TODAY

① Algebraic / Semi-algebraic Proof Systems

IPS (Ideal Proof System)

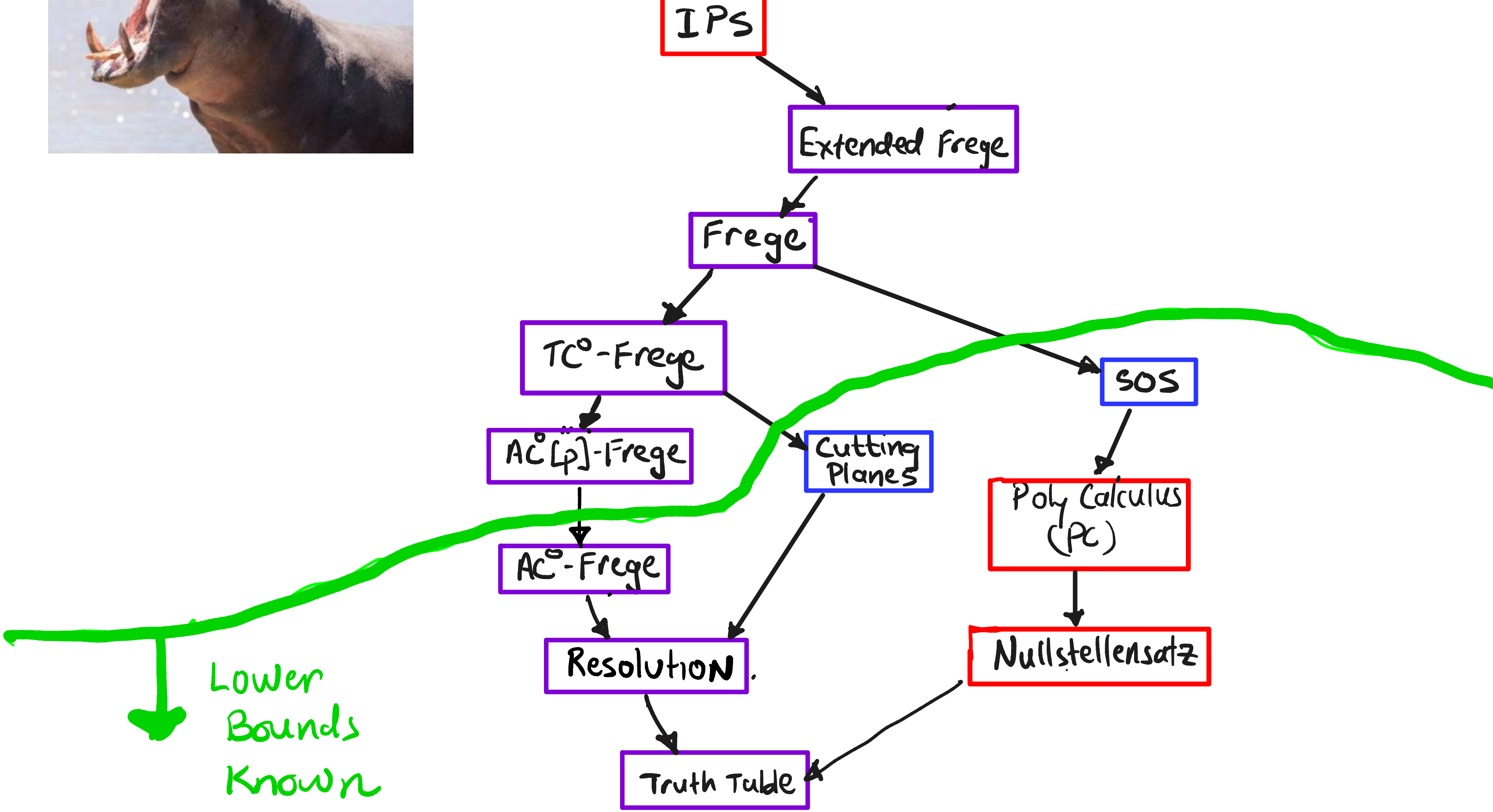
Subsystems of IPS : Nullsatz, Poly Calculus

