Some Open Problems
in Proof Complexity

Susanna F. de Rezende

LTH, Lund University

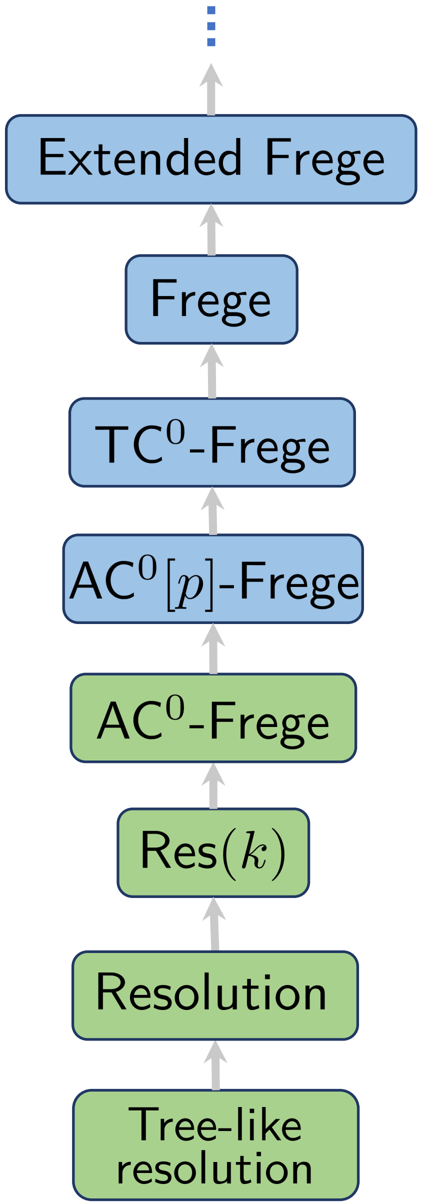
FOCS ’21 Workshop:
Reflections on Propositional Proofs in Algorithms and Complexity

Origin of proof complexity: NP vs coNP problem

Is there a polynomially-bounded proof system?

Is there an optimal proof system?

Related to many different topics: classical proof theory, finite model theory, structural complexity theory, …
(see Krajíček’s book “Proof Complexity”)



Lower bounds for strong proof systems

Prove superpoly lower bounds for Extended Frege, Frege, TC^0-Frege, $\mathsf{AC}^0[p]$-Frege.

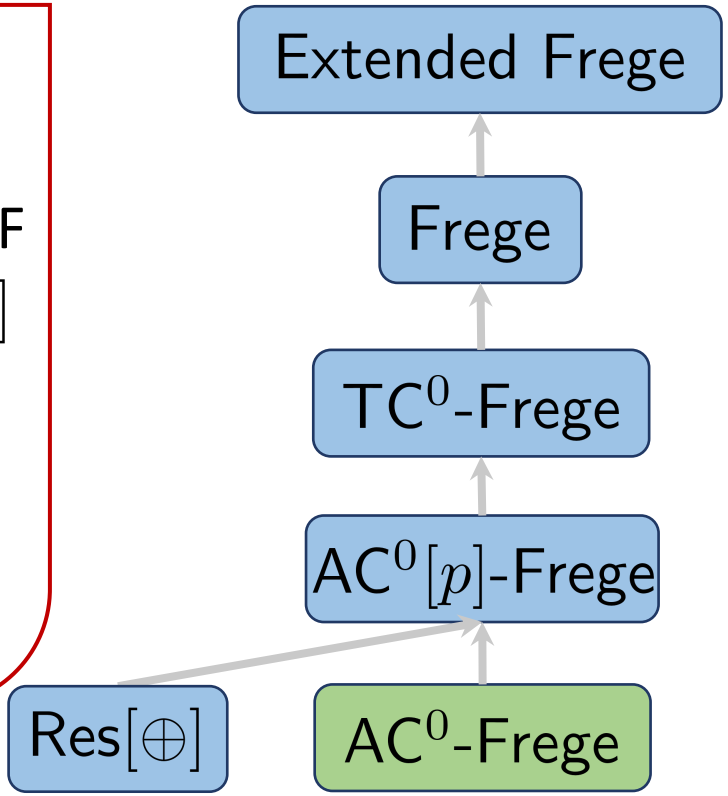
- Conditional lower bounds

(using a conjecture that does not imply NP ≠ coNP)

