TODAY

(1) Algebraic Proof Systems

Nullsatz, Poly Calculus

IPS (Ideal Proof System)

(2) Next week - spring break.
(No class or office hours)

THE PROOF COMPLEXITY ZOO

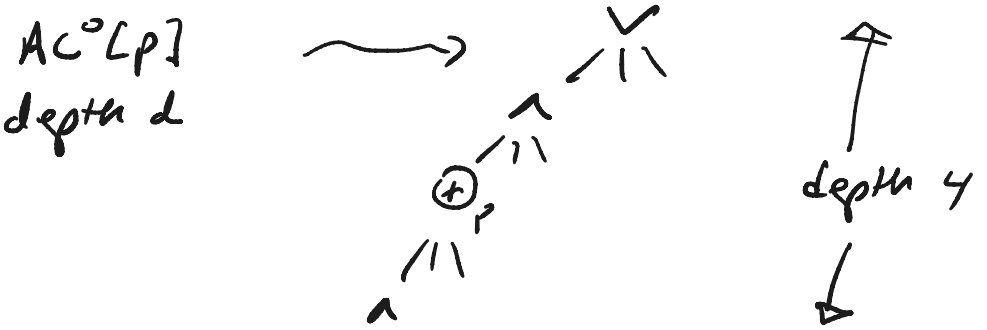
The Next Big Barrier

Prove superpolynomial lower bounds for $AC^0[p]$-Frege systems.

- Why is this so hard, especially when superpolynomial lower bounds have been known for $AC^0[p]$ for over 20 years??
- We don't even have conditional lower bounds (other than the assumption NP ≠ coNP)
- We also don't know if any proof complexity lower bound implies a circuit lower bound
- This motivates the study of algebraic proofs

Mystery of $AC^0[p]$

(1) Beigel-Tarui / Yao / Allender-Hertrampf circuit normal form theorems hold!



(2) Method of probalistic polys [Smolensky, Razborov] doesn't seem to work

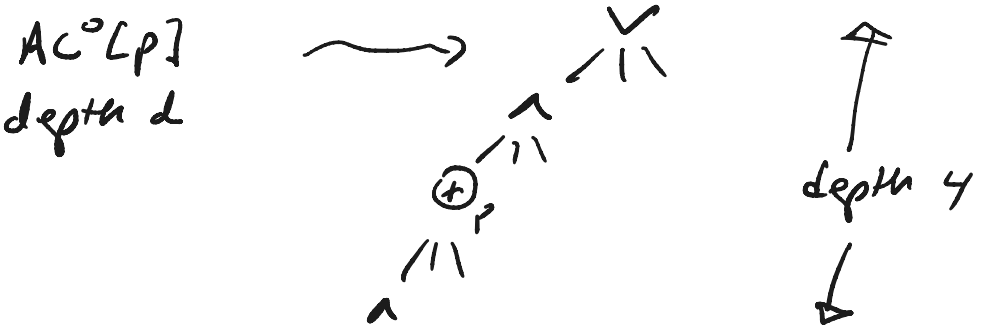
Mystery of $AC^0[p]$

(1) Beigel–Tarui / Yao / Allender–Hertrampf circuit normal form theorems hold!

Theorem [Buss, Kolodziejczyk, Zdanowski]
Any $AC^0[p]$ Frege prof Π of quasipolynomial size can be converted into a depth-4 quasipoly size $AC^0[p]$ Frege proof, where all formulas are: $\bigvee \circ \bigwedge \circ \bigoplus_p \circ$ small-AND

Mystery of $AC^0[p]$

(1) Beigel-Tarui / Yao / Allender-Hertrampf circuit normal form theorems hold!

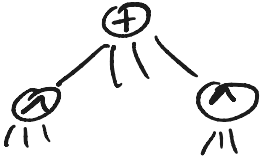


(2) Method of probalistic polys [Smolensky, Razborov] doesn't seem to work

Mystery of $AC^0[p]$

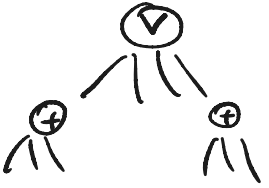
③ Two special cases:

Poly calculus:



Lines are polynomials

$Res(\oplus_p)$:



This motivates a direct study of proofs where lines are low depth $AC^0[p]$.