Cutting Planes, SOS

② Other "Applications" : TFNP, Lower Bounds

③ Some open problems

THE PROOF COMPLEXITY ZOO



The Next Big Barrier

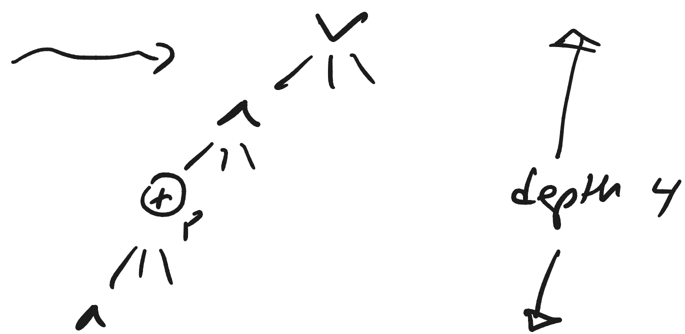
Prove superpolynomial lower bounds for $AC^0[p]$-Frege systems.

- 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

Mystery of $AC^0[p]$

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

$AC^0[p]$
depth d

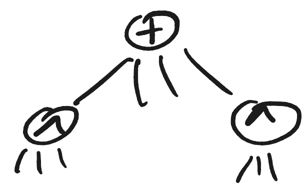


(2) Method of probalistic polys [Smolensky, Razborov] doesn't seem to work

Mystery of $AC^0[p]$

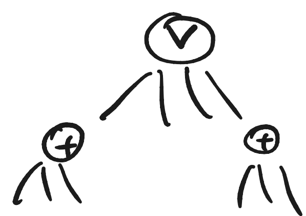
③ Two special cases:

Poly calculus:



Lines are polynomials

$\text{Res}(\oplus_p)$:



UNSOLVABILITY OF POLYNOMIAL EQUATIONS

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

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

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 $P = \{ p_1(\vec{x})=0,\ p_2(\vec{x})=0,\ \dots,\ p_m(\vec{x})=0 \}$,
certify there is no solution satisfying all equations over $\mathbb{F}$

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

$$C = C_1 \wedge C_2 \wedge \dots \wedge C_m \longrightarrow P_C = \{ p_1 = 0, \dots, p_m = 0, \{x_i^2 - x_i = 0\} \}$$

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

NULLSTELLENSATZ

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

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

- $\{q_1 \ldots q_m\}$ IS A NSATZ PROOF OF UNSOLVABILITY
- COMPLEXITY: MAX DEGREE / MONOMIAL SIZE
- FOR CNF SYSTEMS, q_i's ARE MULTILINEAR

POLYNOMIAL CALCULUS (PC)

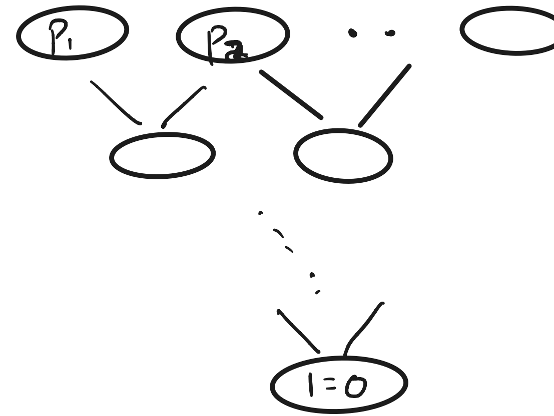
PC is a **dynamic** version of Nullsatz

Axioms: $p_i \in \mathcal{P}$ (initial polynomials)

Rules: $f=0,\ g=0 \implies f+g=0$

$f=0 \implies fg=0$

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)

Example: (Negation of) Induction

$\neg IND_n$:

$$(1-x_1)=0$$

$$(x_1)(1-x_2)=0$$

$$(x_2)(1-x_3)=0$$

$$(x_3)(1-x_4)=0$$

$$\vdots$$

$$(x_{n-1})(1-x_n)=0$$

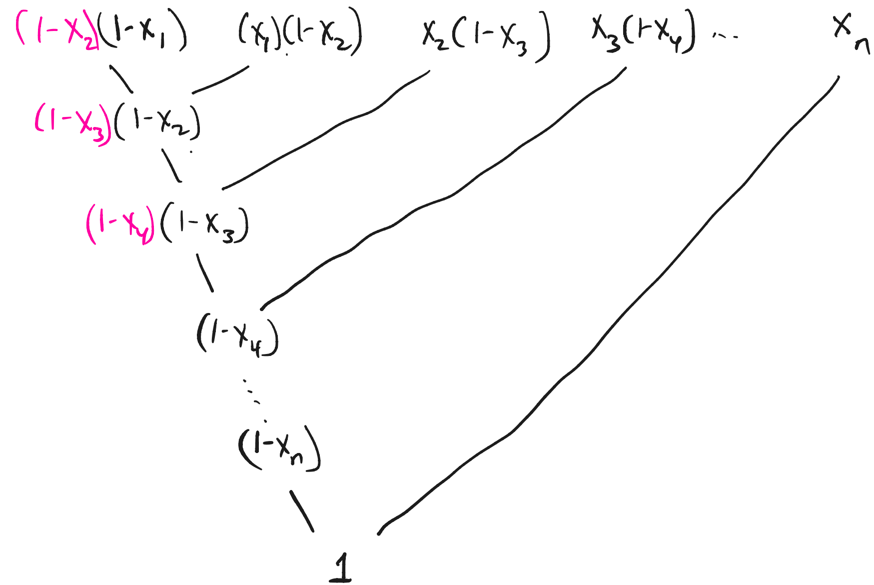
$$x_n=0$$

Example: (Negation of) Induction

$\neg \mathrm{IND}_n$:

$$(1-x_1)=0$$
$$(x_1)(1-x_2)=0$$
$$(x_2)(1-x_3)=0$$
$$(x_3)(1-x_4)=0$$
$$\vdots$$
$$(x_{n-1})(1-x_n)=0$$
$$x_n=0$$

PC refutation of degree 2:

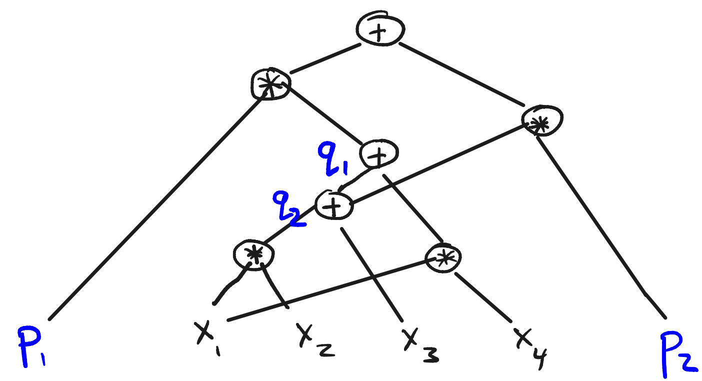


Nsatz requires degree $\Omega(\log n)$ [Buss-P]

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

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



PC/NSATZ $\xrightarrow[\text{generalizes to}]{}$ IPS [P96, P98, GP14]

SOS $\longrightarrow$ CONE PROOF SYSTEM

[Alekseev, Grigoriev, Hirsh, Tzameret '20]

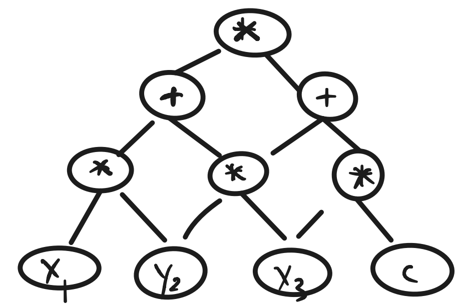
IPS (cont'd)

An IPS certificate/proof of unsolvability of $\mathcal{P} = \{p_1(\vec{x})=0, \dots, p_m(\vec{x})=0\}$ (over $\mathbb{F}$) is an algebraic circuit $C(x_1, \dots, x_n, y_1 \dots y_m)$ such that:

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

(2) $C(x_1, \dots, x_n, p_1(\vec{x}), \dots, p_m(\vec{x})) = 1$

$C(\vec{x}, \vec{y})$



(1) and (2) imply that 1 is in the ideal generated by $\mathcal{P} = \{p_1 = 0, \dots, p_m = 0\}$

(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 <u>not</u> poly-bounded:

<u>Lemma</u> IPS poly-bounded $\rightarrow$ coNP = MA

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:

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

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 $VP \neq VNP$

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

LOWER BOUNDS FOR IPS SUBSYSTEMS

* ① Restrictions of IPS (e.g., multilinear) [FSTW '16]

