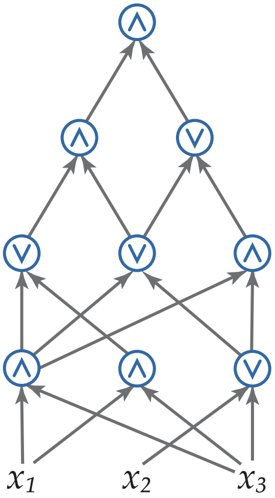
# Adventures in Monotone Complexity and **TFNP**


Mika Göös — *IAS*
Pritish Kamath — *MIT*
Robert Robere — *Rutgers & IAS*
Dmitry Sokolov — *KTH*

# Monotone complexity

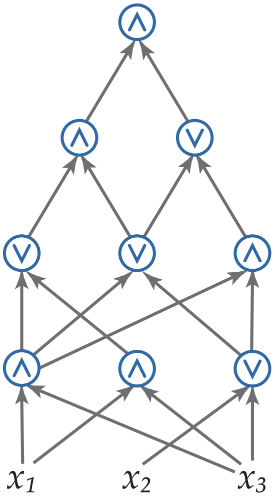



$f\colon \{0,1\}^n \to \{0,1\}$

**Monotone:**

$x \leq y \implies f(x) \leq f(y)$

# Monotone complexity




$f\colon \{0,1\}^n \to \{0,1\}$

**Monotone:**

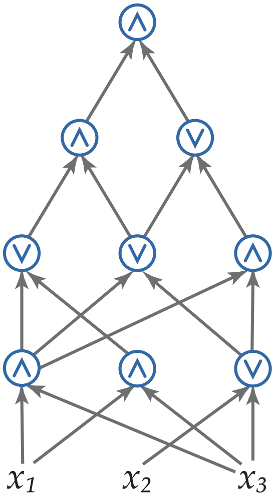
$x \leq y \implies f(x) \leq f(y)$

[Razborov'85]:

$k$-Clique: $\{0,1\}^{\binom{n}{2}} \to \{0,1\}$
has no small monotone circuits

$\implies$ **P** $\neq$ **NP** in monotone world

# Monotone complexity




$f\colon \{0,1\}^n \to \{0,1\}$

**Monotone:**

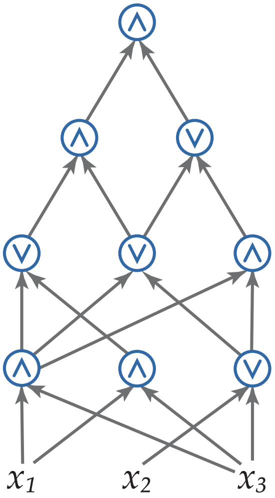
$x \le y \implies f(x) \le f(y)$

[Tardos'88]:

$\textsc{Tardos} \in \mathbf{P}$

has no small monotone circuits

# Monotone complexity




## Connections:

1. Communication complexity
   *KW games; communication* **TFNP**
2. Proof complexity
   *Monotone interpolation*
3. Extended formulations
   *Hrubeš–Razborov*
4. Cryptography
   *Secret sharing*

# Separation result

**Main Theorem**

Mon. circuit complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$

$$\begin{aligned} v_1 \oplus v_2 \oplus v_3 &= 1 \\ v_1 \oplus v_2 \oplus v_3 &= 0 \\ &\vdots \\ v_{n-2} \oplus v_{n-1} \oplus v_n &= 1 \end{aligned}$$

# Separation result

**Main Theorem**

Mon. circuit complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$

$$
\begin{array}{ccc}
\text{input } x & & \\
\downarrow & & \\
\mathbf{1} & v_1 \oplus v_2 \oplus v_3 & = 1 \\
\mathbf{0} & v_1 \oplus v_2 \oplus v_3 & = 0 \\
\vdots & \vdots & \\
\mathbf{1} & v_{n-2} \oplus v_{n-1} \oplus v_n & = 1
\end{array}
$$

# Separation result

**Main Theorem**

Mon. circuit complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$

input $x$

$$\begin{array}{ccrcl} \downarrow & & & & \\ \mathbf{1} & & v_1 \oplus v_2 \oplus v_3 & = & 1 \\ \mathbf{0} & & v_1 \oplus v_2 \oplus v_3 & = & 0 \\ \vdots & & \vdots & & \\ \mathbf{1} & & v_{n-2} \oplus v_{n-1} \oplus v_n & = & 1 \end{array}$$

$\textsc{Xor-Sat}_n(x) = 1 \iff x$ is unsatisfiable

# Separation result

**Main Theorem**

Mon. circuit complexity of $\textsc{Xor-Sat}_n$ is $2^{n^{\Omega(1)}}$

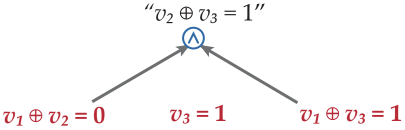
**Monotone vs. non-monotone separations:**

- $\textsc{Xor-Sat} \in \mathbf{NC}^2$
- $\textsc{Tardos} \in \mathbf{P}$ [Tardos'88]
- $\textsc{Matching} \in \mathbf{RNC}^2$ [Razborov'85]