- Superlinear lower bound for CNF or superquadratic for any F
- Lower bounds for subsystems of $\mathsf{AC}^0[p]$-Frege, e.g., $\mathsf{Res}[\oplus]$
- exponential separation between depth-d and depth-$(d+1)$ Frege for k-CNFs

Initial case: $\mathsf{Res}(\log)$ from AC^0-Frege

- And analogous questions in bounded arithmetic



See, e.g., Krajíček's book and Pudlák's "Twelve Problems in Proof Complexity"

Algebraic proof complexity

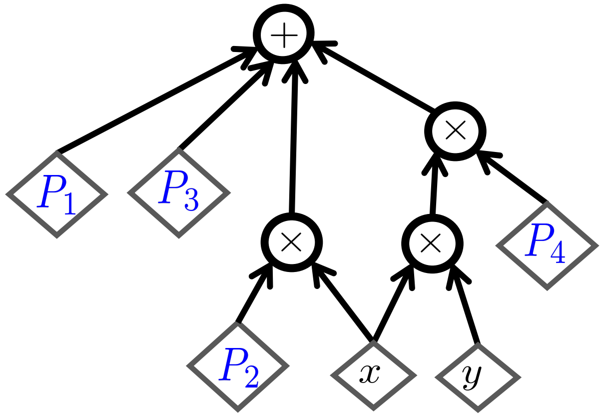
Polynomials $\{P_1 = 0, P_2 = 0, \ldots, P_m = 0\}$ in $\mathbb{F}[x_1, \ldots, x_n]$

e.g., $\{1-x\,,\ \ 1-y\,,\ \ xy(1-z)\,,\ \ z\}$

NS refutation: $\sum_{i\in[m]} Q_i P_i = 1$

e.g., $\boxed{1}\cdot(1-x)+\boxed{x}\cdot(1-y)+\boxed{1}\cdot xy(1-z)+\boxed{xy}\cdot z=1$

IPS refutation:



Ideal Proof System (IPS)
And others (e.g. CPS)

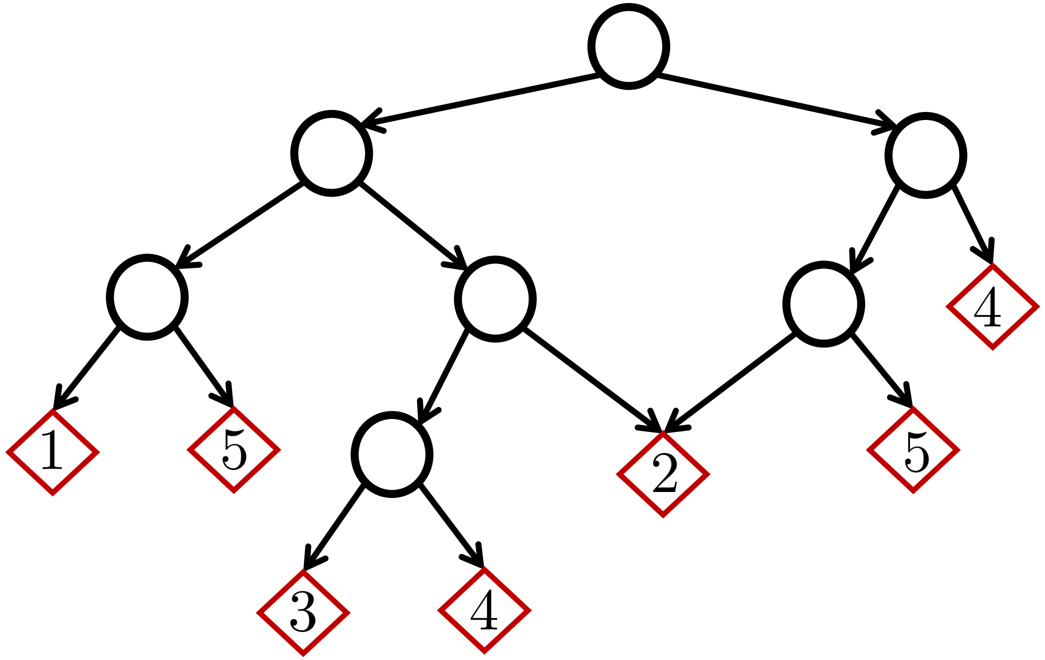
Prove lower bound for (some restriction of) IPS for CNF formulas.

