Separations and Intersections in Proof Complexity and TFNP

Robert Robere, McGill


Mika Göös

Siddhartha Jain
Gilbert Maystre


EPFL


Alexandros Hollender

Oxford


William Pires

Ran Tao

McGill

Part 1:

Resolution vs. Sherali-Adams

Resolution Refutation

"clause" := disjunct of literals

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ is an unsatisfiable CNF formula
- Interested in the complexity of the "simplest" refutation of F.
- A resolution refutation of F is a sequence of clauses

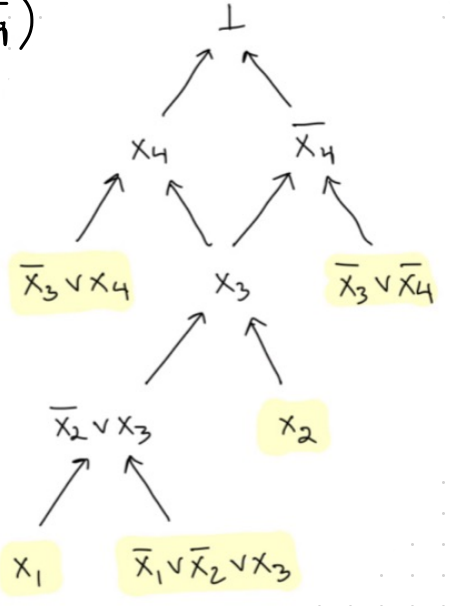
$$\pi := (B_1, B_2, \cdots, B_s = \bot)$$

s.t. $B_i \in F$ or B_i is deduced from earlier clauses via

Resolution $\dfrac{C \vee x \quad D \vee \overline{x}}{C \vee D}$ $\qquad$ $\dfrac{C}{C \vee \ell}$ Weakening

Resolution Refutation: Example

- Handy to draw these as as dags:
- $F = x_1 \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_3 \vee x_4) \wedge x_2 \wedge (\bar{x}_3 \vee \bar{x}_4)$
- Width $\equiv 3$ (size of largest clause)
- Length $\equiv 10$ (# of clauses)



Resolution Refutation: Complexity Measures

- Let $\pi = (B_1, \cdots, B_s = \bot)$ be a Resolution refutation of F
- Width of π, $w(\pi) := \max_i |B_i|$
- Length of π, $L(\pi) := s$
- $Res(\pi) := w(\pi) + \log L(\pi)$
- $Res(F) := \min_\pi Res(\pi)$

} Joint complexity measure is atypical.
low-width and low-size proofs

- "Efficient" means $Res(\pi) = \log^{O(1)} n$

Resolution Refutation: Background

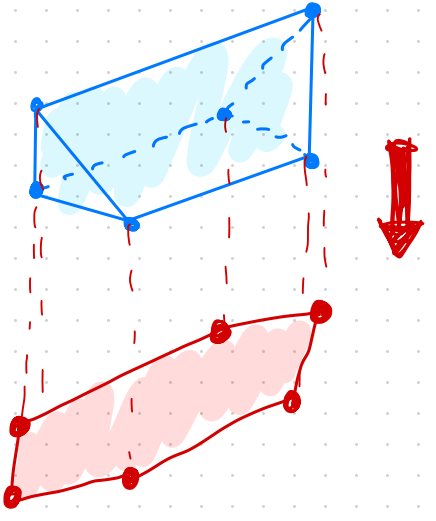
- Probably the most well-studied propositional proof system.
- Forms the "base" system for modern CDCL SAT solvers.
  - Automatability
- Strengths and limitations are very well-understood.
  - Exponential length lower bounds for $O(1)$-width CNFs [Urq]
  - "Size-width" relation: width LBs $\Rightarrow$ size LBs [BSW]
  - Tradeoffs between many measures

Sherali-Adams: History

- Introduced in the context of linear programming [SA]
  Given an LP $P \subseteq [0,1]^n$ for approximation problem, can we automatically generate a better one?

- Closely related to extended formulations [Yann]

- Strong lower bounds known for size and degree for $O(1)$-width CNFs and many natural optimization problems (e.g. Max Cut, Colouring, ...)



Sherali-Adams (SA) Proofs: Background

- $\mathcal{J} \overset{syn}{:=} \sum_i \lambda_i D_i$ is a conical junta (i.e. $\mathcal{J} \in$ cone(conjuncts))
  - $\lambda_i \geq 0$, $\lambda_i \in \mathbb{R}$
  - D_i: conjunction of literals e.g. $D_i = x_1 \wedge \bar{x}_2 \wedge x_3 = x_1(1-x_2)x_3$
- $\mathcal{J}$ is integral if $\lambda_i \in \mathbb{Z}$, degree of $\mathcal{J}$ is $\max_i |D_i|$
- $f : \{0,1\}^n \to \mathbb{R}_{\geq 0}$ then $\deg^+(f) :=$ minimum degree of conical junta $\mathcal{J}$ s.t. $f = \mathcal{J}$
- Note $\deg^+(f) \leq n$: $f(x) = \sum_{y \in \{0,1\}^n} f(y) [\![y = x]\!]$ → width-n conjunct

Sherali-Adams (SA) Proofs

- $F = C_1 \wedge \cdots \wedge C_m$ is an unsat CNF over $x_1, \cdots, x_n$
- A Sherali-Adams refutation Π of F is an expression:

$$\sum_{i=1}^{m} p_i \overline{C}_i + \mathcal{I} \overset{syn}{=} -1$$

- $p_i \in \mathbb{Z}[x_1, \cdots, x_n]$ multilinear poly
- $\overline{C}_i$ is the conjunction of negated lits in C
- $\mathcal{I}$ is an integral conical junta

$\mathcal{I} \in \text{cone}_{\mathbb{Z}}(\text{conjunctions})$

- All arithmetic is multilinear (mod $x_i^2 = x_i$)

e.g. $x_1(x_1 + x_2 - 3x_1x_2) = x_1 - 2x_1x_2$

Sherali-Adams (SA) Proofs

$$\sum_{i=1}^{m} p_i \overline{C}_i + \mathcal{I} = -1$$

- Why is this a refutation?

If $\exists x \in \{0,1\}^n : F(x) = 1$ then

$$-1 = \sum_{i=1}^{m} p_i(x)\,\overline{C}_i(x) + \mathcal{I}(x)$$

$$= 0 + \geq 0 \quad \text{Contradiction!}$$

- Completeness also holds. (We'll see this in a second)

Sherali-Adams : Complexity Measures

$$\sum_{i=1}^{m} p_i(x)\,\overline{C}_i(x) + \mathcal{I}(x)$$

- Degree of $\Pi := \max \deg(p_i \overline{C}_i), \deg^+(\mathcal{I})$
- Size of $\Pi := \underbrace{\sum \text{size}(p_i \overline{C}_i) + \text{size}(\mathcal{I})}_{\text{bit length of encodings of } \Sigma \text{ monomials}} = O(\log \overbrace{c(\Pi)}^{\text{largest coeff. in } \Pi} \underbrace{\text{msize}(\Pi)}_{\substack{\#\text{ monomials} \\ \text{before} \\ \text{cancellation}}})$
- $SA(\Pi) := \deg(\Pi) + \log \text{size}(\Pi)$
- $SA(F) := \min_{\Pi} SA(\Pi)$

} Joint complexity measure is atypical

- Efficient is $SA(F) = \log^{O(1)} n$

Sherali-Adams vs. Resolution

- Known: Sherali-Adams can efficiently* simulate Resolution:

Thm [OMR09] For any unsat CNF F, $SA(F) = O(Res(F))$.
Precisely: width-w, length-L Res $\Rightarrow$ degree-w, size $2^{O(w)} O(L)$ SA

- Note: $SA(F) \leq w + \log\left(2^{O(w)} O(L)\right) = O(w + \log L) = O(Res(F))$

- Recall $\text{size}_{SA}(\pi) = O(\log c(\pi) \, \text{msize}(\pi))$ $\left(= 2^{O(w)} O(L)\right)$

- This theorem does produce proofs with exponentially large coefficients.

Main Question: Are large coefficients necessary?

Large Coefficients in SA

- Every unsat CNF F has a degree-n, size-$2^{O(n)}$ proof with $O(1)$-size coefficients:

Pf. $F = C_1 \wedge \cdots \wedge C_m$ then

width-n conjunct

$$-1 = \sum_{y \in \{0,1\}^n} -[\![y = x]\!]$$

$$= \sum_{y \in \{0,1\}^n} -p_y(x)\,\overline{C}_y(x)$$

← C_y is any clause in F falsified by y

- Explains the joint measure $\deg(\pi) + \log \text{size}(\pi)$: a tradeoff between degree and coefficient size is inherent.

Unary Sherali-Adams vs. Resolution

$\text{size}_{SA}(\pi) \approx \Theta(\log c(\pi)\ \text{msize}(\pi))$

- If π is a Sherali-Adams proof define

$$\text{size}_{uSA}(\pi) := c(\pi)\ \text{msize}(\pi)$$

$$uSA(\pi) := \deg(\pi) + \log \text{size}_{uSA}(\pi)$$

$$uSA(F) := \min_{\pi} uSA(\pi)$$

- Equivalently: if the coefficient of monomial m is $c \in \mathbb{Z}$ then the size contributed is $|c|$, not $\log|c|$.

- **Question**: Is $uSA(F) = O(\text{Res}(F))$?

Coefficient Question: Motivation

- Why should we care about this question?

(1) Simple and natural!

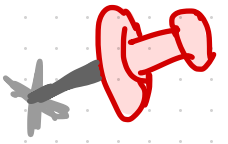
(2) Coefficient size is well-studied but badly-understood.

