Separations in Proof Complexity and TFNP

William Pires
Robert Robere
Ran Tao
McGill

Alexandros Hollender
Oxford

Mika Göös
Siddhartha Jain
Gilbert Maystre
EPFL

Separations in Proof Complexity and TFNP

Mika Göös
Gilbert Maystre
Alexandros Hollender
EPFL

William Pires
Columbia

Siddhartha Jain
UT Austin

Ran Tao
Robert Robere
McGill

Separations in Proof Complexity and TFNP

Ran Tao
Robert Robere
McGill

Mika Göös
Gilbert Maystre
Alexandros Hollender
EPFL

William Pires
Columbia

Siddhartha Jain
UT Austin

Understanding The Title

TFNP := Total Function NP

Polytime $R(x,y)$

TFNP := Total Function NP

Polytime $R(x,y)$

Input x

Output $y : R(x,y) = 1$ & $|y| \leq |x|^{O(1)}$

TFNP := Total Function NP

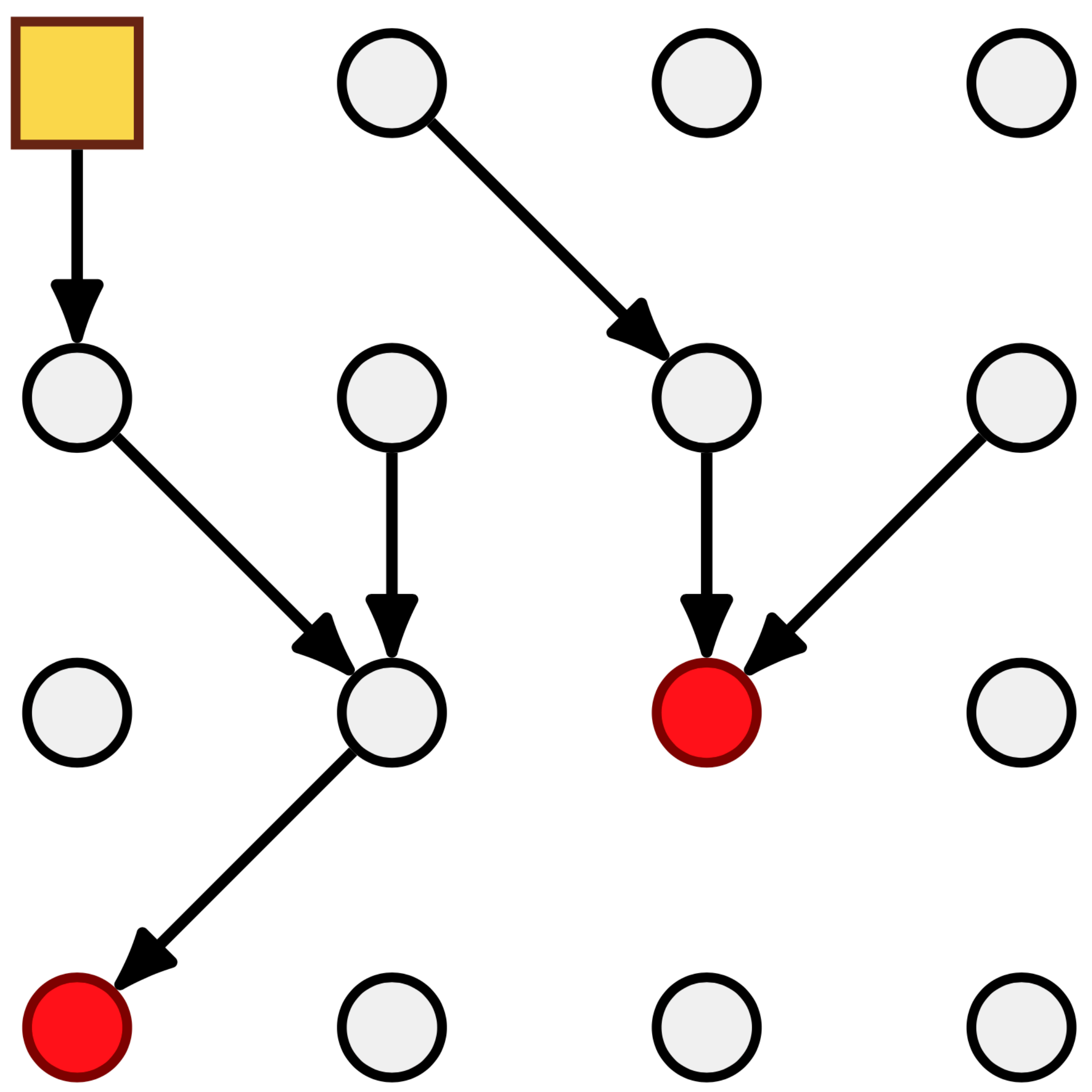
Polytime $R(x,y)$

Input x

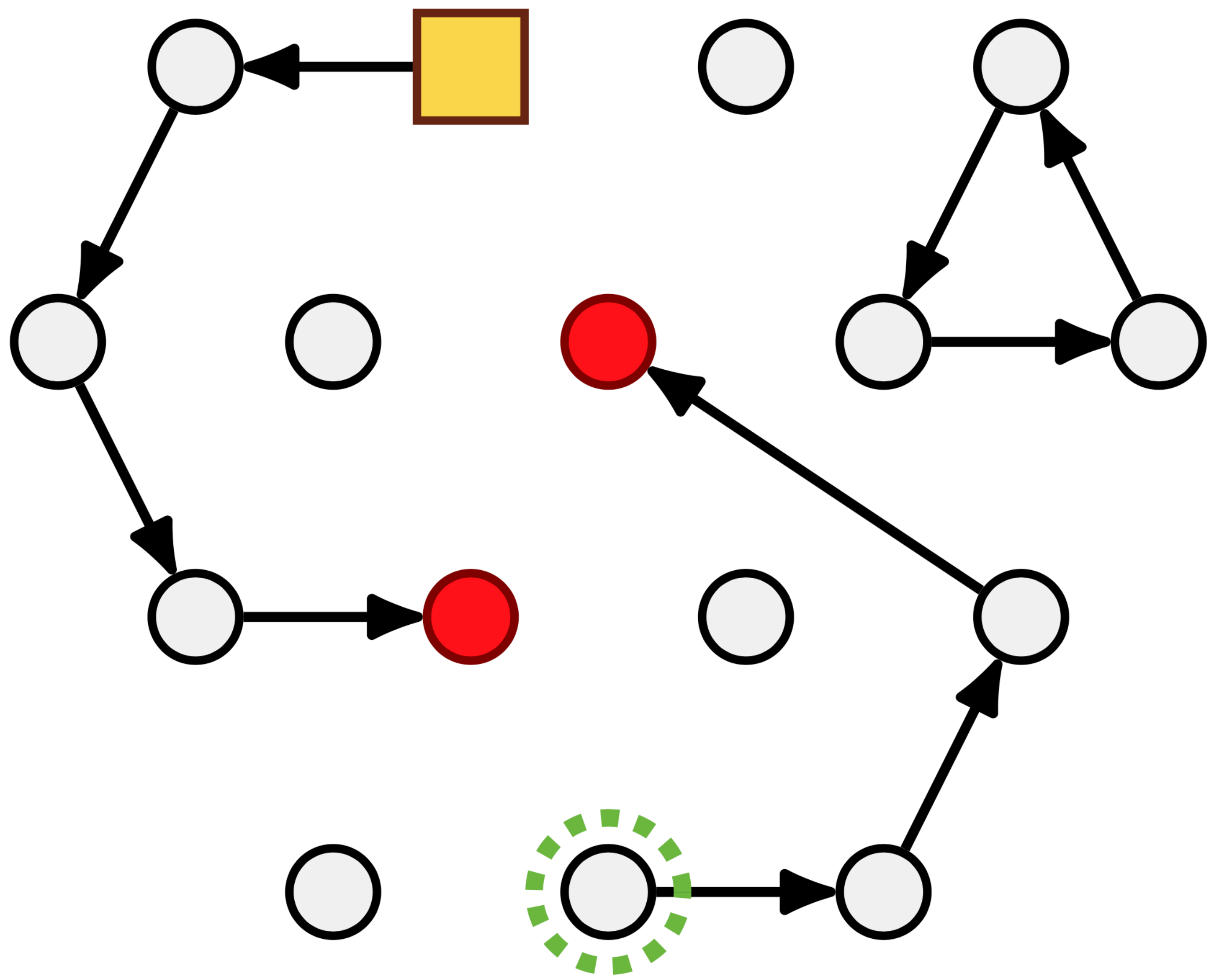
Output $y : R(x,y) = 1$ & $|y| \leq |x|^{O(1)}$

Promise R is total: $\forall x\, \exists y\; R(x,y) = 1$

Two Problems

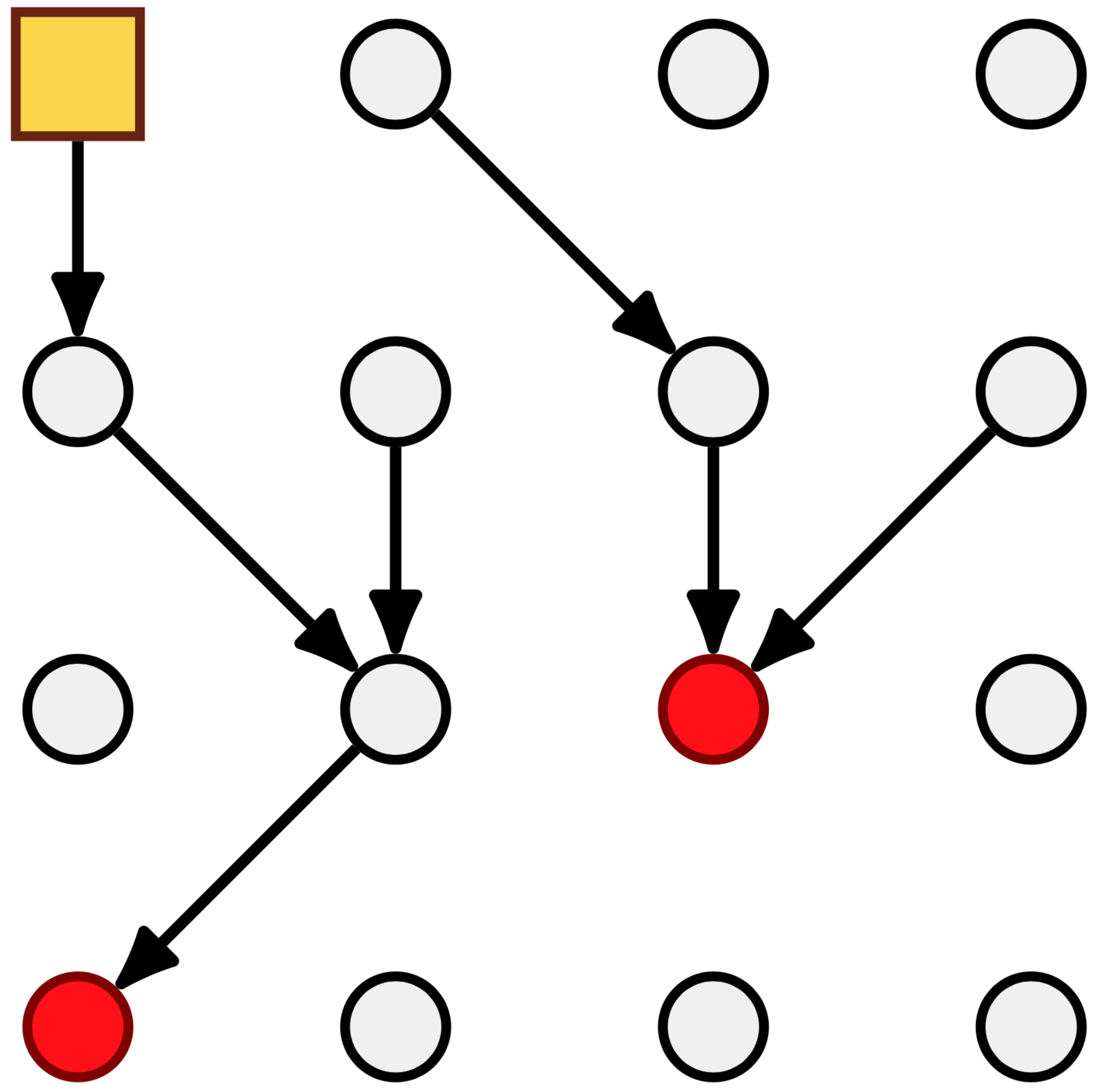


Sink-of-DAG (SoD)

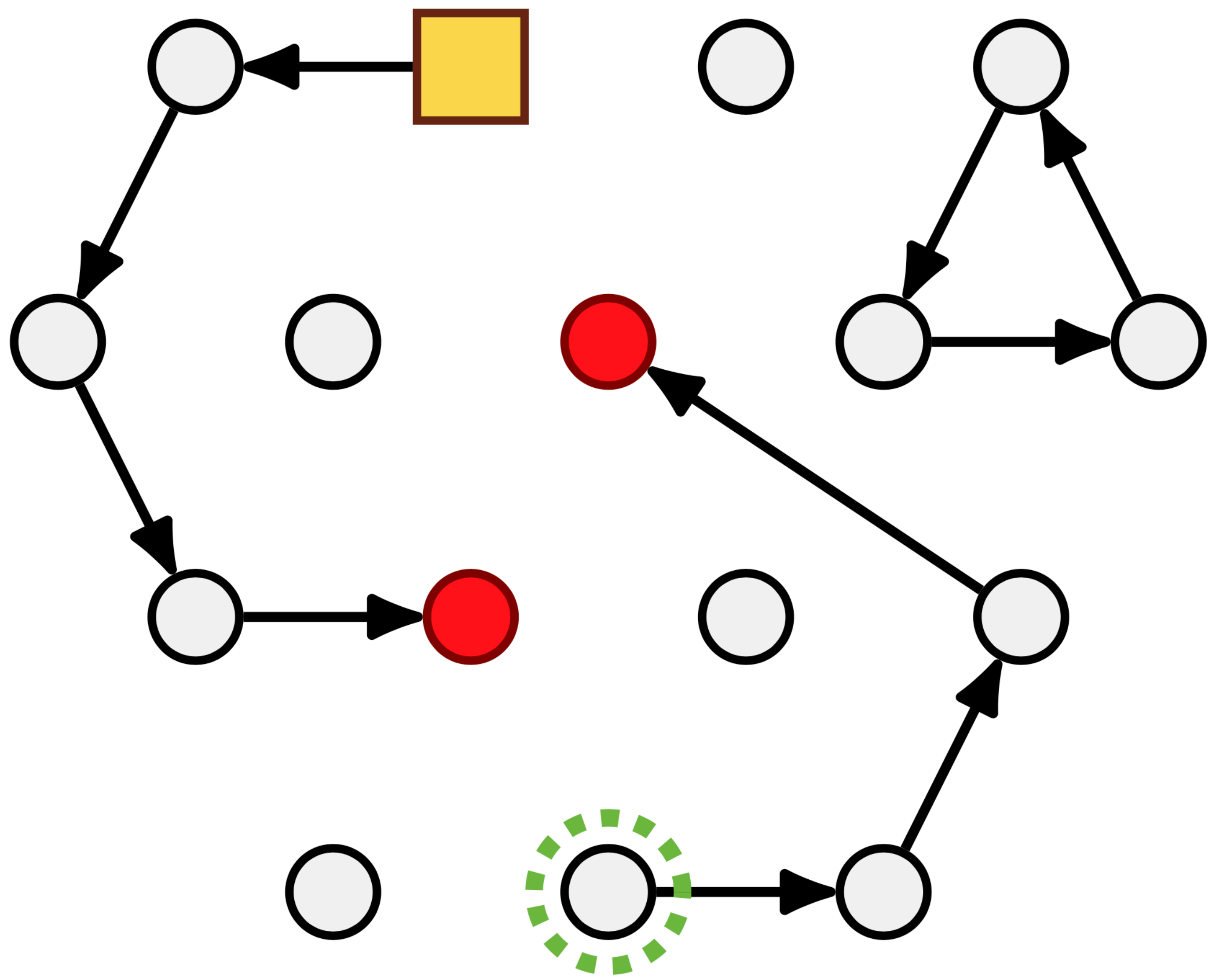


Sink-of-Line (SoL)

Two (& ½) Problems



Sink-of-DAG (SoD)



Sink-of-Line (SoL)
End-of-Line (EoL)