Improve [Andrews, Forbes ‘22]: superpoly lbs for constant-depth IPS for input polys that also have constant depth and poly size.

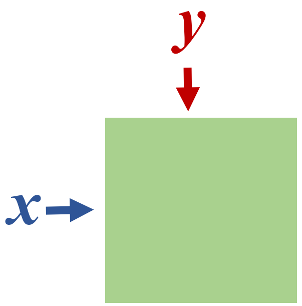
Can extended Frege simulate IPS?
What is the proof complexity of polynomial identity testing (PIT)?

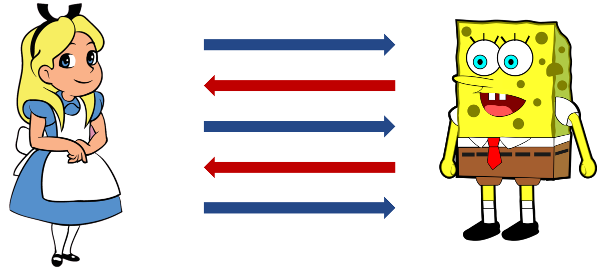
See Pitassi’s and Grochow’s earlier talks

Monotone protocols

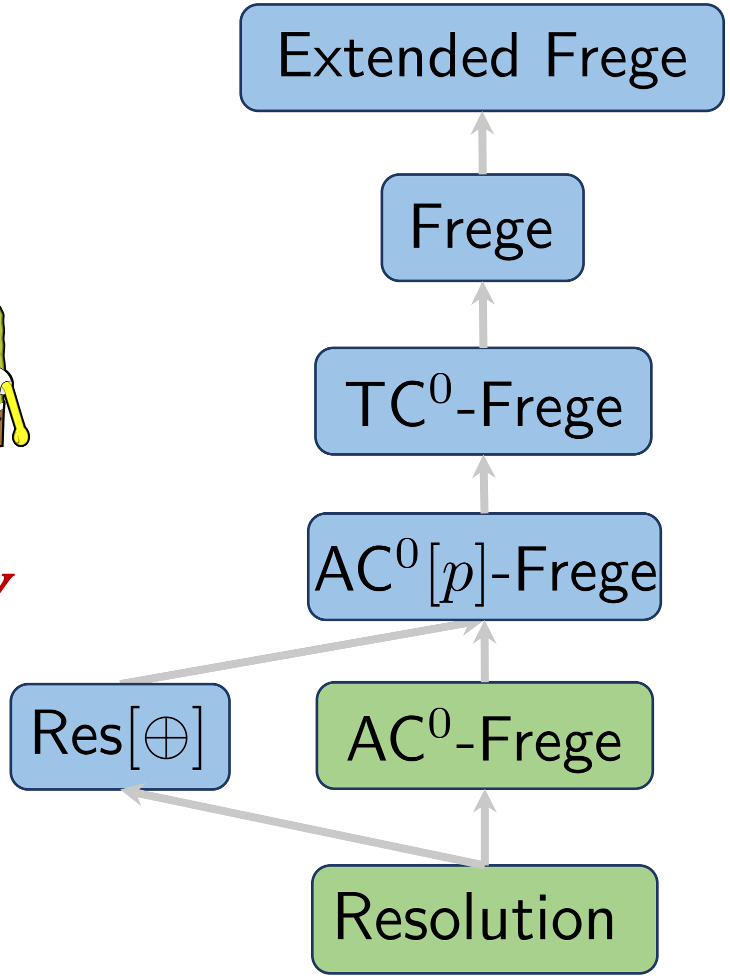


Matrix: $X \times Y$





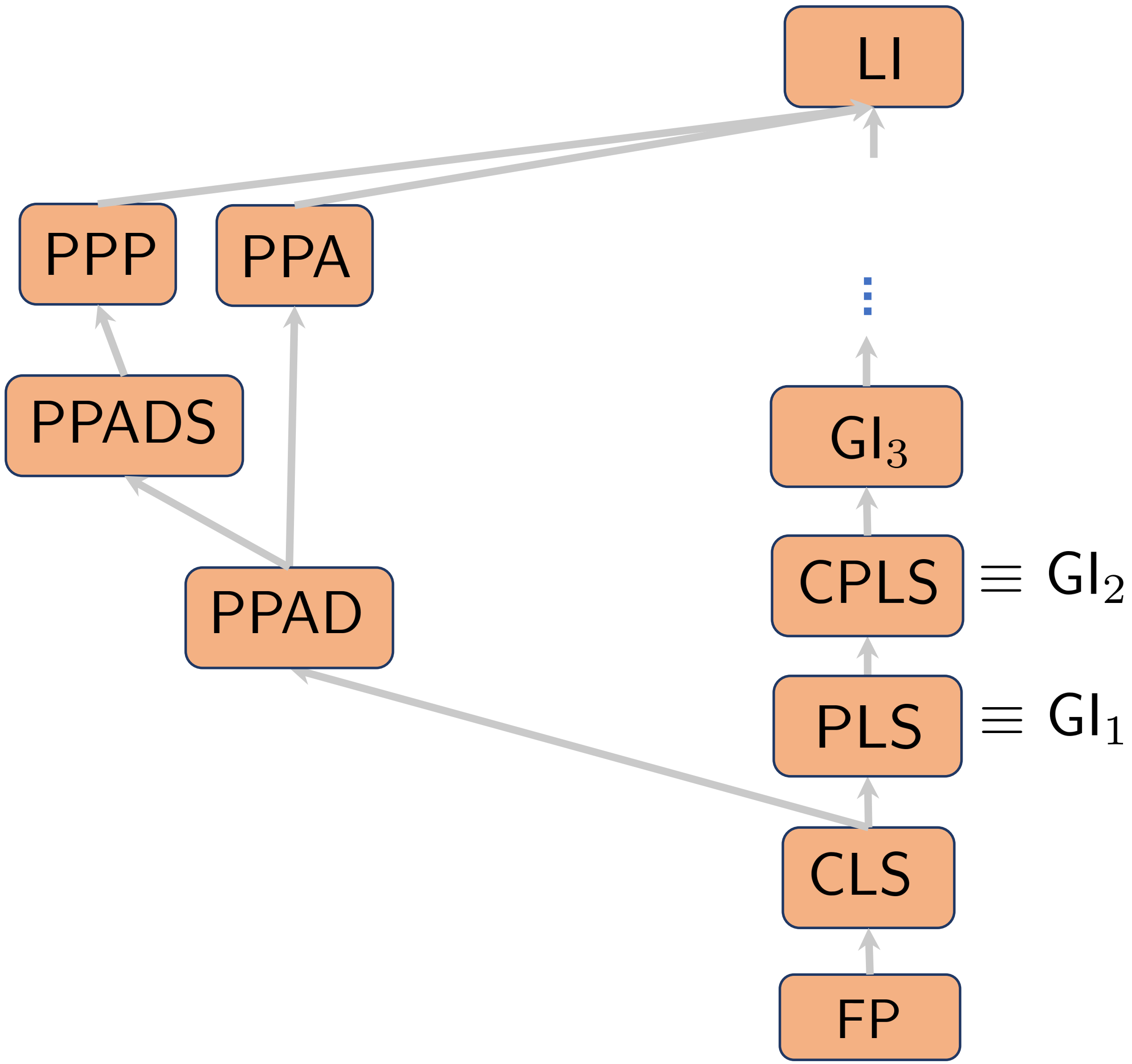
$x \in X$ $y \in Y$



Prove lower bound for monotone protocols solving mKW (with two rounds of real communication per node).

