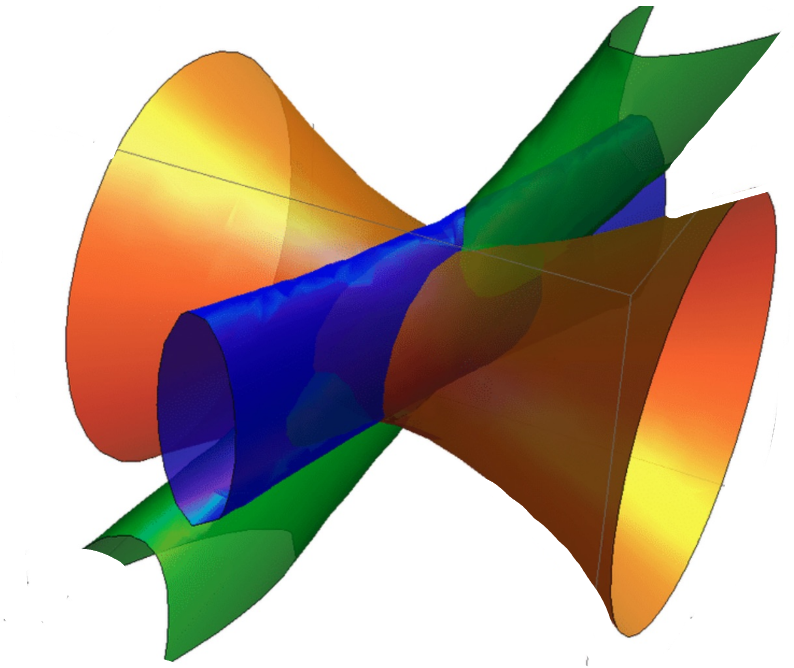
ALGEBRAIC PROOF COMPLEXITY



Toniann Pitassi

U. Toronto, U. Columbia

+ IAS

BURNING QUESTIONS

- What is the difference between circuit lower bounds and proof complexity lower bounds?
- Why can't we manage to prove $AC^0[p]$-Frege lower bounds?
- Are proof complexity lower bounds really going to solve P vs NP? NP vs coNP?
- Are algebraic circuit lower bounds easier to prove?

PROOF COMPLEXITY

K-SAT

INPUT: KCNF formula f

$$f = (x_1 \vee x_2 \vee x_3)(\bar{x}_1 \vee x_4 \vee x_7)(\bar{x}_2 \vee x_3) \ldots (x_9 \vee \bar{x}_{10})$$

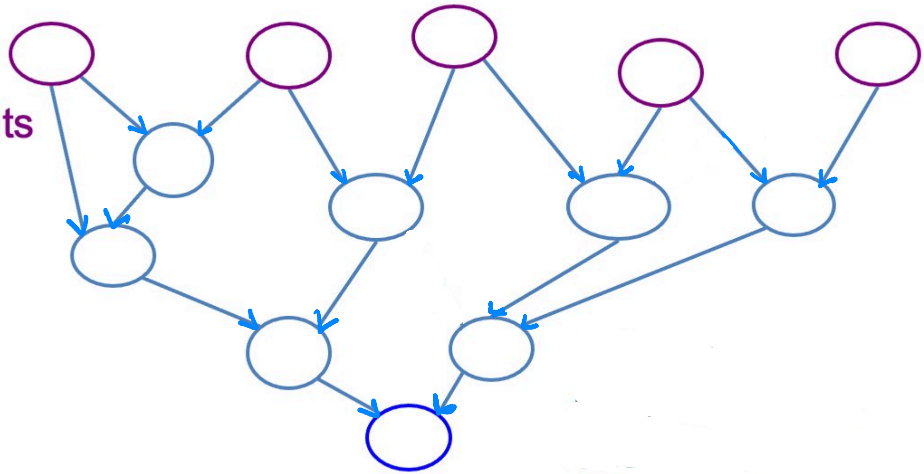
OUTPUT: SAT iff $\exists \alpha \; f(\alpha) = 1$

UNSAT iff $\forall \alpha \; f(\alpha) = 0$

- K-SAT is NP-COMPLETE
- HOW TO CERTIFY/PROVE f IS UNSAT ?

The graph of a proof

Axioms/inputs are sources

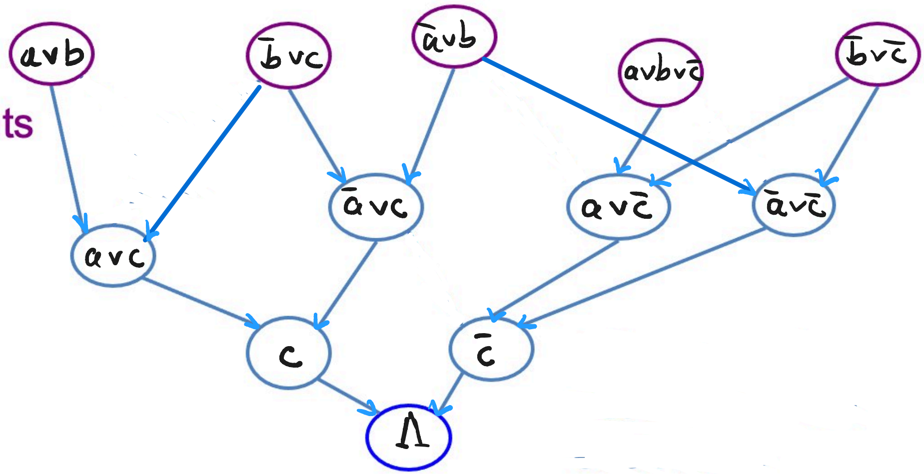


Sink labelled by tautology
(or Λ for refutation)

