Lifting Theorems: A Survey

Robert Robere
School of Computer Science
McGill University

McGill

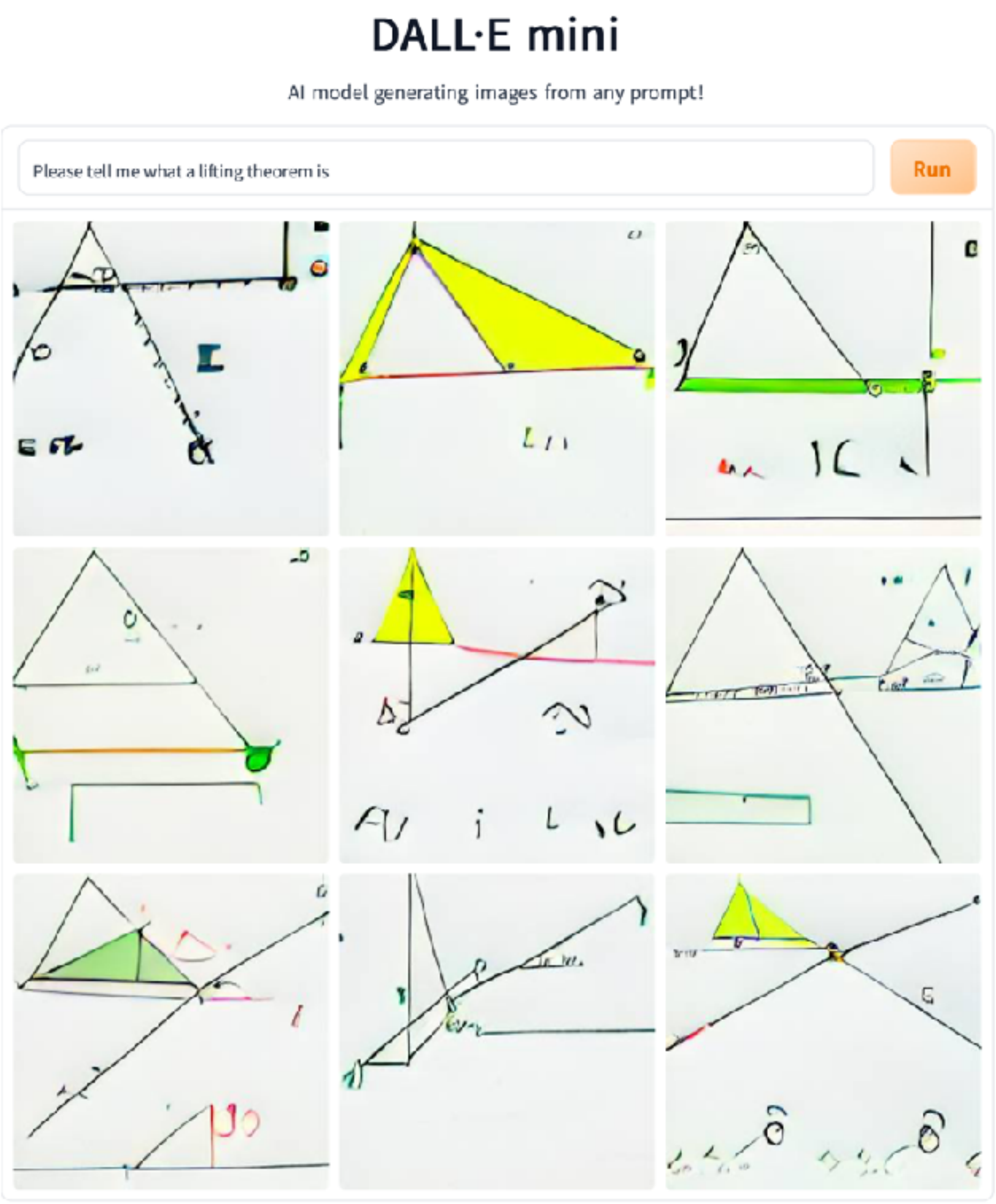
Mathematical Approaches to Lower Bounds: Complexity of Proofs and Computation