See, e.g., Krajíček's book and Folwarczný '22 "On Protocols for Monotone Feasible Interpolation"

TFNP classes



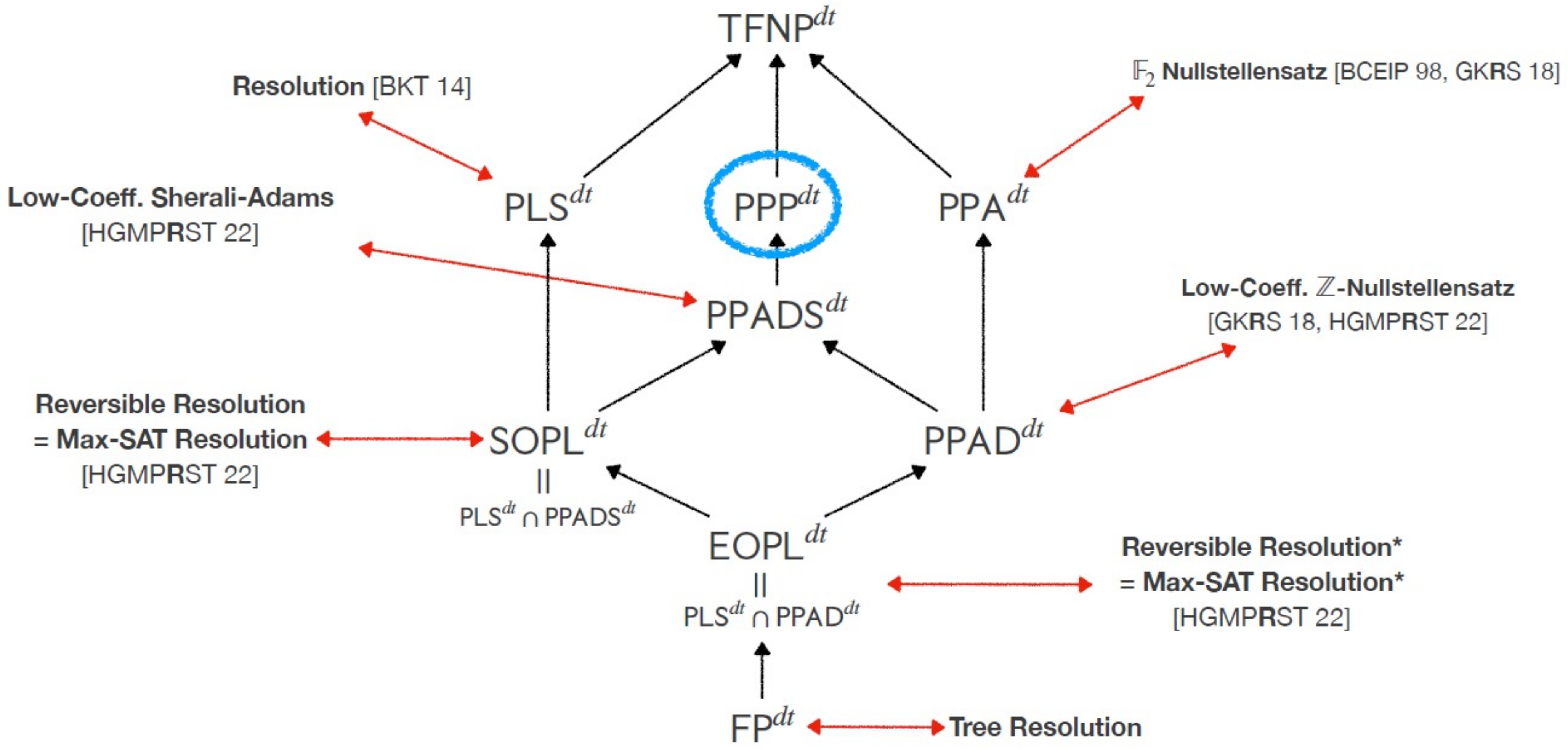
Are there "simpler" characterizations of $\mathsf{GI}_{\boldsymbol{k}}$?

Prove relativized separation between $\mathsf{GI}_{\boldsymbol{i}}$ and $\mathsf{GI}_{\boldsymbol{i+1}}$.