Example: graph of a RESOLUTION Proof

$f = (a \vee b)(\bar{b} \vee c)(\bar{a} \vee b)(a \vee b \vee \bar{c})(\bar{b} \vee c)$

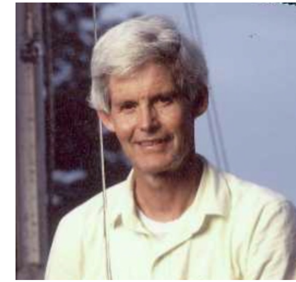
Axioms/inputs are sources



Resolution Rule:

$(x \vee C)\ (\bar{x} \vee D) \rightarrow (C \vee D)$

COOK'S PROGRAM FOR PROVING $NP \neq coNP$



UNSAT = { f | f is an UNSAT CNF formula }

Def'n (Cook-Reckhow 1975)

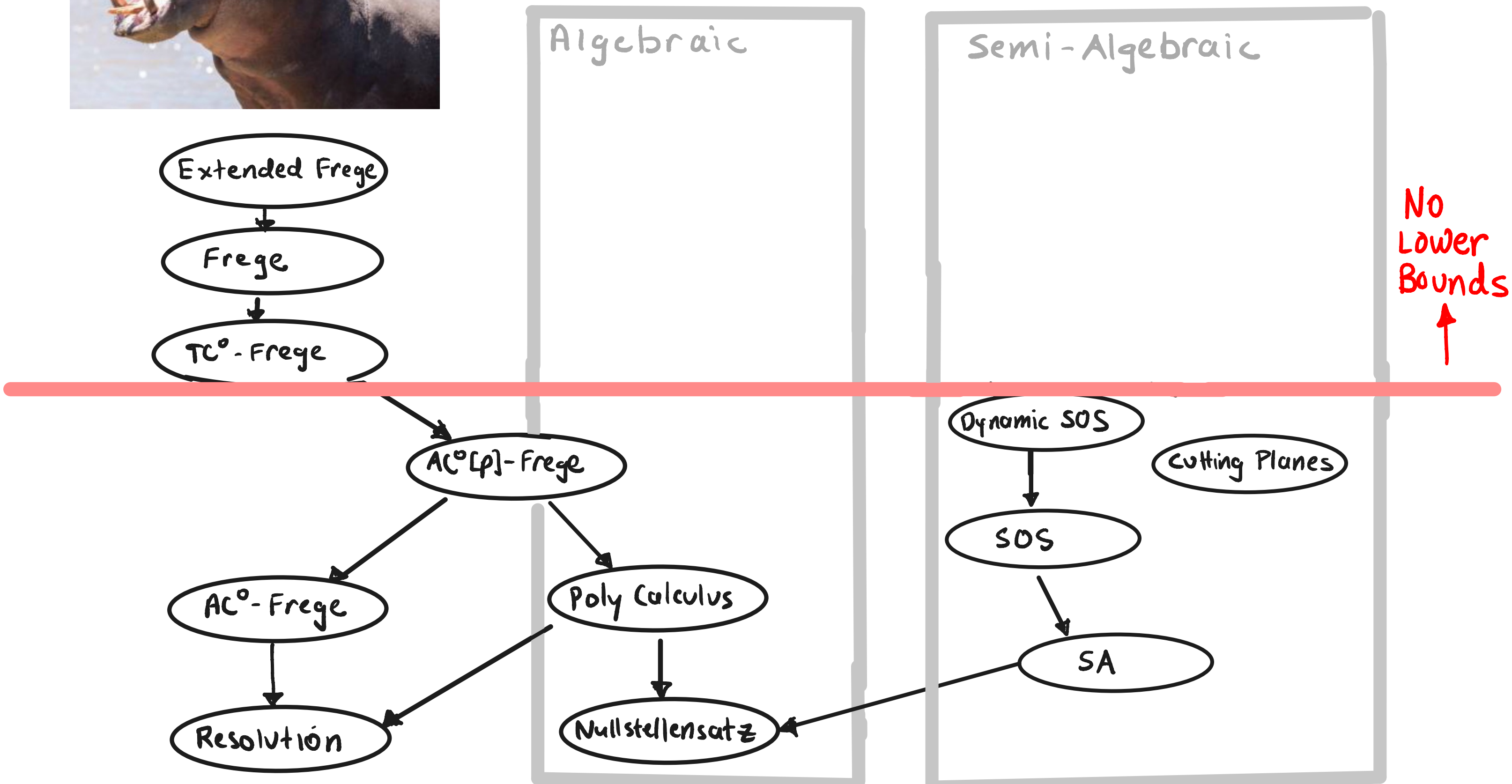
An abstract proof system is a polynomial-time function A from $\{0,1\}^*$ onto the set of all UNSAT CNFs

