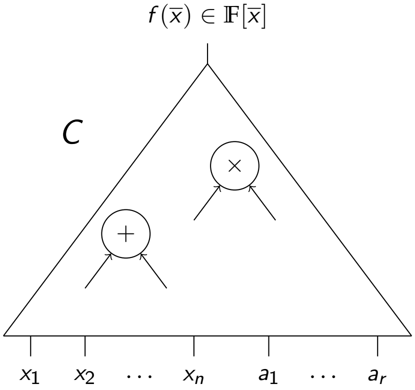


Computing Polynomials



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

Computing Polynomials

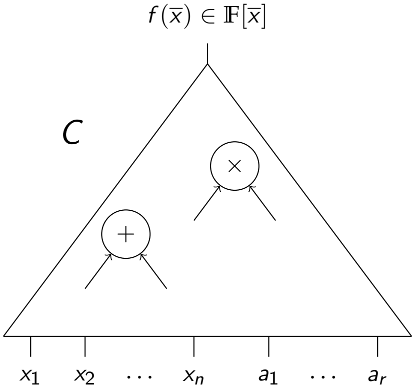


Algebraic Circuit for $f(\overline{x})$

Size(C): Number of *gates*

- Operations used by C

Computing Polynomials



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

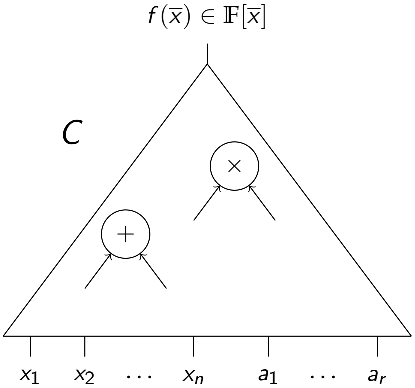
Size(C): Number of *gates*

- Operations used by C

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

- Min operations to compute f

Computing Polynomials



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

Size(C): Number of *gates*

- Operations used by C

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

- Min operations to compute f

For this talk.

Variables: n, Degree: d,

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

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\text{size}(f_n) = \text{poly}(n)$.

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\mathrm{size}(f_n) = \mathrm{poly}(n)$.
  - e.g.,

$$\mathrm{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in s_n} \mathrm{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\mathrm{size}(f_n) = \mathrm{poly}(n)$.
  - e.g.,
$$\mathrm{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in s_n} \mathrm{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$
  - *Random polynomial* is hard (outside VP), but not “explicit”.

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\text{size}(f_n) = \text{poly}(n)$.
  - e.g.,

$$\text{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

  - *Random polynomial* is hard (outside VP), but not "explicit".
- VNP (efficiently definable polynomials):

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\text{size}(f_n) = \text{poly}(n)$.
  - e.g.,

$$\text{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in s_n} \text{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

  - *Random polynomial* is hard (outside VP), but not "explicit".
- VNP (efficiently definable polynomials):
  - **Criterion.** $\{f_n\}$ s.t. $\text{coeff}_{f_n}(m)$ is computable in time $\text{poly}(n)$ for any m.

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\text{size}(f_n) = \text{poly}(n)$.
  - e.g.,

$$\text{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

  - *Random polynomial* is hard (outside VP), but not "explicit".
- VNP (efficiently definable polynomials):
  - **Criterion.** $\{f_n\}$ s.t. $\text{coeff}_{f_n}(m)$ is computable in time $\text{poly}(n)$ for any m.
  - e.g.,

$$\text{Perm}_n(\{x_{i,j}\}) = \sum_{\sigma \in S_n} x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

Algebraic P vs NP [Val79]

- VP (efficiently computable polynomials):
  - **Definition.** $\{f_n\}$ with $\mathrm{size}(f_n) = \mathrm{poly}(n)$.
  - e.g.,

$$\mathrm{Det}_n(\{x_{i,j}\}) = \sum_{\sigma \in s_n} \mathrm{sgn}(\sigma) x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

  - *Random polynomial* is hard (outside VP), but not "explicit".
- VNP (efficiently definable polynomials):
  - **Criterion.** $\{f_n\}$ s.t. $\mathrm{coeff}_{f_n}(m)$ is computable in time $\mathrm{poly}(n)$ for any m.
  - e.g.,

$$\mathrm{Perm}_n(\{x_{i,j}\}) = \sum_{\sigma \in s_n} x_{1,\sigma(1)} x_{2,\sigma(2)} \cdots x_{n,\sigma(n)}$$

Question. Is VP $=$ VNP?

