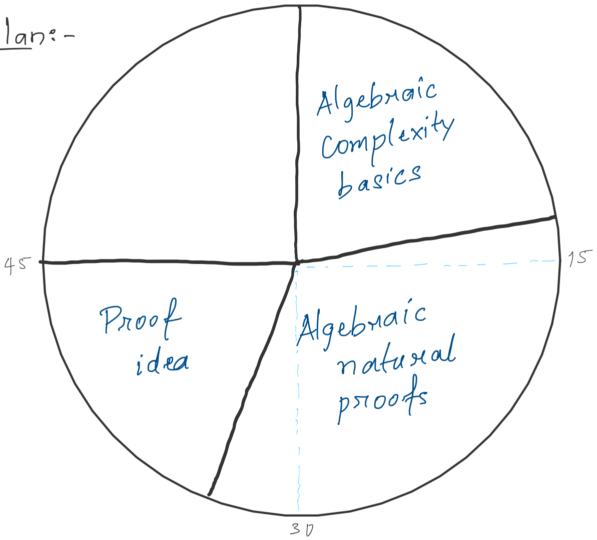
Natural Proofs: Student Talk
Thursday, 31 December 2020 1:28 PM

VNP probably does not have natural proofs

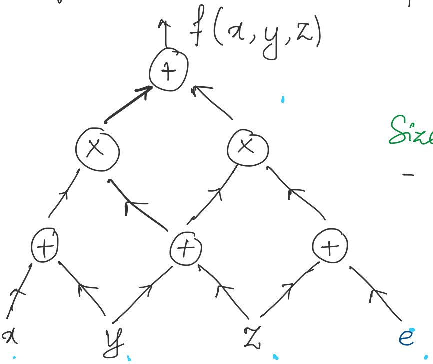
Based on joint works with

Prerona Chatterjee (TIFR, Mumbai)
Mrinal Kumar (IITB, Mumbai)
C. Ramya (TIFR, Mumbai)
Ramprasad Saptharishi (TIFR, Mumbai)

Plan:-



Algebraic Circuit Complexity



Size of the circuit
- no. of gates (+, ×)

- For this talk:
  * $f(\bar{x})$: n-variate, degree $d = \text{poly}(n)$
  * size(f) : size (smallest ckt for f).

VP : Efficiently computable polynomials. [Val '79]

- n-variate $f(\bar{x})$, $\text{size}(f) = \text{poly}(n)$.

E.g. Det_n =

Determinant

$$\begin{vmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{vmatrix}$$

- almost all polynomials are hard.
  (Dimension counting)

- "explicit" hard polynomials?

Intuitive definition:

Explicit : Efficiently "describable" polynomials

- Given a monomial $\underline{x_1^{e_1}}\ \underline{x_2^{e_2} \cdots x_n^{e_n}}$ of degree $\leq d$,

  $\text{coeff}_f(x_1^{e_1} \cdots x_n^{e_n})$ can be computed efficiently.

VNP : Efficiently definable polynomials [Val '79]

- Contains all "explicit" polynomials.
- E.g. the permanent

$$\text{Perm}_n = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}$$

Goal: Find an explicit f outside VP.

VP vs VNP

Det_n vs Perm_n

NC $\leftarrow \text{Det}_n$

$\text{Perm}_n \rightarrow$ #P ~ #SAT

Current status:

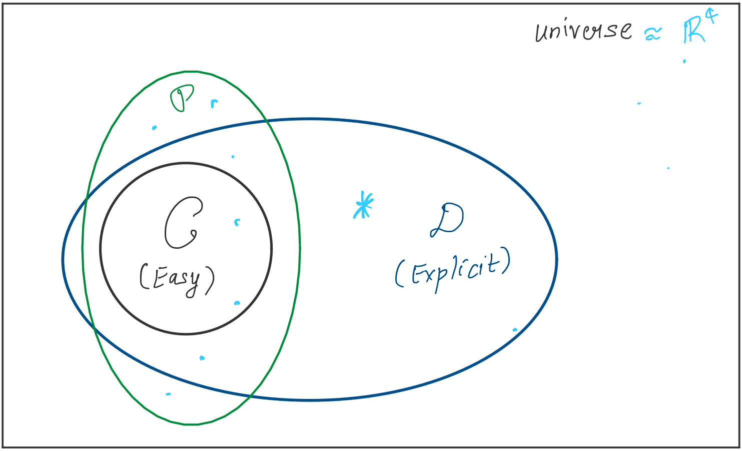
- Best circuit lower bound : $\Omega(n \log n)$ [BS'83]
- Structured models:

- Homogeneous constant depth : $\exp(n^{\varepsilon})$
  [NW95, GKKS13, FLMS14, KS14, ...]
- Multilinear formulas : $n^{\Omega(\log n)}$
  [Raz09, DMPY12, ...]
- Non-commutative models : $\exp(n)$
  [Nis91, LMP16, ...]
- Monotone models : $\exp(n)$
  [Yeh19, Sri19]

⋮

Q. Can "similar" techniques give lower bounds against VP?

* Finding explicit polynomials outside $\mathcal{C}$



* Proving non-membership in $\mathcal{C}$ is hard.

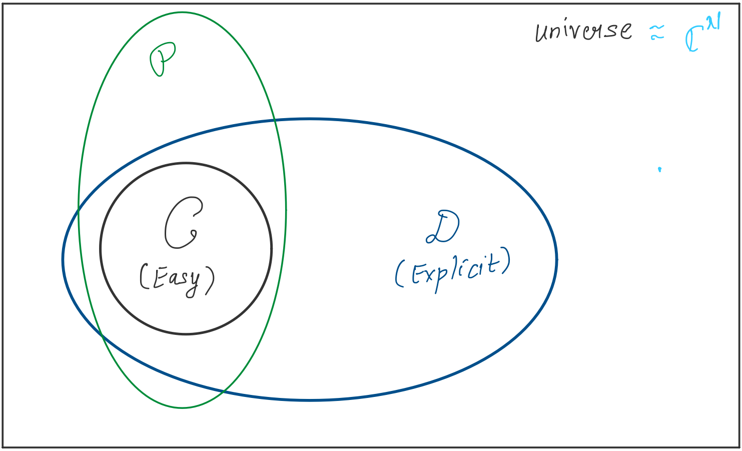
* Membership & non-membership is "easy".

Example:

Universe	$\boxed{\mathcal{C}}$	$\mathcal{D}$
$\{ax^3+bx^2+cx+d : (a,b,c,d) \in \mathbb{R}^4\}$	$\{(\alpha x+\beta)^3 : \alpha,\beta \in \mathbb{R}\}$	Polynomials with "simple" coefficients

$$(\alpha x+\beta)^3 = \overset{a}{\alpha^3}\cdot x^3 + \overset{b}{3\alpha^2\beta}\cdot x^2 + \overset{c}{3\alpha\beta^2}x + \overset{d}{\beta^3}$$

$$\mathcal{P} := \{(a,b,c,d) : \underline{9ad - bc} = 0\}, \quad (1,1,1,1)$$



* "Natural" lower bounds for multivariate polynomials

- Universe: n-var, deg-d polys $\cong \mathbb{C}^N$, $N = \binom{n+d}{d}$
- $\mathcal{C} \subseteq \mathbb{C}^N$, $\mathcal{D} \subseteq \mathbb{C}^N$

Step 1:- Find "weakness" of $\mathcal{C}$.

↪ equation $P_N \neq 0$, $P_N(\overrightarrow{\text{coeff}(f)}) = 0 \ \forall f \in \mathcal{C}$

Step 2:- Find explicit $h \in \mathcal{D}$ that is not weak.

↪ argue this using P_N is "simple".

Equations and algebraic natural proofs

$N = \binom{n+d}{d}$ = # n-variate, degree-d mons.

Defn (Equation for $\mathcal{C}$):

Let $\mathcal{C} \subseteq \mathbb{C}^N$, P_N - non-zero, N-variate

P_N is an equation for $\mathcal{C}$, if

$\forall f \in \mathcal{C}, \ P_N(\overrightarrow{\text{coeff}(f)}) = 0.$

Defn (VP-Natural Proof for $\mathcal{C}$ [FSV'18, GKSS'17])

Let $\mathcal{C} \subseteq \mathbb{C}^N$, P_N - non-zero, N-variate

P_N is a VP-Natural Proof for $\mathcal{C}$, if:

▷ P_N is an equation for $\mathcal{C}$

- ▷ $P_N \in \underline{\underline{VP}}_N$ ..
- ▷ $P_N(\overrightarrow{\text{coeff}}(h)) \neq 0$ for "most" $h \in \mathbb{C}^N$.