(For proof system P, define $A(w)$ = UNSAT CNF that w refutes)

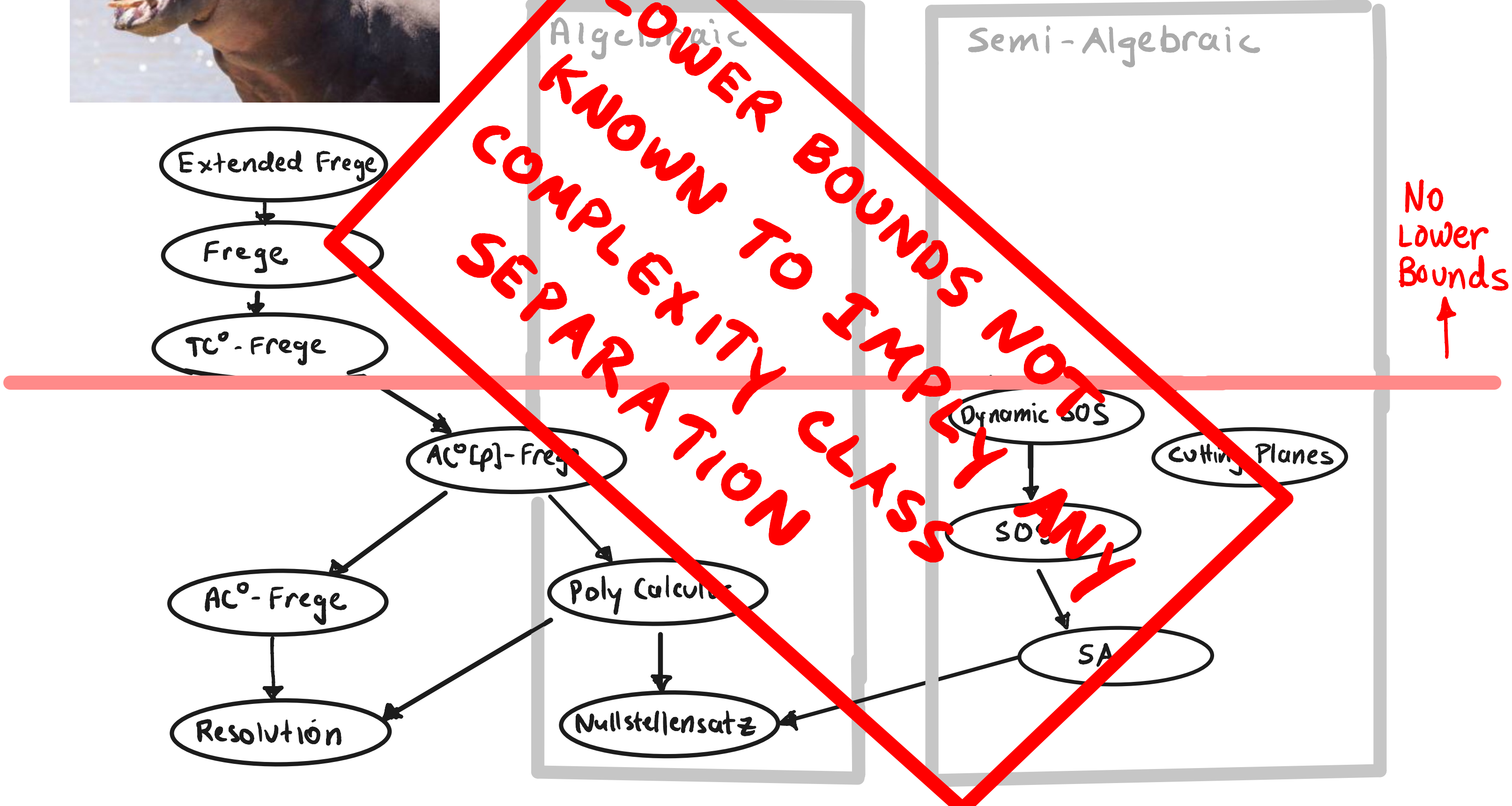
Theorem

There exists an abstract proof system in which all UNSAT CNFs have polynomial-size proofs iff $NP = coNP$

THE PROOF COMPLEXITY ZOO



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 $NP \neq coNP$)

- We also don't know if any proof complexity lower bound implies a circuit lower bound

- This motivates the study of algebraic proofs

TODAY

1. Algebraic Proof Systems

   IPS (Ideal Proof System)

   Subsystems of IPS : Nullsatz, Poly Calculus
   and the surprising power of low-depth IPS