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

* ③ Superpoly lower bounds on bit complexity [Alekseev '21]

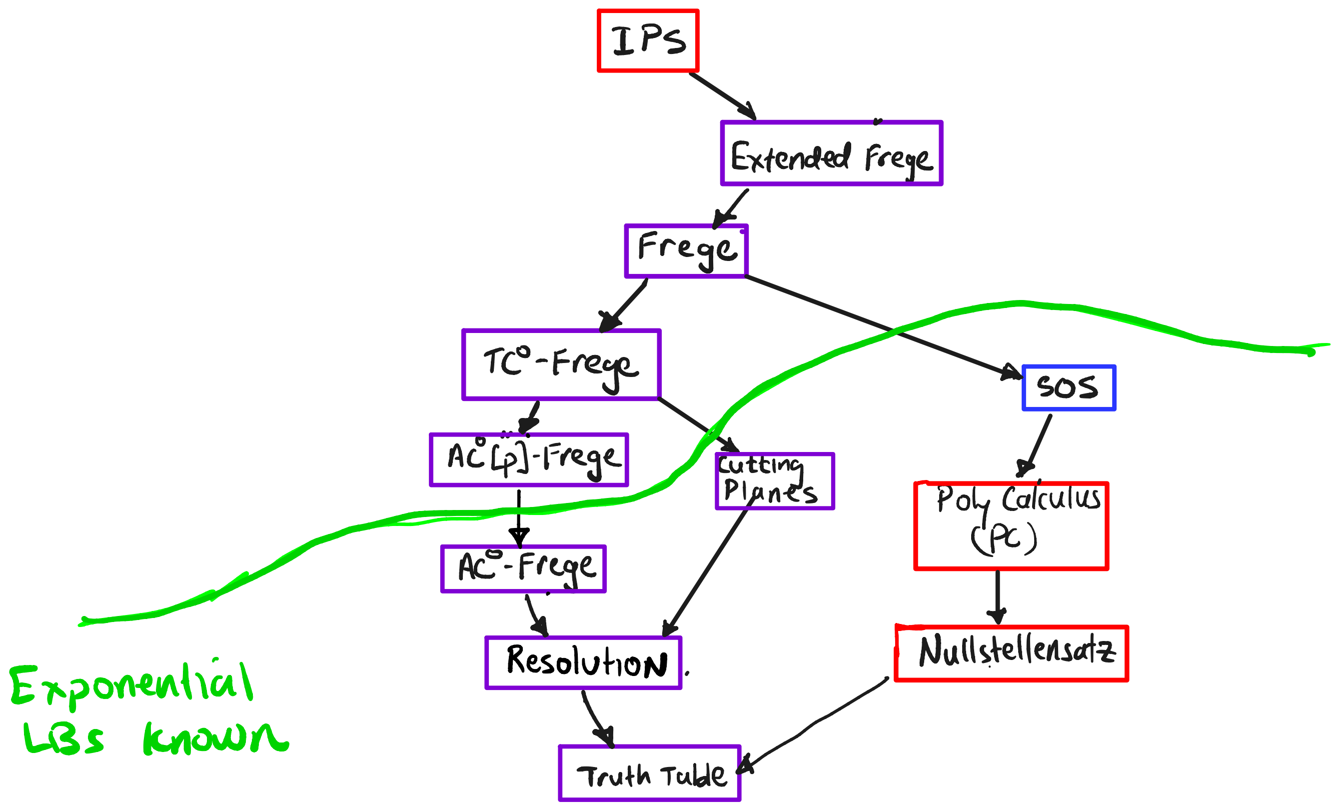
* ④ $VP \neq VNP \Rightarrow$ superpoly IPS lower bounds for $\{F_n\}$ [ST '21]

* 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



SEMI-ALGEBRAIC PROOF SYSTEMS

- SEMI-ALGEBRAIC PROOF SYSTEMS CERTIFY UNSOLVABILITY OF A SYSTEM OF POLYNOMIAL INEQUALITIES OVER $\mathbb{R}$

given $P = \{ p_1(\vec{x}) \geq 0, \ p_2(\vec{x}) \geq 0, \ \ldots, \ p_m(\vec{x}) \geq 0 \}$,
certify there is no solution satisfying all equations over $\mathbb{R}$