... And Three Classes

$$\mathrm{PLS} = \{ P : P \leq \mathrm{S \circ D} \}$$

$$\mathrm{PPADS} = \{ P : P \leq \mathrm{S \circ L} \}$$

$$\mathrm{PPAD} = \{ P : P \leq \mathrm{E \circ L} \}$$

… And Three Classes

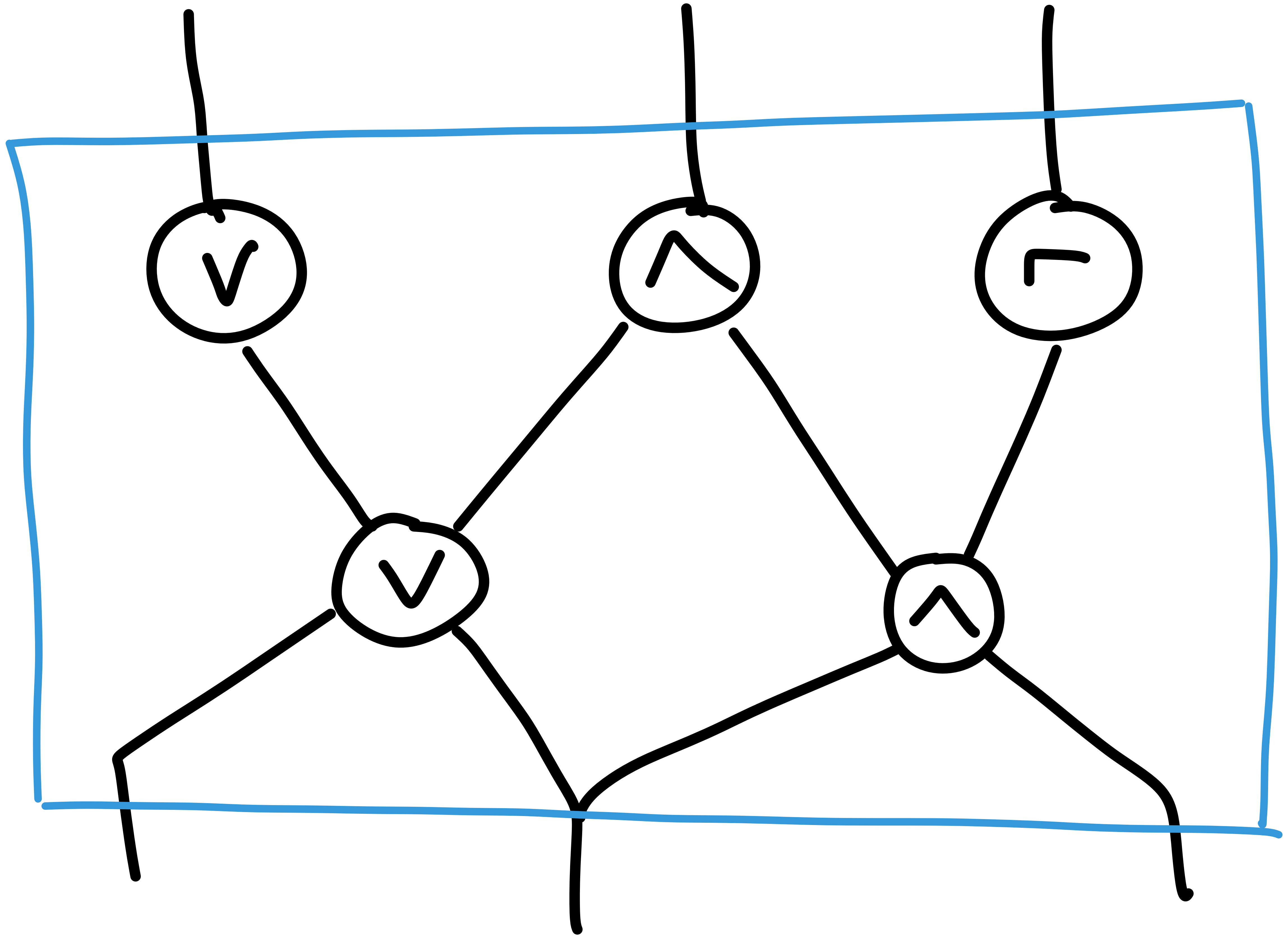
$$\mathrm{PLS} = \{ P : P \leq \mathrm{SoD} \}$$

$$\mathrm{PPADS} = \{ P : P \leq \mathrm{SoL} \}$$

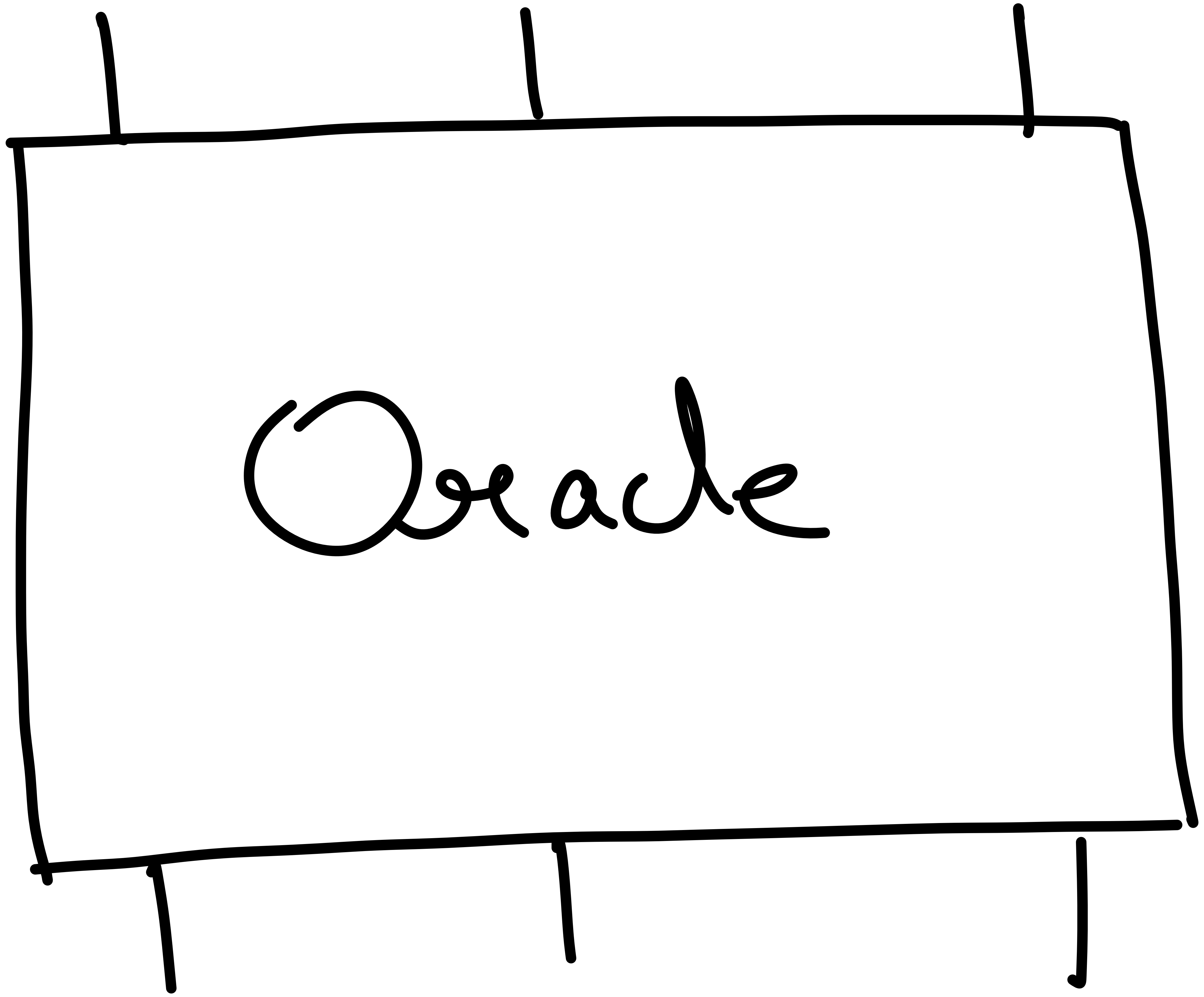
$$\mathrm{PPAD} = \{ P : P \leq \mathrm{EoL} \}$$

$A \leq B$ if $\exists\, R_1, R_2$

$$\begin{tikzcd}
x \arrow[r, "R_1"] \arrow[d, dashed, "\text{Solves } A"'] & x' \arrow[d, "\text{Solve } B"] \\
y & y' \arrow[l, "R_2"]
\end{tikzcd}$$

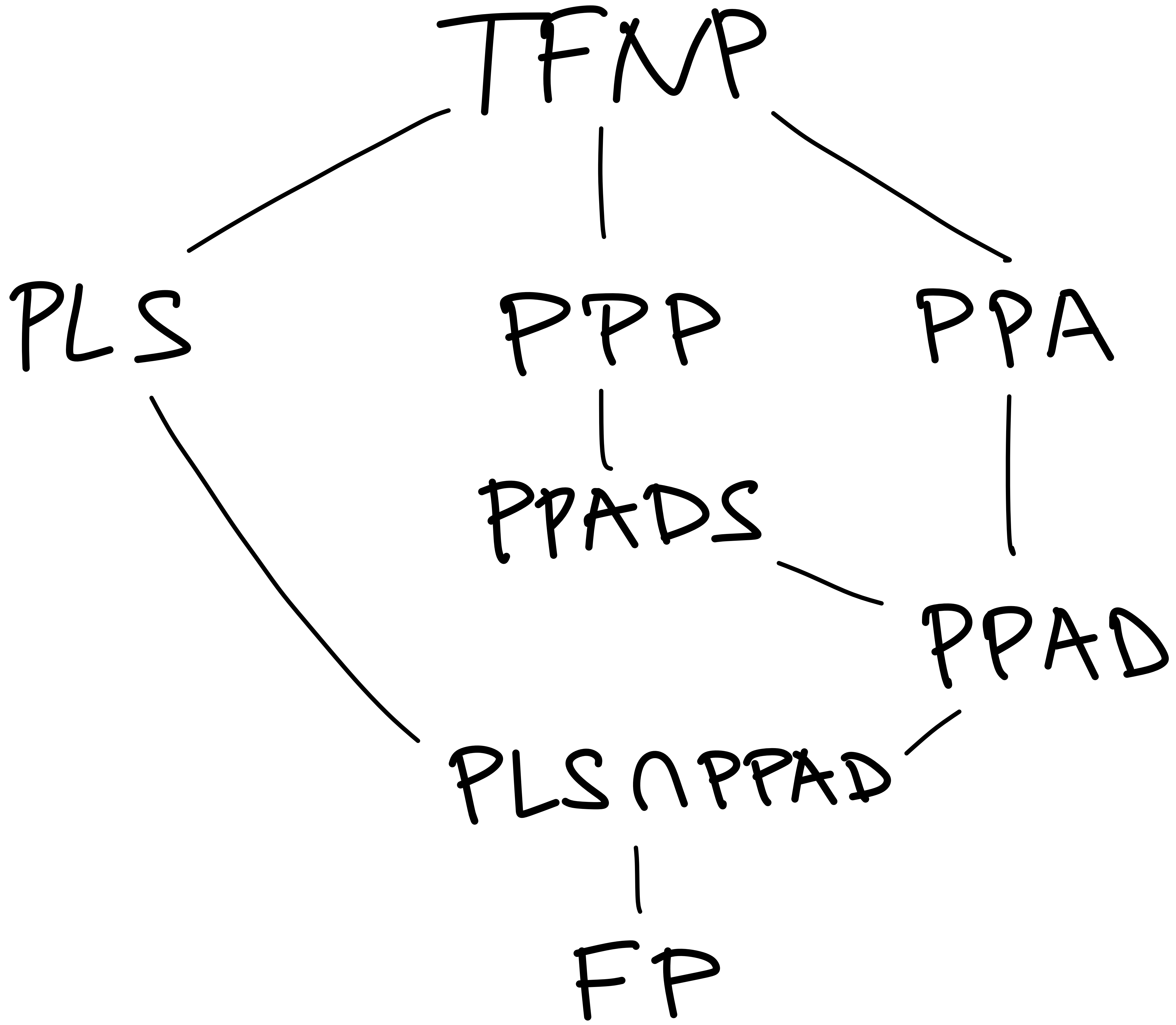


White-box



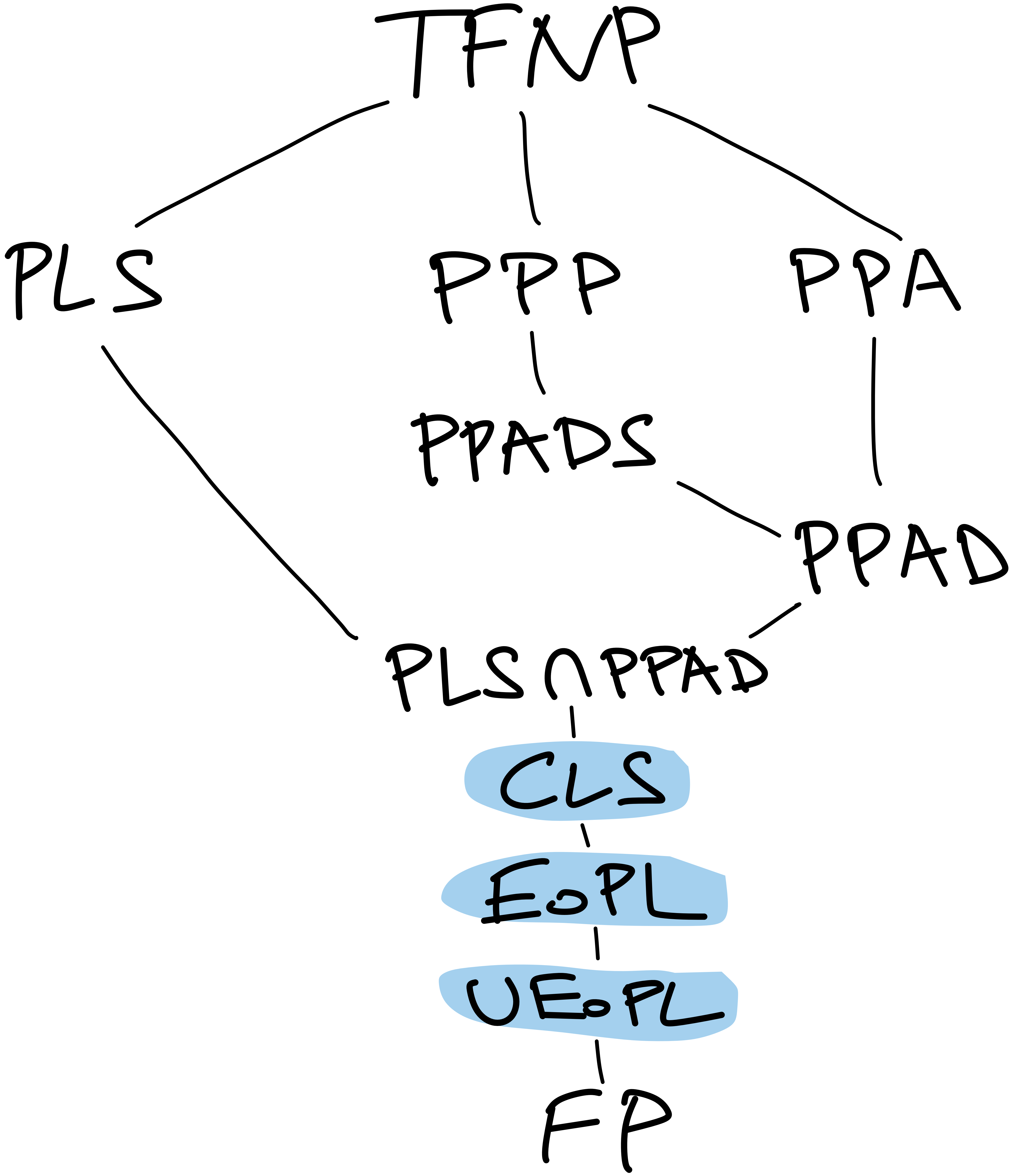
Black-box

Classical hierarchy (90's and 00's)