2. IPS Lower Bounds $\Rightarrow$ $VP \neq VNP$

3. IPS Lower Bounds
   - conditional LBs for strong subsystems
   - unconditional LBs for weak subsystems

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

UNSOLVABILITY OF POLYNOMIAL EQUATIONS

NP complete

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

$\boxed{\text{kCNF-Polynomial system of eqns}}$

$$\mathcal{C} = C_1 \wedge C_2 \wedge \ldots \wedge C_m \longrightarrow P(\mathcal{C}) = \{ p_1, \ldots, p_m, \{x_i^2 - x_i\} \}$$

$$C_i = (x_1 \vee x_2 \vee \bar{x}_4) \longrightarrow p_i = (1-x_1)(1-x_2)x_4$$

* Our primary focus is on KCNF-polynomial systems

Hilbert's Nullstellensatz [BIKPP'96]

Input: An unsolvable system of polynomial equations:

$P = \{p_1(x)=0,\dots,p_m(x)=0\}$

Hilbert's Nullstellensatz: $p_1=p_2=\dots=p_m=0$ has no solution iff there are polynomials $q_1,\dots,q_m$ such that

$p_1q_1 + p_2q_2 + \dots + p_mq_m = 1$

$q_1, \dots, q_m$ is a proof of unsolvability of P
By Hilbert's Nullstellensatz, sound and complete
Degree is max degree of $q_1, \dots, q_m$
Nullsatz degree of P = min degree over all refutations

Polynomial Calculus (PC)

[CEI'96]

Dynamic version of Nullsatz

- Start with $p_1 = 0, \ldots, p_m = 0$
- Addition rule: $f=0$, $g=0$ implies $f+g=0$
- Multiplication rule: $f=0$ implies $fg=0$
- Want to derive $1=0$
- Degree is max degree over all lines (polys) in the refutation
- PC degree of $\{p_1,\ldots,p_m\}$ is min degree over all PC refutations

The Ideal Proof System
[P96,P98,Grochow-P]

Input: An unsatisfiable system of polynomial equations:

$$P = \{p_1(x)=0,\dots,p_m(x)=0\}$$

Hilbert's Nullstellensatz: $p_1=p_2=\dots=p_m=0$ has no solution iff there are polynomials $q_1,\dots,q_m$ such that

$$p_1q_1 + p_2q_2 + \dots + p_mq_m = 1$$

Introduce new placeholder variables $y_1,\dots,y_m$, to get a new polynomial:

$$C(x,y) = y_1\, q_1(x) + \dots + y_m\, q_m(x)$$

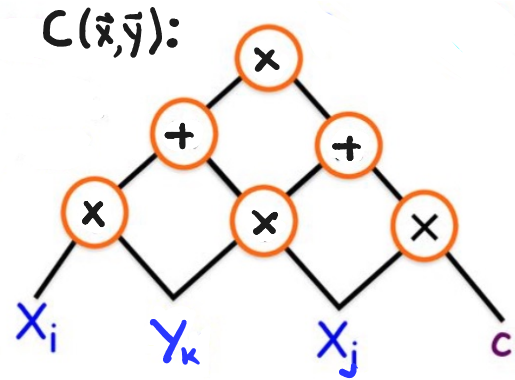
The Ideal Proof System

An IPS certificate that a system

$\mathbf{P} = \{P_1(\vec{x})=0,\dots,P_m(\vec{x})=0\}$ of polynomial equations is unsatisfiable (over F) is a polynomial $C(\vec{x},\vec{y})$ such that:

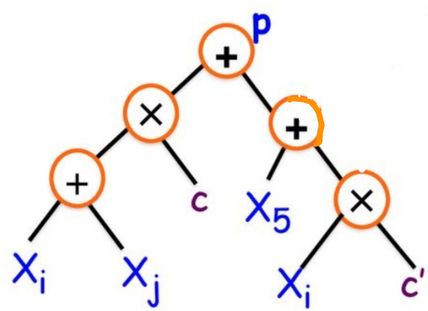
(1) $C(x_1, \dots, x_n, 0)=0$

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

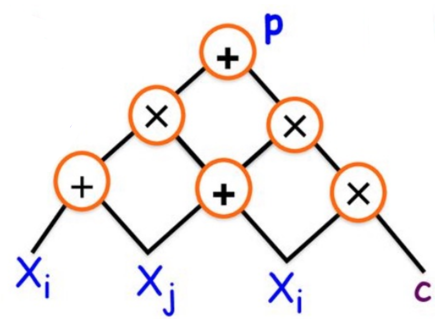


- (1) forces C to be in the ideal generated by the y's
- (1) and (2) imply that 1 is in the ideal generated by the P_i 's (and hence $\mathbf{P}$ is unsolvable).