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

$$C = C_1 \wedge C_2 \wedge \ldots \wedge C_m \longrightarrow P_C = \{ p_1, \ldots, p_m, \ x_i^2 - x_i \geq 0 \}$$

$$C_i = (x_1 \vee x_2 \vee \bar{x}_4) \longrightarrow p_i : \ x_1 + x_2 + (1 - x_4) - 1 \geq 0$$

SOS

Let $\mathcal{P} = \{ p_1(x) \geq 0, \ldots, p_m(x) \geq 0 \}$ be a system of polynomial inequalities obtained by translating an UNSAT CNF.

Then $\mathcal{P}$ is unsatisfiable over $\mathbb{R}$

iff there exists sum-of-squares polys $q_0, q_1, \ldots, q_m$ such that

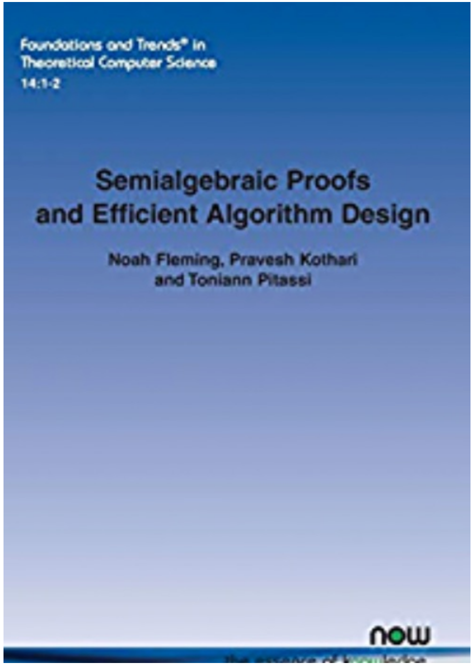
$$q_0 + \sum_{i=1}^{m} q_i(x)\, p_i(x) = -1$$

- COMPLEXITY: MAX DEGREE / MONOMIAL SIZE

- A flurry of degree Lower Bounds for Nullstellensatz, Poly Calculus, SA, SOS

- SOS mania:

  SOS upper bounds $\Rightarrow$ learning algs (via automatizability)



PC autom.
SOS automatizability

wrt degree

$\exists$ alg A_{SOS} s.t. $\forall$ $P = \{P_1 \dots P_m\}$, if

~~if~~ $\exists$ a degree d $\overset{\text{SOS}}{\text{refut}}$ of $\{P_1 \dots P_m\}$