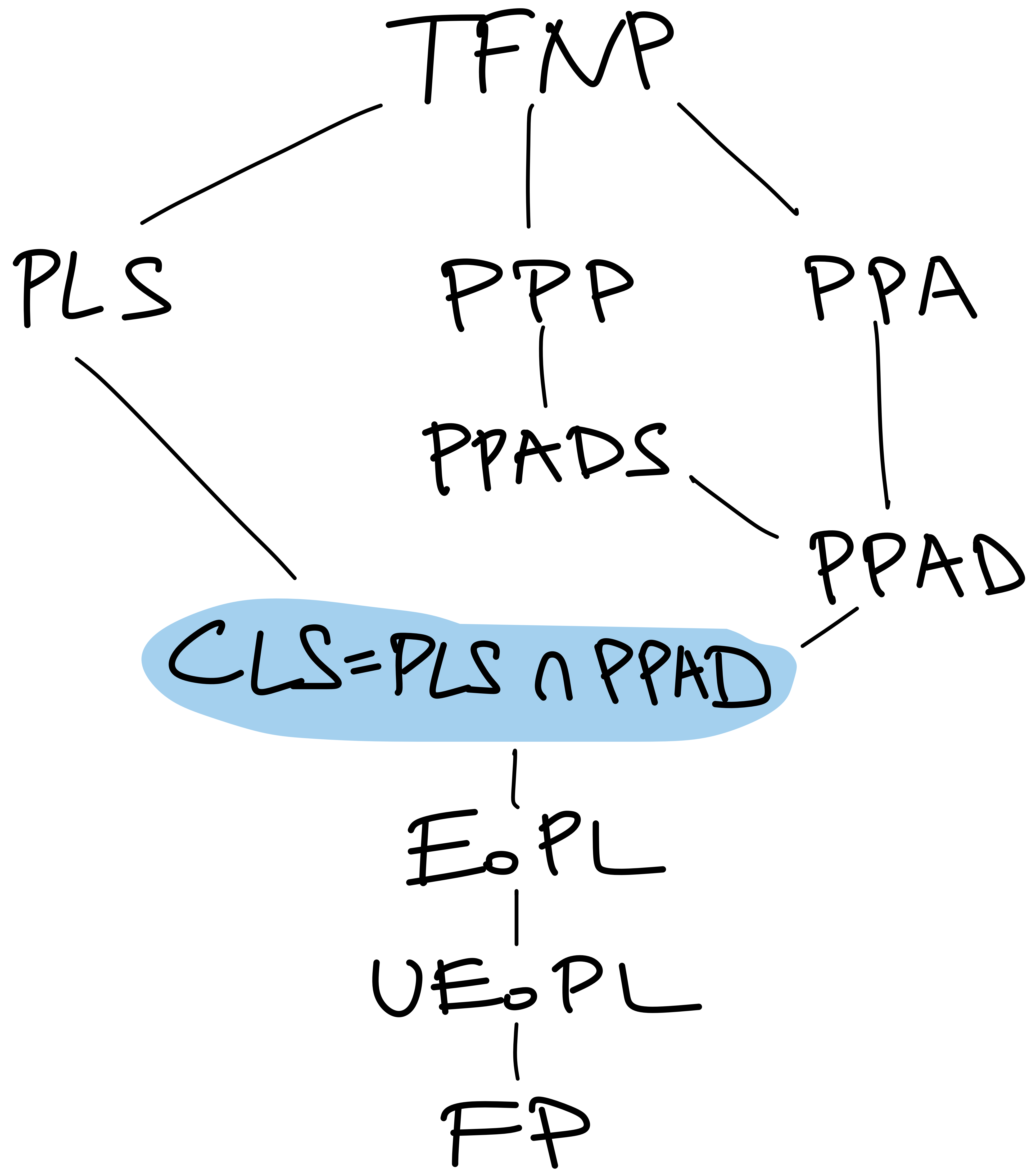
[Pap94]
[JPY88]

New classes (10's)



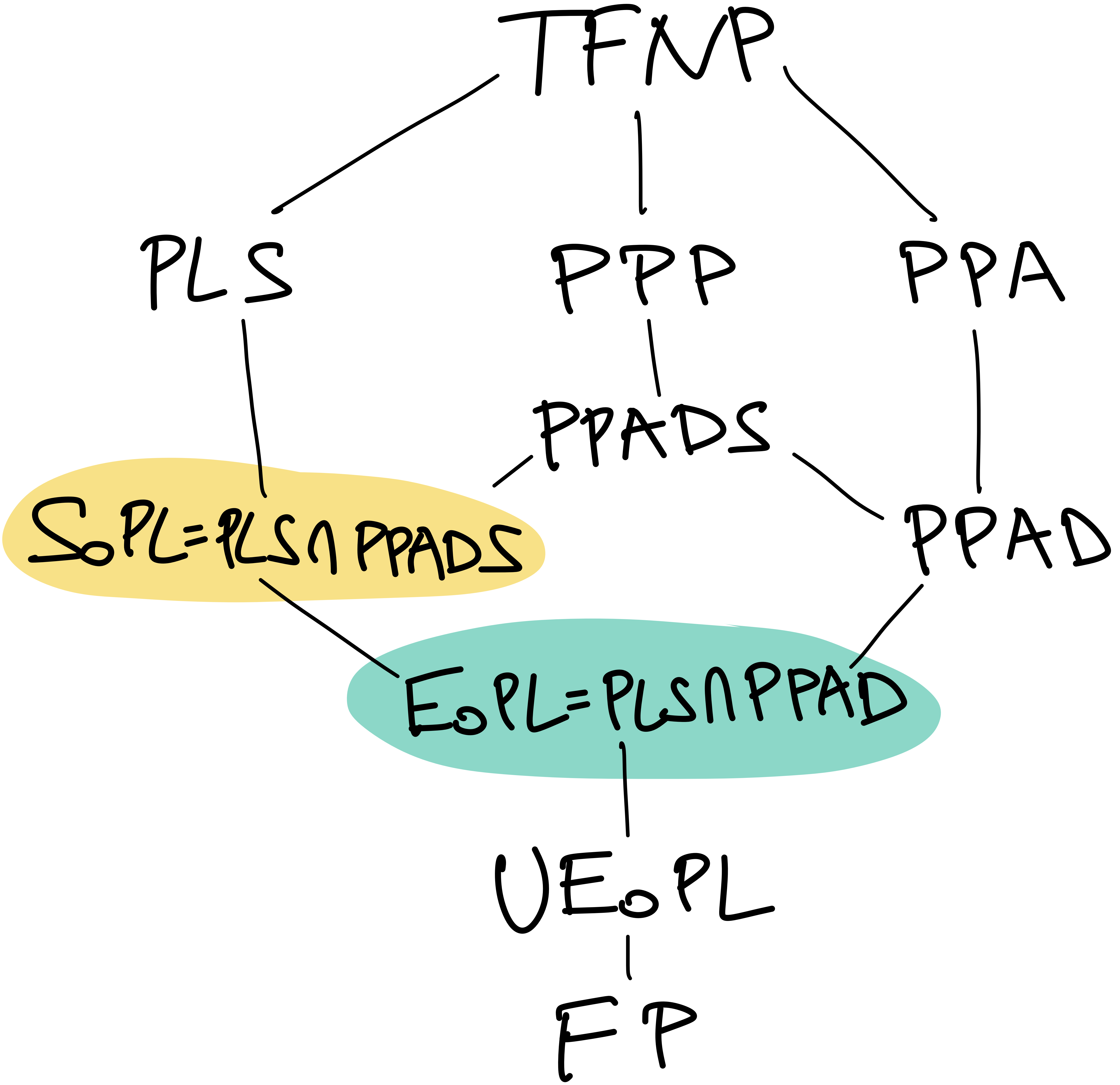
[HY20]
[FGMS20]
[DP11]

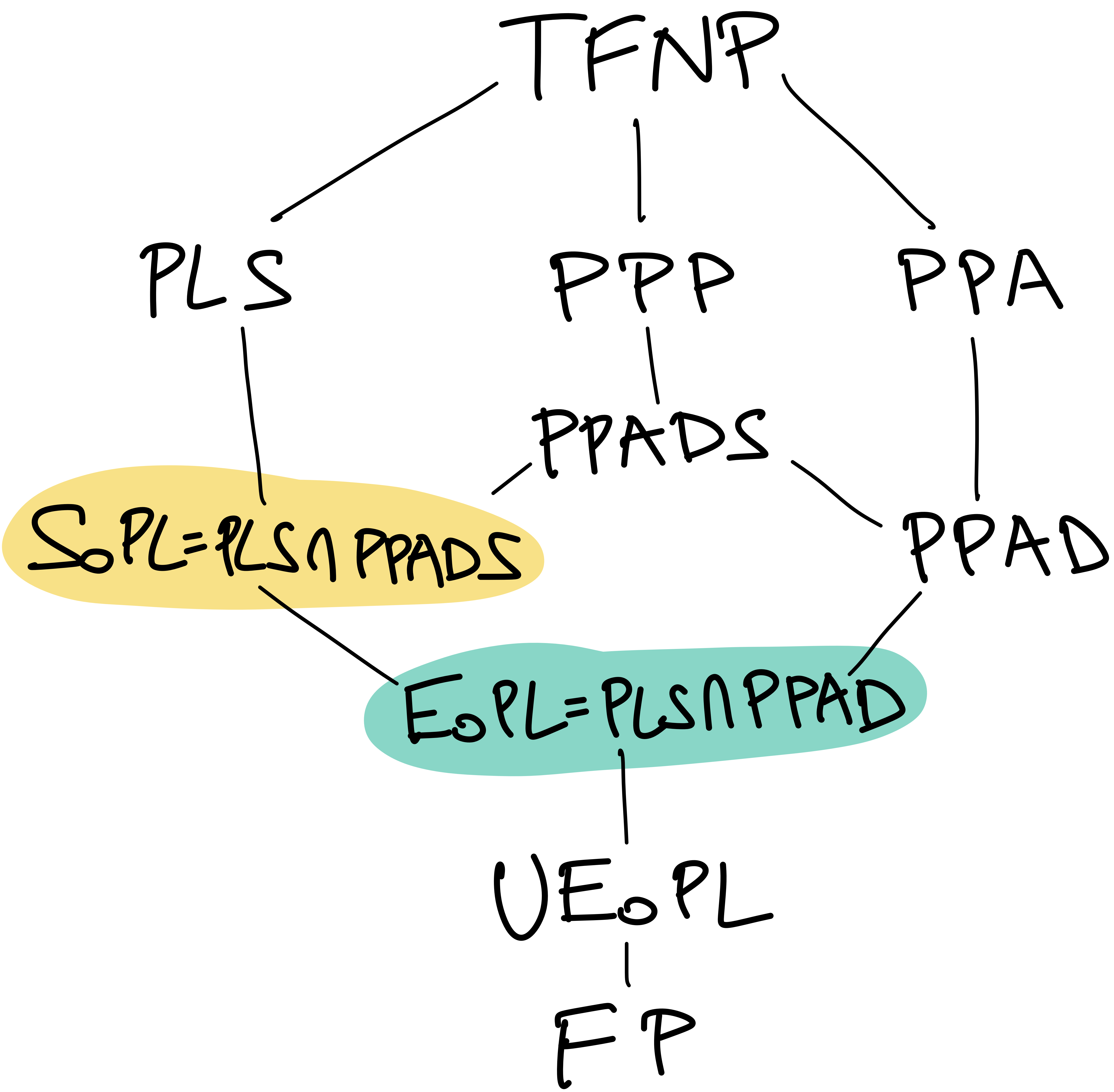
A Breakthrough Collapse (2021)



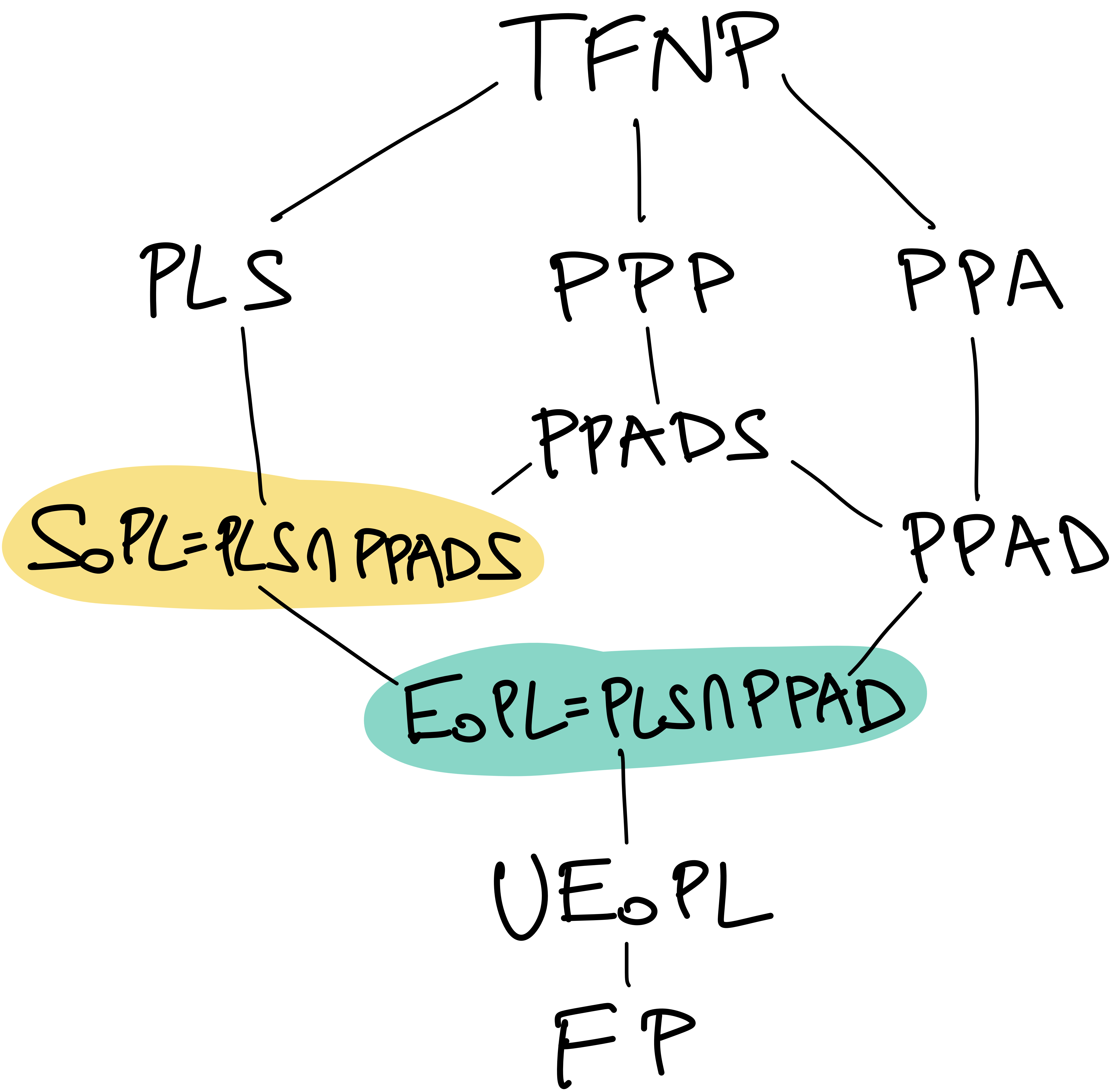
(Best paper!)
[FGHS21]

Further Collapses (2022)





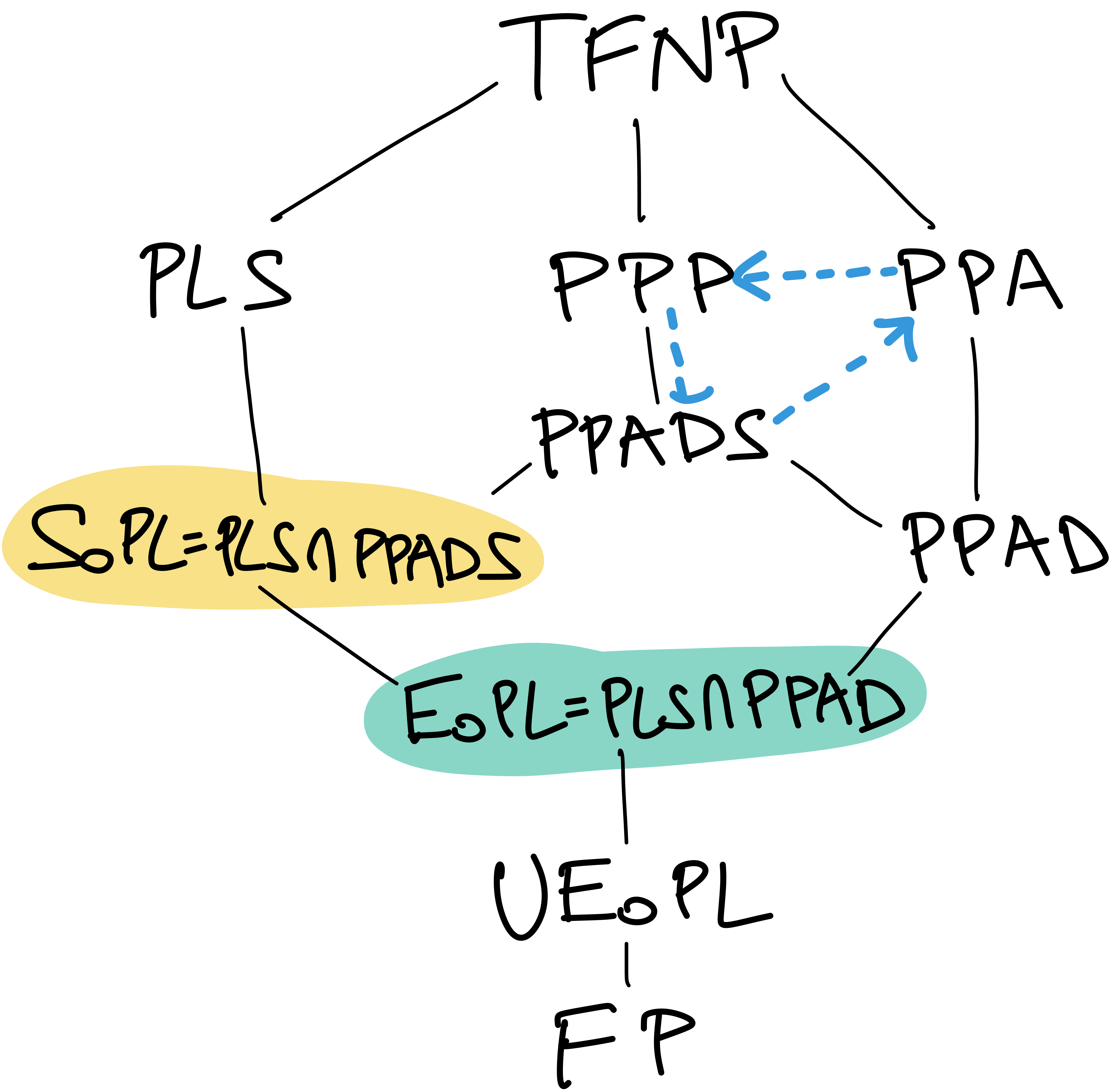
More Collapses?