- No good lower bounds in **any** proof system for CNFs. (e.g. Cutting Planes, SA, SOS, $NS_{\mathbb{R}}$, ...)
- Important ramifications in practice: e.g. to what precision should we run LP/IP solvers?

(3) Many connections to total NP-Search problems (TFNP)

Coefficient Question: Motivation

- Why should we care about this question?



(1) Simple and natural!

(2) Coefficient size is well-studied but badly-understood.

- No good lower bounds in any proof system for CNFs. (e.g. Cutting Planes, SA, SOS, $NS_{\mathbb{R}}$, ...)
- Important ramifications in practice: e.g. to what precision should we run LP/IP solvers?

(3) Many connections to total NP-Search problems (TFNP) ⇦

Part 2:

Proof Complexity and (Black-Box) TFNP

Theory of TFNP: A Primer

- TFNP := { total search problems solvable in nondeterministic poly-time }

- TFNP contains many important problems, like
  - Factoring: Given a number, find a prime factor
  - Nash: Given a bimatrix game, find an equilibrium

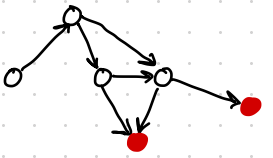
- No TFNP problem is NP-Hard if NP ≠ coNP [MP91] and TFNP is believed not to have complete problems [Pud15]

∴ To understand TFNP better, researchers study subclasses defined by reductions to complete problems!

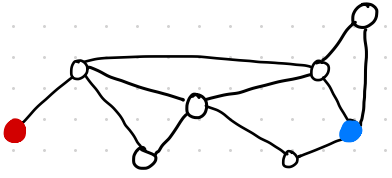
Subclasses of TFNP

- Defined by reductions to nice total search problems, e.g:

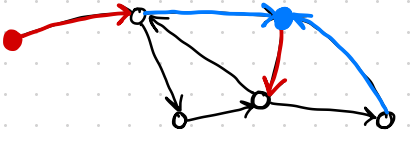
PLS: Given a DAG G, find a sink.



PPA: Given a graph with an odd-degree node find a different odd-degree node.

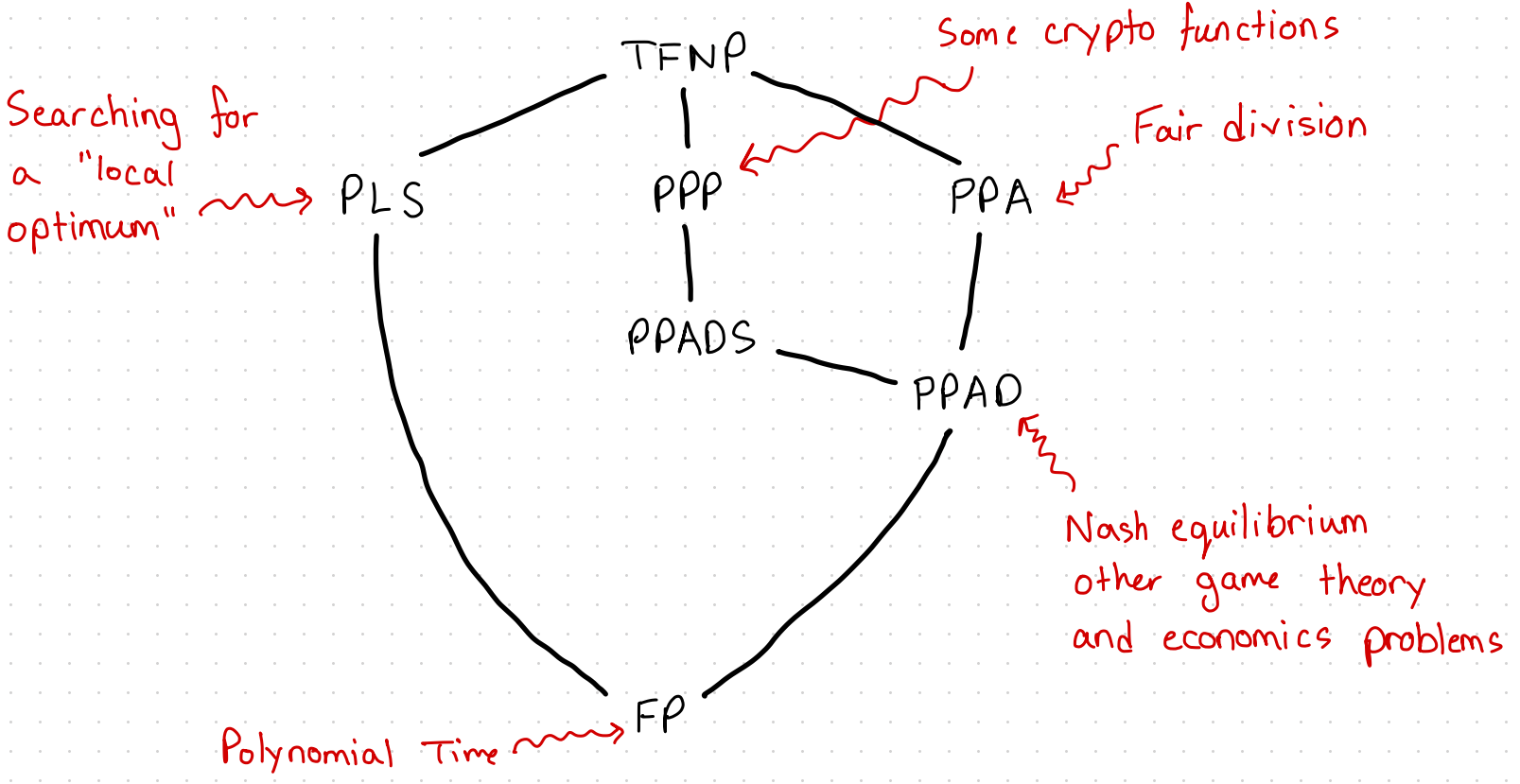


PPAD: Given a directed graph with an unbalanced node (in-deg $\neq$ out-deg), find another.

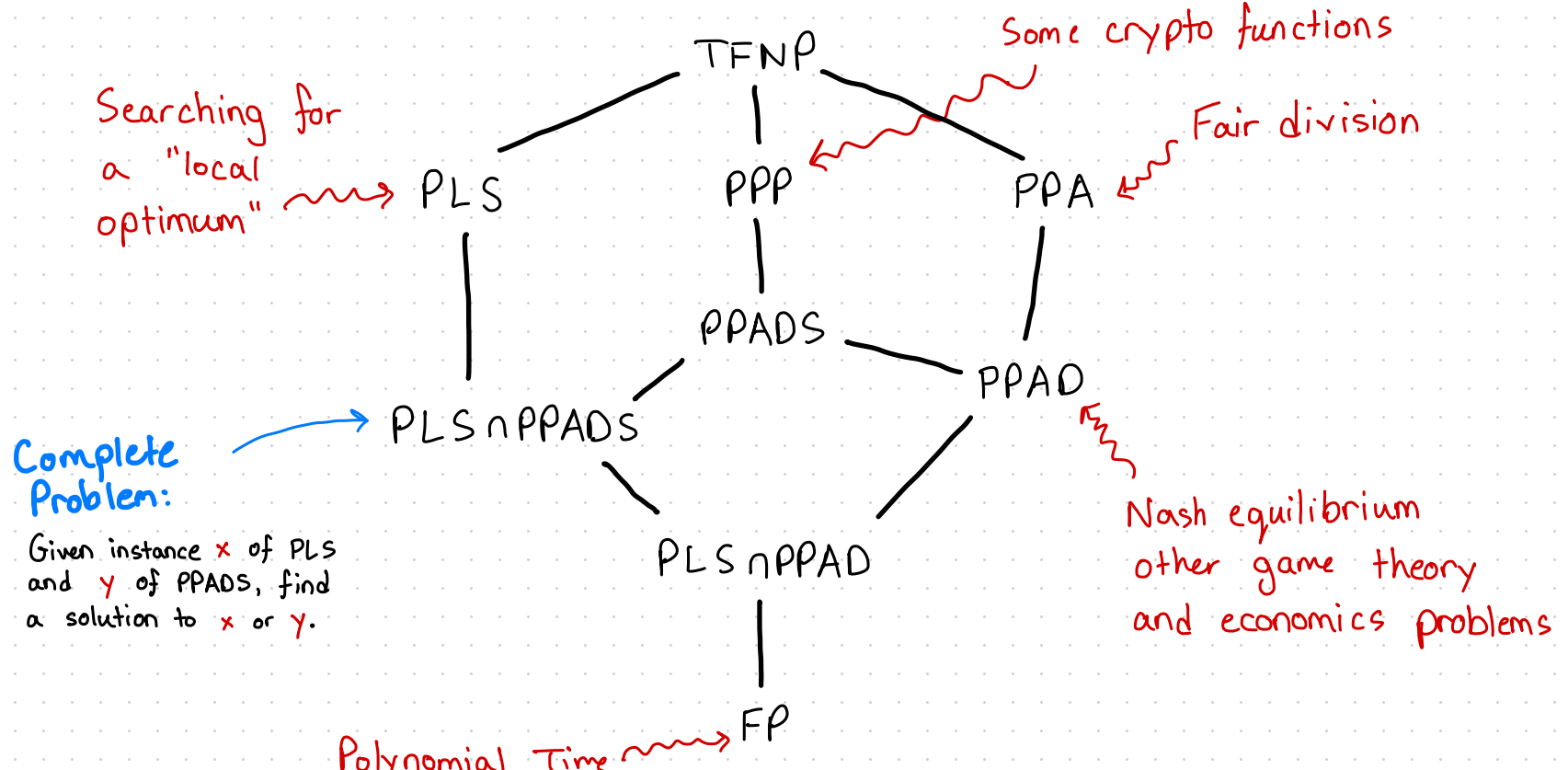


- Problems defined so state space (e.g. $|V(G)|$) is exponentially large.
  e.g. the graph G is defined by a boolean circuit computing $v \mapsto N(v)$