then ~~$\exists$ alg~~ A outputs an SOS ref

in time $n^{O(d)}$

degree d has $\mathrm{poly}(n^d)$

THE AMAZING USEFULNESS OF SOS : LOWER BOUNDS

LOWER BOUNDS IMPLY LOWER BOUNDS FOR A BROAD CLASS OF ALGORITHMS

[LRS'15, CLRS'16] LP/SDP EXTENSION COMPLEXITY OF Δ $\approx$ SA/SOS DEGREE OF P_Δ

[RPRC'16, PR'18] MONOTONE FORMULA SIZE / SPAN PROGRAM SIZE $\approx$ NSATZ DEGREE

[GGKS'18] MONOTONE CIRCUIT SIZE $\approx$ PC DEGREE

THE AMAZING USEFULNESS OF SOS : UPPER BOUNDS

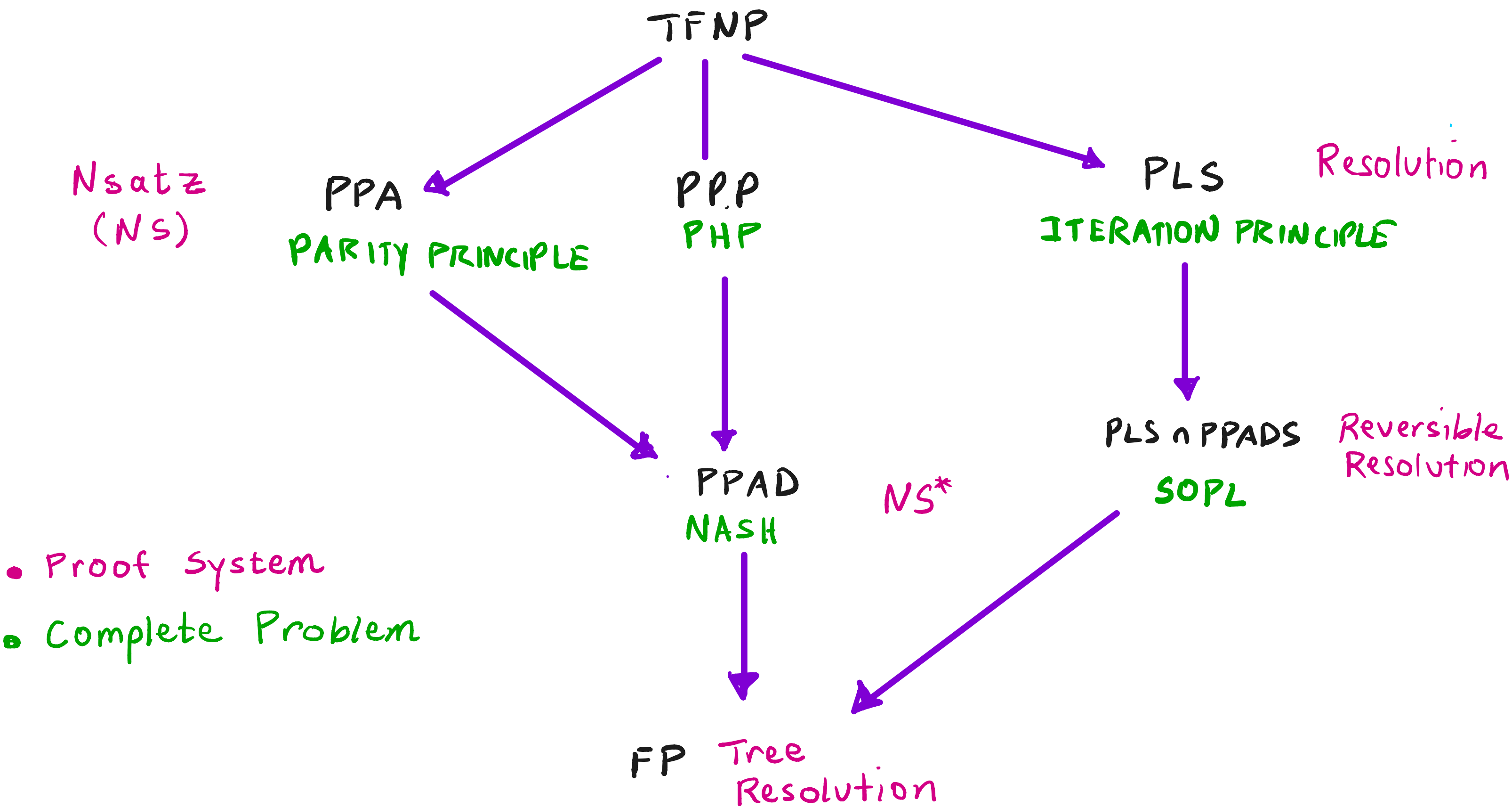
UPPER BOUNDS CAN AUTOMATICALLY GENERATE EFFICIENT ALGS!

- PC / SA / SOS are automatizable: degree d proofs can be found in time $n^{O(d)}$

$\therefore$ Low degree proofs certifying the mere existence of a solution automatically give ptime algorithms

- Dictionary Learning [BKS'15]
- Tensor completion [BM16, PS17]
- Tensor decomposition [MSS16]
- Robust moment estimation [KS17]
- Clustering [HL18] [KS17]
- Robust linear regression [KKM18]

PROPOSITIONAL PROOFS & TFNP



Some open Problems

(1) Nontrivial size Lower bounds for Frege / Extended Frege

$AC^0[p]$ - Frege Lower Bounds

(even under plausible assumptions)

(2) Random K-CNF Lower Bounds : Cutting Planes

AC^0 Frege

Weak PHP Lower bounds : AC^0 - Frege

(3) Separate depth-d Frege + depth d+1 - Frege

(with CNF formulas)

(4) "Average-case" TFNP separations or equivalences
(+ crypto)

(5) UPPER BOUNDS

PCP Theorem in polysized/quasipoly size Frege?

Refutation Algorithm for random 3CNF, $m = n^{1.4}$