More Collapses?

White-box sep. $\Rightarrow$ P $\neq$ NP

Black-box sep. possible

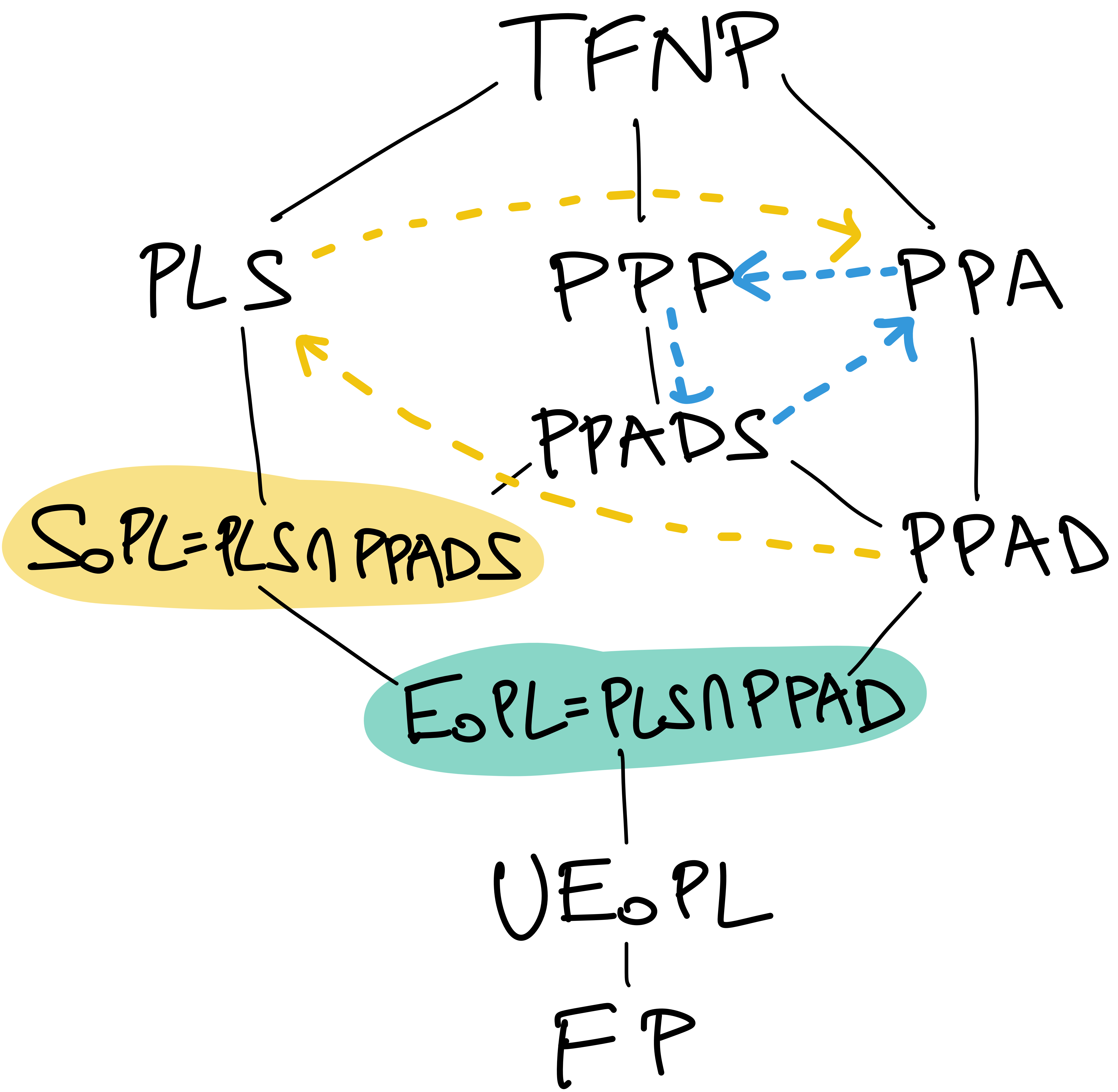


More Collapses?

White-box sep. $\Rightarrow P \neq NP$

Black-box sep. possible

Beame et al. 98'



More Collapses?

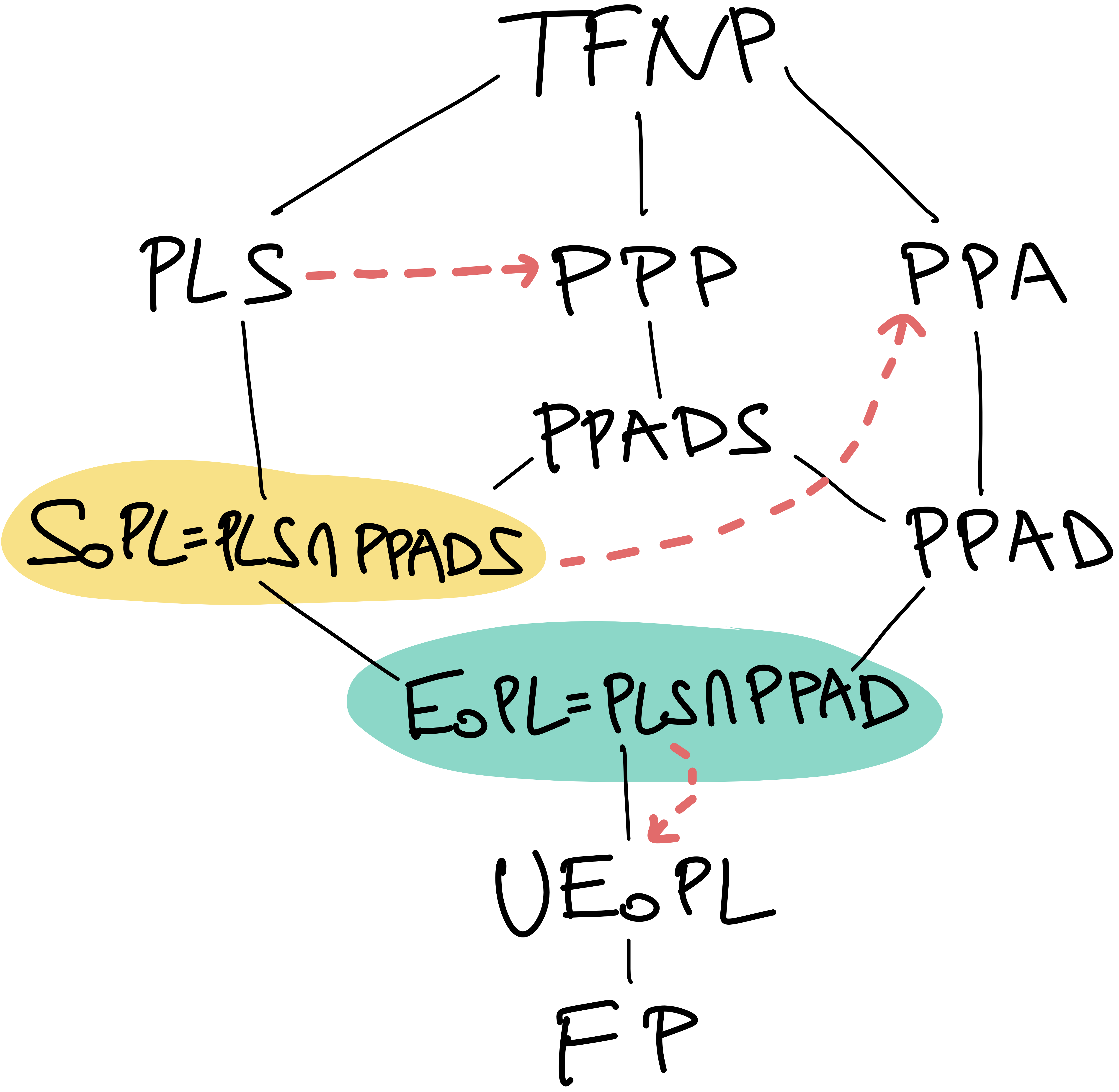
White-box sep. ⇒ P ≠ NP

Black-box sep. possible

Beame et al. 98'

Morioka 01'

Buresh-Openheim 04'



More Collapses?

NO MORE (BLACK-BOX)

OUR WORK

Image from https://fanart.tv/movie/9267/and-now-for-something-completely-different/

Resolution v.s. Sherali-Adams

Resolution

$$\frac{A \vee x \;,\; B \vee \neg x}{A \vee B}$$

measure : width

Simulated by

Sherali-Adams

$$\sum_i p_i(x) q_i(x) = 1 + J(x)$$

measure : degree

Resolution v.s. Sherali-Adams

Resolution

$$\frac{A \vee x \,,\; B \vee \neg x}{A \vee B}$$

measure: width

Simulated by

Sherali-Adams

$$\sum_i p_i(x) q_i(x) = 1 + J(x)$$

measure: degree

OUR RESULT: Simulation needs exp. large coefficients

Resolution v.s. Sherali-Adams

Resolution

$$\frac{A \vee x, \quad B \vee \neg x}{A \vee B}$$

measure: width

Simulated by

Sherali-Adams

$$\sum_i p_i(x) q_i(x) = 1 + J(x)$$

measure: degree

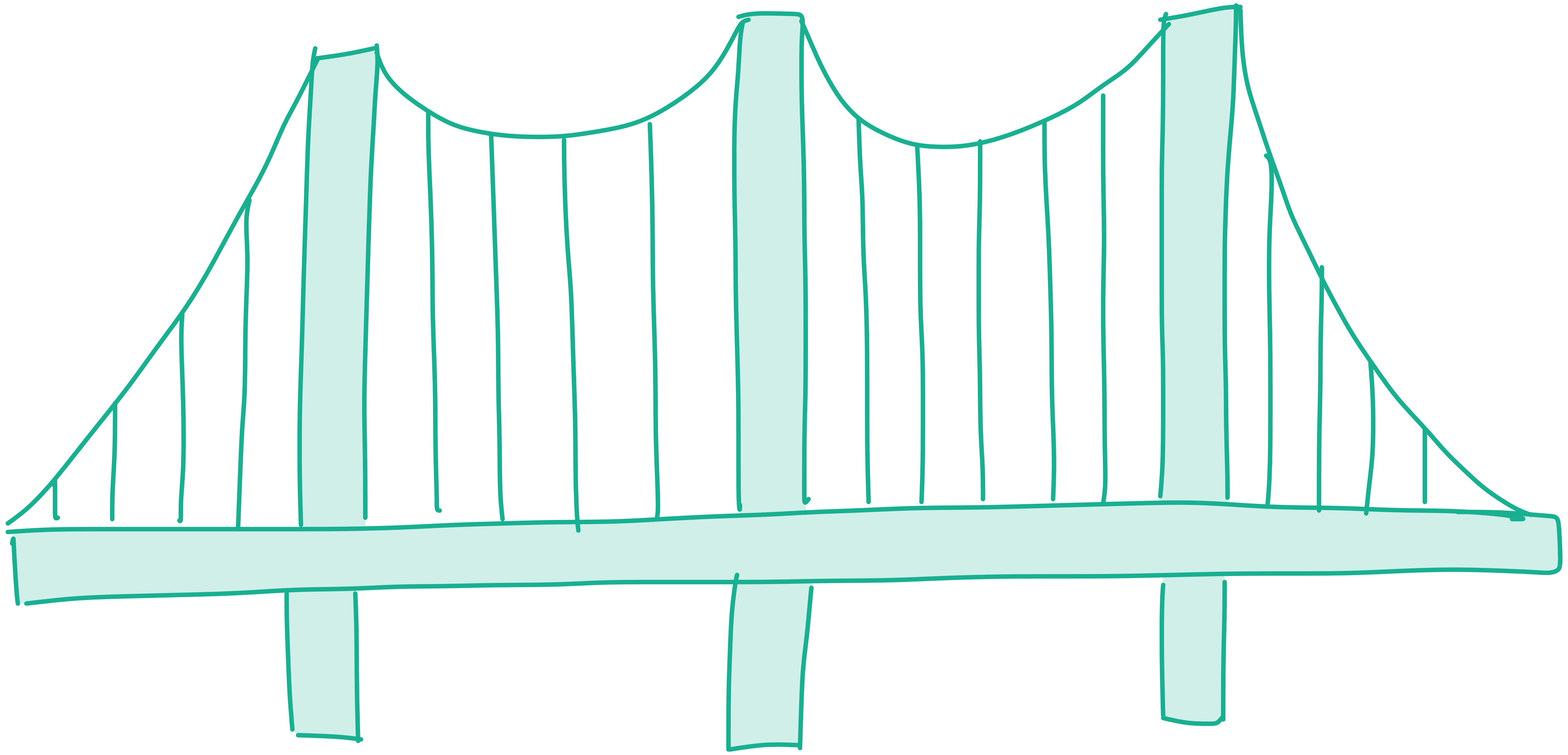
OUR RESULT: Simulation needs exp. large coefficients