Nsatz / PC : Lines are $\oplus_p \circ$ AND (= polynomials mod p)

UNSOLVABILITY OF POLYNOMIAL EQUATIONS

INPUT: A system of polynomial equations over $\mathbb{F}$

$$P = \{ p_1(\vec{x}) = 0,\ p_2(\vec{x}) = 0,\ \ldots,\ p_m(\vec{x}) = 0 \}$$

OUTPUT: 1 iff $\exists \alpha \in \mathbb{F}^n$ that satisfies all equations

ALGEBRAIC PROOF SYSTEMS

- ALGEBRAIC PROOF SYSTEMS CERTIFY UNSOLVABILITY OF A SYSTEM OF POLYNOMIAL EQUATIONS OVER $\mathbb{F}$

GIVEN $P = \{P_1(\vec{x}) = 0, P_2(\vec{x}) = 0, \ldots, P_m(\vec{x}) = 0\}$,
certify there is NO solution satisfying all equations over $\mathbb{F}$

HILBERT'S NULLSTELLENSATZ

Let $P = \{ p_1(x) = 0, \ldots, p_m(x) = 0 \}$. Then P is unsolvable over $\mathbb{F}$ (alg. closed) iff there exist polys $q_1(x), \ldots, q_m(x)$ such that

$$\sum_{i=1}^{m} q_i(x)\, p_i(x) = 1$$

NULLSTELLENSATZ REFUTATIONS

Let $P = \{p_1(x) = 0, \ldots, p_m(x) = 0\}$, over $\mathbb{F}$.

A Nullstellensatz refutation of P is an explicit list of polynomials $\{q_1, \ldots, q_m\}$ over $\mathbb{F}$ such that

$$\sum_{i=[m]} f_i \cdot g_i = 1$$

(g_i's given as sum of terms)

NULLSTELLENSATZ REFUTATIONS FOR CNF's

OUR FOCUS IS ON REFUTING UNSAT CNF, SO APPLY STANDARD TRANSLATION:

Let $F = C_1 \wedge C_2 \wedge \dots \wedge C_m$. Convert each C_i to poly equation:

Example $C_i = (x_1 \vee x_2 \vee \bar{x}_4) \Rightarrow P_{C_i} = (1-x_1)(1-x_2)x_4$

$F = C_1 \wedge C_2 \wedge \dots \wedge C_m \Rightarrow P_F = \{P_{C_1}=0, \dots, P_{C_m}=0, \{x_i^2 - x_i = 0\}\}$

For CNF formula $F = C_1 \wedge C_2 \wedge \dots \wedge C_m$, we define a Nullstellensatz refutation of F over $\mathbb{F}$ to be a Nullstellensatz refutation of $P = \{P_{C_1}=0, P_{C_2}=0, \dots, P_{C_m}=0, x_1^2-x_1=0, \dots, x_n^2-x_n=0\}$

$NSdeg_{\mathbb{F}}(F)$ = min degree of any Nullstellensatz refutation of F

Example: (Negation of) Induction

$\neg IND_n$:

$(1 - X_1) = 0$ $\qquad$ X_1

$(X_1)(1 - X_2) = 0$ $\qquad$ $X_1 \Rightarrow X_2$

$(X_2)(1 - X_3) = 0$ $\qquad$ $X_2 \Rightarrow X_3$

$(X_3)(1 - X_4) = 0$ $\qquad$ $\vdots$

$\vdots$

$(X_{n-1})(1 - X_n) = 0$ $\qquad$ $X_{n-1} \Rightarrow X_n$

$X_n = 0$ $\qquad$ $\neg X_n$

Example: (Negation of) Induction

$\neg IND_n$:

A_1 $(1-X_1)=0$

A_2 $(X_1)(1-X_2)=0$

A_3 $(X_2)(1-X_3)=0$

A_4 $(X_3)(1-X_4)=0$

$\vdots$

A_n $(X_{n-1})(1-X_n)=0$

A_{n+1} $X_n=0$

Nsatz refutation:

1. $X_1=1$

2. $\underbrace{X_1 \to X_2}_{A_2}$ $\underbrace{X_2 \to X_3}_{A_3}$ $\Rightarrow$ $X_1 \to X_3$