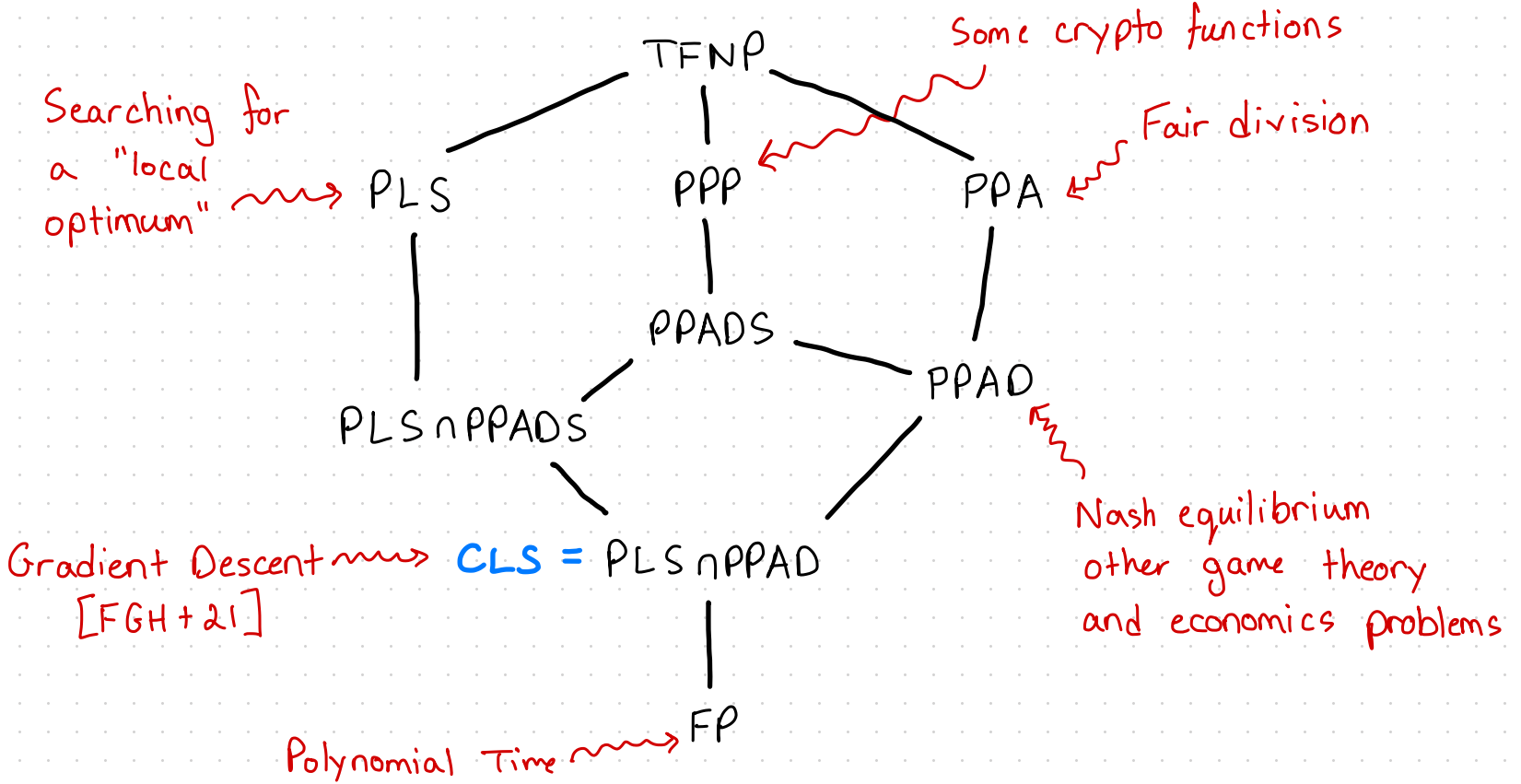
World of TFNP (Classic Classes [Pap 91])



World of TFNP (Classic Classes + Intersections)



World of TFNP (Classic Classes + Intersections)



Black-Box TFNP

- Rather than use white boxes (e.g. circuits) to define the classes, we use black boxes (equiv: oracles, decision trees)

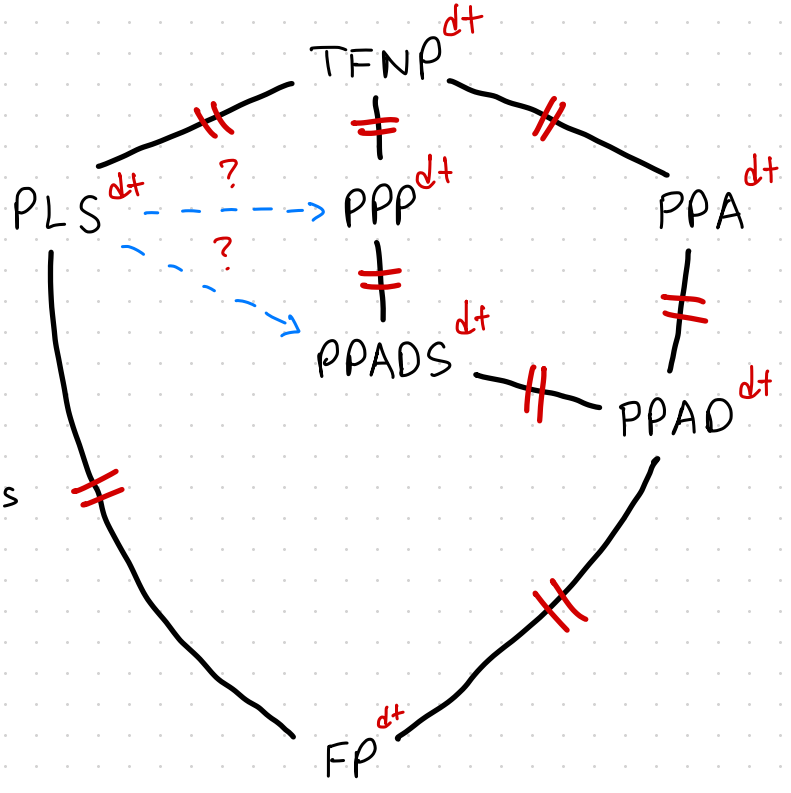
Defn. A query total search problem is a sequence $R = (R_n)_{n \geq 0}$ s.t. $R_n \subseteq \{0,1\}^n \times O_n$ and $\forall x \in \{0,1\}^n \; \exists o \in O_n$ s.t. $(x, o) \in R_n$.

Defn. $R \in \text{TFNP}^{dt}$ if $\forall n, o \in O_n$, $\exists$ decision tree T_o deciding $(x, o) \in R_n$ with depth polylog n.

- Define subclasses using $\log^{O(1)} n$-depth decision-tree reductions to fixed problems $R = (R_n)_{n \geq 0}$.

- **Why care about this?**

World of Black-Box TFNP: Unconditional Separations



Black-Box TFNP
=
Relativized TFNP
("type-2 complexity" [BCEIP98])

[BCEIP98, BM01]
Proved all separations except

$PLS^{dt} \stackrel{?}{\subseteq} PPADS^{dt}$

$PLS^{dt} \stackrel{?}{\subseteq} PPP^{dt}$

Black-Box TFNP and Proof Complexity

- Black-box TFNP is intimately related to proof complexity.
- $F = C_1 \wedge \cdots \wedge C_m$ is unsat CNF let

"Given x, find false clause"

$$S(F) \subseteq \{0,1\}^n \times [m] \quad \text{by} \quad (x,i) \in S(F) \iff C_i(x) = 0$$

- Clearly total since F unsat
- $w(F) = \text{polylog}(n) \Rightarrow S(F) \in TFNP^{dt}$

The problem solved by SAT solvers

- Converse holds: $R = (R_n)_n \in TFNP^{dt}$ then

write as CNF

$$R_n \cong S\left(\bigwedge_{o \in O_n} \neg T_o \right)$$

Black-box TFNP and Proof Complexity

- $\mathrm{TFNP}^{\mathrm{dt}} \longleftrightarrow$ polylog n -width unsat CNFs
- Subclasses $\mathrm{R}^{\mathrm{dt}} \subseteq \mathrm{TFNP}^{\mathrm{dt}} \longleftrightarrow$ propositional proof systems P!