Some known hardness results

- Hardness Results for Structured Models:
  - Homogeneous constant depth formulas (exponential hardness) [NW95,GKKS13,KS14,...]
  - Multilinear formulas (quasipolynomial hardness) [Raz09,DMPY12,...]
  - Non-commutative formulas (exponential hardness) [Nis91,LMP16,...]
  - Monotone circuits (exponential hardness) [Yeh19,Sri19]

Some known hardness results

- Hardness Results for Structured Models:
  - Homogeneous constant depth formulas (exponential hardness) [NW95,GKKS13,KS14,...]
  - Multilinear formulas (quasipolynomial hardness) [Raz09,DMPY12,...]
  - Non-commutative formulas (exponential hardness) [Nis91,LMP16,...]
  - Monotone circuits (exponential hardness) [Yeh19,Sri19]

Formulas: Circuits where the underlying DAG is a tree.

Some known hardness results

- Hardness Results for Structured Models:
  - Homogeneous constant depth formulas (exponential hardness) [NW95,GKKS13,KS14,...]
  - Multilinear formulas (quasipolynomial hardness) [Raz09,DMPY12,...]
  - Non-commutative formulas (exponential hardness) [Nis91,LMP16,...]
  - Monotone circuits (exponential hardness) [Yeh19,Sri19]

  Formulas: Circuits where the underlying DAG is a tree.

- Best Hardness Result for Circuits: $\Theta(n \log d)$ [BS83,Smo97]
- Best Hardness Result for Formulas: $\Theta(n^2)$ [Kal85,CKSV20]

Some known hardness results

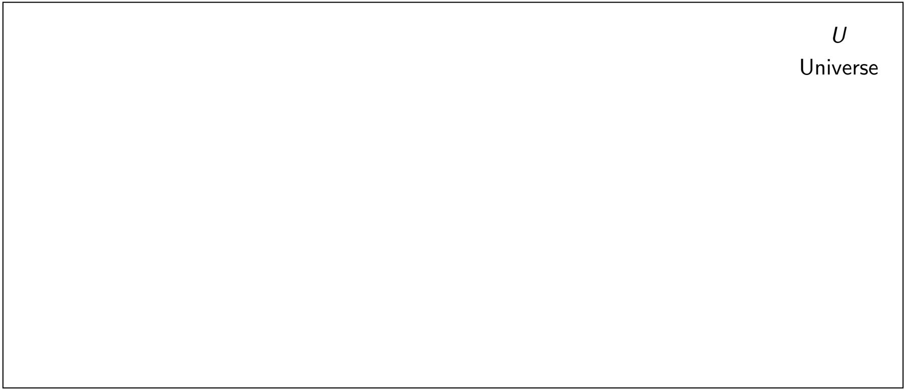
- Hardness Results for Structured Models:
  - Homogeneous constant depth formulas (exponential hardness) [NW95,GKKS13,KS14,...]
  - Multilinear formulas (quasipolynomial hardness) [Raz09,DMPY12,...]
  - Non-commutative formulas (exponential hardness) [Nis91,LMP16,...]
  - Monotone circuits (exponential hardness) [Yeh19,Sri19]

  Formulas: Circuits where the underlying DAG is a tree.

- Best Hardness Result for Circuits: $\Theta(n \log d)$ [BS83,Smo97]
- Best Hardness Result for Formulas: $\Theta(n^2)$ [Kal85,CKSV20]

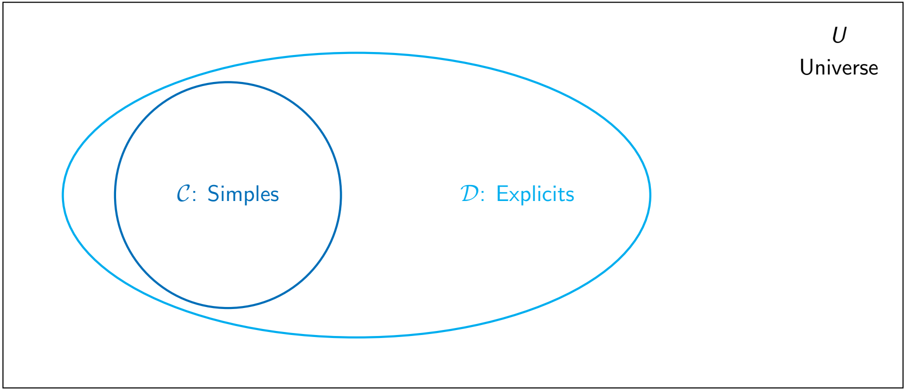
Question. Are the *"natural techniques"* insufficient?