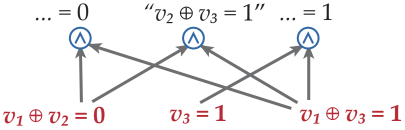
# Example monotone computation

$v_1 \oplus v_2 = 0$ $\qquad v_3 = 1$ $\qquad v_1 \oplus v_3 = 1$

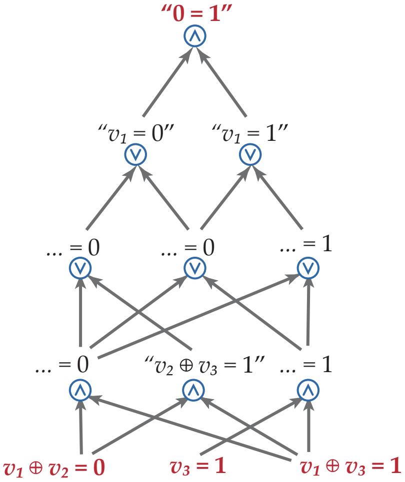
# Example monotone computation



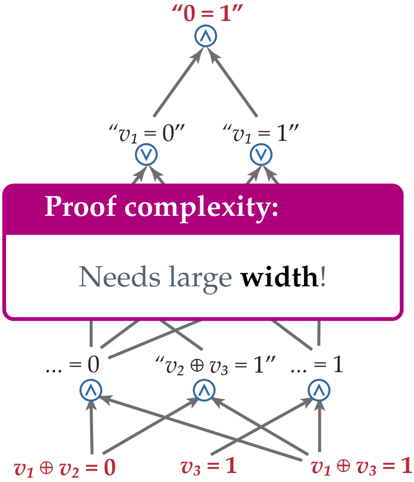
# Example monotone computation



# Example monotone computation



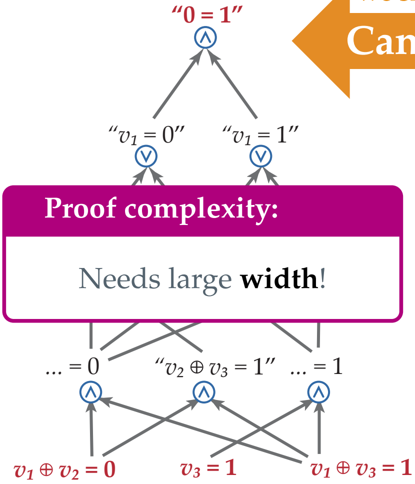
# Example monotone computation




**Proof complexity:**

Needs large **width**!

# Example monotone computation

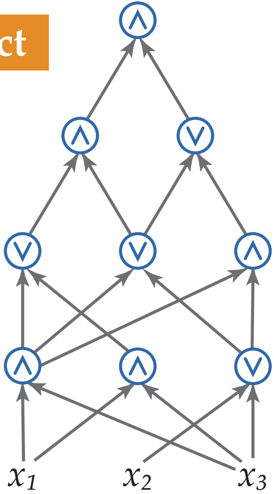



**Proof complexity:**

Needs large **width**!

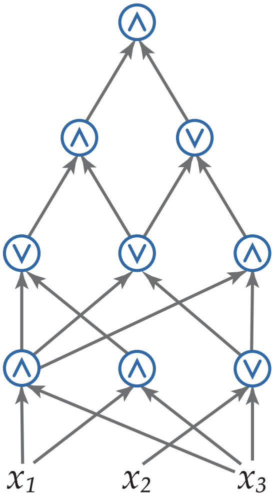
we show:

**Can extract**



## Circuits $\leftrightarrow$ Communication protocols

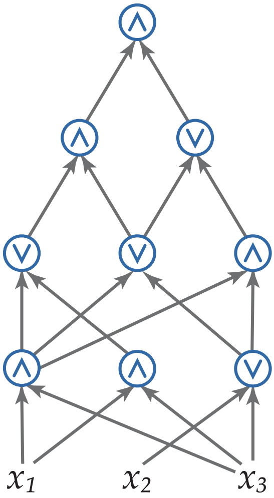
*Karchmer–Wigderson, 1988*
*Razborov, 1995*




# Monotone KW game

for monotone $f\colon \{0,1\}^n \to \{0,1\}$

| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |




## Monotone KW game

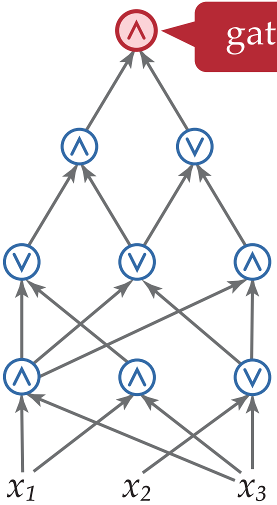
for monotone $f\colon \{0,1\}^n \to \{0,1\}$

| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |

**Theorem** [KW'88]

Mon. circuit depth of $f$
$=$ CC of **mKW game**

# Circuit depth [KW'88]



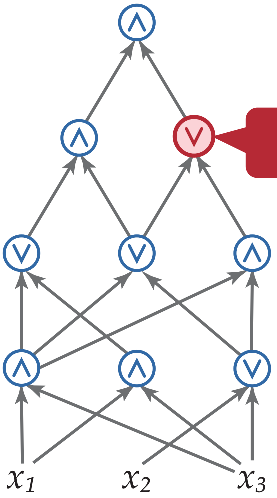

## e KW game

$f\colon \{0,1\}^n \to \{0,1\}$

| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |

**Theorem** **[KW'88]**

Mon. circuit depth of $f$
$=$ CC of **mKW game**




## Monotone KW game

for monotone $f\colon \{0,1\}^n \to \{0,1\}$

gate($x$) > gate($y$)