$\equiv$ better-than-quasipoly separation between depth-$\boldsymbol{d}$ and depth-$(\boldsymbol{d}+\mathbf{1})$ Frege for $\boldsymbol{k}$-CNFs

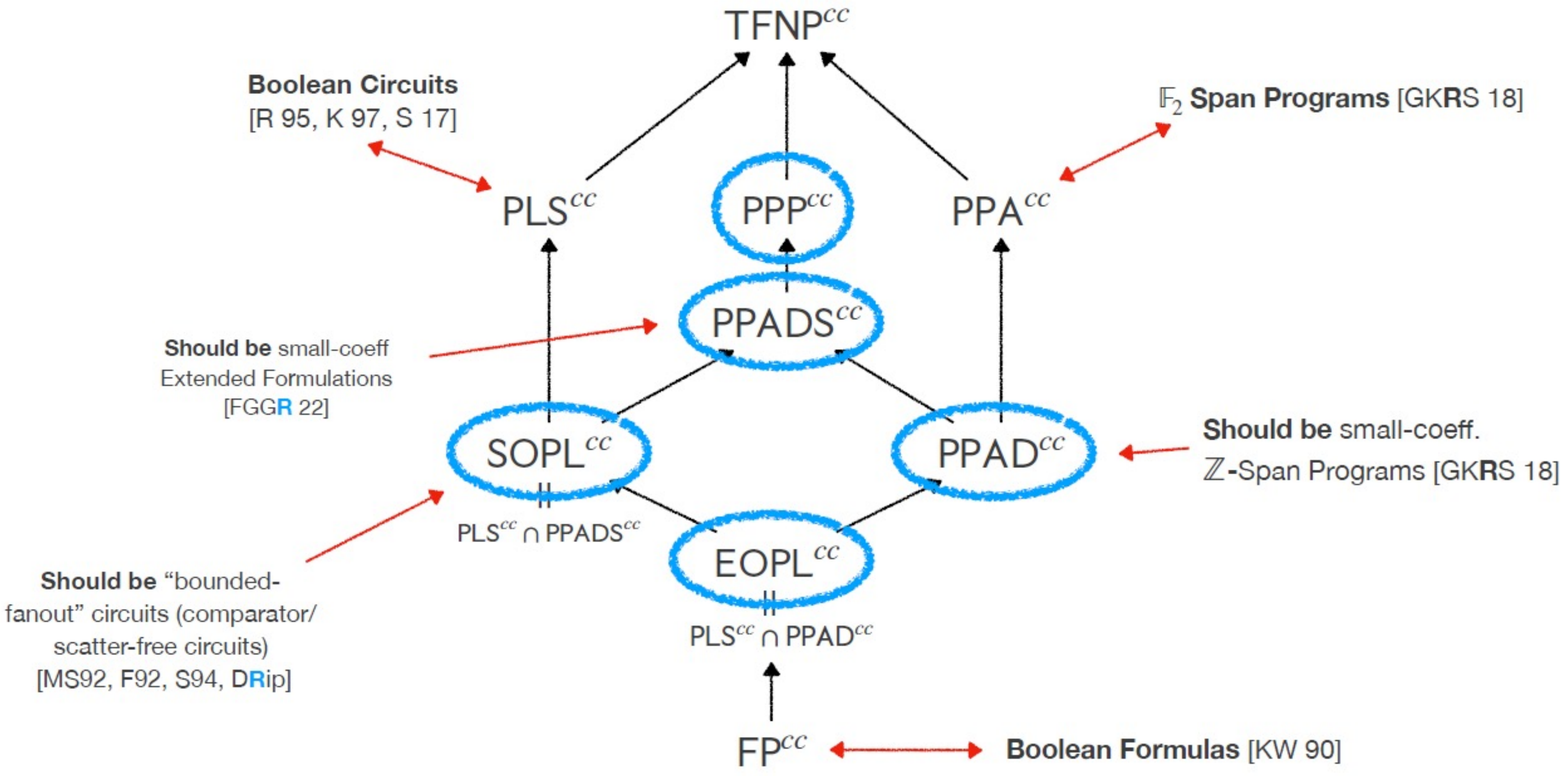
See earlier talks on TFNP (Thapen, Buss and Robere)