$\Updownarrow$

PLS & PPADS

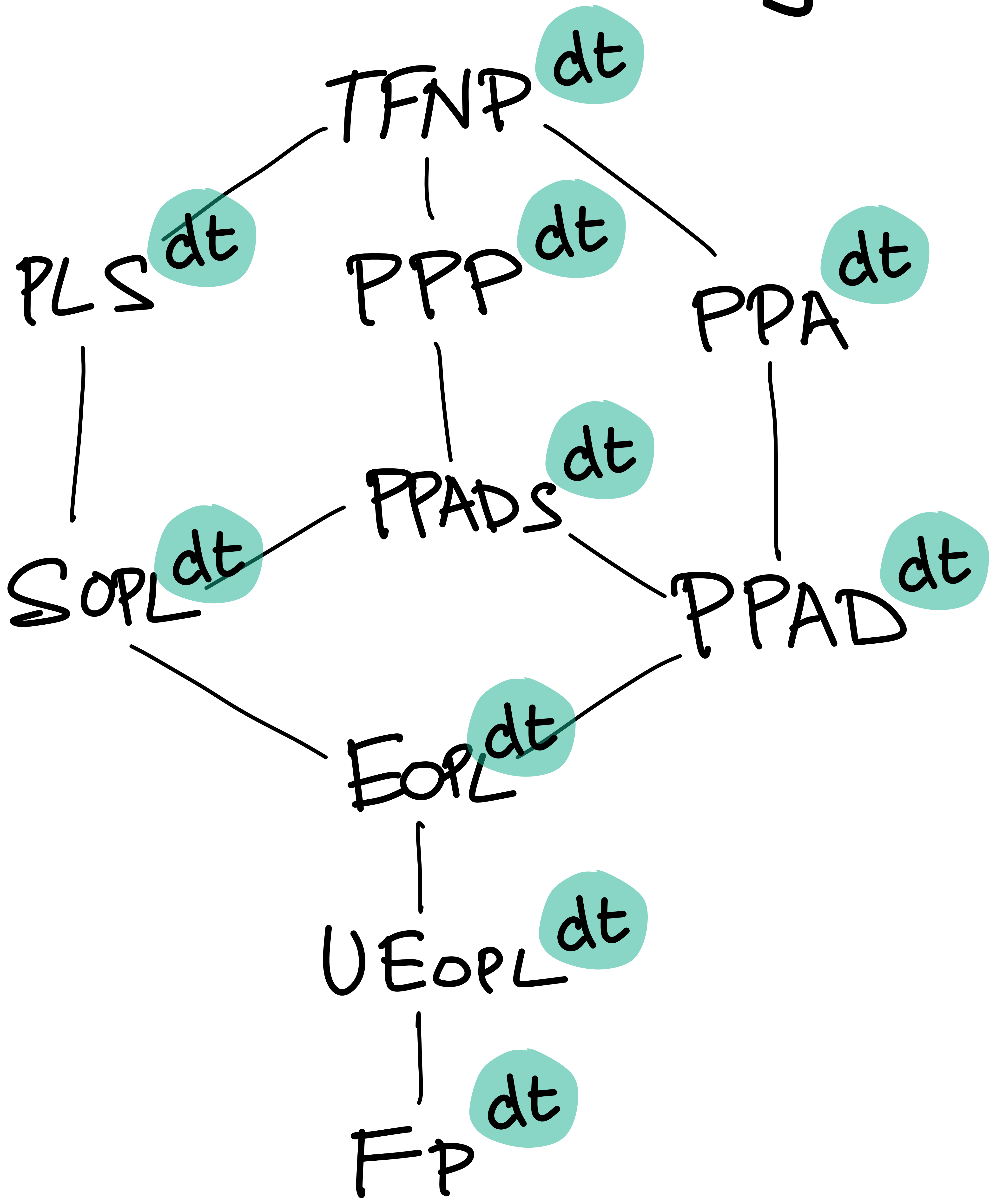
THE BRIDGE

Proof Complexity

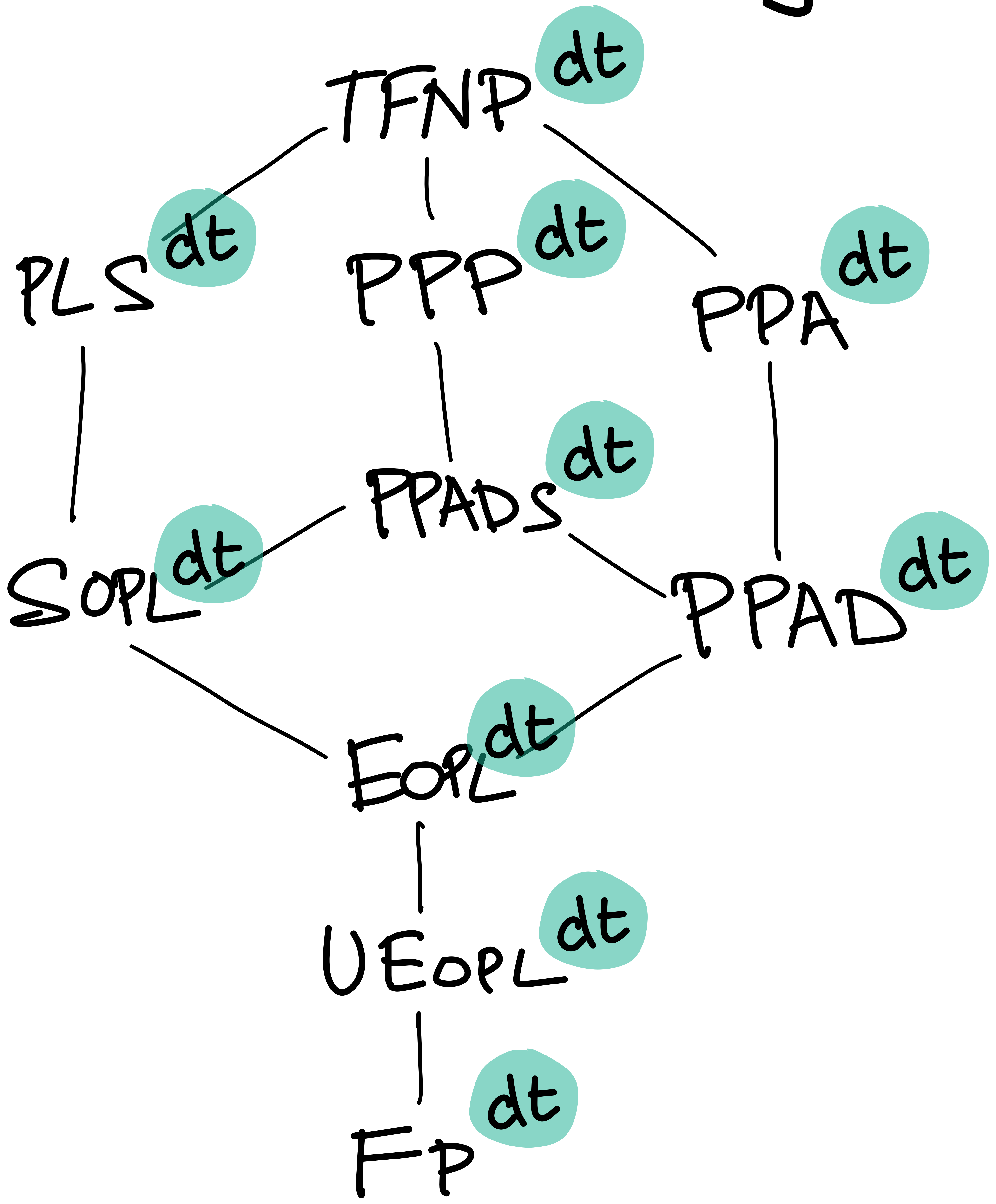


TFNP

World 1: Query analogues

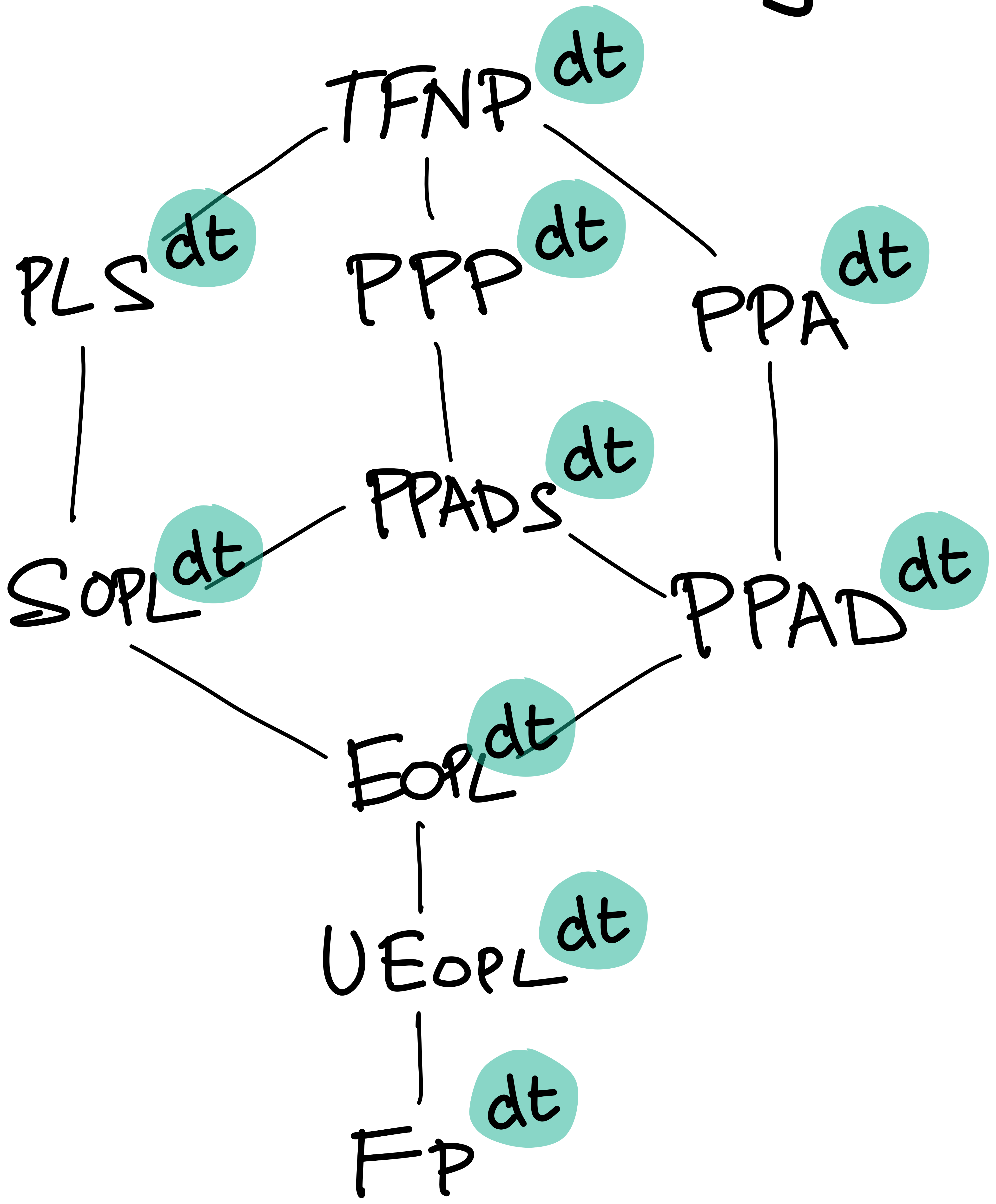


World 1: Query analogues



- dt
  $\equiv$
  query analogue

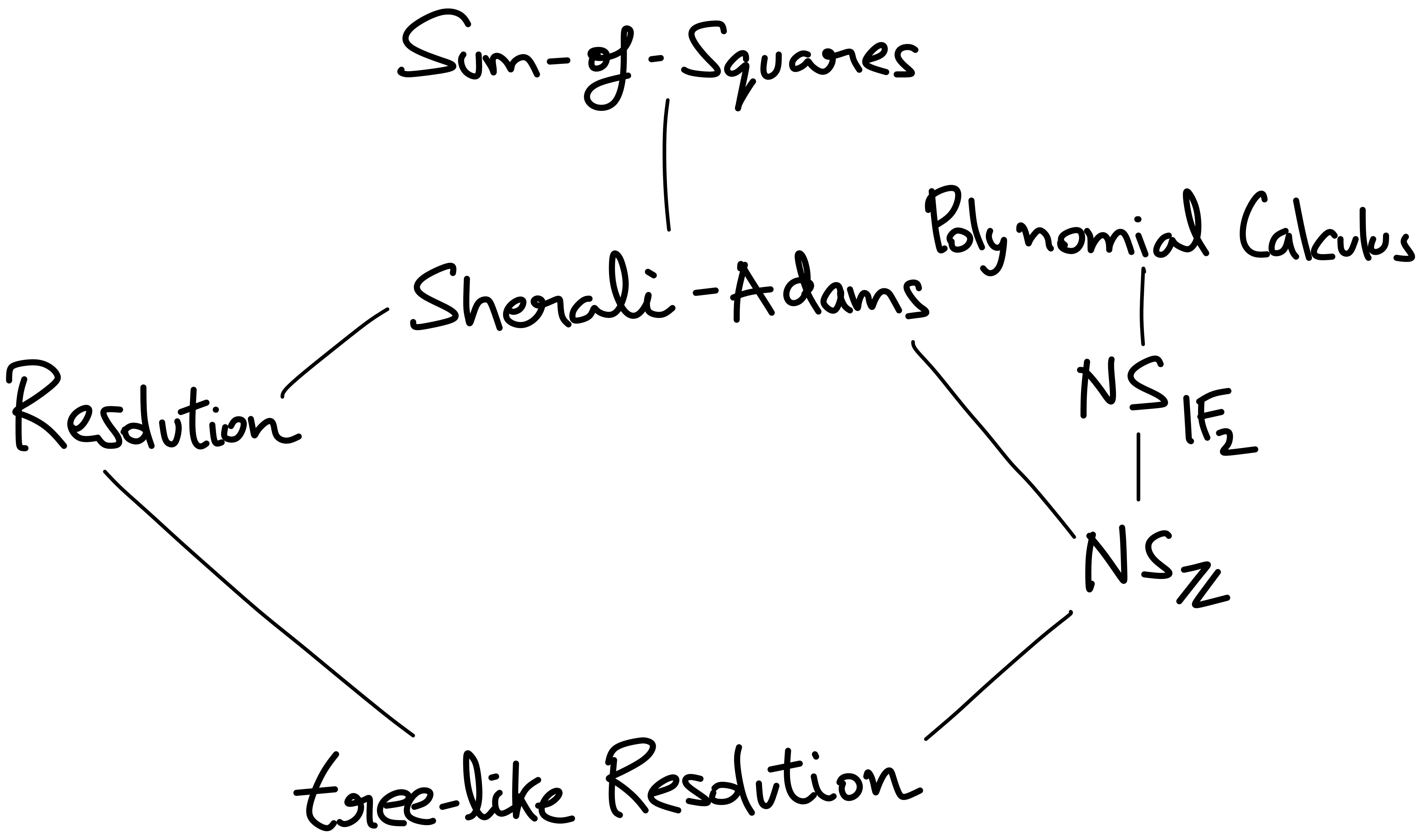
World 1: Query analogues



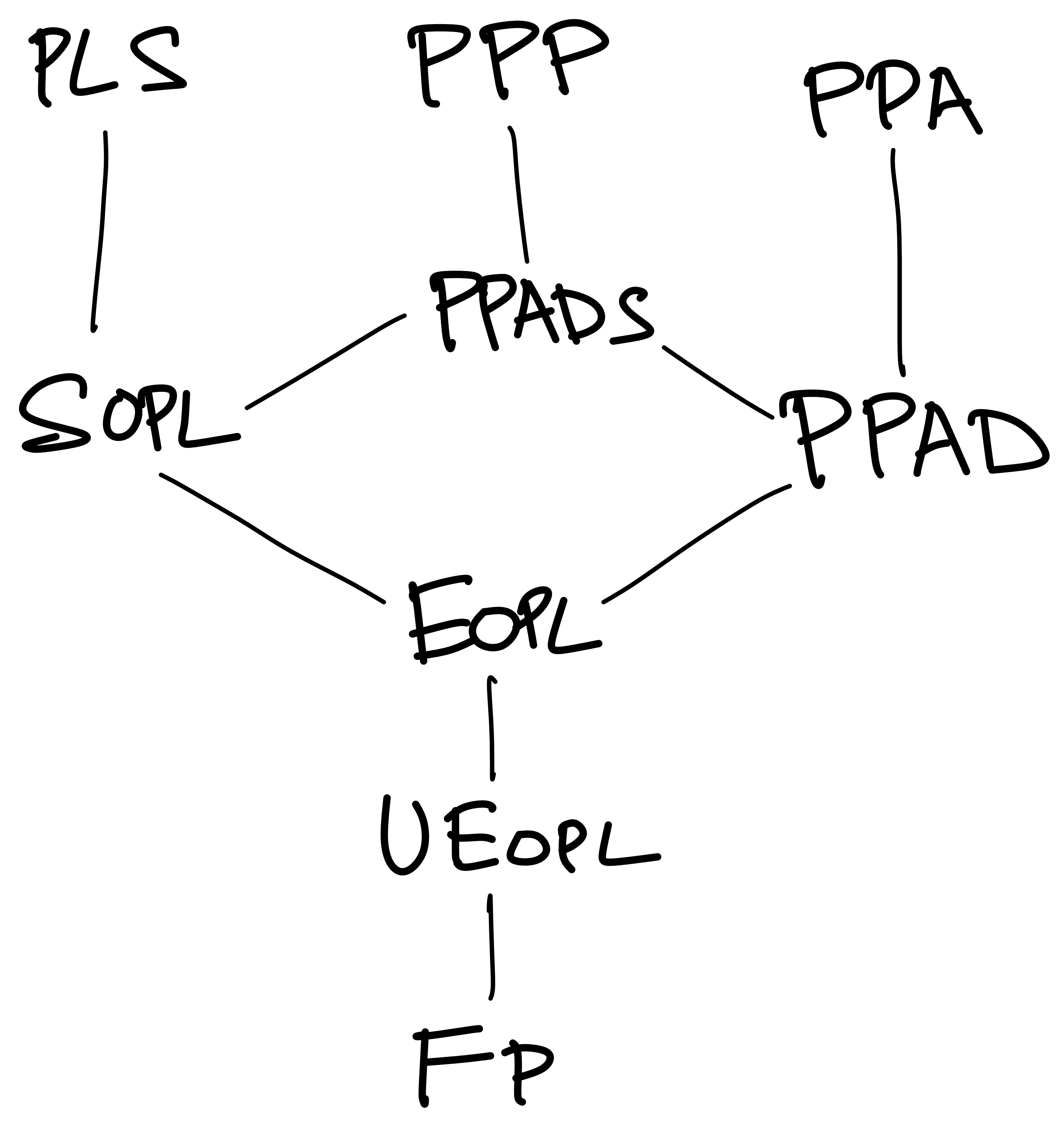
- dt ≡ query analogue
- Reductions ≡ shallow decision trees