$d(n) = \text{poly}(n)$

$\boxed{VP(n, d(n))}$

Dream : $\exists$ nonzero $\underline{P_N} \in \underline{\underline{VP}}_N$:

✓
- ▷ P_N is an equation for $\underline{VP(n,d)}$.
- ▷ P_N is not an equation for $V\underline{NP(n,d)}$.

★ Existence of efficient equations :-

① [Forbes - Shpilka - Volk 2018] :

Constant depth multilinear circuits

Sparse polynomials; depth-3-diagonal circuits

Equations for simple classes are not too simple

Equations for $\boxed{VP}$ that are in $\boxed{VP}$.

"Weak evidence against existence of VP_N- natural proofs for VP_n."

② [Chatterjee - Kumar - Ramya - Saptharishi - T. 2020]

Consider VP' ~ polynomials in VP that have $\{-1, 0, 1\}$ coefficients.

e.g. Det^n, ESym, IMM, . . .
(most of the "interesting" polynomials)

Theorem [CKRST '20]

$\forall n, d$, $N = \binom{n+d}{d}$, $\exists$ P_N non-zero, s.t.

(a) $\forall f \in VP'(n,d)$, $P_N(\overrightarrow{\mathrm{coeff}}(f)) = 0$.

(b) $P_N(\overrightarrow{\mathrm{coeff}}(h)) \neq 0$ for many $h \in \{-1, 0, +1\}$

(c) $P_N \in VP(N, D)$ for $D = \mathrm{poly}(N)$.

" Interesting polys in VP have almost-natural proofs"

Thm :- Similar statement for VNP'...

Chow 2011 : P/poly has quasi-natural proofs.

Consequence:

There could be a "natural proof" that shows that $\mathrm{Perm}_n \notin VP$.

e.g. P_N that is an equation for VP',
but $P_N(\overrightarrow{\mathrm{coeff}}(h_n)) \neq 0$ for $h_n \in VNP'$.

③ [Kumar- Ramya- Saptharishi-T. 2020]

If Perm_n requires circuits of size 2^{n^ϵ} $(\epsilon>0)$, then VNP does not have VP-natural proofs.

Theorem: If $\text{size}(\text{Perm}_n) > 2^{n^\epsilon}$ for $\epsilon>0$, then for any nonzero $\{P(z_1,\dots,z_N)\}$

$$\forall f \in \text{VNP} \quad P(\overline{\text{coeff}}(f)) = 0$$

$$\Downarrow$$

$$\text{size}(P_N) = \boxed{N^{\omega(1)}}.$$

- -

$d(n) = \text{poly}(n)$

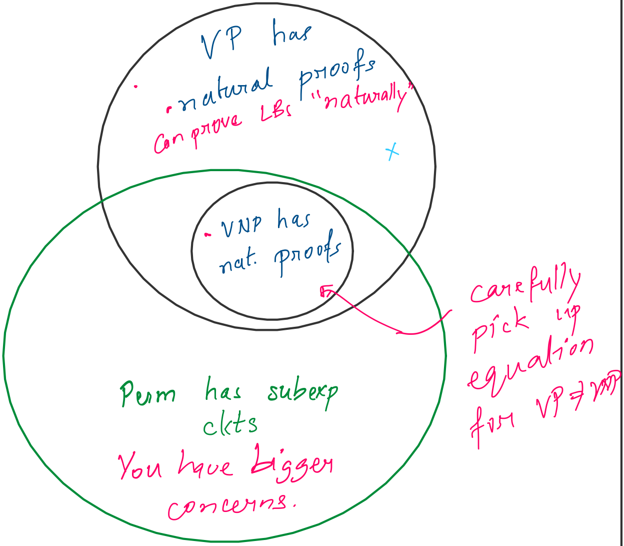
$\text{VP}(d(n))$ = families of polys whose n^{th} poly

- deg $\leq d(n)$
- $\exists n_0$: if $n>n_0$, $\text{size}(f_n) \leq \text{poly}$

P_N is eq^n for $\text{VP}(d(n))$

if $\exists n_0 : \forall n > n_0$, P_N vanishes on the nth slice of $\text{VP}(d(n))$

* Putting our result in context:-


VP has
• natural proofs
Can prove LBs "naturally"
• VNP has
nat. proofs
carefully pick up equation for VP ≠ VNP
Perm has subexp ckts
You have bigger concerns.