3. $X_1 \to X_3$ $\underbrace{X_3 \to X_4}_{A_4}$ $\Rightarrow$ $X_1 \to X_4$

4. $X_1 \to X_4$ $X_4 \to X_5$ $\Rightarrow$ $X_1 \to X_5$

$\vdots$

$(n+1)$: $X_1 \to X_{n-1}$ $\underbrace{X_{n-1} \to X_n}_{A_n}$ $\Rightarrow$ $X_1 \to X_n$

$1 + (n+1) + A_{n+1} : 1=0$

Example: (Negation of) Induction

$\neg IND_n$:

A_1 $(1-X_1)=0$

A_2 $(X_1)(1-X_2)=0$

A_3 $(X_2)(1-X_3)=0$

A_4 $(X_3)(1-X_4)=0$

$\vdots$

A_n $(X_{n-1})(1-X_n)=0$

A_{n+1} $X_n=0$

Nsatz refutation:

1. $X_1=1$

2. $\underbrace{X_1 \to X_2}_{A_2}$ $\underbrace{X_2 \to X_3}_{A_3}$ $\Rightarrow$ $\underbrace{X_1 \to X_3}_{B_3}$ $\quad (1-X_3)\overbrace{X_1(1-X_2)}^{A_2} + X_1\overbrace{X_2(1-X_3)}^{A_3}=0$

3. $\underbrace{X_1 \to X_3}_{B_3}$ $\underbrace{X_3 \to X_4}_{A_4}$ $\Rightarrow$ $\underbrace{X_1 \to X_4}_{B_4}$ $\quad (1-X_4)\overbrace{X_1(1-X_3)}^{B_3} + X_1\overbrace{X_3(1-X_4)}^{A_4}=0$

4. $\underbrace{X_1 \to X_4}_{B_4}$ $\underbrace{X_4 \to X_5}_{A_5}$ $\Rightarrow$ $\underbrace{X_1 \to X_5}_{B_5}$

$\vdots$

$(n+1)$: $\underbrace{X_1 \to X_{n-1}}_{B_{n-1}}$ $\underbrace{X_{n-1} \to X_n}_{A_n}$ $\Rightarrow$ $\underbrace{X_1 \to X_n}_{B_n}$

$(n+2)$: $\underbrace{X_1}_{A_1}$ $\underbrace{X_1 \to X_n}_{B_n}$ $\underbrace{\neg X_n}_{A_{n+1}}$ $\Rightarrow 1=0$ $\quad \frac{A_1}{1-X_1} + \frac{B_n}{X_1(1-X_n)} + (X_1)\frac{A_{n+1}}{X_n}=0$

Proof has degree $\Theta(n)$

Example: (Negation of) Induction

Can get a degree $O(\log n)$ Nsatz refutation by divide-and-conquer

$\neg IND_n$:

A_1 $(1-X_1)=0$

A_2 $(X_1)(1-X_2)=0$

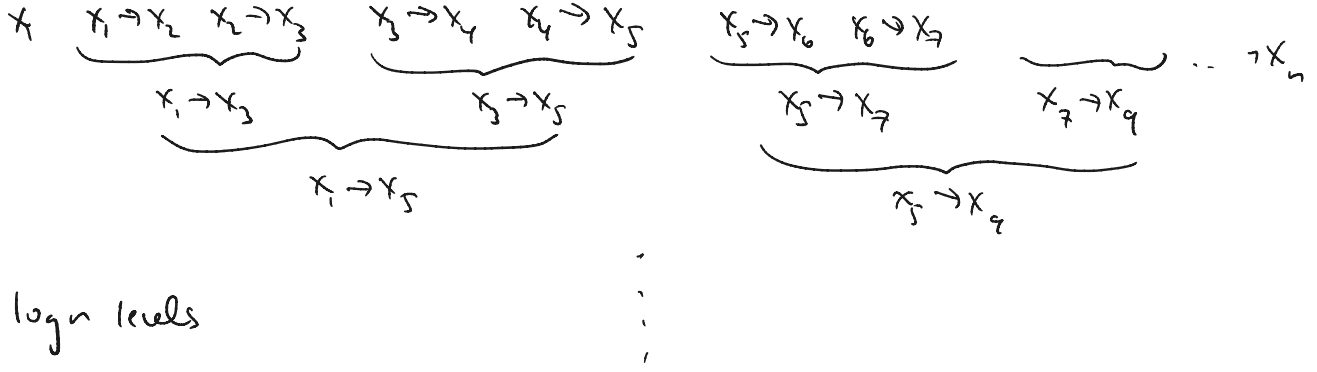
A_3 $(X_2)(1-X_3)=0$

A_4 $(X_3)(1-X_4)=0$

$\vdots$

A_n $(X_{n-1})(1-X_n)=0$

A_{n+1} $X_n=0$



$\log n$ levels

$1=0$

This is optimal degree:

Theorem [Buss-P]

Any Nsatz refutation of $\neg IND_n$ has degree $\Omega(\log n)$

Finding degree-d Nsatz refutations in time $n^{O(d)}$

Let $F = C_1 \wedge \cdots \wedge C_m$ be an unsat 3CNF

Let $P_{C_1} = 0, \ldots P_{C_m} = 0$ be degree 3 poly eqns

Suppose there are degree $\leq d$ multilinear polys $q_1 \ldots q_m$ such that $\sum P_i q_i = 1$

Write system of linear equations:

variables: $c_{i,t}$: $i \in [m]$, $t \subseteq [n]$, $|t| \leq t$

$c_{i,t}$: coefficient in front of term t in q_i

equations: for each term $t \subseteq [n]$, $1 \leq |t| \leq d$:

one equation that says coeff's corresponding to term t sum to 0

for $t = \phi$: one eqn says coeffs corresponding to term $t = \phi$ sum to 1

Finding degree-d Nsatz refutations

Let $F = C_1 \wedge \cdots \wedge C_m$ be an unsat 3CNF

Let $P_{C_1} = 0, \ldots P_{C_m} = 0$ be degree 3 poly eqns

Suppose there are degree $\leq d$ multilinear polys $q_1 \ldots q_m$ such that $\sum P_i q_i = 1$

Write system of linear equations:

variables: $c_{i,t}$: $i \in [m]$, $t \subseteq [n]$, $|t| \leq t$

$c_{i,t}$: coefficient in front of term t in q_i

equations: for each term $t \subseteq [n]$, $1 \leq |t| \leq d$:

one equation that says coeff's corresponding to term t sum to 0

for $t = \phi$: one eqn says coeffs corresponding to term $t = \phi$ sum to 1

# of variables $\sim m \cdot n^t$

equations $\sim n^t$

? solve in time poly(m, n^t) = poly(n^t)

Degree Automatizability of Nsatz Refutations

This gives:

Theorem There is an algorithm A^{NS} such that for any unsatisfiable 3CNF F, $A^{NS}(P_F)$ outputs a Nsatz refutation in time $n^{O(d)}$ where d = min degree of any Nsatz refutation of P

Size-Degree Relationship for Nullstellensatz Refutations of CNFs

Recall: For Resolution we have the following width-size relationship

Theorem For any CNF F if F has a Res refutation of size s then F has a Res refutation of width $O(\sqrt{\log s \cdot n})$

A similar relationship holds for Nsatz refutations

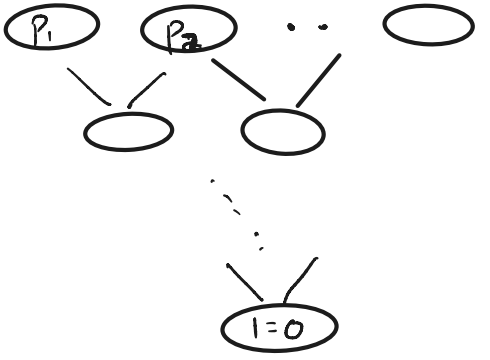
Defn The monomial-size of a poly q = number of nonzero monomials in q

monomial size of a Nsatz refutation $Q = \{q_1 \dots q_m\}$ is $\sum_{i=1}^{m}$ monomial-size(q_i)

The monomial size of CNF F = min monomial-size over all Nsatz refutations of F

Theorem For any CNF F, if F has a Nsatz refutation of monomial-size S then F has a degree $O(\sqrt{n \log s})$ Nsatz refutation

POLYNOMIAL CALCULUS (PC)



PC is a dynamic version of Nullsatz

Axioms: $P_i \in \mathcal{P}$ (initial polynomials over $\mathbb{F}$)

Rules: $f=0,\ g=0 \Rightarrow \alpha f + \beta g = 0,\ \alpha, \beta \in \mathbb{F}$