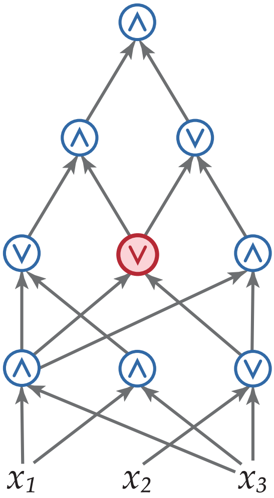
$^{-1}(1)$

$^{-1}(0)$

Output $i$ with $x_i > y_i$

**Theorem** [KW'88]

Mon. circuit depth of $f$
= CC of **mKW game**



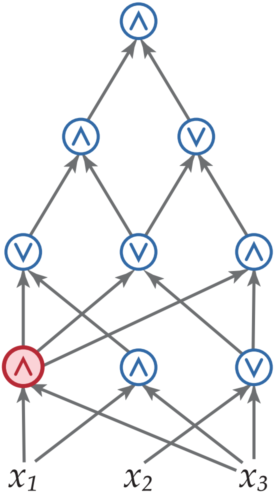

# Monotone KW game

for monotone $f\colon \{0,1\}^n \to \{0,1\}$

| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |

**Theorem** [KW'88]

Mon. circuit depth of $f$
$=$ CC of **mKW game**



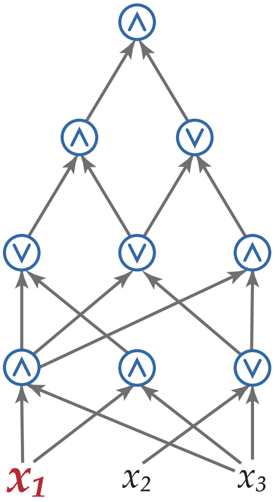

# Monotone KW game

for monotone $f\colon \{0,1\}^n \to \{0,1\}$

| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |

**Theorem** **[KW'88]**

Mon. circuit depth of $f$
$=$ CC of **mKW game**




# Monotone KW game

for monotone $f\colon \{0,1\}^n \to \{0,1\}$

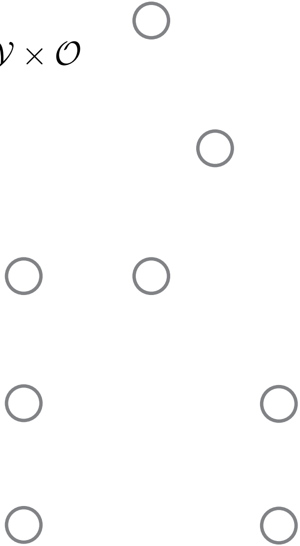
| | |
|---|---|
| **Alice** | $x \in f^{-1}(1)$ |
| **Bob** | $y \in f^{-1}(0)$ |
| Output | $i$ with $x_i > y_i$ |

**Theorem** **[KW'88]**

Mon. circuit depth of $f$
$=$ CC of **mKW game**

## PLS$^{cc}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Defined by $(V, \Pi_v)$ where for $v \in V$

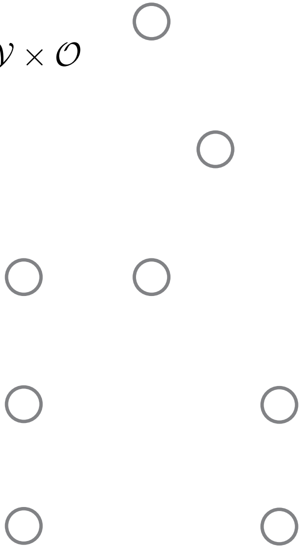


# Circuit size [R'95]

## PLS$^{\text{cc}}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Defined by $(V, \Pi_v)$ where for $v \in V$

- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$



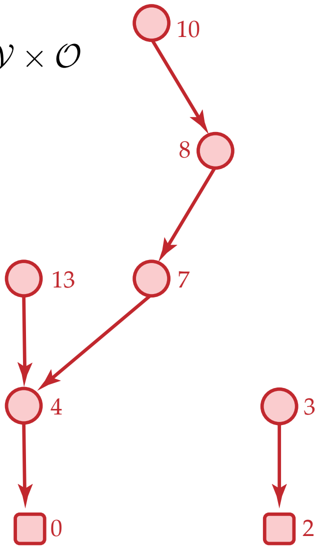
## PLS$^{cc}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Defined by $(V, \Pi_v)$ where for $v \in V$

- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases



# PLS$^{\text{cc}}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

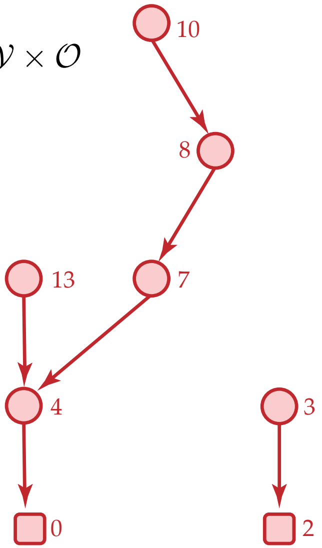
Defined by $(V, \Pi_v)$ where for $v \in V$

- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x, y)$



## PLS$^{\text{cc}}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Defined by $(V, \Pi_v)$ where for $v \in V$

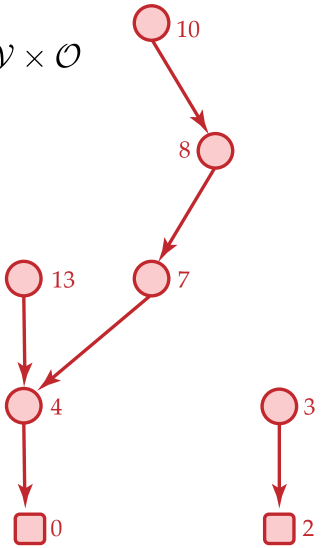
- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x, y)$

**Cost:** $\log |V| + \max_v |\Pi_v|$



## PLS$^{cc}$-protocol for $S \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{O}$

Defined by $(V, \Pi_v)$ where for $v \in V$

- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x, y)$

**Cost:** $\log |V| + \max_v |\Pi_v|$

**Theorem [R'95]:**

$$\log \mathrm{monCkt}(f) = \mathbf{PLS}^{cc}(\mathrm{mKW}(f))$$

# Circuit size [R'95]

## $\text{PLS}^{\text{cc}}$-protocol

Defined by $(V, \Pi_v)$ where for $v \in V$

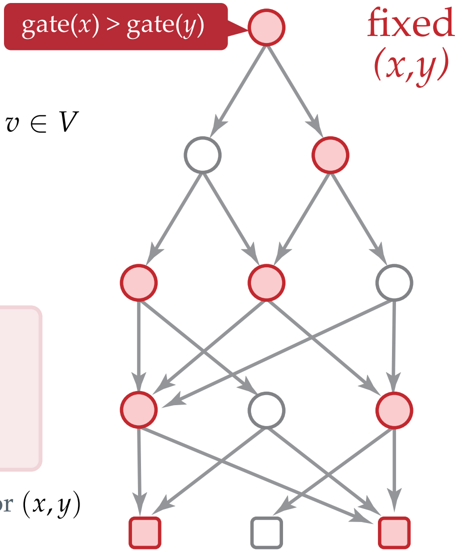
- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x, y)$

**Cost:** $\log|V| + \max_v |\Pi_v|$



## PLS$^{cc}$-protocol

Defined by $(V, \Pi_v)$ where for $v \in V$

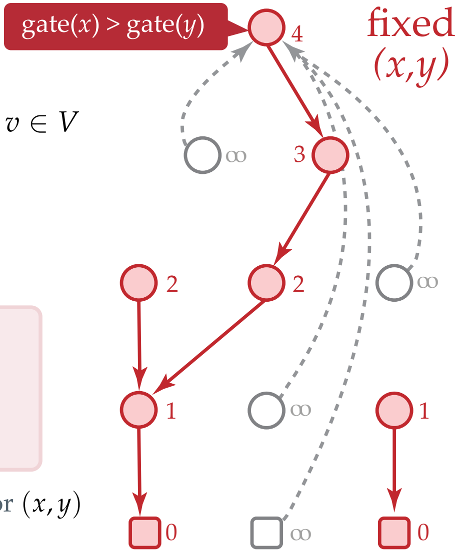
- Protocol $\Pi_v(x, y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u, v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x, y)$