ALGEBRAIC COMPLEXITY



F field
n variables,
deg p < n^c



$L(p)$ = formula size

$S(p)$ = circuit size

[VSBR] $S(p) \le L(p) \le S(p)^{\log n}$

VP = $\{p : S(p) \le \text{poly}\, n,\ \deg(p) = \text{poly}(n)\}$

IPS SUBSYSTEMS

Let $\mathcal{C}$ be an algebraic circuit class
(e.g., $\Sigma\Pi$, depth-d circuits, formulas)

$\mathcal{C}$-IPS: circuit $C(\vec{x},\vec{y}) \in \mathcal{C}$

For a system of polynomials $\mathcal{P} = \{p_1(\vec{x}), \ldots, p_m(\vec{x})\}_n$
the $\mathcal{C}$-IPS complexity of $\mathcal{P}$ is the minimum size
of a $\mathcal{C}$-IPS refutation of $\mathcal{P}$

IPS SIMULATES FREGE SYSTEMS

Theorem IPS p-simulates Extended Frege
(but degree of IPS circuit may be exponential in n)

Theorem Formula-IPS p-simulates Frege
(degree of IPS circuit is poly(n).)

IPS : CRUCIAL FACT

* Proofs are just ordinary algebraic circuits that satisfy 2 properties, both of which can be verified in randomized poly time

Lemma coNP $\not\subseteq$ MA $\Rightarrow$ SUPERPOLY IPS LOWER BOUNDS

Proof idea (contrapositive)

Merlin guesses polysize IPS proof
Arthur verifies the 2 properties using Swartz-Zippel PIT algorithm

WHICH ALGEBRAIC CIRCUIT RESULTS APPLY TO IPS?

All of them!

DEPTH REDUCTION: IPS PROOFS OF SIZE $s(n)$, DEGREE $d(n)$
IMPLY IPS PROOFS OF:

SIZE	DEPTH	REFERENCE
$\mathrm{poly}(ds)$	$O(\log d(\log s + \log d))$	[VSBR'83]
$\exp\sqrt{d \log n \log s}$	3	[T13], [GKKS13]

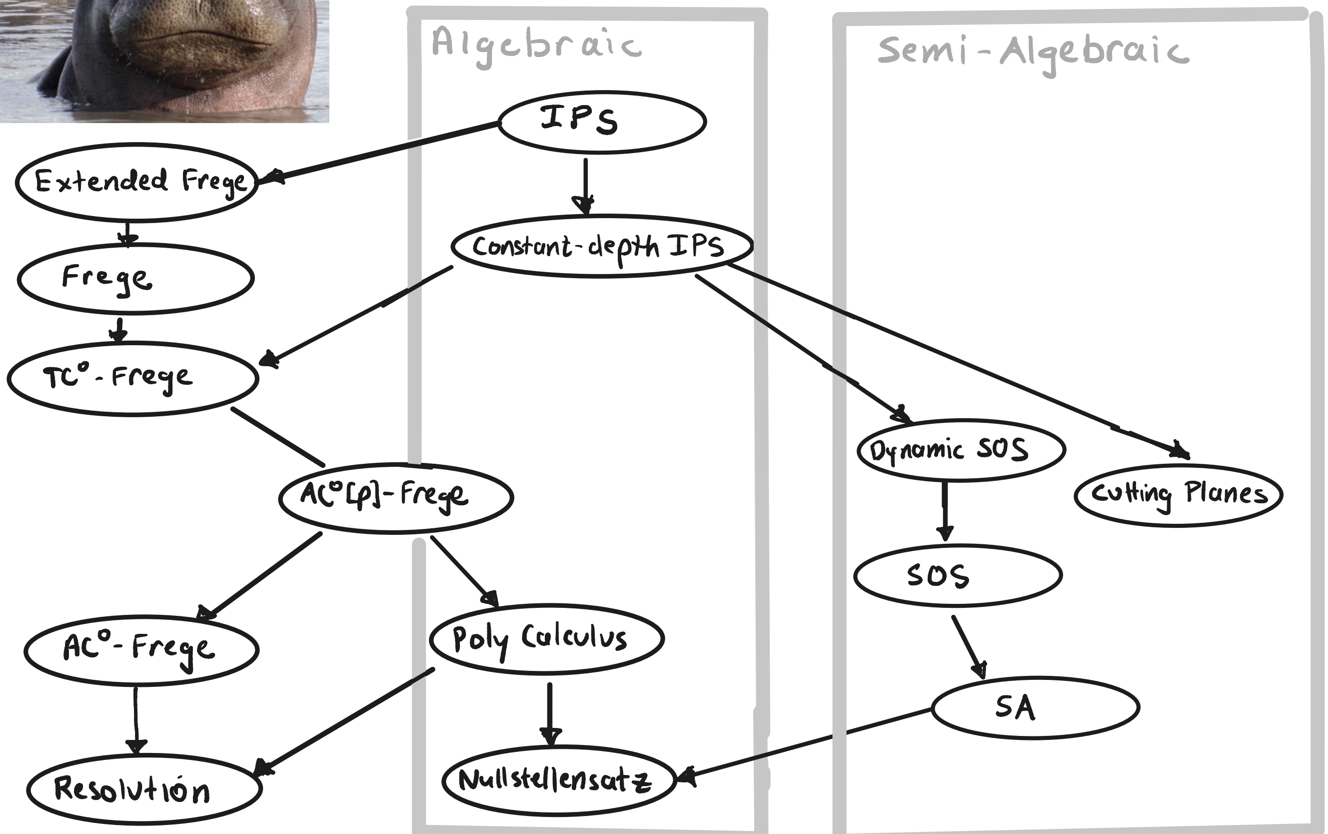
THE SURPRISING POWER OF LOW-DEPTH IPS

Theorem [BKZ'15]
Depth-3 $AC^0[p]$-Frege quasipoly simulates $AC^0[p]$-Frege.