$f=0 \Rightarrow x f = 0,\ (1-x) f = 0$

Last derived polynomial: $1=0$

complexity:

degree is max degree over all polynomials in refutation

size is sum of sizes of all polys (total # of occurrences of monomials)

Nsatz vs Poly Calculus

- PC can simulate Nsatz with respect to degree:

  Let F be unsat 3CNF. If Nullsatz has a degree-d refutation of P_F, then PC also has degree $\leq d$ refutation of P_F

Nsatz vs Poly Calculus

- PC can simulate Nsatz with respect to degree:

  Let F be unsat 3CNF. If Nullsatz has a degree-d refutation of P_F, then PC also has degree $\leq d$ refutation of P_F

- Nsatz cannot simulate PC with respect to degree:

  there exist UNSAT 3CNFs that have degree $O(1)$ PC refutations, but require $\Omega(n)$ degree Nsatz refutations [Clegg-Edmonds-Impagliazzo]

  Weaker result: INDUCTION has PC refutations of degree $O(1)$ but require $\Omega(\log n)$ Nsatz degree [Buss-Pitassi]

A slight generalization of PC/Nsatz that poly-simulates Nsatz

PCR: Let F be unsat 3CNF

PCR conversion of F to system $\hat{P}_F$ of poly eqns:

vars: $x_i, i \in [n]$, $\tilde{x}_i, i \in [n]$

$\tilde{x}_i$: dual vars; represent $\bar{x}$

Equations:

$C_i = (x_1 \vee x_2 \vee \bar{x}_3) \rightarrow \tilde{P}_{C_i} \stackrel{d}{=} \tilde{x}_1 \tilde{x}_2 x_3 = 0$

plus $\{x_i + \tilde{x}_i - 1 = 0\} \quad \forall i \in [n]$

plus $x_i^2 - x_i = 0, \tilde{x}_i^2 - \tilde{x}_i = 0 \quad \forall i \in [n]$

Theorem PCR poly simulates Resolution

Degree Automatizability of PC

Theorem [Clegg - Edmonds - Impagliazzo]

There is an algorithm A^{PC} such that for any unsatisfiable 3CNF F, $A^{PC}(P_F)$ outputs a PC refutation in time

$n^{O(d)}$ where d = min degree of any PC refutation of P_F

Proof uses modified version of Gröbner basis algorithm

Size-Degree Relationship for PC Refutations

Defn The monomial-size of a poly q = number of nonzero monomials in q

The monomial size of a PC refutation $\{P_1, P_2, \ldots, 1=0\}$ is $\leq \sum_i$ monomial-size(P_i)

The PC monomial size of CNF F = min monomial-size over all PC refutations of F

theorem For any CNF F, if F has a PC refutation of monomial-size s then F has a degree $O(\sqrt{n \log s})$ PC refutation

PC Degree Lower Bounds

There are a variety of tight $\Omega(n)$ lower bounds for example:

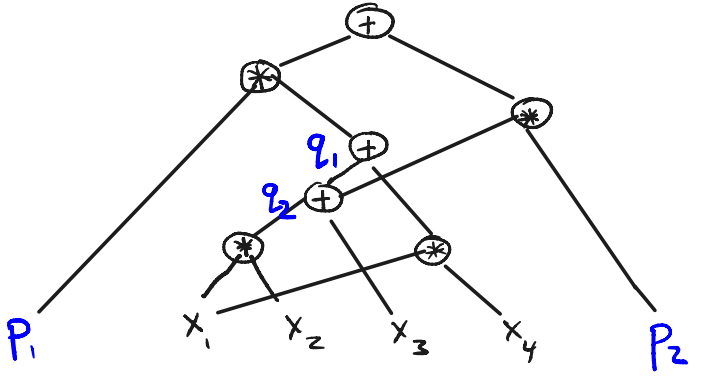
(1) PHP

(2) Mod_q principle, for PC proofs over $\mathbb{F}_\ell$, $\ell \neq p$

IPS (The Ideal Proof System) [P'96, P'98, gP'14]

- INSTEAD OF MEASURING COMPLEXITY OF q_i's BY NUMBER OF MONOMIALS, MEASURE BY THE ALGEBRAIC CKT SIZE

$$\underbrace{(x_1x_2 + x_3 + x_1x_4)}_{q_1} p_1 + \underbrace{(x_3 + x_1x_2)}_{q_2} p_2 + \ldots = 1$$