**Cost:** $\log |V| + \max_v |\Pi_v|$



## PLS$^{\text{cc}}$-protocol

Defined by $(V, \Pi_v)$ where for $v \in V$

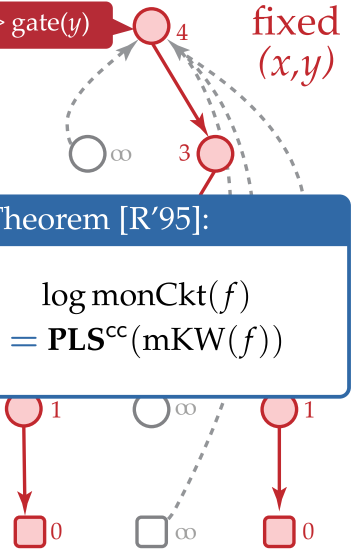
- Protocol $\Pi_v(x,y)$ outputs
  1. *Successor* in $V$
  2. *Potential* in $\mathbb{Z}$
  3. *Solution* in $\mathcal{O}$

Implicitly describes dag $G_{x,y}$ with edges $(u,v)$ s.t.

- $u$'s successor is $v$
- potential decreases

**Correct:** sinks have solutions for $(x,y)$

**Cost:** $\log|V| + \max_v |\Pi_v|$




**Theorem [R'95]:**

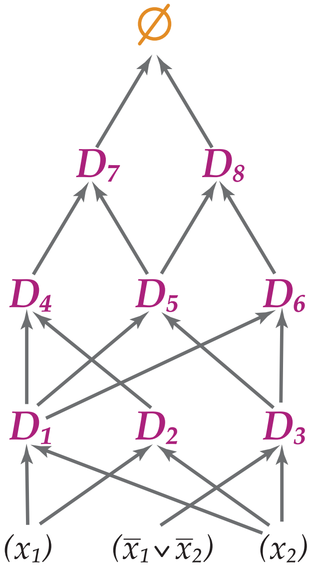
$$\log \text{monCkt}(f) = \textbf{PLS}^{\text{cc}}(\text{mKW}(f))$$

Query analogue of **PLS**:

*Resolution proof system*

# PLS$^{\mathrm{dt}}$ and Resolution

Unsat $k$-CNF formula $F$

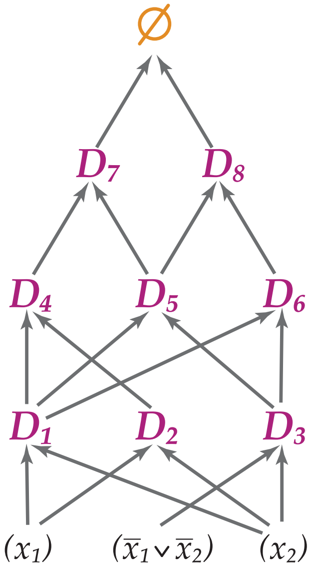


# PLS$^{\mathrm{dt}}$ and Resolution

Unsat $k$-CNF formula $F$

**Search problem $S(F)$:**

Input: Assignment $x \in \{0,1\}^n$
Output: Clause $D$ with $D(x) = 0$



# PLS$^{\text{dt}}$ and Resolution

Unsat $k$-CNF formula $F$

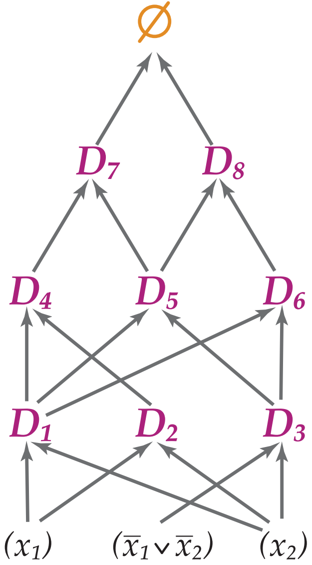
**Search problem** $S(F)$**:**

Input: Assignment $x \in \{0,1\}^n$
Output: Clause $D$ with $D(x) = 0$

**PLS**$^{\text{dt}}$–decision tree for $S(F)$

Same as **PLS**$^{\text{cc}}$-protocol except:

- Vertices have decision trees $\mathcal{T}_v$
- **Cost:** max height of $\mathcal{T}_v$



# $\mathbf{PLS}^{\mathrm{dt}}$ and Resolution

Unsat $k$-CNF formula $F$

**Search problem $S(F)$:**

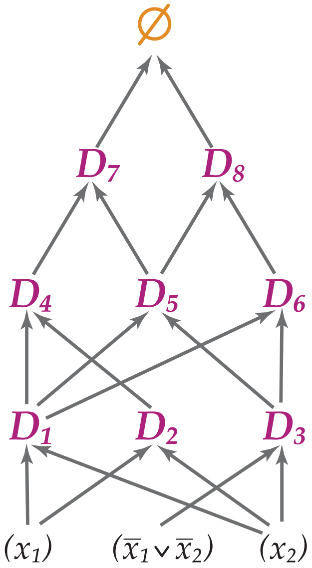
Input: Assignment $x \in \{0,1\}^n$
Output: Clause $D$ with $D(x) = 0$

**$\mathbf{PLS}^{\mathrm{dt}}$**–decision tree for $S(F)$

Same as $\mathbf{PLS}^{\mathrm{cc}}$-protocol except:

- Vertices have decision trees $\mathcal{T}_v$
- **Cost:** max height of $\mathcal{T}_v$