What are "natural techniques"?



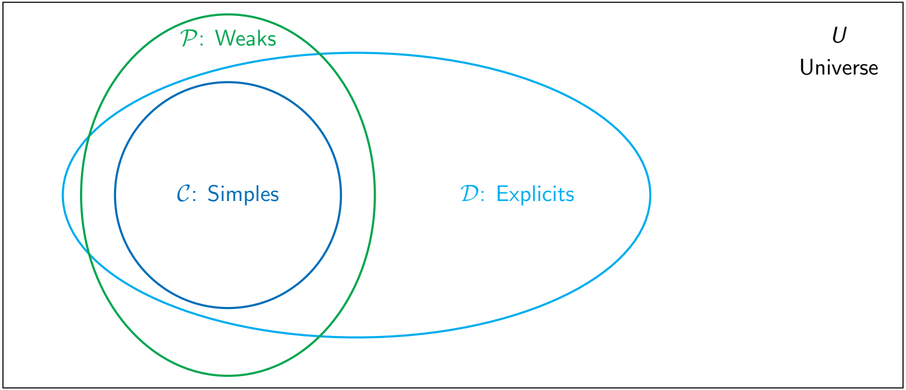
What are “natural techniques”?

What are "natural techniques"?



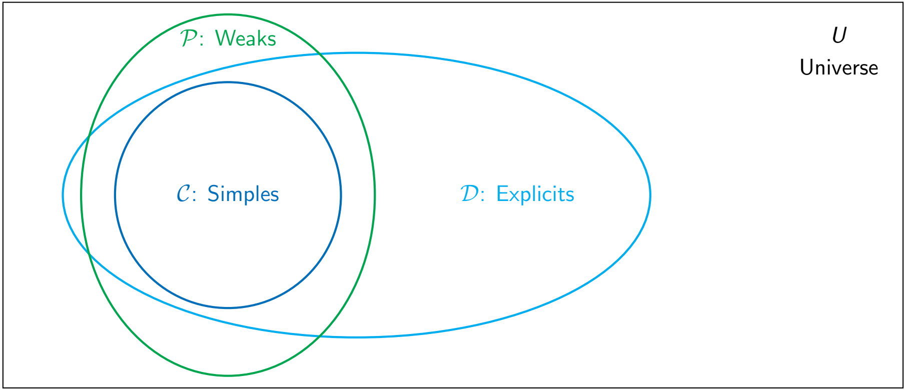
Simples: Non-membership is difficult.

What are "natural techniques"?



Simples: Non-membership is difficult. Weaks: Non-membership is easy.

What are “natural techniques”?



Simples: Non-membership is difficult. Weaks: Non-membership is easy.

Easy weakness $\Rightarrow$ Something explicit should be non-weak.

Natural techniques in action

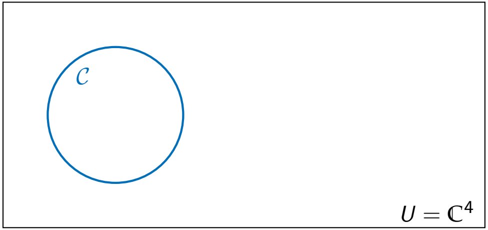
Warm-up

$U = \mathbb{C}^4$

- U - univariates of deg ≤ 3 over $\mathbb{C}$.

Natural techniques in action

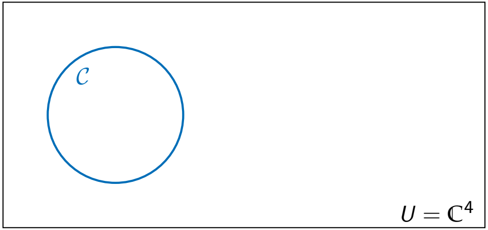
Warm-up



- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.

Natural techniques in action

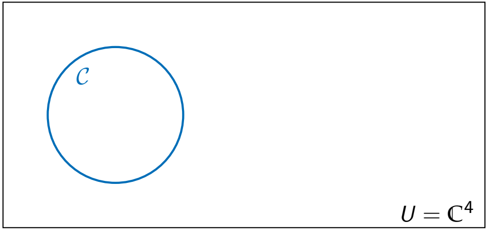
Warm-up



- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.