TFNP classes



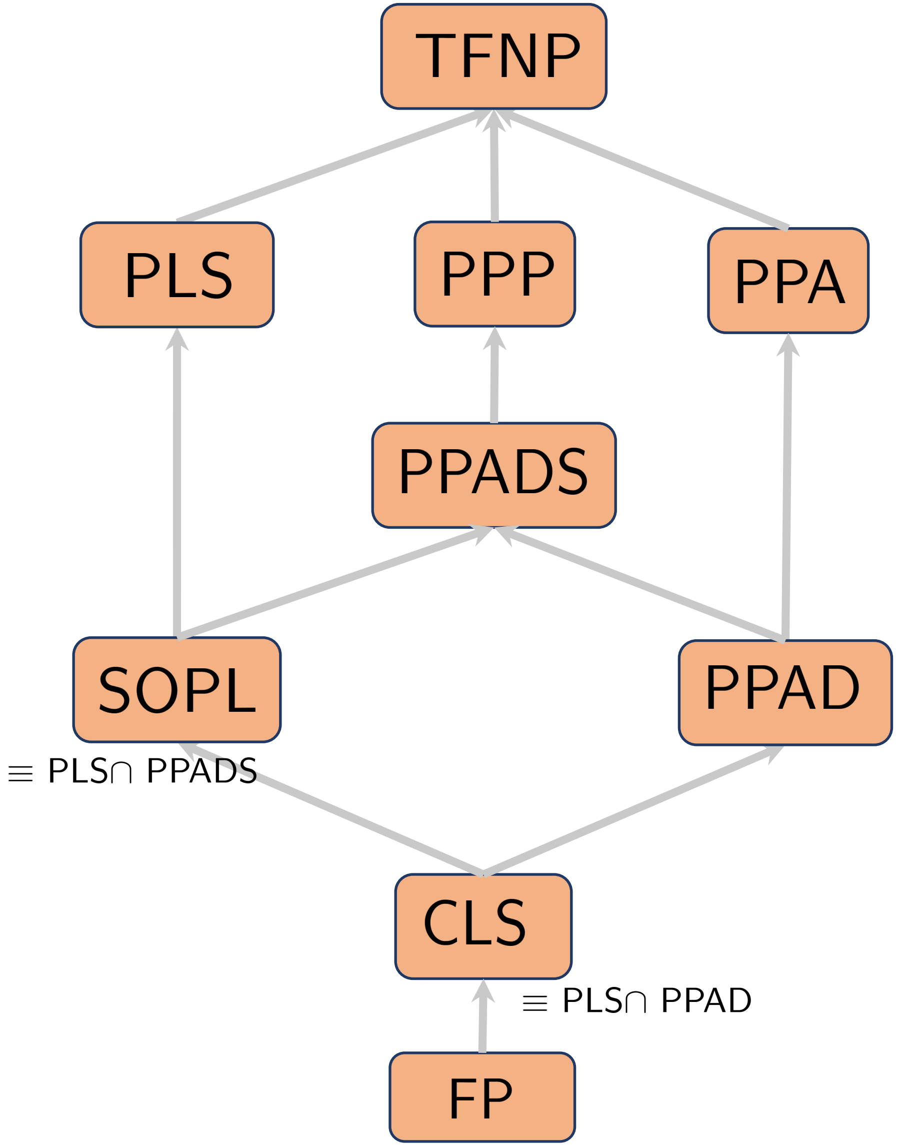
See earlier talks on TFNP (Thapen, Buss and Robere)

TFNP classes



See earlier talks on TFNP (Thapen, Buss and Robere)

TFNP classes



Are there “simpler” characterizations of GI_k?

Prove relativized separation between GI_i and GI_{i+1}.

$\equiv$ better-than-quasipoly separation between depth-d and depth-$(d+1)$ Frege for k-CNFs

Complete the picture: separations, relations to proof, circuit, and communication

Other intersection results?

(e.g. Max-SAT resolution = resolution ∩ unary-SA)

Lifting for non-monotone circuit lower bounds?

Is there a class that captures SOS?

Is there a class beyond TFNP that capture IPS?

Can we characterize CP, LS in terms of TFNP?