Template Theorem Sequence $F = (F_n)_n$ of unsat CNFs has

$\log^{O(1)} n$-degree, $n^{\log^{O(1)} n}$-size P-proofs (i.e. $P(F_n) = \log^{O(1)} n$)

$\Longleftrightarrow$

Search problem $S(F) := (S(F_n))_n \in \mathrm{R}^{\mathrm{dt}}$

DPLL / TreeRes $\equiv \mathrm{FP}^{\mathrm{dt}}$

[Folklore]

Degree = depth

$\mathbb{F}_2$-Nullstellensatz $\equiv \mathrm{PPA}^{\mathrm{dt}}$

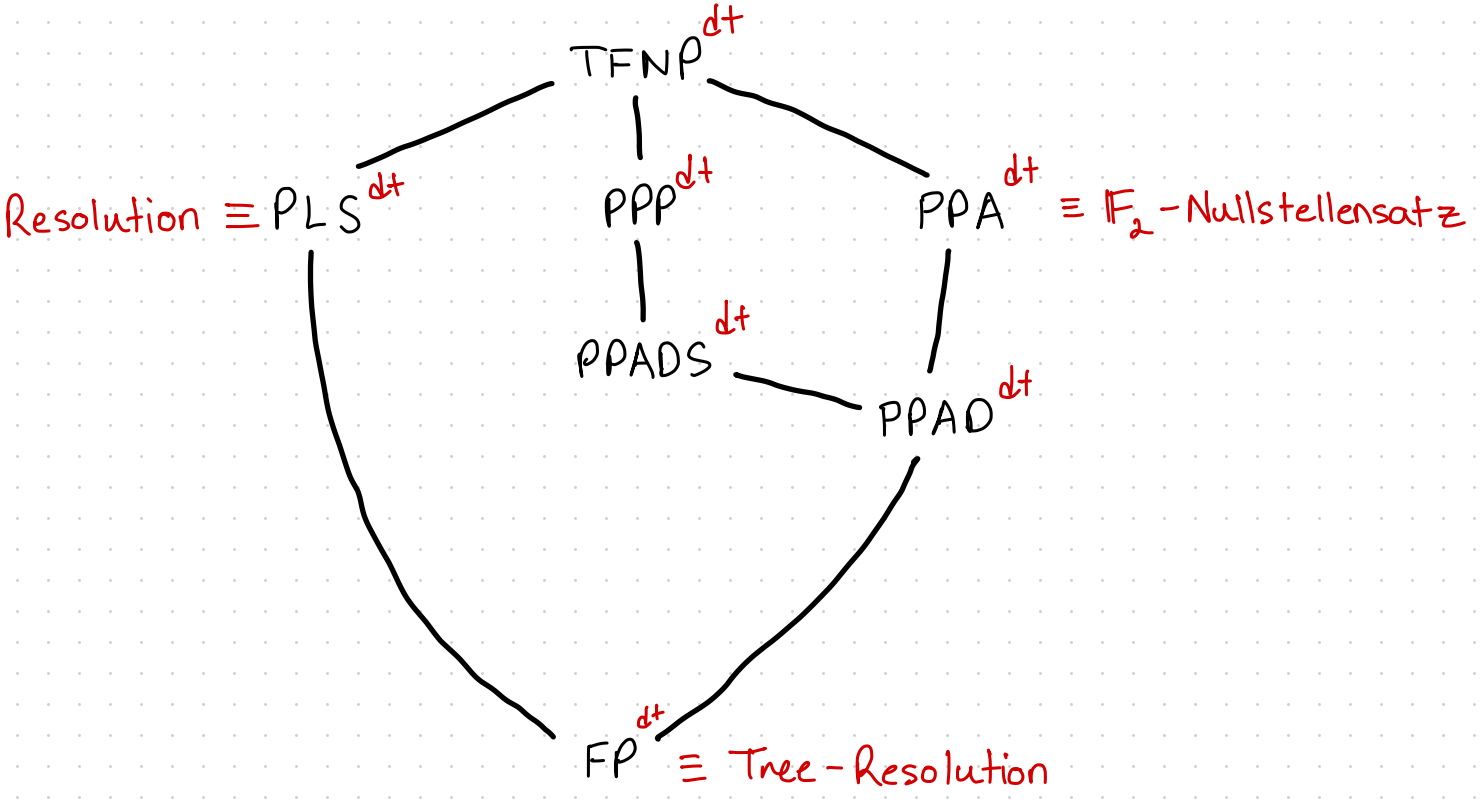
[BCEIP 98, GKRS 18]

Resolution $\equiv \mathrm{PLS}^{\mathrm{dt}}$

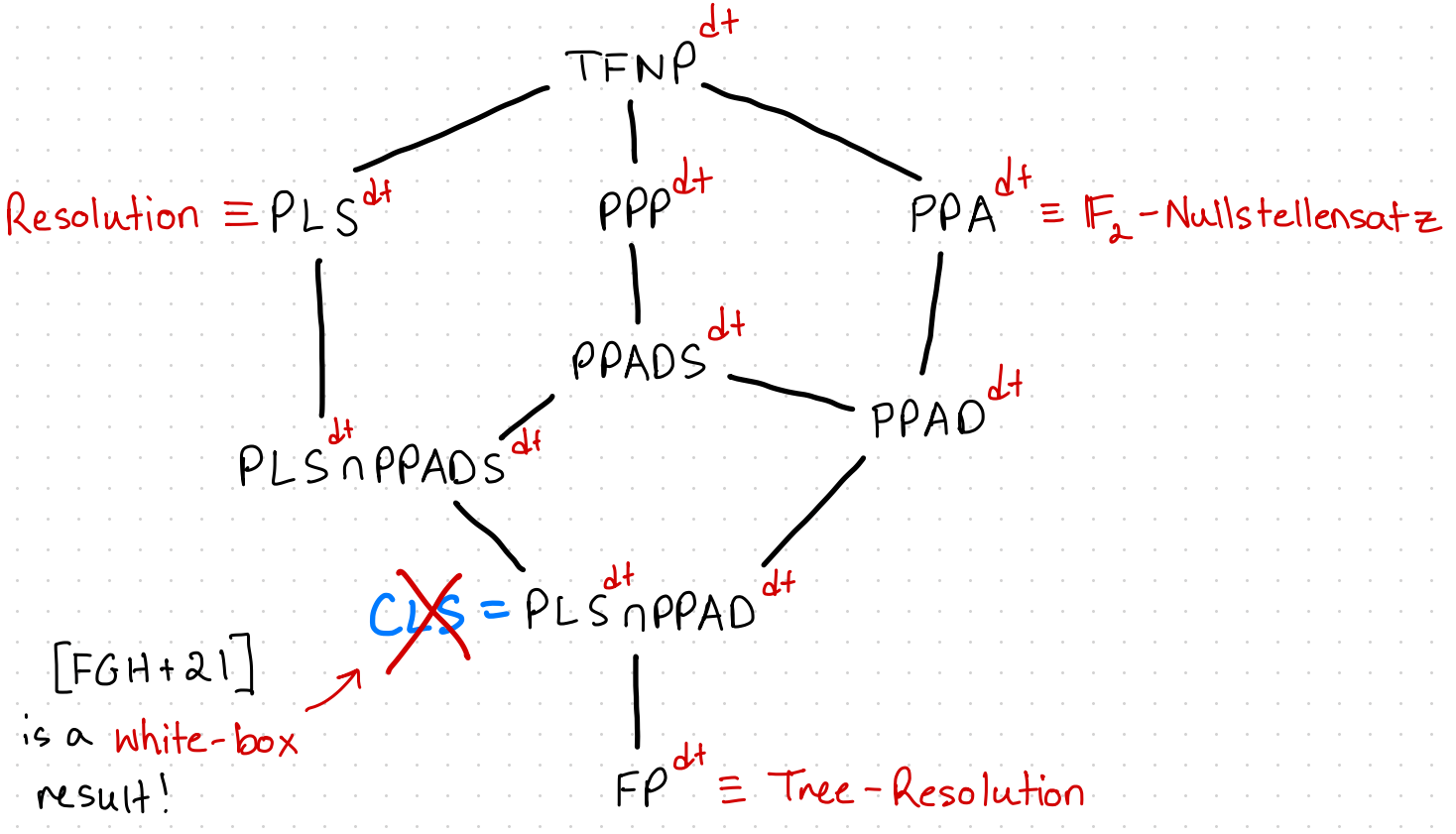
[BKT 14, Kam 20]