Natural techniques in action

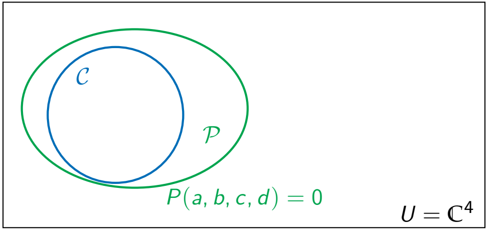
Warm-up



- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a, b, c, d) \in \mathcal{C}$,
  then $P(a, b, c, d) = 9ad - bc = 0$.

Natural techniques in action

Warm-up

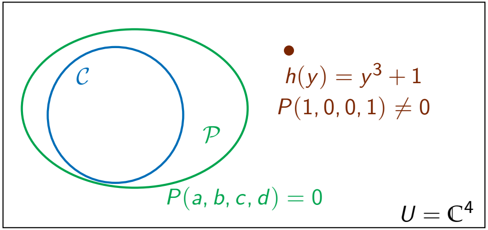


- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a, b, c, d) \in \mathcal{C}$,

  then $P(a, b, c, d) = 9ad - bc = 0$.

Natural techniques in action

Warm-up

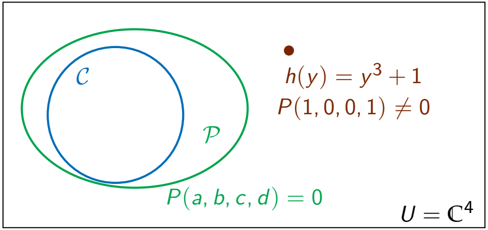


- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,

  then $P(a,b,c,d) = 9ad - bc = 0$.

Natural techniques in action

Warm-up



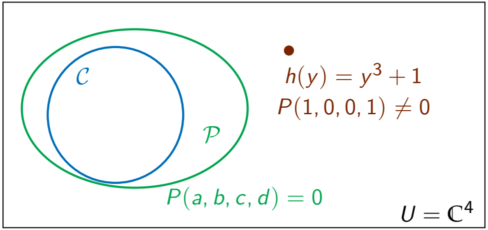
- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,
  then $P(a,b,c,d) = 9ad - bc = 0$.

Algebraic Natural Proofs

[FSV18,GKSS17]

Natural techniques in action

Warm-up

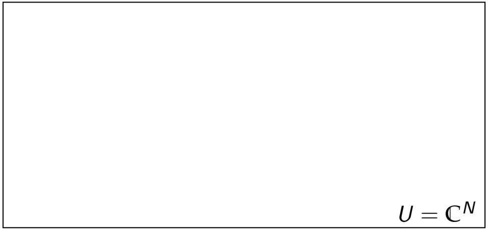


- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \left\{ (\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C} \right\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,

  then $P(a,b,c,d) = 9ad - bc = 0$.

Algebraic Natural Proofs

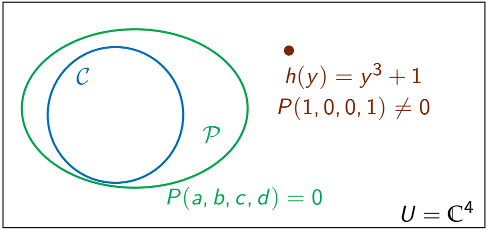
[FSV18,GKSS17]



- U - n-variates of deg $\leq d$, $N = \binom{n+d}{d}$.

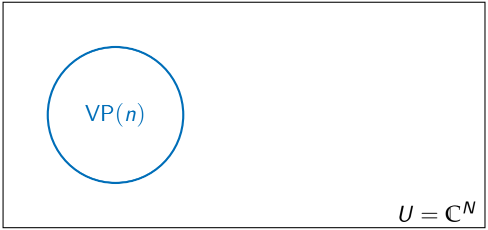
Natural techniques in action

Warm-up



- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,
  then $P(a,b,c,d) = 9ad - bc = 0$.

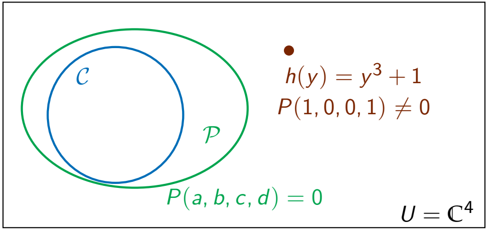
Algebraic Natural Proofs
[FSV18,GKSS17]



- U - n-variates of deg $\leq d$, $N = \binom{n+d}{d}$.
- $\mathcal{C} = \mathrm{VP}(n)$.