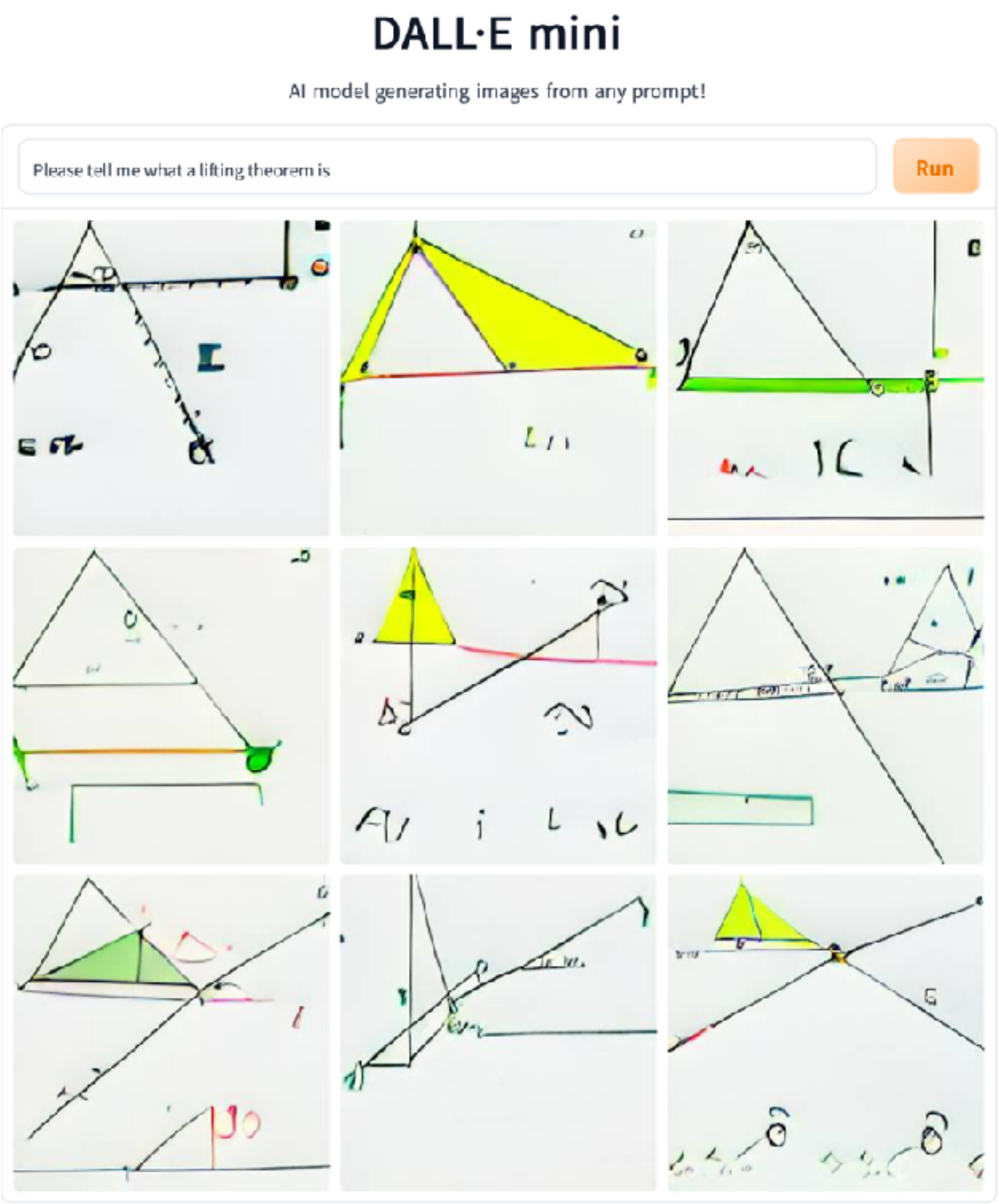
ICMS Edinburgh

July 6, 2022

What is a Lifting Theorem?