Resolution width of $F$
$= \mathbf{PLS}^{\mathrm{dt}}(S(F))$



# $\mathbf{PLS}^{\mathrm{dt}}$ and Resolution

Unsat $k$-CNF formula $F$

**Search problem** $S(F)$**:**

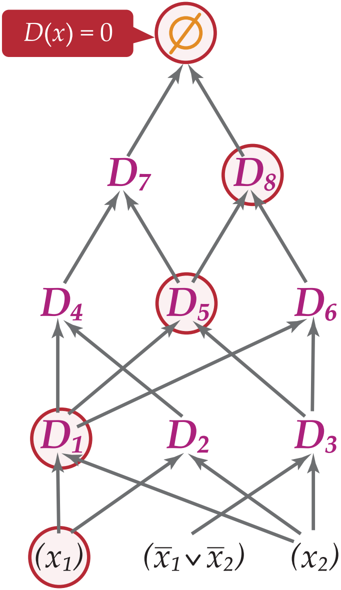
Input: Assignment $x \in \{0,1\}^n$
Output: Clause $D$ with $D(x) = 0$

**PLS**$^{\mathrm{dt}}$–decision tree for $S(F)$

Same as **PLS**$^{\mathrm{cc}}$-protocol except:

- Vertices have decision trees $\mathcal{T}_v$
- **Cost:** max height of $\mathcal{T}_v$

Resolution width of $F$
$= \ \mathbf{PLS}^{\mathrm{dt}}(S(F))$

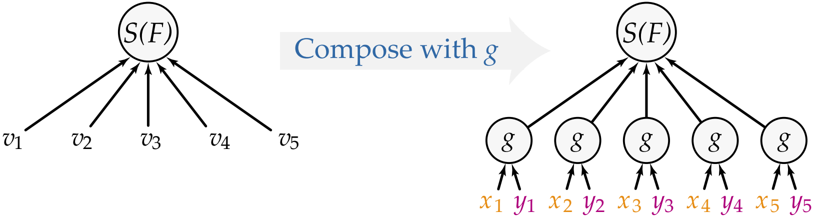


# Query-to-communication lifting

$$\mathbf{PLS}^{\mathsf{cc}}(S(F) \circ g) \quad \overset{\text{[GGKS'18]}}{=} \quad \mathbf{PLS}^{\mathsf{dt}}(S(F))$$

# Query-to-communication lifting

$$\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) \overset{\text{[GGKS'18]}}{=} \mathbf{PLS}^{\mathsf{dt}}(S(F))$$




*Index gadget* $g\colon [m]\times\{0,1\}^m \to \{0,1\}$ mapping $(x,y)\mapsto y_x$

# Query-to-communication lifting

$$\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) \overset{\text{[GGKS'18]}}{=} \mathbf{PLS}^{\mathsf{dt}}(S(F))$$

$$\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) \geq \mathbf{PLS}^{\mathsf{cc}}(\mathrm{mKW}(f)) = \log \mathrm{monCkt}(f)$$

$$\mathbf{PLS}^{\mathsf{dt}}(S(F)) = \text{Resolution width of } F$$

# Query-to-communication lifting

$$\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) \overset{\text{[GGKS'18]}}{=} \mathbf{PLS}^{\mathsf{dt}}(S(F))$$

$$\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) \geq \mathbf{PLS}^{\mathsf{cc}}(\mathrm{mKW}(f)) = \log \mathrm{monCkt}(f)$$

$$\downarrow$$

XOR-SAT is hard

$$\mathbf{PLS}^{\mathsf{dt}}(S(F)) = \text{Resolution width of } F$$

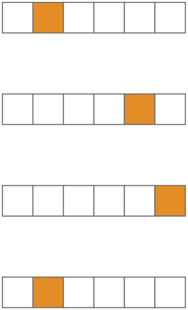
$$\uparrow$$

XOR-CSP $F$

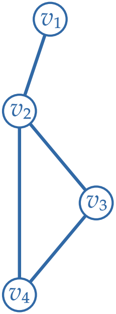
# Reduction: $S(F) \circ g \leq \mathrm{mKW}(\textsc{Xor-Sat})$

## Alice

$x \in [m]^4$



unsat $F$




## Bob

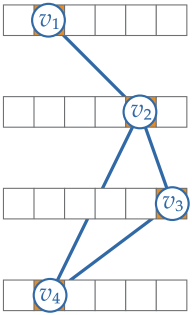
$y \in \{0,1\}^{4m}$

| | | | | | |
|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 |

# Reduction: $S(F) \circ g \;\; \leq \;\; \mathrm{mKW}(\textsc{Xor-Sat})$

**Alice**

$x \in [m]^4$




$\in \textsc{Xor-Sat}^{-1}(1)$

unsat $F$

**Bob**

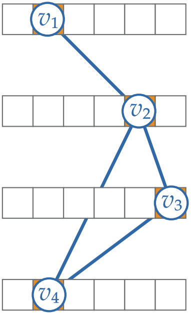
$y \in \{0,1\}^{4m}$

| | | | | | |
|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 |

# Reduction: $S(F) \circ g \le \mathrm{mKW}(\textsc{Xor-Sat})$

**Alice**

$x \in [m]^4$



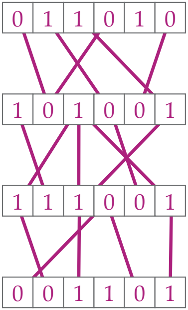

$\in \textsc{Xor-Sat}^{-1}(1)$

unsat $F$

add all constraints satisfied by $y$

**Bob**

$y \in \{0,1\}^{4m}$




$\in \textsc{Xor-Sat}^{-1}(0)$

# Query-to-communication lifting

$$
\begin{array}{ccc}
\mathbf{PLS}^{\mathsf{cc}}(S(F)\circ g) & \overset{\text{[GGKS'18]}}{=} & \mathbf{PLS}^{\mathsf{dt}}(S(F)) \\
\rotatebox{90}{$\leq$} & & \parallel \\
\mathbf{PLS}^{\mathsf{cc}}(\mathrm{mKW}(f)) & & \text{Resolution width of } F \\
\parallel & & \uparrow \\
\log \mathrm{monCkt}(f) & & \text{unsat } \mathcal{C}\text{-CSP } F \\
\downarrow & & \\
\mathcal{C}\text{-}\textsc{Sat} \text{ is hard} & &
\end{array}
$$