Degree = width

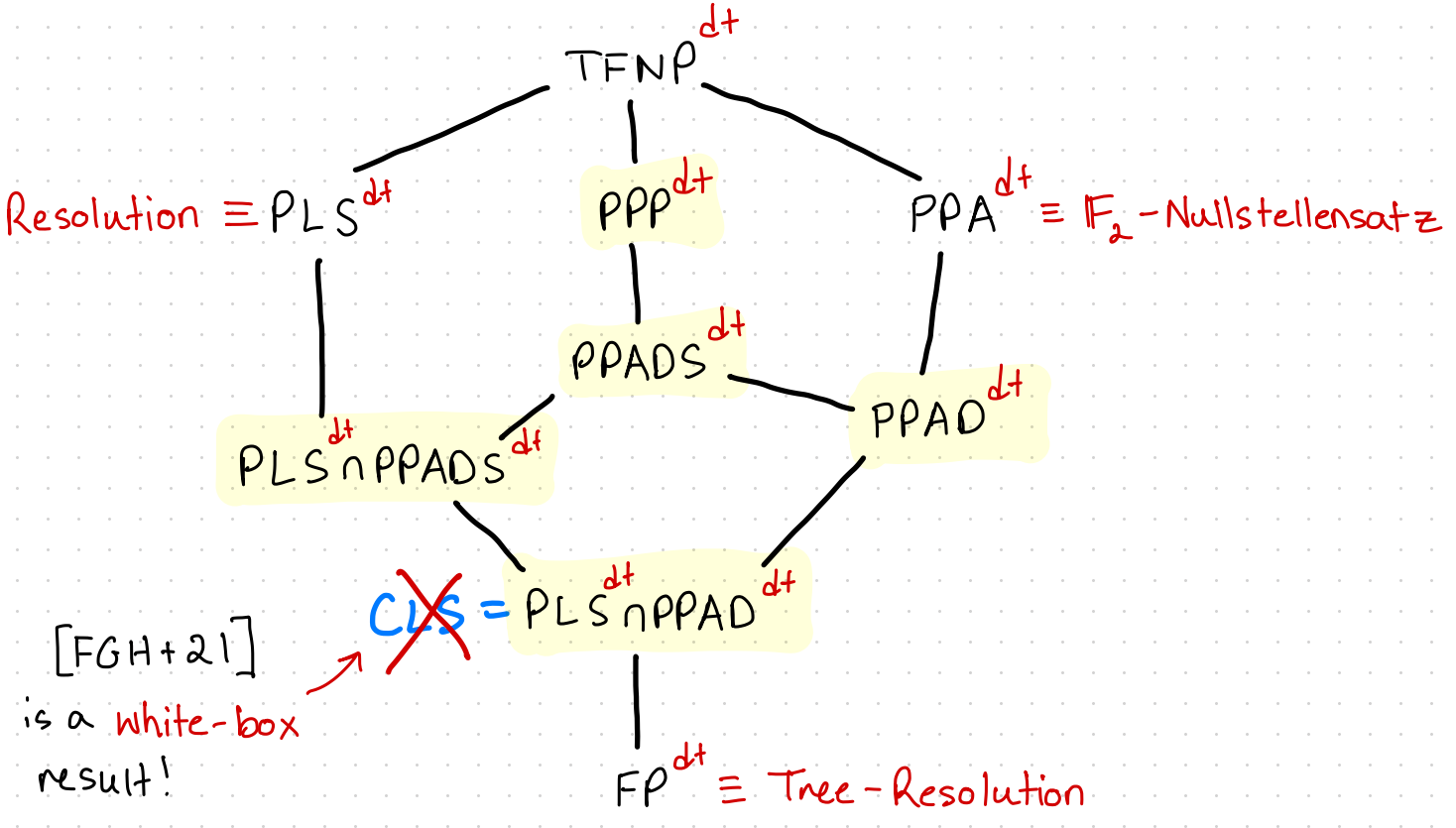
World of Black-Box TFNP



World of Black-Box TFNP + Intersections



World of Black-Box TFNP + Intersections



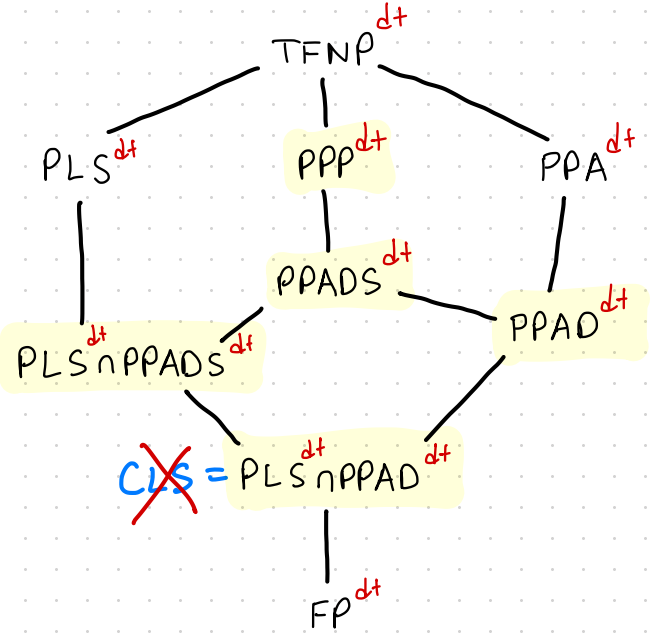
Black-Box TFNP: Open Questions

- Are there natural proof systems corresponding to the highlighted classes?
- Are there natural characterisations of the intersection classes in the black-box model? (EoPL, SoPL?)
- [BCEIP98, BOM01] unconditionally separated all classical (non-intersection) classes except

$$\mathrm{PLS}^{dt} \stackrel{?}{\subseteq} \mathrm{PPADS}^{dt}$$

$$\mathrm{PLS}^{dt} \stackrel{?}{\subseteq} \mathrm{PPP}^{dt}$$

Can we separate these? What about the intersection classes?



(I + II = III)

Part III

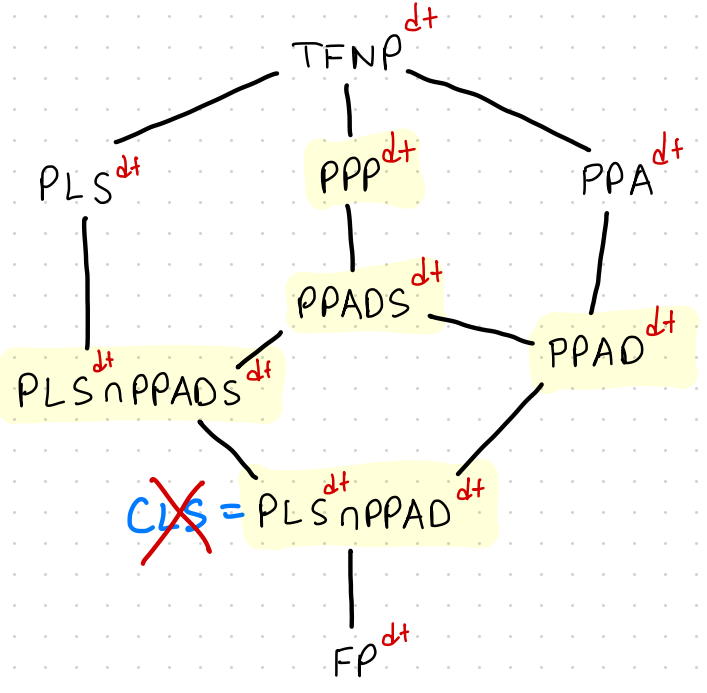
New Results

Open Questions

(1) Is $uSA(F) = O(Res(F))$?

(2) Are there natural characterisations of the intersection classes in the black-box model? (EoPL, SoPL?)

(3) Are there natural proof systems corresponding to the highlighted classes?



(4) $PLS^{dt} \stackrel{?}{\subseteq} PPADS^{dt}$ $\quad$ $PLS^{dt} \stackrel{?}{\subseteq} PPP^{dt}$?

Open Questions

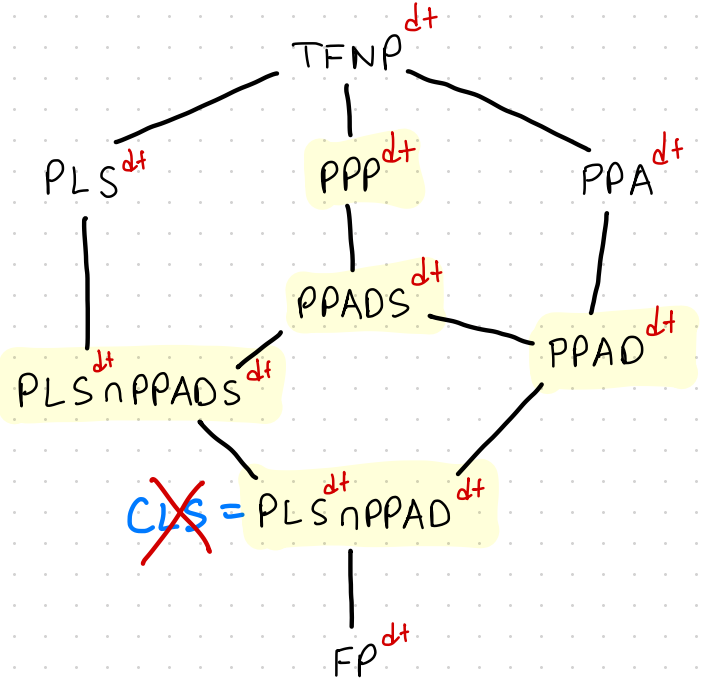
(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

(2) Are there natural characterisations of the intersection classes in the black-box model?

(3) Are there natural proof systems corresponding to the highlighted classes?

(4) $PLS^{dt} \stackrel{?}{\subseteq} PPADS^{dt}$ $\quad$ $PLS^{dt} \stackrel{?}{\subseteq} PPP^{dt}$?



Open Questions

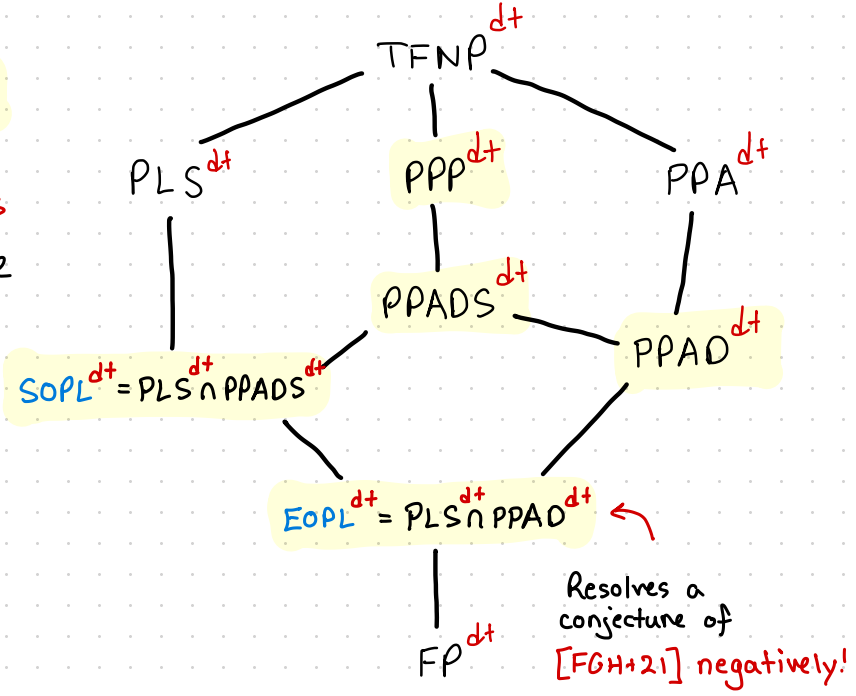
(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

(2) Are there natural characterisations of the intersection classes in the black-box model? **Yes!**

(3) Are there natural proof systems corresponding to the highlighted classes?

(4) $PLS^{dt} \stackrel{?}{\subseteq} PPADS^{dt}$ $\quad$ $PLS^{dt} \stackrel{?}{\subseteq} PPP^{dt}$?