Natural techniques in action

Warm-up

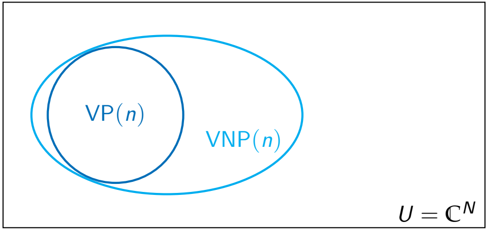


- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,

  then $P(a,b,c,d) = 9ad - bc = 0$.

Algebraic Natural Proofs

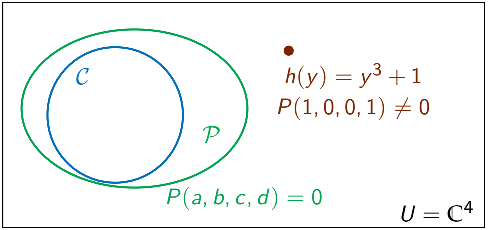
[FSV18,GKSS17]



- U - n-variates of deg $\leq d$, $N = \binom{n+d}{d}$.
- $\mathcal{C} = \mathrm{VP}(n)$.
- $\mathcal{D} = \mathrm{VNP}(n)$.

Natural techniques in action

Warm-up

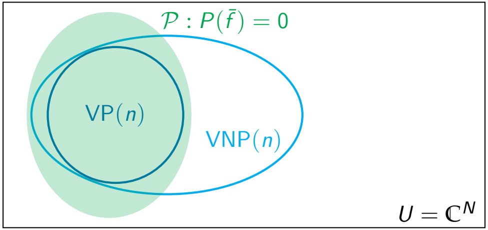


- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$,

  then $P(a,b,c,d) = 9ad - bc = 0$.

Algebraic Natural Proofs

[FSV18,GKSS17]

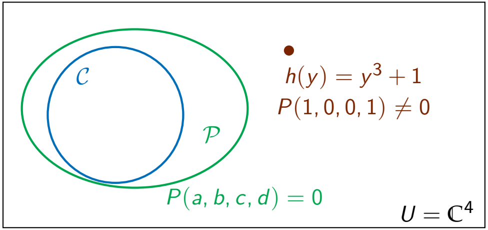


- U - n-variates of deg $\leq d$, $N = \binom{n+d}{d}$.
- $\mathcal{C} = \mathrm{VP}(n)$.
- $\mathcal{D} = \mathrm{VNP}(n)$.
- **Is there a "simple"** $P(Z_1, \ldots, Z_N)$ **s.t.**

  $P(\bar{f}) = 0$ **for all** $f \in \mathrm{VP}(n)$**?**

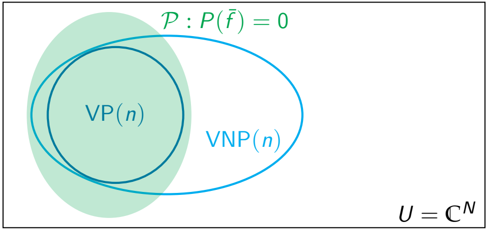
Natural techniques in action

Warm-up



- U - univariates of deg ≤ 3 over $\mathbb{C}$.
- $\mathcal{C} = \{(\alpha y + \beta)^3 : \alpha, \beta \in \mathbb{C}\}$.
- $(\alpha y + \beta)^3 = \alpha^3 y^3 + 3\alpha^2\beta y^2 + 3\alpha\beta^2 y + \beta^3$.
- If $q(y) \equiv (a,b,c,d) \in \mathcal{C}$, then $P(a,b,c,d) = 9ad - bc = 0$.

Algebraic Natural Proofs [FSV18,GKSS17]



- U - n-variates of deg $\leq d$, $N = \binom{n+d}{d}$.
- $\mathcal{C} = \mathrm{VP}(n)$.
- $\mathcal{D} = \mathrm{VNP}(n)$.
- **Is there a $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ s.t. $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$?**

Algebraic Natural Proofs [FSV18,GKSS17]

Definition (Natural Proof for $\mathcal{C}$)

For $n, d \in \mathbb{N}$, $N = \binom{n+d}{d}$, and $\mathcal{C}(n, d) \subseteq \mathbb{C}^N$,

Algebraic Natural Proofs [FSV18,GKSS17]

Definition (Natural Proof for $\mathcal{C}$)

For $n, d \in \mathbb{N}$, $N = \binom{n+d}{d}$, and $\mathcal{C}(n, d) \subseteq \mathbb{C}^N$,
a *nonzero* $P(Z_1, \ldots, Z_N)$ is a VP-natural proof for $\mathcal{C}(n, d)$, if:

- $P(\bar{f}) = 0$ for all $f \in \mathcal{C}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$.