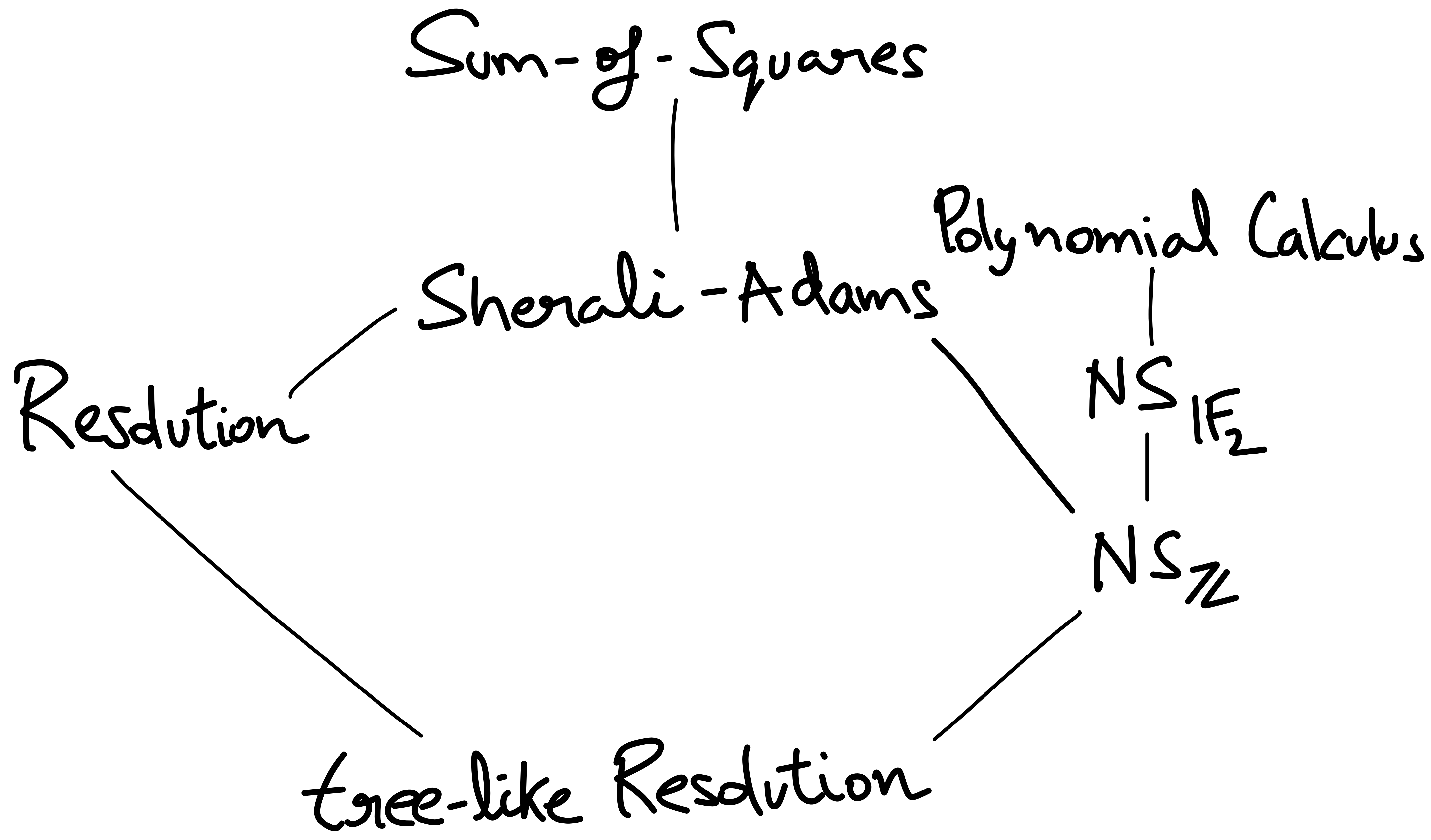
World 2: Proof Complexity

Is there a short derivation that this CNF is unsat?

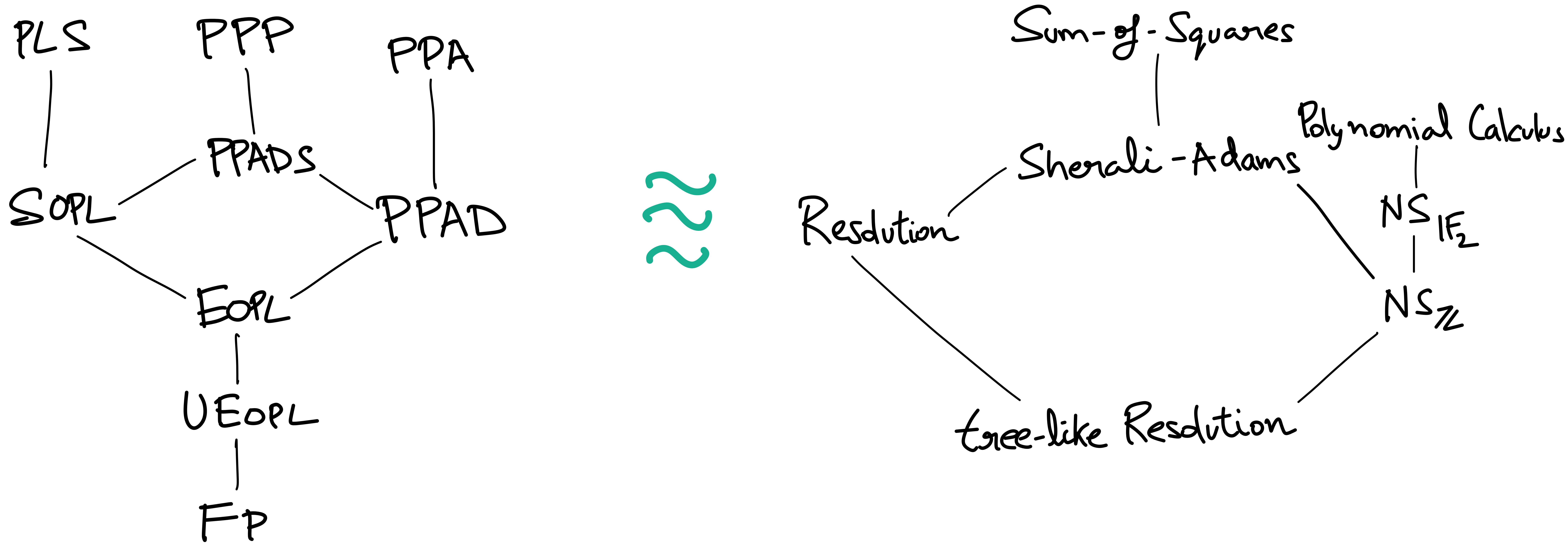


Time to squint





Time to squint



The Bridge: Characterizations

- TFNP^{dt} search problems can be translated into CNF fallacies

SINK-OF-DAG $\mapsto$ "this dag has no sinks"

The Bridge: Characterizations

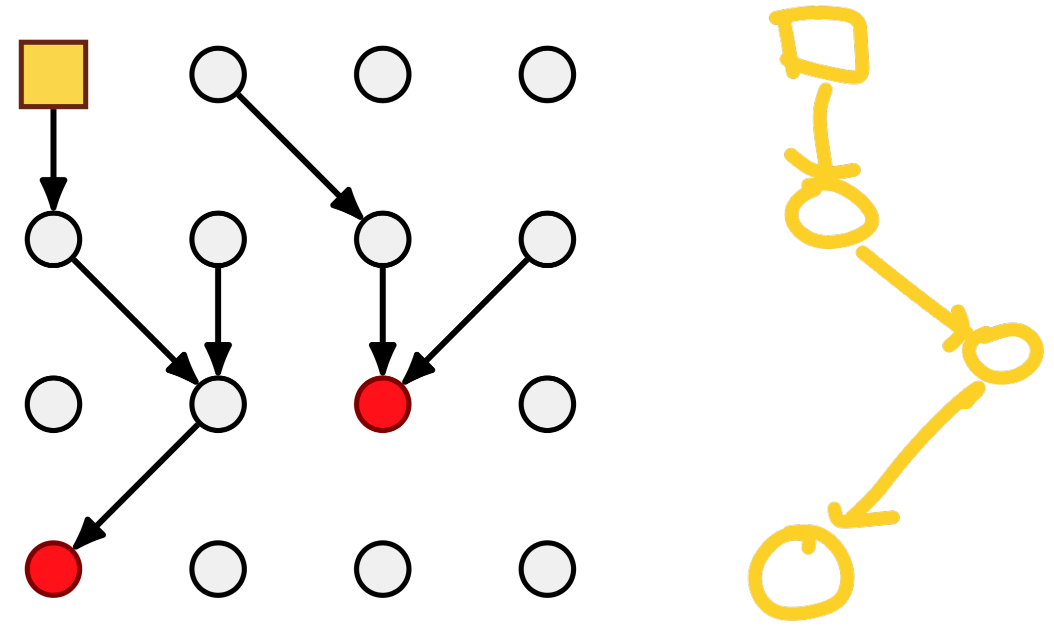
- TFNP^{dt} search problems can be translated into CNF fallacies

SINK-OF-DAG $\mapsto$ "this dag has no sinks"

Example: Res Width $\lesssim \mathrm{PLS}^{dt}$ depth

Search $\mapsto$ CNF

Keep going down the dag



The Bridge: Characterizations

- TFNP^{dt} search problems can be translated into CNF fallacies

- CNF fallacies define search problems

$$\varphi = x_1 \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge x_2 \longmapsto \text{find}(x_1, x_2)$$

falsified clause

The Bridge: Characterizations

- TFNP^{dt} search problems can be translated into CNF fallacies

- CNF fallacies define search problems

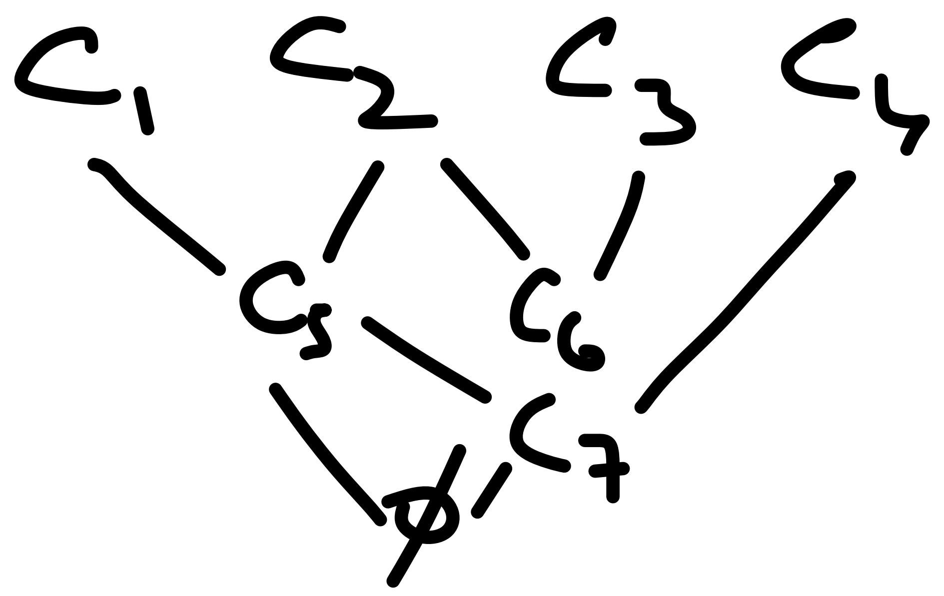
$$\varphi = x_1 \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge x_2 \mapsto \text{find}(x_1, x_2)$$

falsified clause

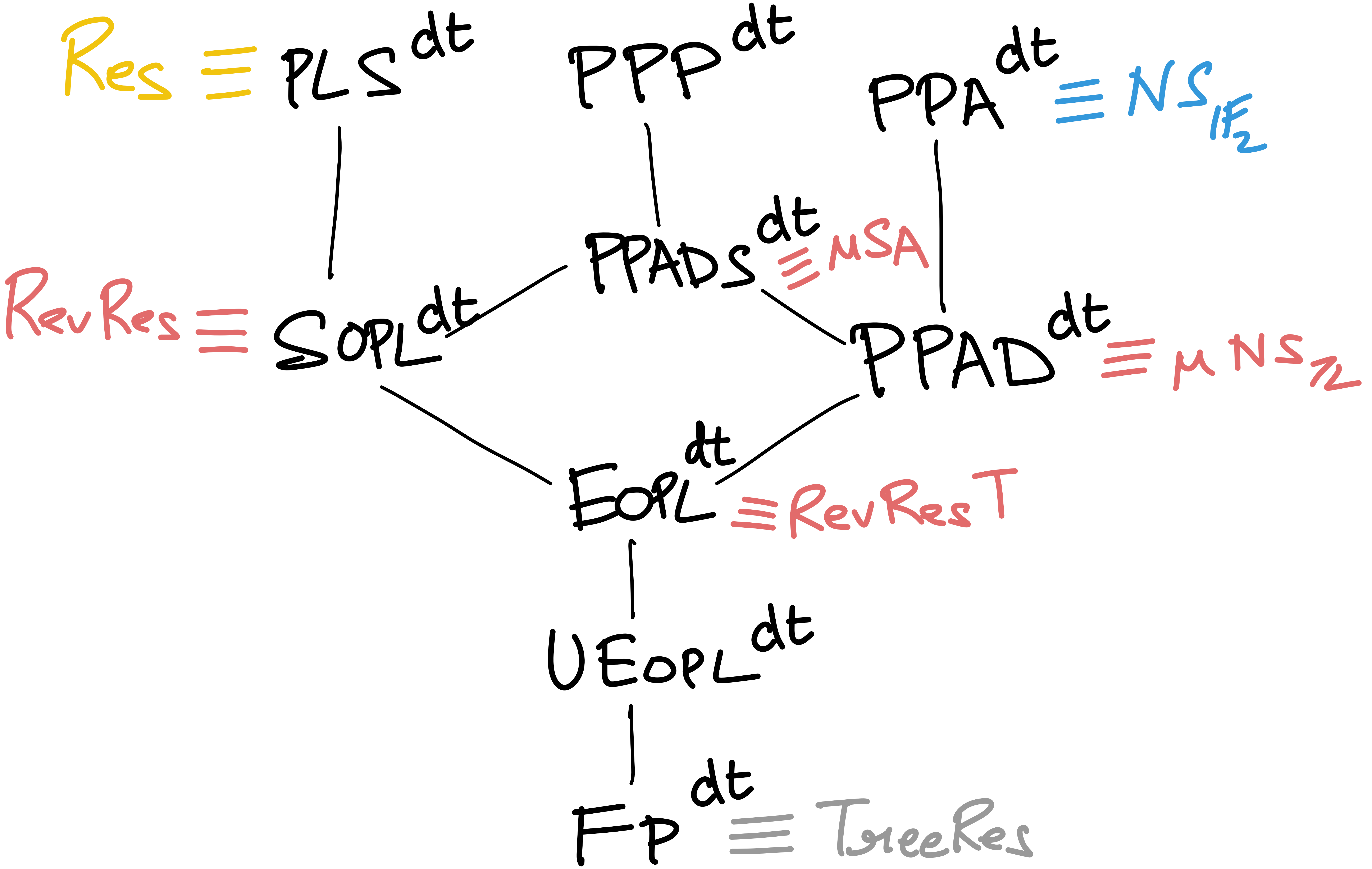
Example: Res Width $\gtrsim \mathrm{PLS}^{dt}$ depth