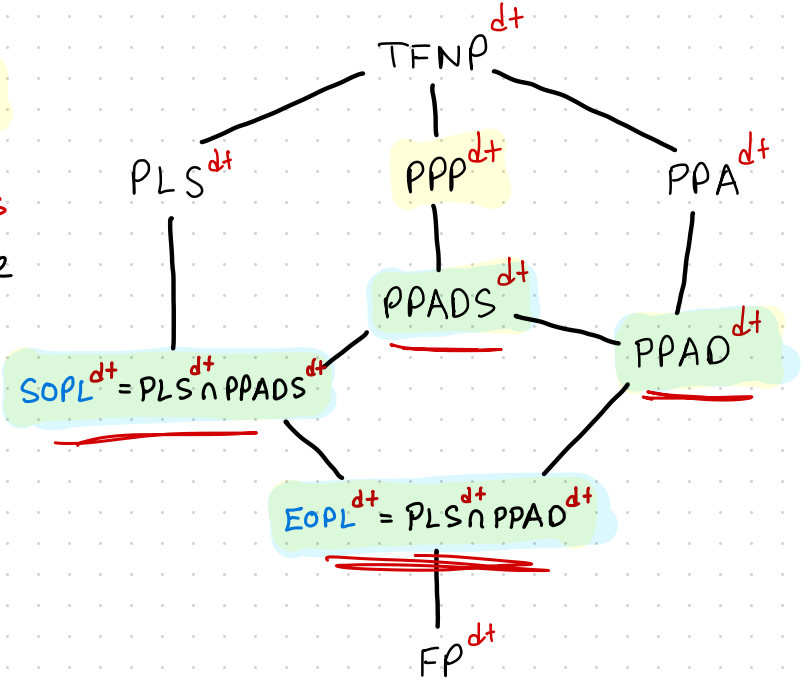
Open Questions

(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

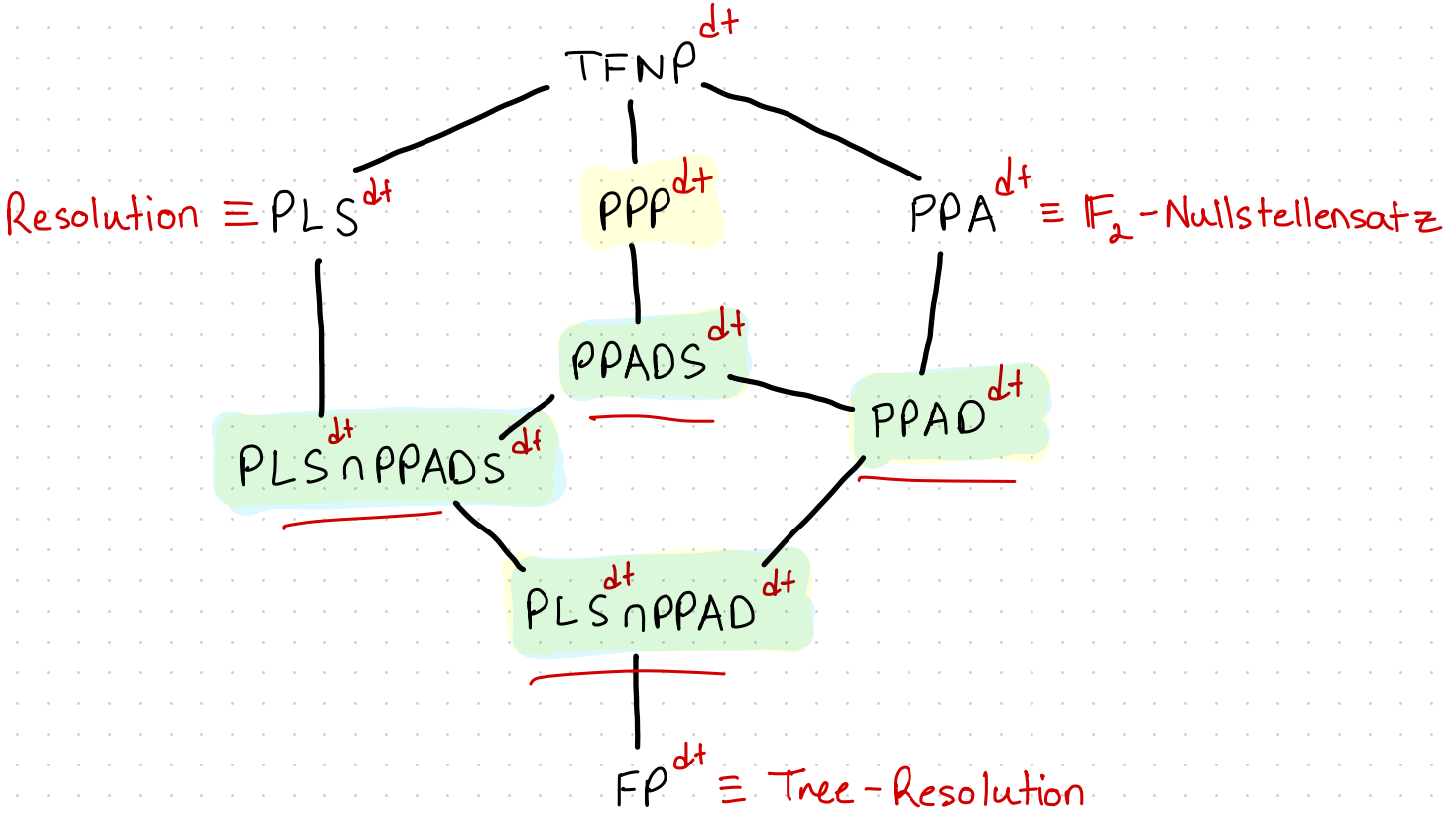
(2) Are there natural characterisations of the intersection classes in the black-box model? **Yes!**

(3) Are there natural proof systems corresponding to the highlighted classes? **Yes!**

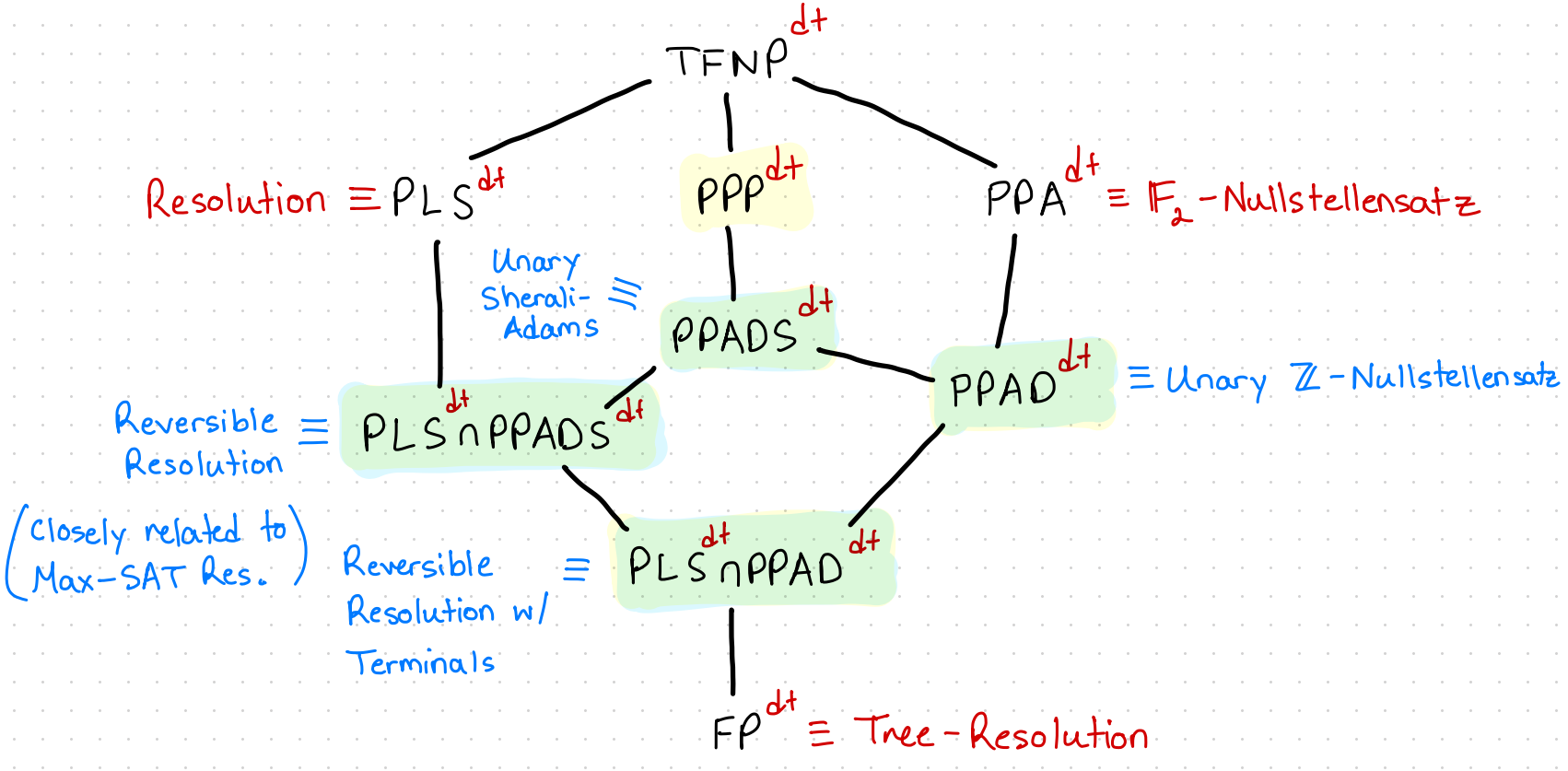


(4) $PLS^{dt} \overset{?}{\subseteq} PPADS^{dt}$ $\quad$ $PLS^{dt} \overset{?}{\subseteq} PPP^{dt}$?