Algebraic Natural Proofs [FSV18,GKSS17]

Definition (Natural Proof for $\mathcal{C}$)

For $n, d \in \mathbb{N}$, $N = \binom{n+d}{d}$, and $\mathcal{C}(n,d) \subseteq \mathbb{C}^N$,
a *nonzero* $P(Z_1, \ldots, Z_N)$ is a VP-natural proof for $\mathcal{C}(n,d)$, if:

- $P(\bar{f}) = 0$ for all $f \in \mathcal{C}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$.

Best Case Scenario: There exists a $P \in \mathrm{VP}(N)$ vanishing on $\mathrm{VP}(n)$, but not on $\mathrm{VNP}(n)$.

Algebraic Natural Proofs [FSV18,GKSS17]

Definition (Natural Proof for $\mathcal{C}$)

For $n, d \in \mathbb{N}$, $N = \binom{n+d}{d}$, and $\mathcal{C}(n,d) \subseteq \mathbb{C}^N$,
a *nonzero* $P(Z_1, \ldots, Z_N)$ is a VP-natural proof for $\mathcal{C}(n,d)$, if:

- $P(\bar{f}) = 0$ for all $f \in \mathcal{C}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$.

Best Case Scenario: There exists a $P \in \mathrm{VP}(N)$ vanishing on $\mathrm{VP}(n)$, but not on $\mathrm{VNP}(n)$.

Barrier: No $P \in \mathrm{VP}(N)$ witnesses the separation of $\mathrm{VP}(n)$ and $\mathrm{VNP}(n)$.

$\equiv$ "Natural techniques" cannot prove $\mathrm{VP} \neq \mathrm{VNP}$.

Algebraic natural proofs barrier?

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P / poly.

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P / poly.
  - Existence of OWFs is widely believed and heavily used in modern cryptography.

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P / poly.
  - Existence of OWFs is widely believed and heavily used in modern cryptography.
- Algebraic natural proofs [FSV18,GKSS17]:
  - If $\mathrm{VP}(n)$ has $\mathrm{poly}\log(n)$-*succinct hitting sets*, then no natural proofs for VP.

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P / poly.
  - Existence of OWFs is widely believed and heavily used in modern cryptography.
- Algebraic natural proofs [FSV18,GKSS17]:
  - If $\mathrm{VP}(n)$ has $\mathrm{poly}\log(n)$-*succinct hitting sets*, then no natural proofs for VP.
  - Succinct hitting sets are not well-studied.

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P/ poly.
  - Existence of OWFs is widely believed and heavily used in modern cryptography.
- Algebraic natural proofs [FSV18,GKSS17]:
  - If $\mathrm{VP}(n)$ has $\mathrm{poly}\log(n)$-*succinct hitting sets*, then no natural proofs for VP.
  - Succinct hitting sets are not well-studied.
- Explicit succinct hitting sets [FSV18]:
  - $\Sigma\Pi\Sigma(\mathrm{poly}\log(n))$-succinct hitting sets against weak classes (depth-3-powering,...).

Algebraic natural proofs barrier?

- (Boolean) natural proofs [RR97]:
  - If One-Way-Functions (OWFs) exist, then no natural proofs for P / poly.
  - Existence of OWFs is widely believed and heavily used in modern cryptography.

- Algebraic natural proofs [FSV18,GKSS17]:
  - If $\mathrm{VP}(n)$ has $\mathrm{poly}\log(n)$-*succinct hitting sets*, then no natural proofs for VP.
  - Succinct hitting sets are not well-studied.

- Explicit succinct hitting sets [FSV18]:
  - $\Sigma\Pi\Sigma(\mathrm{poly}\log(n))$-succinct hitting sets against weak classes (depth-3-powering,...).
  - Weak evidence for $\mathrm{VP}(n)$ having $\mathrm{poly}\log(n)$-succinct hitting sets.

Our results

Dream. There is a $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$,
- $P(\bar{h}) \neq 0$ for some $h \in \mathrm{VNP}(n)$.

Our results

Dream. There is a $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$,
- $P(\bar{h}) \neq 0$ for some $h \in \mathrm{VNP}(n)$.

Our Results.

- [Chatterjee-Kumar-Ramya-Saptharishi-T 2020]:
  Let VP' be the polynomials in VP that additionally have $\{-1, 0, 1\}$ coefficients.
  There exists $P(Z_1, \ldots, Z_N)$ such that $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}'(n)$.

Our results

Dream. There is a $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$,
- $P(\bar{h}) \neq 0$ for some $h \in \mathrm{VNP}(n)$.