Theorem [RT'08]
Depth-3 IPS p-simulates CP^* over $\mathbb{Q}$

Theorem [IMP'20]
- Depth-K IPS (over $\mathbb{F}_{p^m}$) quasipoly simulates:
  - Cutting Planes (K = 43)
  - SA, SOS, and Dynamic SOS (K = 43)
  - $AC^0[q]$-Frege (K = 3)
- Constant-depth IPS p-simulates TC^0-Frege

THE PROOF COMPLEXITY ZOO



CAN EXTENDED FREGE P-SIMULATE IPS?

HIGH LEVEL: IF C-PIT IS "PROVABLE" IN D-Frege then D-FREGE p-simulates C-IPS

Definition PIT AXIOMS FOR BOOLEAN PIT CIRCUIT K:

1. $K([C(x)]) \rightarrow K([C(b)])$
2. $K([C(x)]) \rightarrow \neg K([1-C(x)])$
3. $K([g(x)]) \wedge K([C(x,0)]) \rightarrow K([C(x,g(x))])$
4. $K([C(x)]) \rightarrow K([C(\pi(x))])$

Theorem If C-PIT AXIOMS PROVABLE IN D-FREGE THEN D-FREGE p-SIMULATES C-IPS

CONSEQUENCE FOR $AC^0[p]$-FREGE

Either:

- Bounded-depth PIT Axioms are provable in $AC^0[p]$-Frege
  (so $AC^0[p]$-Frege lower bounds $\rightarrow$ bded depth algebraic LBs)

- Bounded-depth PIT Axioms are not provable in $AC^0[p]$-Frege
  (so unconditional LBs for $AC^0[p]$ Frege)

"Life is a constant oscillation between the sharp horns of a dilemma." –H. L. Mencken

ALGEBRAIC CIRCUIT COMPLEXITY: VP versus VNP

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:

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

VP versus VNP

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:

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

- Permanent is VNP-complete
- SAT $\notin$ P/POLY $\Rightarrow$ VP $\neq$ VNP

IPS lower bounds implies $VP \neq VNP$

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

Proof of Key Lemma

Let $P = \{p_1(\vec{x})=0, \ldots, p_m(\vec{x})=0\}$ be UNSAT KCNF (translated)

Let $b(e,x) \overset{d}{=} ex + (1-e)(1-x)$ so $b(1,x)=x$ and $b(0,x)=1-x$

Let $$C(\vec{x},\vec{y}) \overset{d}{=} \sum_{\vec{e}\in\{0,1\}^n} \sum_{i=1}^{m} y_i \cdot p_i(\vec{e}) \left(\prod_{j<i} (1-p_j(\vec{e}))\right)\left(\prod_{j:\, x_j \in C_i} b(e_j,x_j)\right)$$

SHOW: ① $C(\vec{x},\vec{y}) \in VNP$
② $C(\vec{x},\vec{0}) = 0$
③ $C(\vec{x}, p_1(\vec{x}), \ldots, p_m(\vec{x})) = 1$

Proof of Key Lemma

Let $\mathcal{P} = \{p_1(\vec{x})=0, \ldots, p_m(\vec{x})=0\}$ be UNSAT KCNF (translated)

Let $b(e,x) \overset{d}{=} ex + (1-e)(1-x)$ so $b(1,x)=x$ and $b(0,x)=1-x$

Let $$C(\vec{x},\vec{y}) \overset{d}{=} \sum_{\vec{e}\in\{0,1\}^n} \sum_{i=1}^{m} y_i \cdot p_i(\vec{e}) \left(\prod_{j<i} (1-p_j(\vec{e}))\right)\left(\prod_{j:\, x_j \in C_i} b(e_j, x_j)\right)$$

SHOW : ① $C(\vec{x},\vec{y}) \in VNP$ ✓

② $C(\vec{x},\vec{0}) = 0$ ✓

③ $C(\vec{x}, p_1(\vec{x}), \ldots, p_m(\vec{x})) = 1$

SHOW : ① $C(\vec{x},\vec{y}) \in VNP$

② $C(\vec{x},\vec{0}) = 0$

③ $C(\vec{x}, p_1(\vec{x}), .., p_m(\vec{x})) = 1$

Let $b(e,x) \overset{d}{=} ex + (1-e)(1-x)$ so $b(1,x) = x$ and $b(0,x) = 1-x$

Let
$$C(\vec{x},\vec{y}) \overset{d}{=} \sum_{\vec{e}\in\{0,1\}^n} \sum_{i=1}^{m} y_i \cdot p_i(\vec{e}) \left(\prod_{j<i} (1-p_j(\vec{e}))\right)\left(\prod_{j:x_j \in C_i} b(e_j,x_j)\right)$$
$$= \sum_{i=1}^{m} y_i \left(\sum_{\vec{e}\in\{0,1\}^n} \left(p_i(\vec{e}) \prod_{j<i} (1-p_j(\vec{e}))\right) \prod_{j:x_j \in C_i} b(e_j,x_j)\right)$$
$$= \sum_{i=1}^{m} y_i \left(\sum_{\vec{e}\in\{0,1\}^n} [\![\vec{e} \text{ falsifies } C_i \text{ and satisfies } C_1,..,C_{i-1}]\!] \prod_{j:x_j \in C_i} b(e_j x_j)\right)$$

partition of assignments:

$\vec{e}\in\{0,1\}^n$ maps to minimal i st $\vec{e}$ falsifies clause C_i

Claim:
$$C(\vec{x}, p_1(\vec{x}), .., p_m(\vec{x})) = \sum_{\vec{e}\in\{0,1\}^n} b(e_1 x_1)\cdot b(e_2 x_2)\cdot \ldots \cdot b(e_n x_n)$$
$$= 1$$

SHOW : ① $C(\vec{x},\vec{y}) \in VNP$

② $C(\vec{x},\vec{0}) = 0$

③ $C(\vec{x}, p_1(\vec{x}), \dots, p_m(\vec{x})) = 1$

Let $b(e,x) \stackrel{d}{=} ex + (1-e)(1-x)$ so $b(1,x) = x$ and $b(0,x) = 1-x$

Let
$$C(\vec{x},\vec{y}) \stackrel{d}{=} \sum_{\vec{e}\in\{0,1\}^n} \sum_{i=1}^{m} y_i \cdot p_i(\vec{e}) \left(\prod_{j<i} (1-p_j(\vec{e}))\right)\left(\prod_{j:\, x_j \in C_i} b(e_j,x_j)\right)$$
$$= \sum_{i=1}^{m} y_i \left(\sum_{\vec{e}\in\{0,1\}^n} \left(p_i(\vec{e}) \prod_{j<i} (1-p_j(\vec{e}))\right) \prod_{j:\, x_j \in C_i} b(e_j,x_j)\right)$$
$$= \sum_{i=1}^{m} y_i \left(\sum_{\vec{e}\in\{0,1\}^n} [\![\vec{e} \text{ falsifies } C_i \text{ and satisfies } C_1,\dots,C_{i-1}]\!] \prod_{j:\, x_j \in C_i} b(e_j,x_j)\right)$$

partition of assignments:

$\vec{e}\in\{0,1\}^n$ maps to minimal i st $\vec{e}$ falsifies clause C_i

Claim:
$$C(\vec{x}, p_1(\vec{x}), \dots, p_m(\vec{x})) = \sum_{\vec{e}\in\{0,1\}^n} b(e_1,x_1)\cdot b(e_2,x_2)\cdot \ldots \cdot b(e_n,x_n)$$
$$= 1$$

IPS LOWER BOUNDS

1. Subsystems of IPS (lowdepth/multilinear) [FSTW '16]

2. Shub-Smale Conjecture $\rightarrow$ superpoly IPS lower bounds [AGHT '20]

3. Unconditional lower bounds (very strong subsystem of IPS) [Alekseev '21]

4. $VP \neq VNP \Rightarrow$ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]

IPS LOWER BOUNDS

* ① Subsystems of IPS (low depth / multilinear) [FSTW '16]

* ② Shub-Smale Conjecture $\rightarrow$ superpoly IPS lower bounds [AGHT '20]

* ③ Unconditional lower bounds (very strong subsystem of IPS) [Alekseev '21]

* ④ VP $\neq$ VNP $\Rightarrow$ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]

* Not for CNF formulas

* F_n is CNF but not known to be UNSAT

SHUB-SMALE CONJECTURE → IPS LOWER BOUNDS [AGHT]

Let $\{f_n\}_{n \geq 0}$ be a sequence of integers

$\tau(f_n) \stackrel{d}{=}$ min algebraic circuit size to compute f_n from constants $-1, 0, 1$

<u>Fact</u>: $\tau(2^n) = (\log n)^{O(1)}$, $\tau(2^{2^n}) = (\log n)^{\Omega(1)}$

<u>SS Conjecture</u>: $\tau(m_n \cdot n!) = (\log n)^{\Omega(1)}$ for any $m_n \in \mathbb{N}$, $m_n \geq 1$

SHUB-SMALE CONJECTURE $\rightarrow$ IPS LOWER BOUNDS [AGHT]

Binary Value Principle (BVP_n): $1 + x_1 + 2x_2 + 4x_3 + \cdots + 2^{n-1} x_n = 0$

Proof sketch

1. BVP_n easy for $IPS_{\mathbb{Q}}$ $\rightarrow$ BVP_n easy for $IPS_{\mathbb{Z}}$

2. Show $SS \rightarrow BVP_n$ hard for $IPS_{\mathbb{Z}}$

SHUB-SMALE CONJECTURE $\longrightarrow$ IPS LOWER BOUNDS [AgHT]