PC/NSATZ ⇝ IPS [P96, P98, gP14]

generalizes to

SOS ⇝ CONE PROOF SYSTEM

[Alekseev, grigoriev, Hirsh, Tzameret '20]

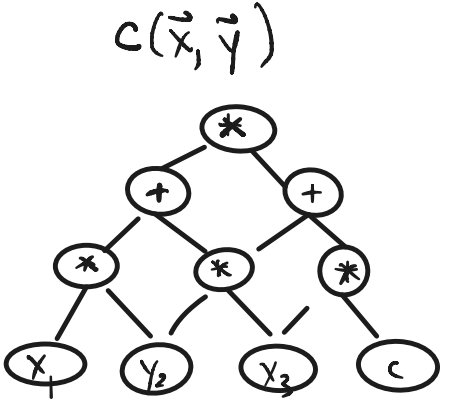
IPS (cont'd)

An IPS certificate/proof of unsolvability of $P = \{P_1(\vec{x}) = 0, \ldots, P_m(\vec{x}) = 0\}$ (over $\mathbb{F}$)

is an algebraic circuit $C(x_1, \ldots, x_n, y_1 \ldots y_m)$ such that:

(1) $C(x_1, \ldots, x_n, \vec{0}) = 0$

(2) $C(x_1, \ldots, x_n, P_1(\vec{x}), \ldots, P_m(\vec{x})) = 1$



(1) and (2) imply that 1 is in the ideal generated by $P = \{P_1 = 0, \ldots, P_m = 0\}$

(1) forces the polynomial $C(\vec{x}, \vec{y})$ to be in ideal generated by $\vec{y}$

IPS (cont'd)

① IPS refutations verifiable in randomized polytime via PIT (polynomial identity testing)

∴ IPS not known to be a "Cook-Reckhow" proof system

Still we expect that IPS is **not** poly-bounded:

Lemma IPS poly-bounded → coNP ∈ MA → Poly hierarchy collapses

② IPS p-simulates Extended Frege

More generally $\mathcal{C}$-IPS p-simulates $\mathcal{C}$-Frege

(for common circuit classes $\mathcal{C}$)

VP and VNP [Valiant]

A family of polynomials (f_n) is in **VP** if its degree and circuit size are poly(n)

A family of polynomials (g_n) is in **VNP** if it can be written:

$$g_n(\vec{x}) = \sum_{\vec{e} \in \{0,1\}^{poly(n)}} F_n(\vec{e}, \vec{x}), \quad \text{for some } (f_n) \in VP$$

Major Open Problem : Show $VP \neq VNP$

CONNECTING LBs FOR STRONG PROOF SYSTEMS TO CIRCUIT LBs ?

Theorem [grochow-P '14]

Superpoly IPS Lower bounds $\Rightarrow$ VP $\neq$ VNP

OPEN superpoly EF Lower bounds $\longrightarrow$ P $\neq$ NP ?

IPS lower bounds implies VP ≠ VNP

Theorem A super-polynomial lower bound for [constant-free] IPS implies VNP ≠ VP [$VNP^0 \neq VP^0$] for any ring R.

Key Lemma: Every DNF tautology has a VNP^0 certificate.