Our Results.

- [Chatterjee-Kumar-Ramya-Saptharishi-T 2020]:
  Let VP′ be the polynomials in VP that additionally have $\{-1, 0, 1\}$ coefficients.
  There exists $P(Z_1, \ldots, Z_N)$ such that $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}'(n)$.

- [Kumar-Ramya-Saptharishi-T 2020]:
  Suppose the Permanent is 2^{n^ϵ}-hard for constant $\epsilon > 0$.
  Then, if $Q(Z_1, \ldots, Z_N)$ is such that $Q(\bar{h}) = 0$ for all $h \in \mathrm{VNP}'(n)$,
  then $Q(Z_1, \ldots, Z_N)$ is $N^{\omega(1)}$-hard.

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathsf{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathsf{VP}(N)$,

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathsf{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathsf{VP}(N)$,
- $P(\bar{h}) \neq 0$ for many h with $\{-1, 0, 1\}$-coefficients.

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$,
- $P(\bar{h}) \neq 0$ for many h with $\{-1, 0, 1\}$-coefficients.

- Almost all well-studied polynomials (Det_n, Perm_n, $\ldots$) have $\{-1, 0, 1\}$ coefficients.

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$,
- $P(\bar{h}) \neq 0$ for many h with $\{-1, 0, 1\}$-coefficients.

- Almost all well-studied polynomials (Det_n, Perm_n, ...) have $\{-1, 0, 1\}$ coefficients.

- **Note.** Such an equation could possibly prove $\mathrm{Perm}_n \notin \mathrm{VP}(n)$.

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$,
- $P(\bar{h}) \neq 0$ for many h with $\{-1, 0, 1\}$-coefficients.

- Almost all well-studied polynomials (Det_n, Perm_n, $\ldots$) have $\{-1, 0, 1\}$ coefficients.

- **Note.** Such an equation could possibly prove $\mathrm{Perm}_n \notin \mathrm{VP}(n)$.

* Similar result also holds for VNP'.

Proofs for "interesting" polynomials

Theorem [CKRST'20]

For all large n, d and $N = \binom{n+d}{d}$, there exists a $P(Z_1, \ldots, Z_N)$ s.t.

- $P(\bar{f}) = 0$ for all $f \in \mathrm{VP}(n)$ with coefficients in $\{-1, 0, 1\}$,
- $P(Z_1, \ldots, Z_N) \in \mathrm{VP}(N)$,
- $P(\bar{h}) \neq 0$ for many h with $\{-1, 0, 1\}$-coefficients.

- Almost all well-studied polynomials (Det_n, Perm_n, $\ldots$) have $\{-1, 0, 1\}$ coefficients.

- **Note.** Such an equation could possibly prove $\mathrm{Perm}_n \notin \mathrm{VP}(n)$.

* Similar result also holds for VNP'.

Idea. Hitting sets for $\mathcal{C}$ give natural proofs for $\mathcal{C}'$.

Algebraic natural proofs for VNP

Theorem [KRST'20]

Suppose Perm_m is $2^{m^{\epsilon}}$-hard for a constant $\epsilon > 0$.

Then for some $n, d = \mathrm{poly}(m)$, and $N = \binom{n+d}{d}$,

Algebraic natural proofs for VNP

Theorem [KRST'20]

Suppose Perm_m is 2^{m^ϵ}-hard for a constant $\epsilon > 0$.
Then for some $n, d = \mathrm{poly}(m)$, and $N = \binom{n+d}{d}$,
if $Q(Z_1, \ldots, Z_N)$ is such that $Q(\bar{h}) = 0$ for all $h \in \mathrm{VNP}(n)$,
then $\mathrm{size}(Q) = N^{\omega(1)}$.

Algebraic natural proofs for VNP

Theorem [KRST'20]

Suppose Perm_m is 2^{m^ϵ}-hard for a constant $\epsilon > 0$.
Then for some $n, d = \mathrm{poly}(m)$, and $N = \binom{n+d}{d}$,
if $Q(Z_1, \ldots, Z_N)$ is such that $Q(\bar{h}) = 0$ for all $h \in \mathrm{VNP}(n)$,
then $\mathrm{size}(Q) = N^{\omega(1)}$.

Message. Essentially no natural proofs for VNP!