World of Black-Box TFNP + Intersections



World of Black-Box TFNP + Intersections



Open Questions

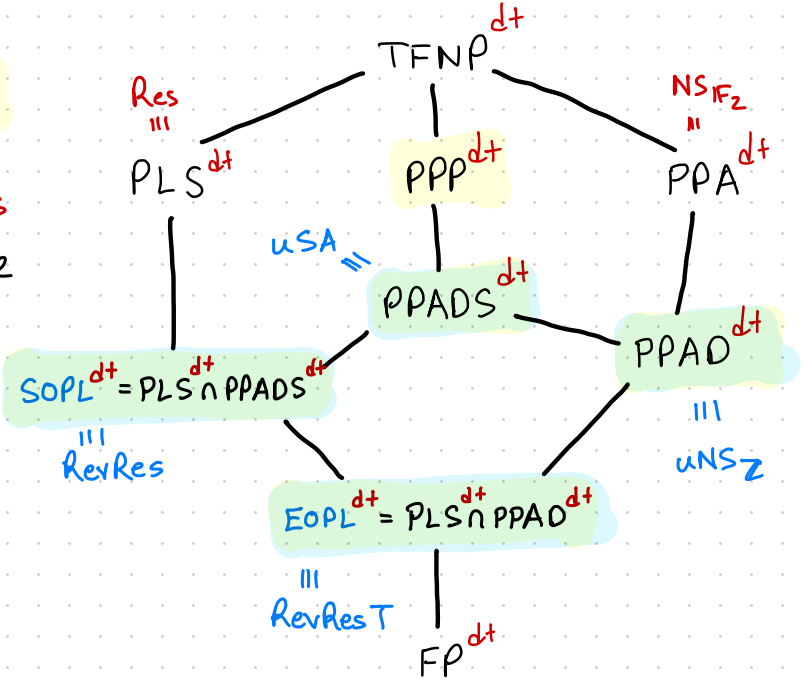
(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

(2) Are there natural characterisations of the intersection classes in the black-box model? **Yes!**

(3) Are there natural proof systems corresponding to the highlighted classes? **Yes!**

(4) $PLS^{dt} \stackrel{?}{\subseteq} PPADS^{dt}$ $\quad$ $PLS^{dt} \stackrel{?}{\subseteq} PPP^{dt}$?



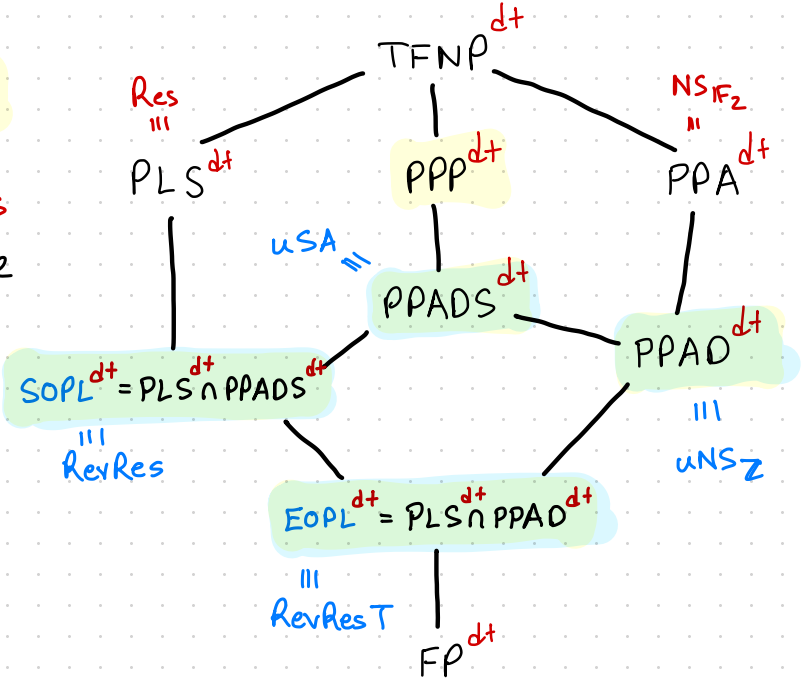
Open Questions

(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

(2) Are there natural characterisations of the intersection classes in the black-box model? **Yes!**

(3) Are there natural proof systems corresponding to the highlighted classes? **Yes!**



(4) $PLS^{dt} \not\subseteq PPADS^{dt}$ (1) + (3)

$PLS^{dt} \overset{?}{\subseteq} PPP^{dt}$?

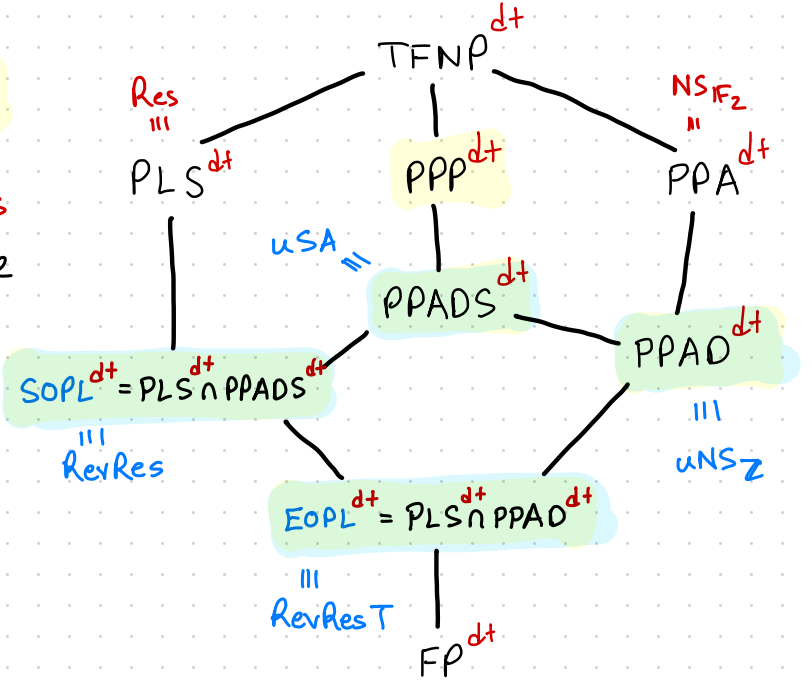
Open Questions

(1) Is $uSA(F) \neq O(Res(F))$?

No! $\exists F_n : uSA(F_n) = n^{\Omega(1)}$, $Res(F_n) = O(\log n)$

(2) Are there natural characterisations of the intersection classes in the black-box model? **Yes!**

(3) Are there natural proof systems corresponding to the highlighted classes? **Yes!**



(4) $PLS^{dt} \not\subseteq PPADS^{dt} \overset{(!)}{\Longrightarrow} PLS^{dt} \not\subseteq PPP^{dt}$?

(1) + (3)

(Along the way we separate other intersections as well.)

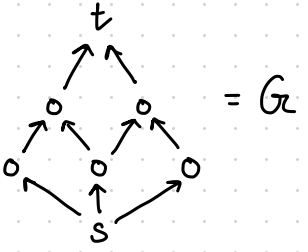
Unary SA vs. Resolution

- We prove the Pebbling principles require large coefficients in SA

  G := dag with unique sink t, source s

  Variable x_u for all $u \in V(G)$,

  $Peb_G := \overline{x_t} \wedge x_s \wedge \bigwedge_{\substack{u \in V \\ u \neq s}} \left(x_u \vee \bigvee_{v \in pred_u} \overline{x_v} \right)$

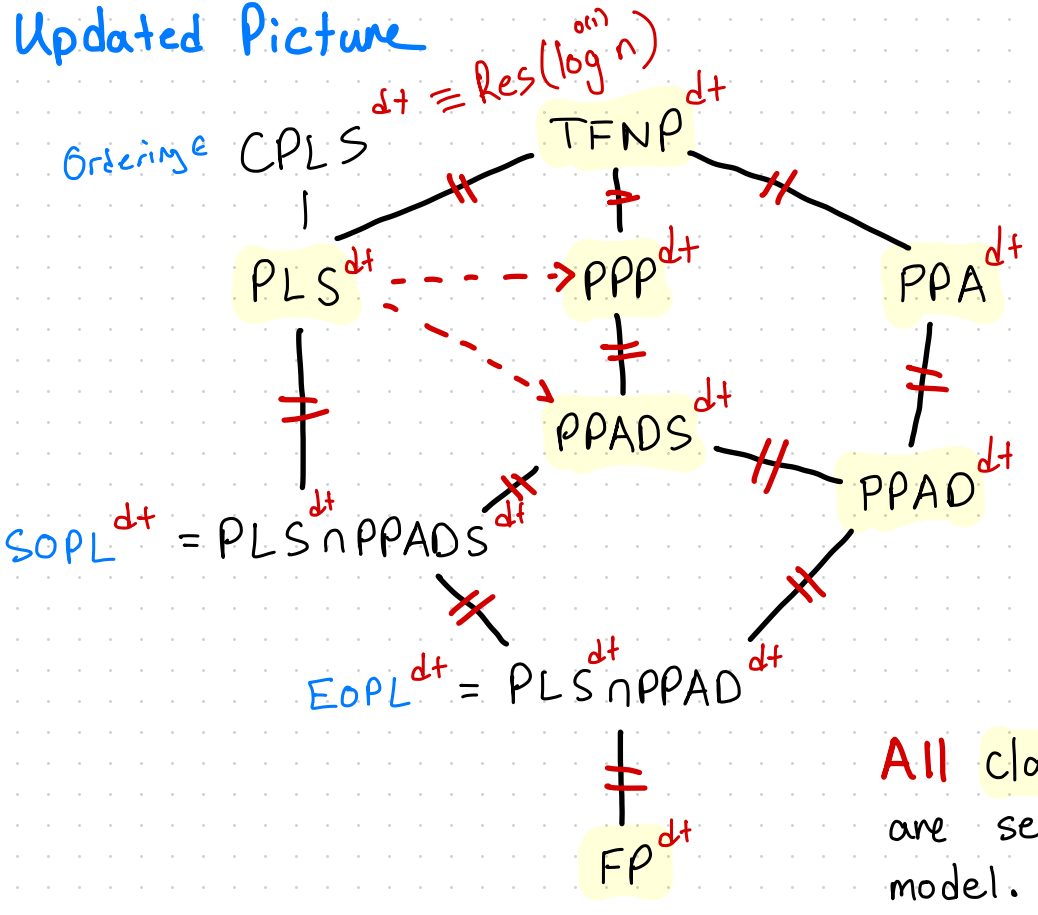


Thm $\exists G$: Peb_G has $O(1)$-width, $n^{O(1)}$-size Res refutations but any SA refutation with degree-$n^{o(1)}$ requires coeffs of magnitude $2^{n^{\Omega(1)}}$.