- Let's ask the expert…





Thanks for Listening!

Lifting Theorems: A Survey

Robert Robere
School of Computer Science
McGill University

McGill

Mathematical Approaches to Lower Bounds: Complexity of Proofs and Computation

ICMS Edinburgh

July 6, 2022

Lifting Theorems in Complexity Theory

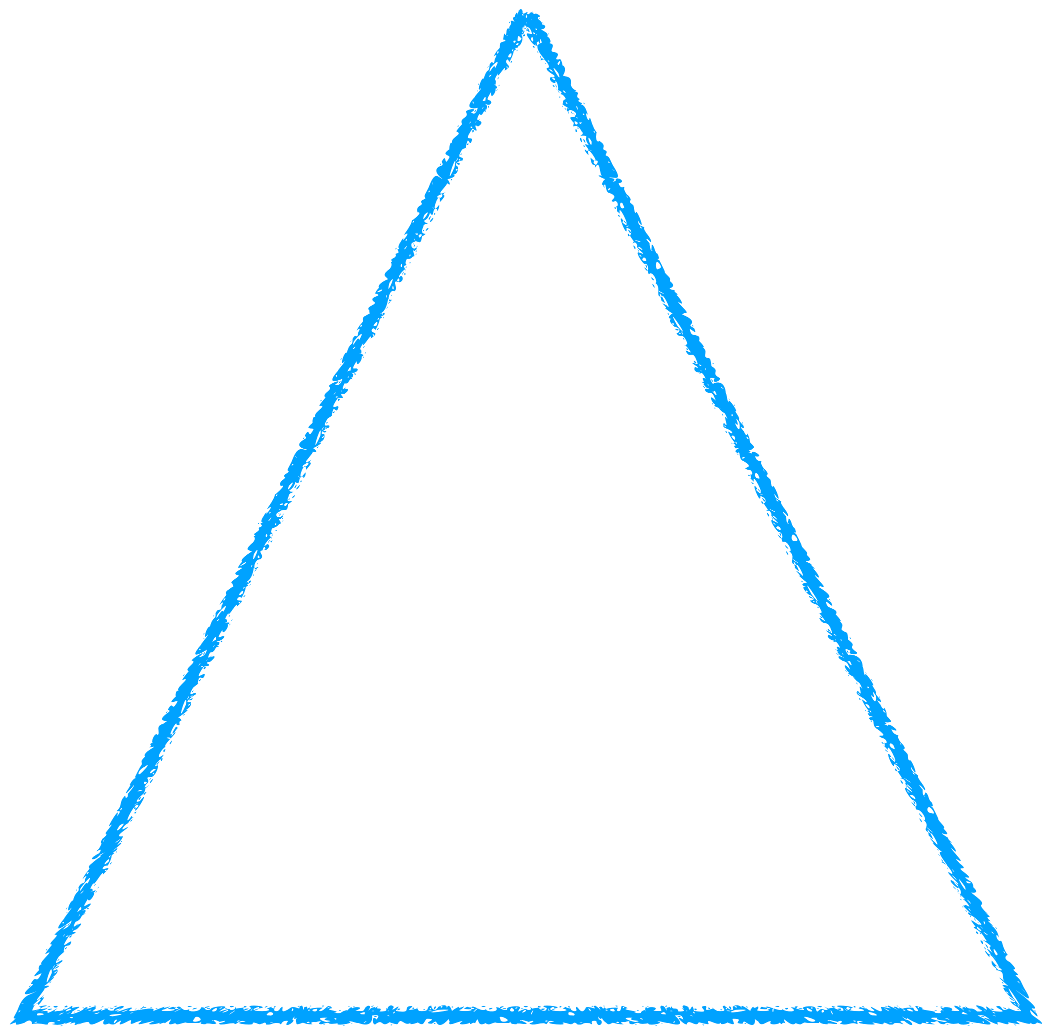
- Many new results in proof and circuit complexity using lifting theorems
  [GP12, GPW14, GLMWZ15, CLRS16, LRS16, RPRC16, PR17, KMR17, PR18, dRNV 16, GGKS18, GKRS18, dRMNPR18, dRMNPRV20, FGGR2022, LMMPZ22]
- These results rely on a fairly sophisticated set of equivalences and formal relationships between different computational models:
  - Proof Systems, Query Algorithms, Communication Protocols, Circuit Models
- Results generalize and extend classic lower bound techniques (such as **monotone feasible interpolation**)
- Place the complexity of **total search problems** at center stage!