# Total **NP** Search Problems (**TFNP**)

# Communication **TFNP**

**TFNP**$^{\mathsf{cc}}$ $=$ Total two-party search problems that admit $\log^{O(1)}(n)$-cost non-deterministic protocol

*Example:* $\mathrm{mKW}(f) \in$ **TFNP**$^{\mathsf{cc}}$ for every monotone $f$

# Communication **TFNP**

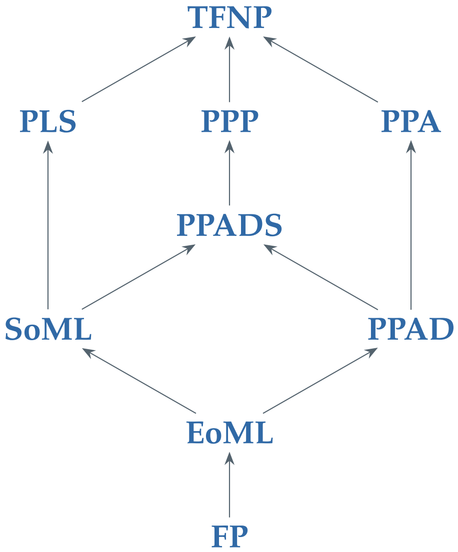
**TFNP**$^{\text{cc}}$ = Total two-party search problems that admit $\log^{O(1)}(n)$-cost non-deterministic protocol

*Example:* $\mathrm{mKW}(f) \in$ **TFNP**$^{\text{cc}}$ for every monotone $f$

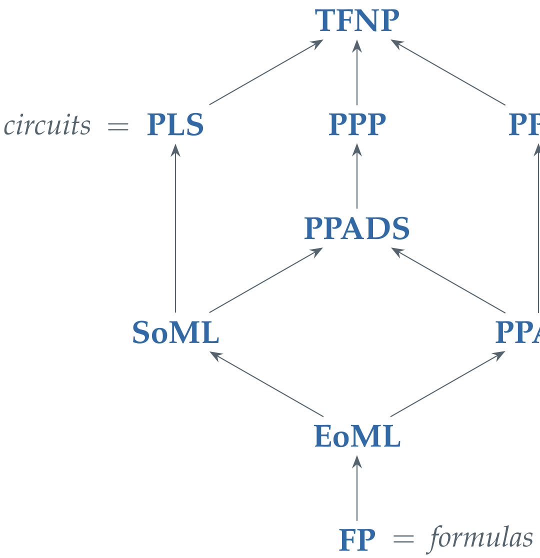
*Converse!* $\forall S \in$ **TFNP**$^{\text{cc}}$ there is $2^{\log^{O(1)}(n)}$-bit **partial** monotone $f$ with $S \leq \mathrm{mKW}(f)$

(*Proof:* reduce to set-disjointness + flip Bob's bits)