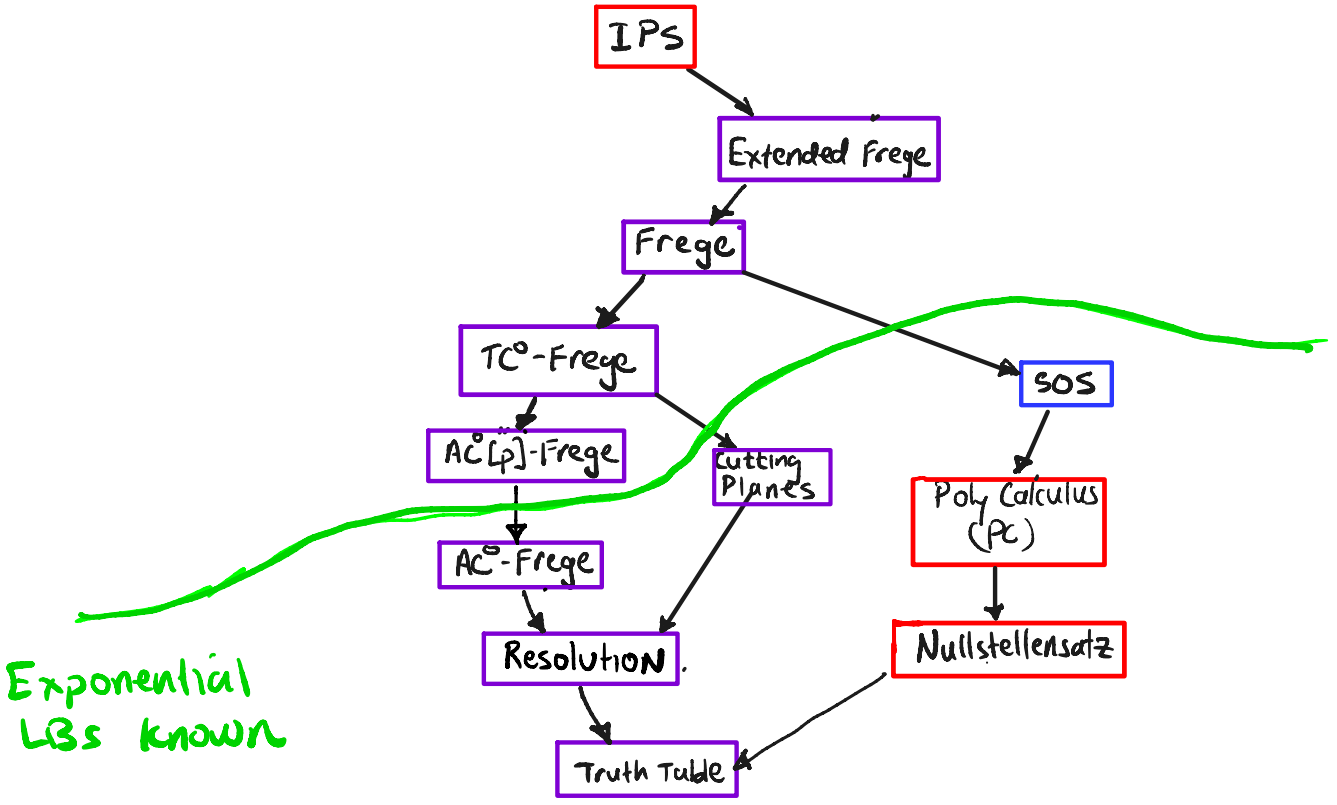
Proof of Theorem assuming Key Lemma: A super-polynomial size lower bound on our system means there are unsat formulas such that *every certificate* requires super-polynomial size. Since some certificate is in VNP^0, that function requires super-poly size circuits. QED

LOWER BOUNDS FOR IPS SUBSYSTEMS

* ① Restrictions of IPS (e.g., multilinear) [FSTW '16]
* ② Shub-Smale Conjecture → superpoly IPS lower bounds [AGHT '20]
* ③ Superpoly lower bounds on bit complexity [Alekseev '21]
* ④ VP ≠ VNP ⇒ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]
* ⑤ Superpoly LBs for constant-depth IPS over $\mathbb{R}$ [AF '22, GHT '22]

* Not for CNF formulas (poly eqns over $\mathbb{R}$)
* CNF but not known to be UNSAT

PROOF COMPLEXITY ZOO



References

1. Beame – Impagliazzo – Krajíček – Pitassi – Pudlák
   Lower Bounds on Hilbert's Nullstellensatz and prop. proofs

2. Clegg – Edmonds – Impagliazzo STOC '96
   Using the groebner Basis Algorithm to find proofs of unsatisfiability

3. Buss – Pitassi
   good degree Bounds on Nullstellensatz Refutations of the Induction Principle

4. Pitassi, Tzameret, SigLog News
   Algebraic Proof Complexity: Progress, Frontiers, Challenges

5. Grochow – Pitassi
   Circuit complexity, Proof complexity and the Ideal Proof System

6. Buss – Grigoriev – Impagliazzo – Pitassi
   Linear gaps Between degrees for the polynomial calculus

7. Fleming – Kothari – Pitassi
   semialgebraic Proofs and Efficient Algorithm Design