Algebraic natural proofs for VNP

Theorem [KRST'20]

Suppose Perm_m is 2^{m^ϵ}-hard for a constant $\epsilon > 0$.
Then for some $n, d = \mathrm{poly}(m)$, and $N = \binom{n+d}{d}$,
if $Q(Z_1, \ldots, Z_N)$ is such that $Q(\bar{h}) = 0$ for all $h \in \mathrm{VNP}(n)$,
then $\mathrm{size}(Q) = N^{\omega(1)}$.

Message. Essentially no natural proofs for VNP!

* Restriction on coefficients is crucial for existence of easy proofs, for VNP.

Algebraic natural proofs for VNP

Theorem [KRST'20]

Suppose Perm_m is 2^{m^ϵ}-hard for a constant $\epsilon > 0$.
Then for some $n, d = \mathrm{poly}(m)$, and $N = \binom{n+d}{d}$,
if $Q(Z_1, \ldots, Z_N)$ is such that $Q(\bar{h}) = 0$ for all $h \in \mathrm{VNP}(n)$,
then $\mathrm{size}(Q) = N^{\omega(1)}$.

Message. Essentially no natural proofs for VNP!

* Restriction on coefficients is crucial for existence of easy proofs, for VNP.

Idea. The Kabanets-Impagliazzo generator [KI04] can be made VNP-succinct.

What all this means...

In the context of $\mathsf{VP}(N)$-natural proofs for $\mathsf{VP}(n)$:

What all this means...

In the context of $\mathsf{VP}(N)$-natural proofs for $\mathsf{VP}(n)$:

- **Believers.** There is a natural separation between VP and VNP!
  - Any natural proof for $\mathsf{VP}(n)$ separates VP and VNP.
  - Prove existence of natural proofs for VP (using standard assumptions)?

What all this means...

In the context of $\mathsf{VP}(N)$-natural proofs for $\mathsf{VP}(n)$:

- **Believers.** There is a natural separation between VP and VNP!
  - Any natural proof for $\mathsf{VP}(n)$ separates VP and VNP.
  - Prove existence of natural proofs for VP (using standard assumptions)?

- **Skeptics.** Pseudorandomness of VP must come from large coefficients.
  - Our proof [KRST20] seems to require the power of VNP.
  - Prove *non-existence* of natural proofs for VP (using standard assumptions)?

What all this means...

In the context of $\mathrm{VP}(N)$-natural proofs for $\mathrm{VP}(n)$:

- **Believers.** There is a natural separation between VP and VNP!
  - Any natural proof for $\mathrm{VP}(n)$ separates VP and VNP.
  - Prove existence of natural proofs for VP (using standard assumptions)?
- **Skeptics.** Pseudorandomness of VP must come from large coefficients.
  - Our proof [KRST20] seems to require the power of VNP.
  - Prove *non-existence* of natural proofs for VP (using standard assumptions)?
- **Undecided.** The natural proofs question for VP seems quite interesting. :)

Thank You

Webpage: anamay.bitbucket.io

Formal statement of [CKRST'20]

$\exists$ a collection $\mathcal{P}$ of proof families such that,

$\forall$ degree functions $d(n) = \text{poly}(n)$,

the proof family $\left\{P_{N(n)}\right\} = \mathcal{P}(d(n))$ is of $N(n) = \binom{n+d(n)}{n}$ variate polynomials,

and $\forall$ size functions $s(n) = \text{poly}(n)$, $\exists n_0$ such that $\forall n > n_0$,

the polynomial $P_{N(n)}$ vanishes on $\text{Ckt}'(n, d(n), s(n))$.

Formal statement of [KRST'20]

The polynomial Perm_m requires size $> 2^{m^{\epsilon}}$, for infinitely many m.

$\exists$ a collection of families of polynomials $\mathcal{H} \subseteq \mathrm{VNP}(n^c)$, such that

the collection $\mathcal{H}(n)$ is a hitting set for VP_N where $N = \binom{n+n^c}{n}$.

Formal statement of [KRST'20]

The polynomial Perm_m requires size $> 2^{m^\epsilon}$, for infinitely many m.

$\exists$ a collection of families of polynomials $\mathcal{H} \subseteq \mathrm{VNP}(n^c)$, such that

for all degree and size functions $d(N), s(N) = \mathrm{poly}(N)$, there exists an m_0, such that

if for some $m > m_0$, Perm_m requires size $> 2^{m^\epsilon}$,

then for $n(m) = \mathrm{poly}(m), d = n^c$, the collection of polynomials $H_{n(m)} \subseteq \mathrm{VNP}_{n(m)}(n^c)$

is a *hitting set* for the collection $\mathrm{VP}_N(d(N), s(N))$ for $N(n) = \binom{n+n^c}{n}$.