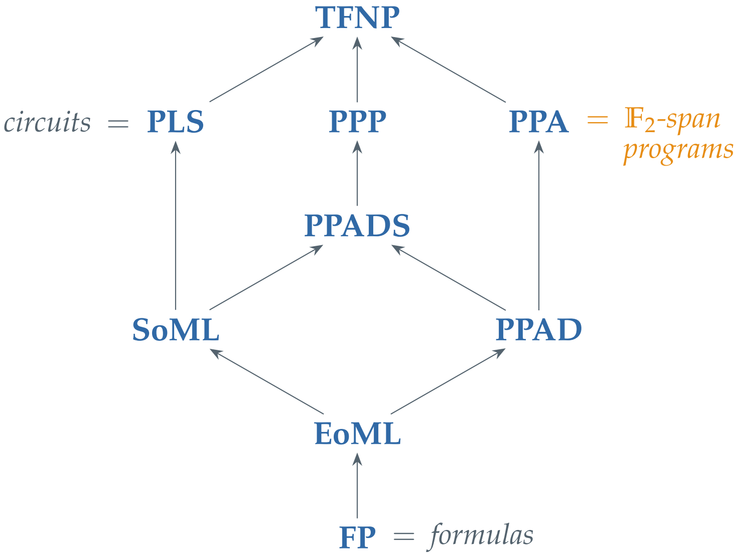
# Communication **TFNP** — What we know



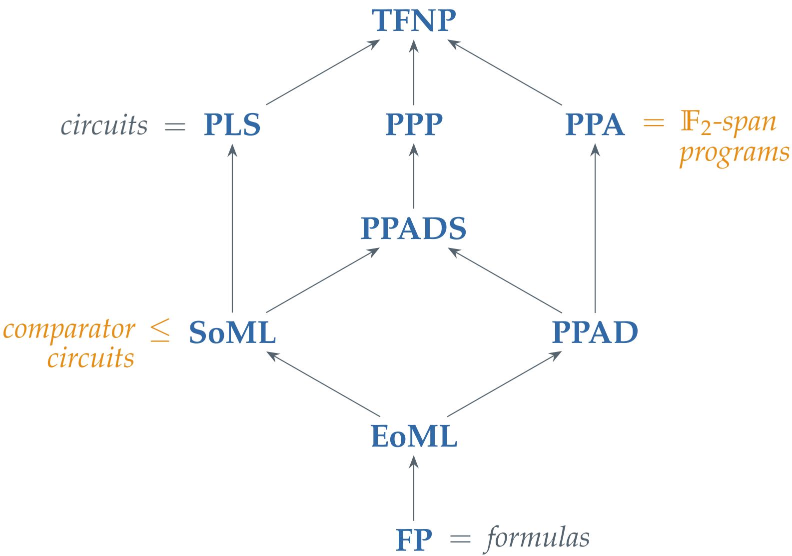
# Communication **TFNP** — What we know



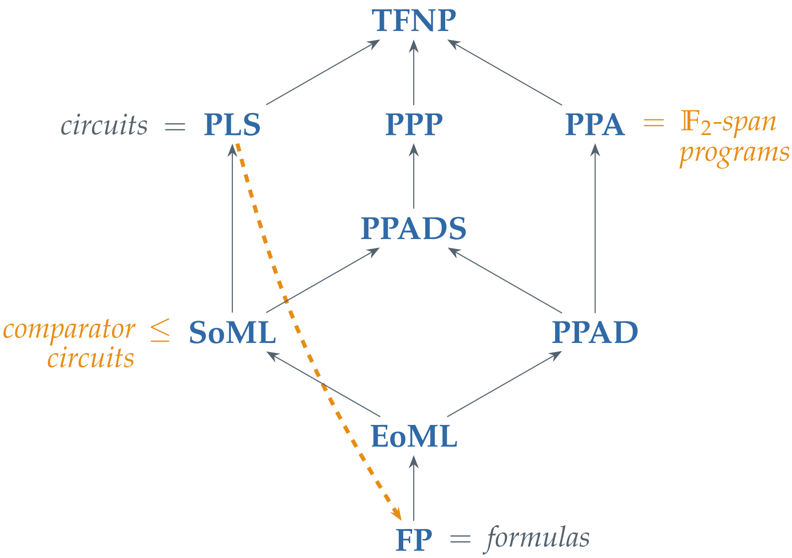
# Communication **TFNP** — What we know



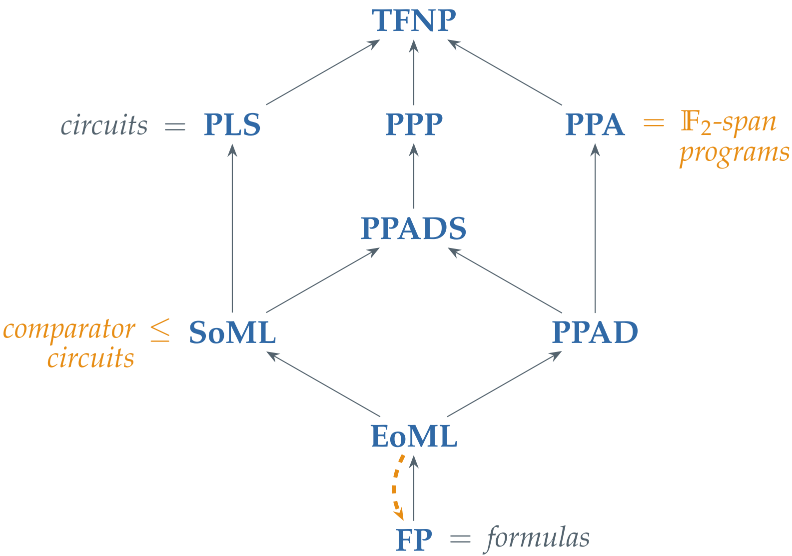
# Communication **TFNP** — What we know



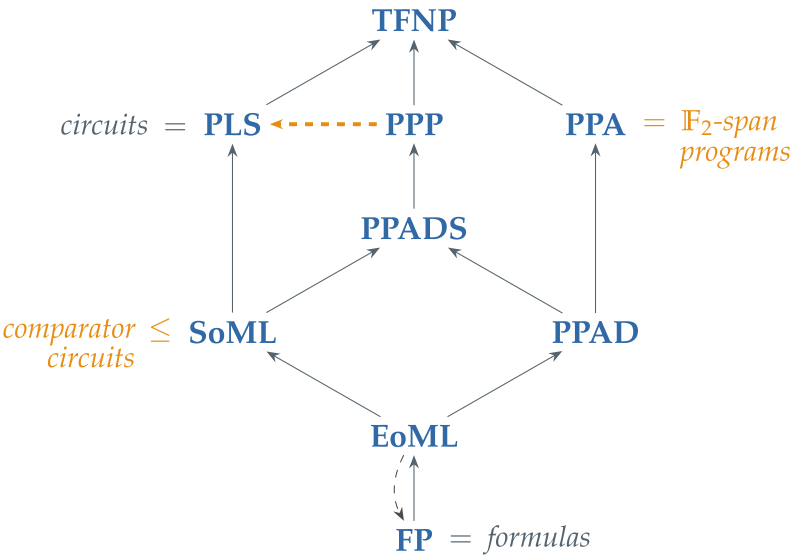
# Communication **TFNP** — What we know



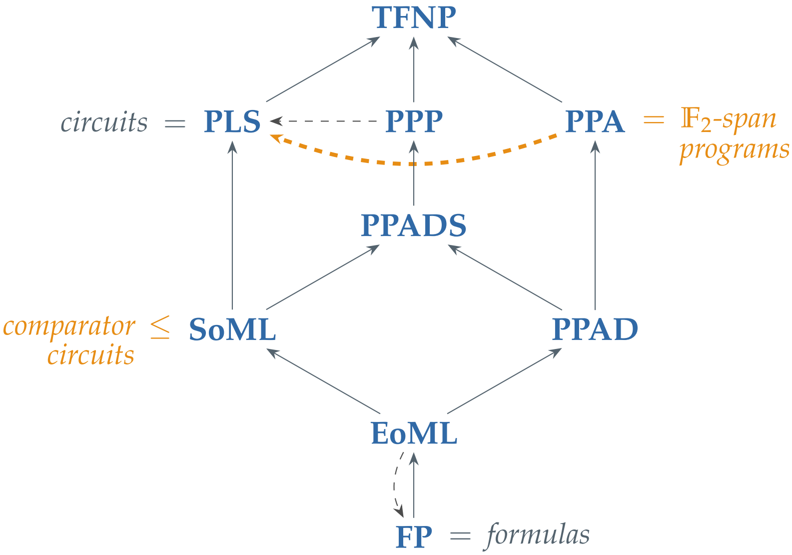
# Communication **TFNP** — What we know



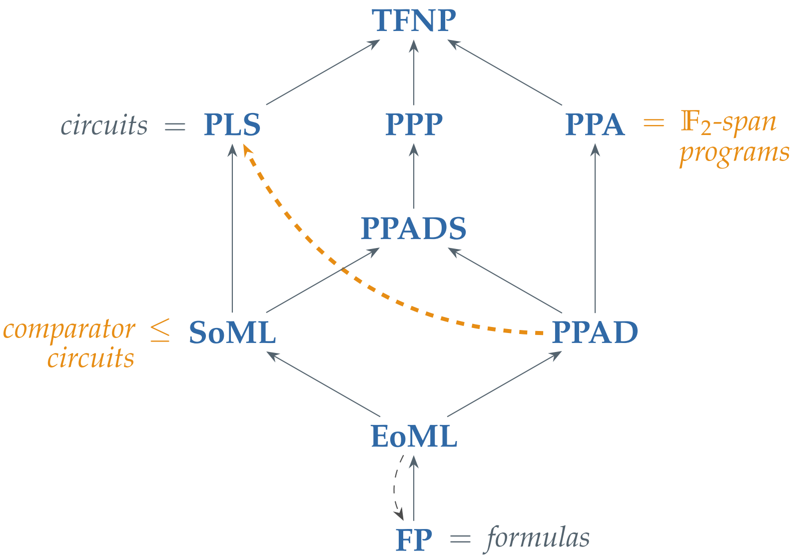