CNF $\mapsto$ Search

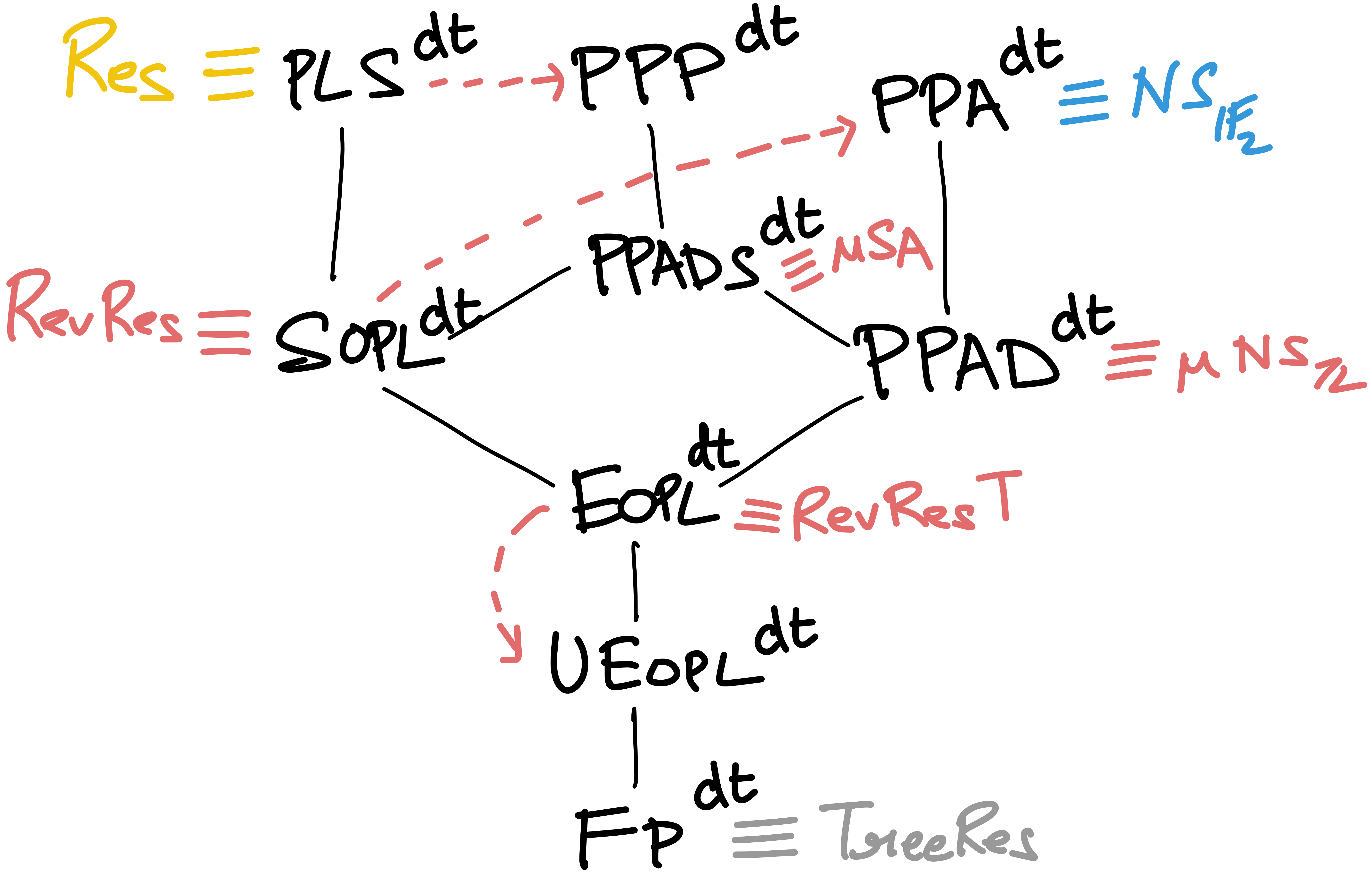
"Flip" proof



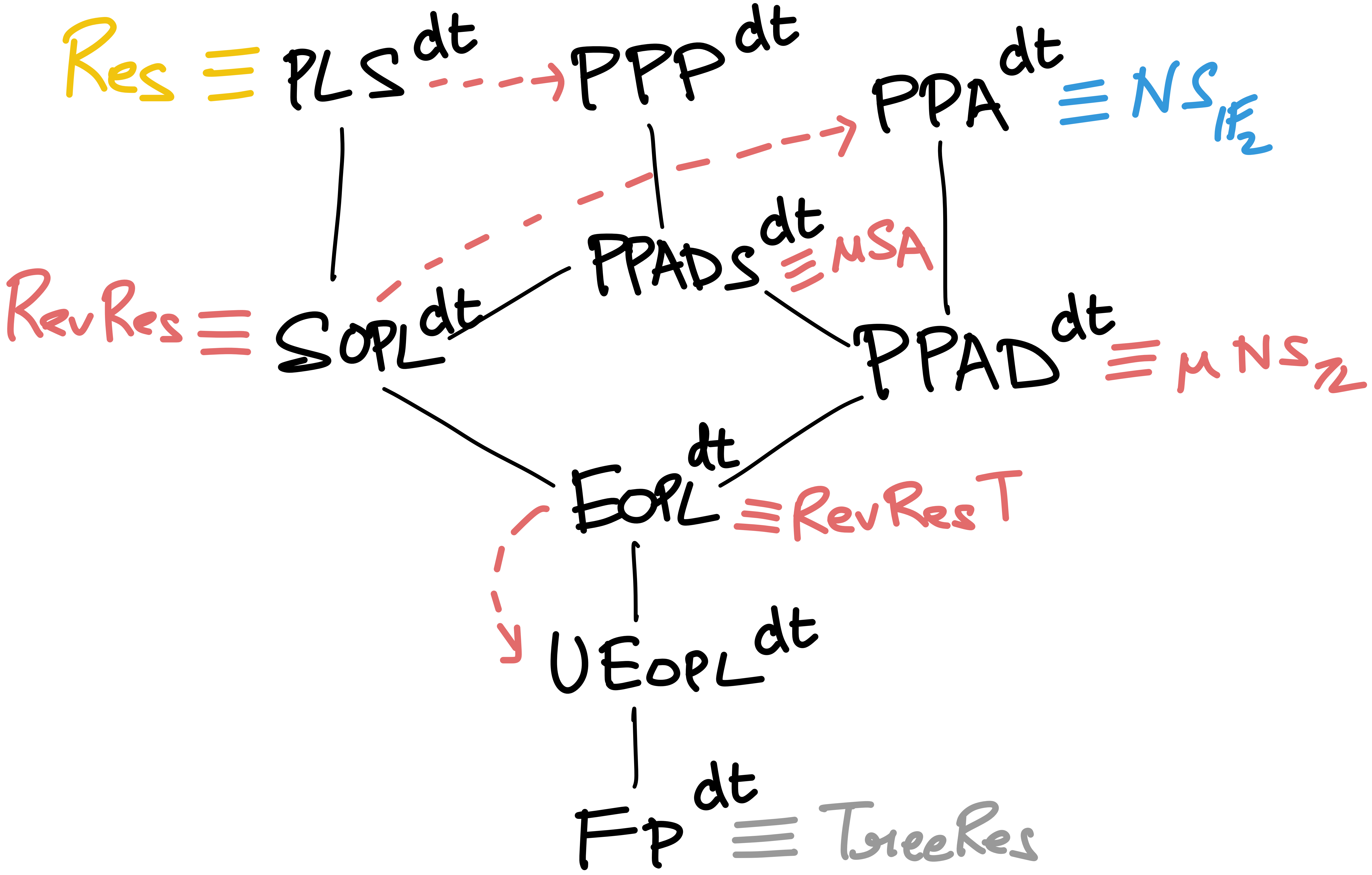
The Bridge: Characterizations



The Bridge: Characterizations

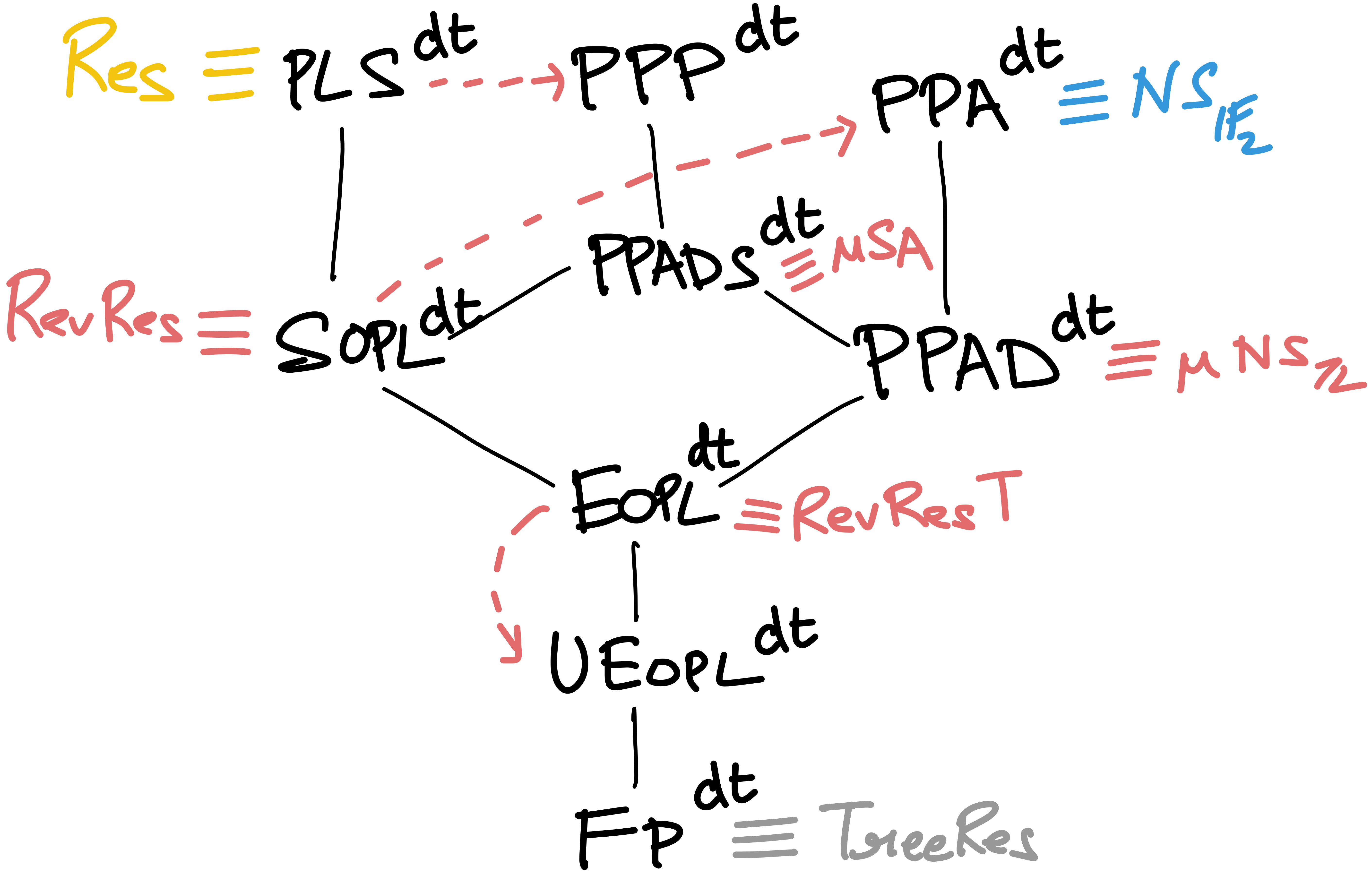


The Bridge : Characterizations



Results rephrased:

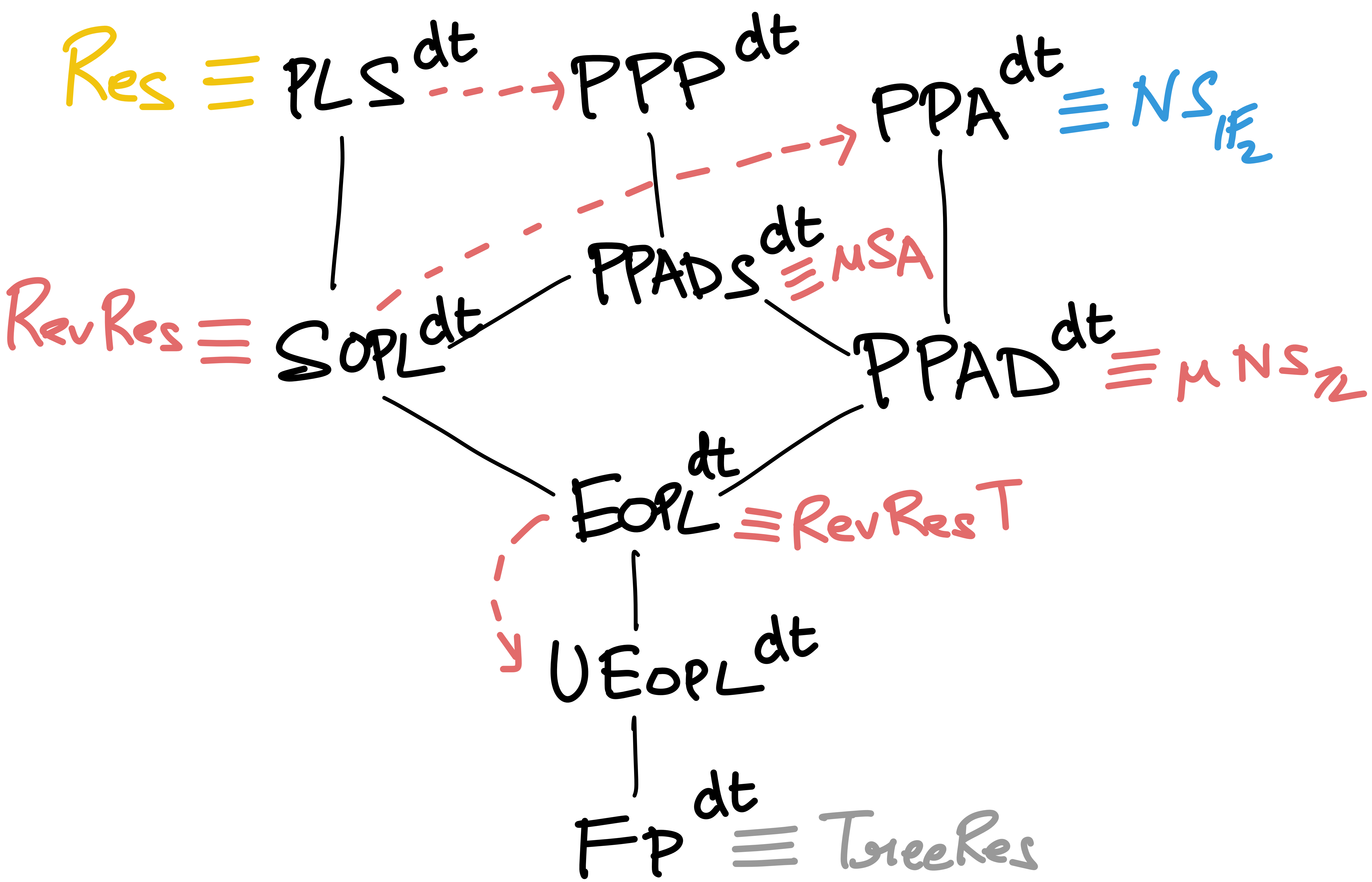
The Bridge: Characterizations



Results rephrased:

- $\mathrm{Res} \not\subseteq \mu\mathrm{SA}$

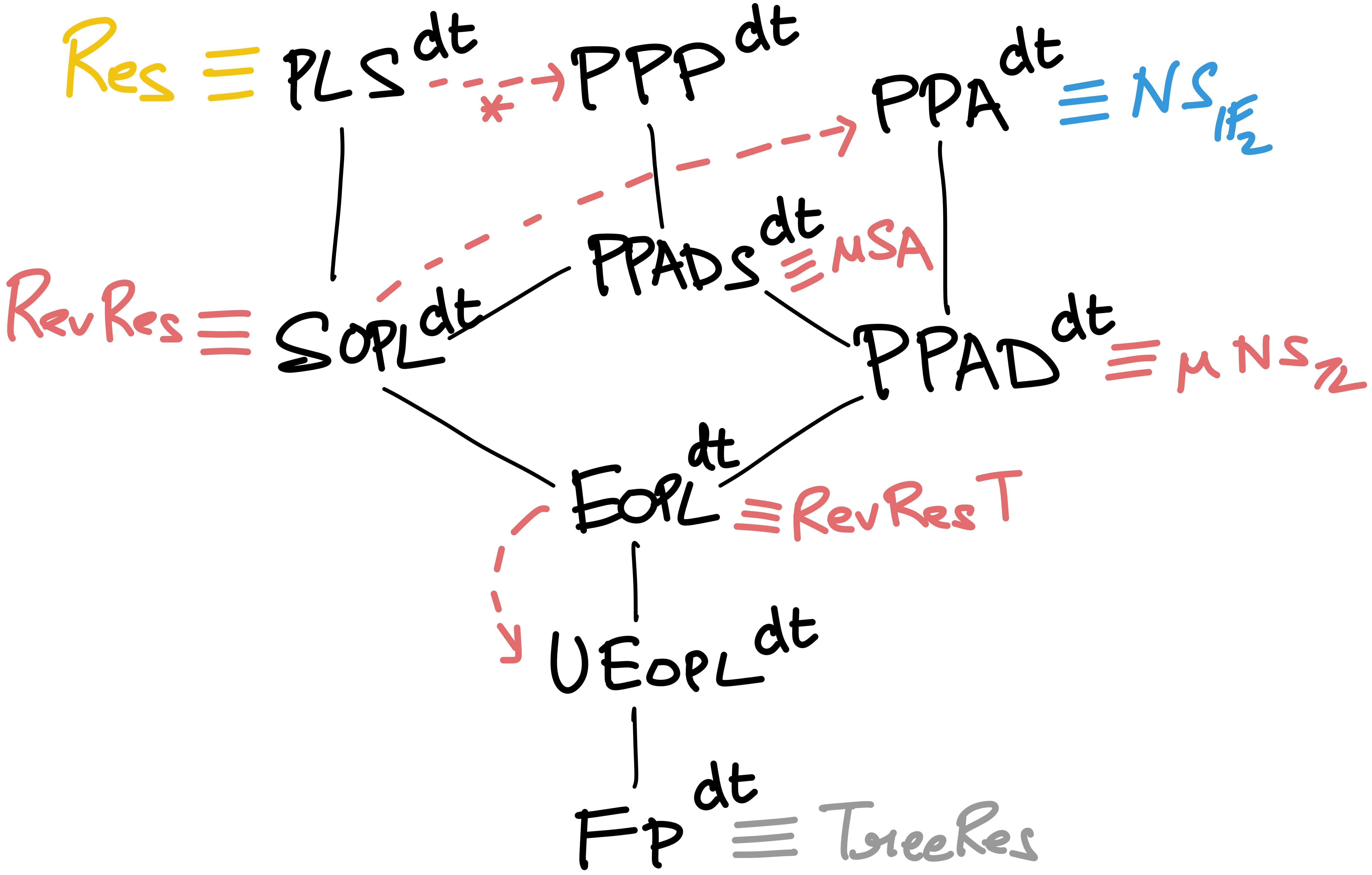
The Bridge: Characterizations



Results rephrased:

- Res $\not\subseteq$ μSA
- RevRes $\not\subseteq$ NS

The Bridge : Characterizations

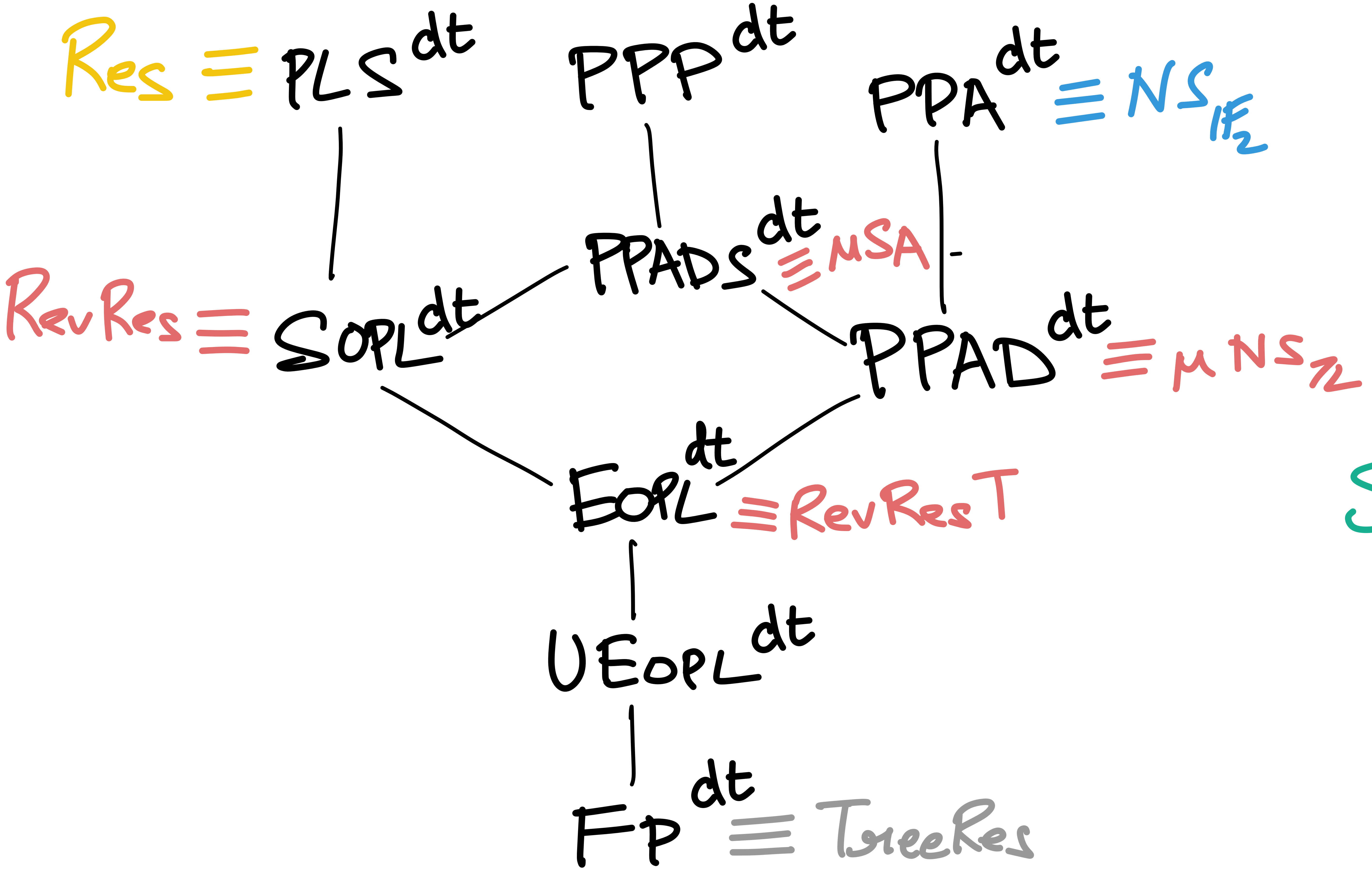


Results rephrased:

- Res $\not\subseteq$ μSA
- RevRes $\not\subseteq$ NS

* Independent work [BT22]

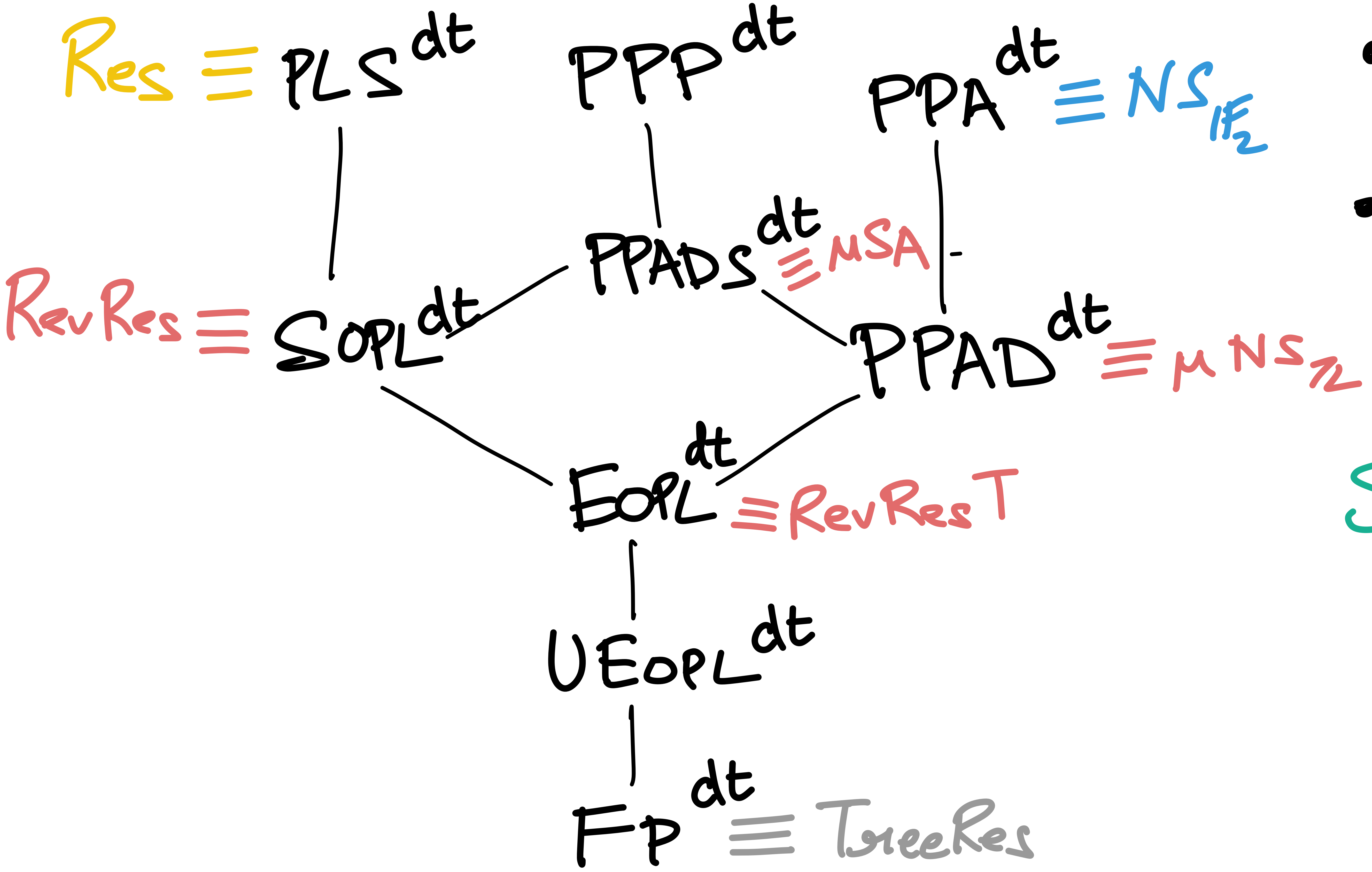
Open Problems



Characterizations

Structure of TFNP

Open Problems



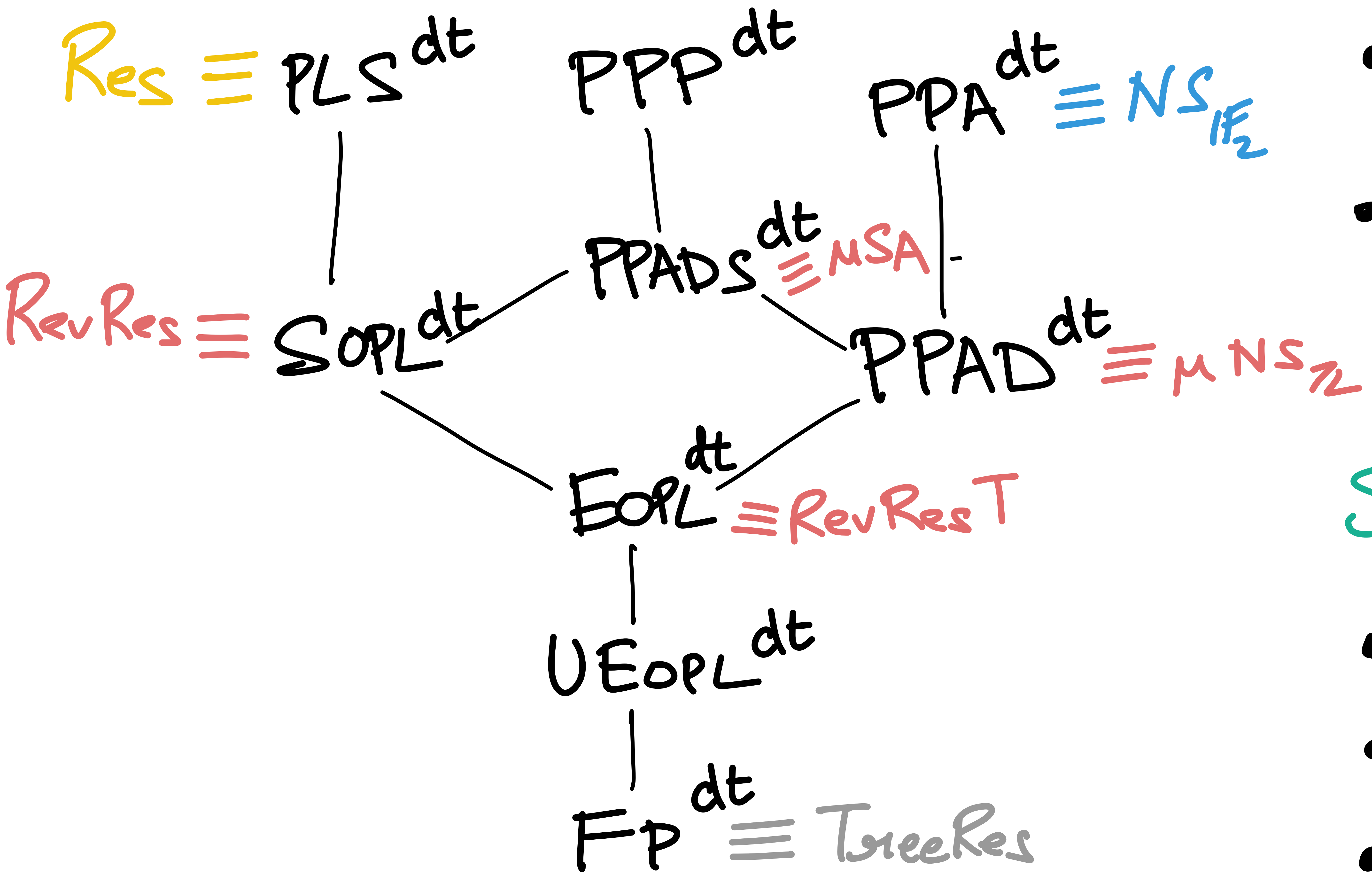
Characterizations

- PPP? UEoPL?
- SoS? [BFI22]

~~Polynomial Calculus~~?

Structure of TFNP

Open Problems



Characterizations

- PPP? UEOPL?
- SoS? [BFI22]
  ~~Polynomial Calculus~~?

Structure of TFNP

- PWPP?
- RAMSEY? SUNFLOWER?
- FACTORING?

Thanks!

for your attention

On Separations

On Separations

Key Lemma: Robust separation of SOPL from NS

On Separations

Key Lemma : Robust separation of SOPL from NS

SoD without merging of paths

On Separations

SoD without merging of paths

Key Lemma: Robust separation of SOPL from NS

$$\varepsilon\text{-NS} := \sum_{i \in [m]} p_i(x) \cdot a_i(x) = 1 \pm \varepsilon \quad \forall x \in \{0,1\}^n$$

On Separations

SoD without merging of paths

Key Lemma: Robust separation of SoPL from NS

$$\varepsilon\text{-NS} := \sum_{i \in [m]} p_i(x) \cdot a_i(x) = 1 \pm \varepsilon \quad \forall x \in \{0,1\}^n$$

NOTE: Not a Cook-Reckhow proof system!
Verification is CoNP-complete.

On Separations

SoD without merging of paths

Key Lemma: Robust separation of SOPL from NS

$$\varepsilon\text{-NS} := \sum_{i \in [m]} p_i(x) \cdot a_i(x) = 1 \pm \varepsilon \quad \forall x \in \{0,1\}^n$$

NOTE: Not a Cook-Reckhow proof system!
Verification is CoNP-complete.

Lemma: Every $\frac{1}{2}$-NS refutation of SOPL_n requires deg $n^{\Omega(1)}$.

On Separations

SoD without merging of paths

Key Lemma: Robust separation of SoPL from NS

$$\varepsilon\text{-NS} := \sum_{i \in [m]} p_i(x) \cdot a_i(x) = 1 \pm \varepsilon \quad \forall x \in \{0,1\}^n$$

NOTE: Not a Cook-Reckhow proof system!
Verification is CoNP-complete.

Lemma: Every $\frac{1}{2}$-NS refutation of $SoPL_n$ requires deg $n^{\Omega(1)}$.

IDEA: Randomized decision-to-search reduction in the style of Raz-Wigderson 92'.
We show that ε-NS proofs imply approx poly for OR.

On Separations

Lemma: Every $\frac{1}{2}$-NS refutation of SOPL_n requires deg $n^{\Omega(1)}$.

$\Downarrow$

Lemma: Any degree-$n^{O(1)}$ SA proof of SoD_{n^2} requires coefficients of magnitude $\exp(\Omega(n))$.