See earlier talks on TFNP (Thapen, Buss and Robere)

Interesting formulas

- Random $\boldsymbol{k}$-CNF formulas

  E.g. for cutting planes, AC^0-Frege

- Combinatorial formulas (e.g. coloring, Ramsey Theorem)

- Weak PHP

  Does AC^0-Frege have poly-size proofs of WPHP_n^{2n} or $\mathrm{WPHP}_n^{n^2}$?

  Does PC have poly-size proofs of $\mathrm{WPHP}_n^{n^2}$?

- Proof complexity generators

  NW-generator, Krajíček's gadget generator, truth table generator

- Reflection principle

Understanding different complexity measures

Complexity measures: size, width/degree, depth, space, …

Are some measures polynomially equivalent?

Trade-offs

Can we minimize measures *simultaneously*?

∃ formulas s.t. any minimal-size proof must have superlinear depth/space?
E.g. Tseitin formulas for cutting planes?

∃ functions s.t. any minimal-size (monotone) circuit must have superlinear depth?
E.g. Matching for monotone circuits?

See, e.g., Papamakarios-Razborov ‘21, Razborov ‘16, Fleming-Pitassi-Robere ‘22

Proof Search (Automatability)

P vs NP

1. Do all tautologies admit poly-size $\boldsymbol{P}$-proofs?
2. If a tautology admits poly-size $\boldsymbol{P}$-proofs, can we find one in poly-time?

$\boldsymbol{P}$ is *automatable* if $\exists$ algorithm s.t.

Tautology $\boldsymbol{T}$ ➡ **poly-time algorithm** ➡ $\boldsymbol{P}$-proof of $\boldsymbol{T}$

runs in **poly-time**($|\mathrm{T}|$ + size of smallest $\boldsymbol{P}$-proof)

Is $\boldsymbol{P}$ automatable?
(assuming P $\neq$ NP)
E.g., sum-of-squares, AC_0-Frege

$\boldsymbol{P}$ is *weakly-automatable* if $\exists$ algorithm s.t.

Tautology $\boldsymbol{T}$ ➡ **poly-time algorithm** ➡ $\boldsymbol{Q}$-proof of $\boldsymbol{T}$

runs in **poly-time**($|\mathrm{T}|$ + size of smallest $\boldsymbol{P}$-proof)

Is resolution weakly-automatable?

Proof Search (Information Complexity)

Is there an optimal way to search for proofs?

if A outputs P-proofs then $\text{time}_A(T) \geq \Omega(2^{i_P(T)})$

$\forall$ proof systems P, $\exists$ A_P s.t. $\text{time}_{A_P}(T) \leq 2^{O(i_P(T))}$

$i_P(T)$: information efficiency function ("What do tautologies know about their proofs?")

size smallest P-proof of $T \leq \text{time}_{A_P}(T) \leq 2^{O(i_P(T))}$

For P for which we don't have size lower bounds, prove strong (super-log) lower bound for $i_P(T)$.

Is it easier to prove lower bounds for $i_P(T)$ than for size?

See Krajíček 's earlier talk & Krajíček '21 "Information in propositional proofs and algorithmic proof search"

Meta-complexity

Why is it hard to prove lower bounds?

$\exists$ distribution $\boldsymbol{D_n}$ over formulas believed to be hard for Extended Frege s.t. under a standard complexity-theoretic conjecture, for $\boldsymbol{F} \sim \boldsymbol{D_n}$ w.h.p. EF cannot prove super-poly EF size lower bounds?

Show that Buss's theory $\boldsymbol{S_2^1}$ cannot prove that NP is average-case hard for coNP/poly.

Show that proof system $\boldsymbol{P}$ cannot prove that SAT is not in P/poly.

Known for resolution and (low-degree) PC

See Rahul Santhanam's earlier talk

Average-case algorithm design

Can you beat the spectral threshold in poly time?

Poly time algo to weak ref. random 3-SAT with $n^{1.5} / \log\log\log\log(n)$ constraints?

=

$f(\ell)n^{O(1)}$ time algo to $\ell \log n$ length cycle in random 3-uniform hypergraph with $n^{1.5}/\ell$ edges?

Will beat known lower bounds for restricted algorithms etc. but no “actual” barrier.

See Pravesh Kothari’s earlier talk