# Communication **TFNP** — What we know



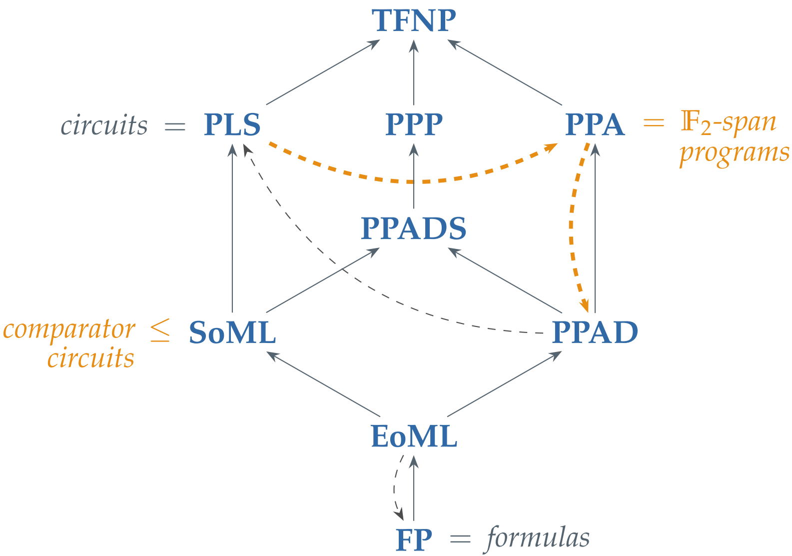
# Communication **TFNP** — What we know



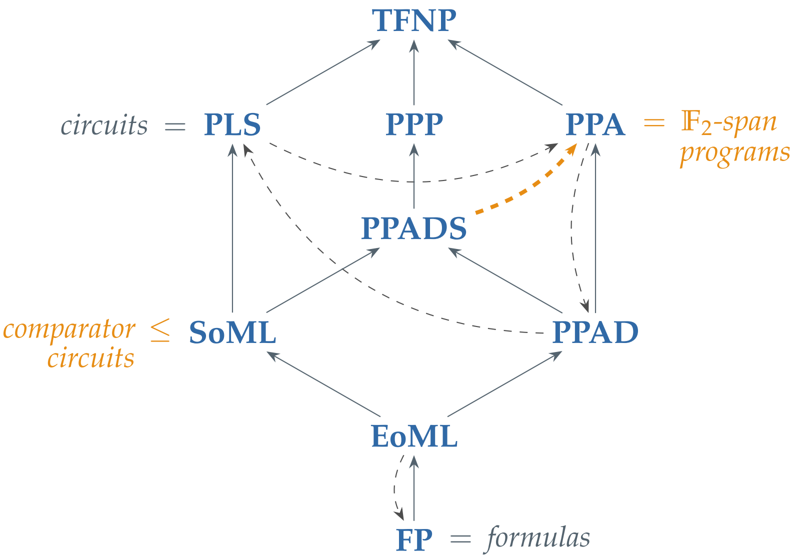
# Communication **TFNP** — What we know



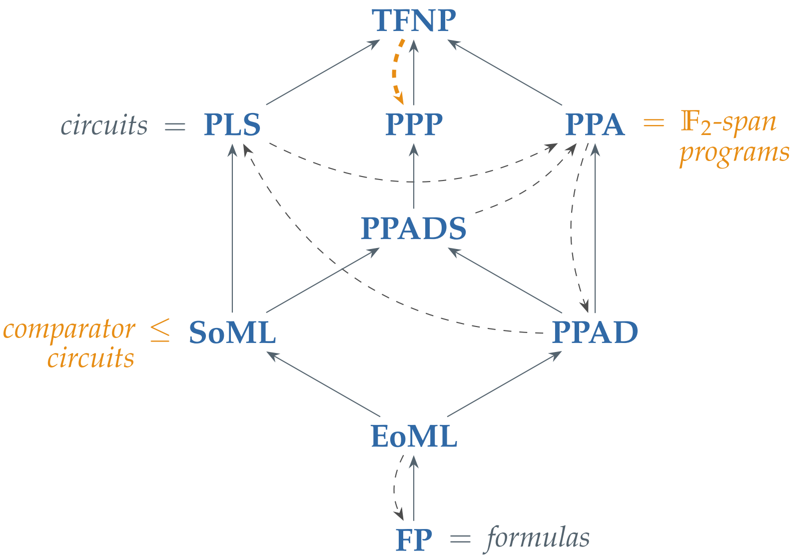
# Communication **TFNP** — What we know



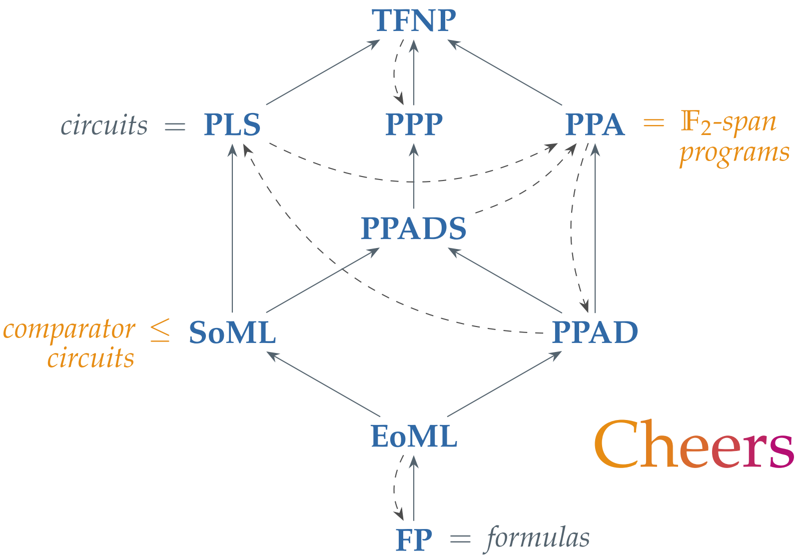
# Communication **TFNP** — What we know



# Communication **TFNP** — What we know



# Communication **TFNP** — What we know




Cheers!