- Note: earlier simulation result $\Rightarrow deg_{uSA}(Peb_G) = O(1)$

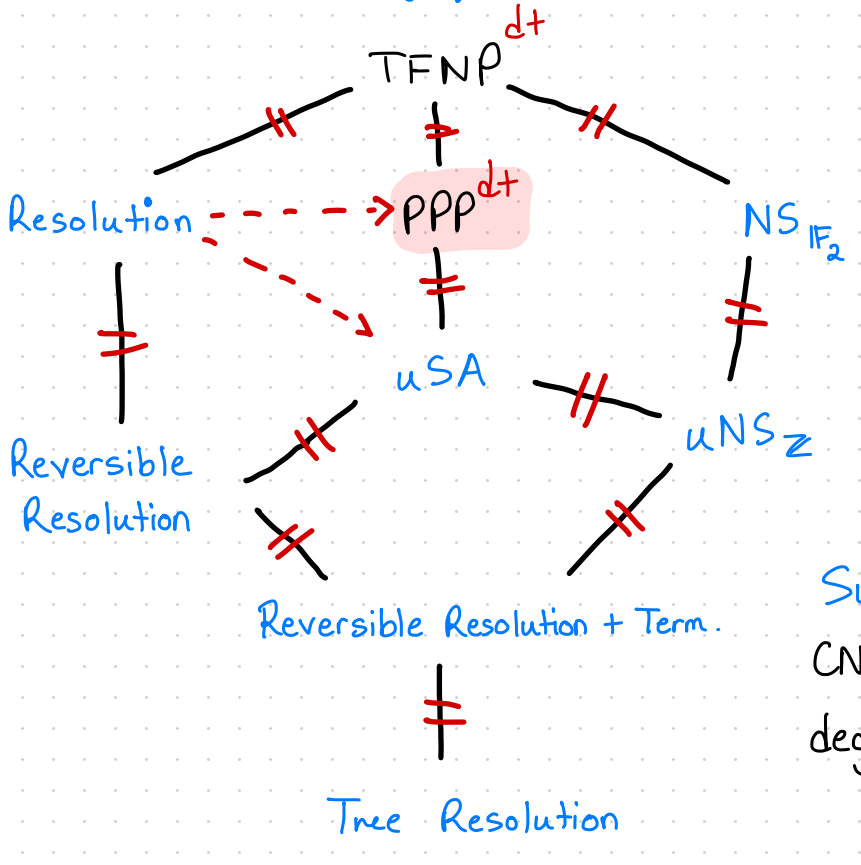
- Alternatively: $Res(Peb_G) = O(\log n)$, $uSA(Peb_G) = n^{\Omega(1)}$.

An Updated Picture



All classical TFNP classes are separated in black-box model.

An Updated Picture (Proofs)



Subclasses are CNFs w/ proofs π:

$\deg(\pi) + \log \text{size}(\pi)$

$= \log^{O(1)} n$

Reversible Resolution

- $F = C_1 \wedge \cdots \wedge C_m$ is an unsat CNF, a Reversible Resolution ref. is a sequence

$$\mathcal{L}_1, \mathcal{L}_2, \cdots, \mathcal{L}_s \ni \bot$$

of multisets of clauses s.t.

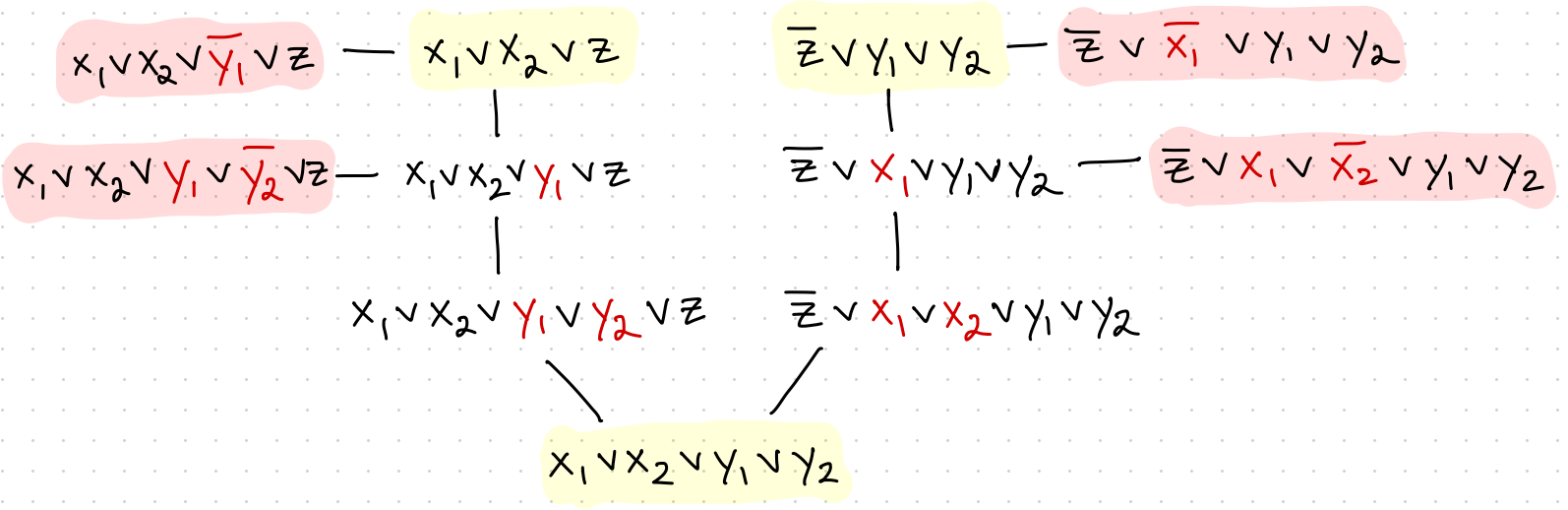
(1) Every clause in $\mathcal{L}_1$ is in F

(2) $\mathcal{L}_i$ is deduced from $\mathcal{L}_{i-1}$ by applying one of $\frac{C \vee x \quad C \vee \bar{x}}{C}$ $\quad \frac{C}{C \vee x \quad C \vee \bar{x}}$ and replacing the input with its outputs.

It is a Reversible Resolution proof with Terminals if every non-$\bot$ clause in $\mathcal{L}_s$ is a weakening of a clause in F.

Reversible Resolution: Example

- We can simulate the usual Resolution rule reversibly:



∴ Reversible Resolution can efficiently simulate Tree Resolution

- However, it is stronger than Tree Resolution.

Reversible Resolution vs. Resolution

- Resolution: Lines are clauses, Proof Rules are

$$\frac{C \vee x \quad D \vee \bar{x}}{C \vee D} \qquad \frac{C}{C \vee \ell}$$

lines can be re-used.

- Reversible Resolution: Lines are clauses, Proof Rules are

$$\frac{C \vee x \quad C \vee \bar{x}}{C} \qquad \frac{C}{C \vee x \quad C \vee \bar{x}}$$

← bi-directional, output ≡ input

lines can **not** be re-used.

Reversible Resolution and Max-SAT

- For every assignment $x \in \{0,1\}^n$, the # of satisfied clauses in every $\mathcal{Y}_i$ is equal!
- # of copies of each initial clause C_i in $\mathcal{Y}_1$ is weight $w_i \in \mathbb{Z}$, $w_i \geq 0$
- RevRes refutation shows any assignment has satisfied weight $\leq \Sigma w_i - 1$
- Experts: Essentially unary MaxResW, but used as a refutation system.

Corollary : Intersection Theorems

- Get a brand-new type of result in proof complexity: Intersection Theorems

Recall the notation $P(F) = \min_{\pi} \deg_p(\pi) + \log \text{size}_p(\pi)$

Thm For any CNF formula F,

$$\text{RevRes}(F) = \Theta\left(\text{Res}(F) + u\text{SA}(F)\right)$$

$$\text{RevResT}(F) = \Theta\left(\text{Res}(F) + u\text{NS}_{\mathbb{Z}}(F)\right)$$

- Efficient RevRes pf if and only if efficient Res pf and efficient uSA pf!
- Reversible Resolution is the "intersection" of Resolution and unary SA.
- Proof crucially uses perspective of total search problems.

Open Questions

- Where does Sum-of-Squares (SOS) fit in?
  - Can we show $uSOS(F) \neq O(Res(F))$?
- Other intersection theorems? Is there a natural proof system for e.g. PLS∩PPA?
- Can we characterize PPP by a proof system? UEOPL?
- Does $uNS_{\mathbb{Z}}$ simulate $NS_{\mathbb{Z}}$?
- What other proof systems fit into this picture?
- Are there communication complexity analogues?