Binary Value Principle (BVP_n): $1 + \underbrace{x_1 + 2x_2 + 4x_3 + \dots + 2^{n-1}x_n}_{S_n} = 0$

<u>Proof sketch</u>

① BVP_n easy for $IPS_{\mathbb{Q}}$ $\rightarrow$ BVP_n easy for $IPS_{\mathbb{Z}}$

② Show SS $\rightarrow$ BVP_n hard for $IPS_{\mathbb{Z}}$:

assume $Q(\vec{x})(1+S_n) + \sum_{i=1}^{n} H_i(\vec{x})(x_i^2 - x_i) = M$, $M \neq 0$

$\Rightarrow Q(\vec{x})(1+S_n) = M$ for all $\vec{x} \in \{0,1\}^n$

$\Rightarrow \forall \vec{x} \in \{0,1\}^n$, $(1+S_n)$ ranges over all numbers in $[1, \dots, 2^n]$

$\Rightarrow M$ divides all numbers in $[1, \dots, 2^n]$

$\Rightarrow M^{2^n}$ divides $2^n!$

$\Rightarrow [Q(\vec{x})(1+S_n)]^{2^n}$ computes $M^{2^n} = m_n \cdot 2^n!$

$\therefore$ SS conjecture $\Rightarrow Q(\vec{x})$ has large size

IPS LOWER BOUNDS

* ① Subsystems of IPS (low depth/ multilinear) [FSTW '16]
* ② Shub-Smale Conjecture $\rightarrow$ superpoly IPS lower bounds [AGHT '20]
* ③ Unconditional lower bounds (very strong subsystem of IPS) [Alekseev '21]
* ④ $VP \neq VNP \Rightarrow$ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]

* Not for CNF formulas
* F_n is CNF but not known to be UNSAT

IPS LOWER BOUNDS

* ① Subsystems of IPS (lowdepth/multilinear) [FSTW '16]

* ② Shub-Smale Conjecture → superpoly IPS lower bounds [AGHT '20]

* ③ Unconditional lower bounds (very strong subsystem of IPS) [Alekseev '21]

* ④ $VP \neq VNP \Rightarrow$ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]

* Not for CNF formulas

* F_n is CNF but not known to be UNSAT

$VP \neq VNP \Rightarrow$ IPS LOWER BOUNDS [ST'21]

$F_n \stackrel{d}{=} LB_{IPS}(\text{"}VP \neq VNP\text{"})$ states that IPS cannot efficiently prove $VP \neq VNP$

Key Lemma [GP] proved IPS lower bounds $\Rightarrow VP \neq VNP$

[ST'21] prove this implication can be efficiently proven in IPS:

$$IPS \vdash^{poly} LB_{IPS}(\text{"}VP \neq VNP\text{"}) \rightarrow VP \neq VNP$$

$VP \neq VNP \Rightarrow$ IPS LOWER BOUNDS [ST'21]

$F_n \overset{d}{=} LB_{IPS}(\text{"}VP \neq VNP\text{"})$ states that IPS cannot efficiently prove $VP \neq VNP$

Key Lemma [GP] proved IPS lower bounds $\Rightarrow VP \neq VNP$

[ST'21] prove this implication can be efficiently proven in IPS:

$$IPS \vdash^{poly} LB_{IPS}(\text{"}VP \neq VNP\text{"}) \rightarrow \text{"}VP \neq VNP\text{"}$$

Assume $VP \neq VNP$ and $IPS \vdash^{poly} LB_{IPS}(\text{"}VP \neq VNP\text{"})$

Then by Key Lemma, $IPS \vdash^{poly} \text{"}VP \neq VNP\text{"}$, which contradicts soundness

$VP \neq VNP \Rightarrow$ IPS LOWER BOUNDS [ST'21]

$F_n \stackrel{d}{=} LB_{IPS}(\text{"}VP \neq VNP\text{"})$ states that IPS cannot efficiently prove $VP \neq VNP$

BUT F_n MAY NOT BE A TAUTOLOGY!

Q: HOW HARD IS IT TO PROVE ALGEBRAIC CIRCUIT LOWER BOUNDS?

Plausible Conjecture: "SAT $\not\subset$ P/poly" hard for Frege

New (Stronger) Conjecture: "Perm $\notin$ VNP" hard for IPS ?

RECENT CNF LOWER BOUNDS

earlier
PC Lower bounds: break under linear transformations

Theorem [Sokolov '21]

PC Lower bounds for random CNF even with extension axioms $\{y_i = 2x_i - 1\}$

Theorem [Impagliazzo, Mouli, P '21]

PC lower bounds even with a linear number of extension axioms, each of support size $o(n)$.

OPEN PROBLEMS

- IS IPS A SUPER PROOF SYSTEM?
  (Can it p-simulate all Cook-Reckhow pps's ?)
- RES(lin) LOWER BOUNDS
- ALGEBRAIC TFNP CLASSES?
  WHICH CLASS CORRESPONDS TO IPS CERTIFICATES?
- PROOF COMPLEXITY OF ALGEBRAIC CIRCUIT LOWER BOUNDS?

Thanks!