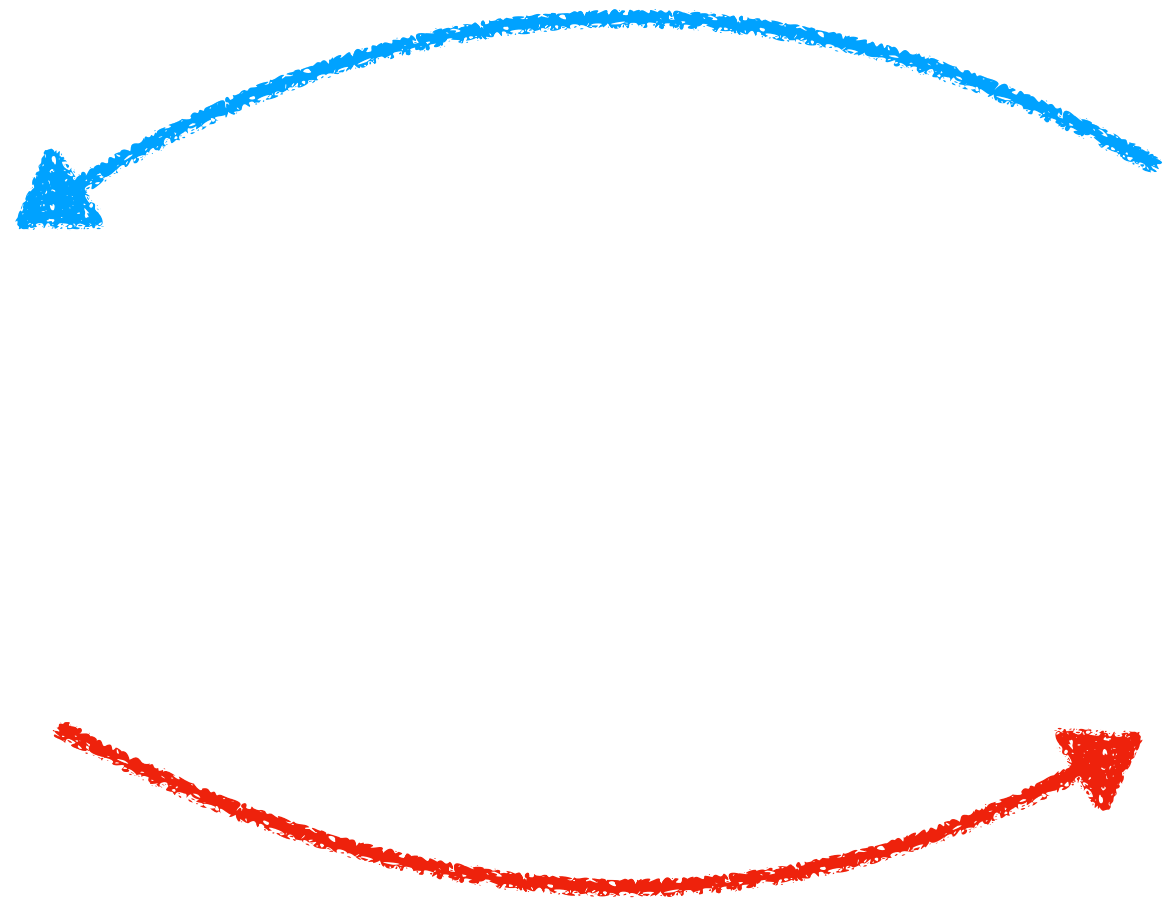
Lifting Theorem: Basic Idea

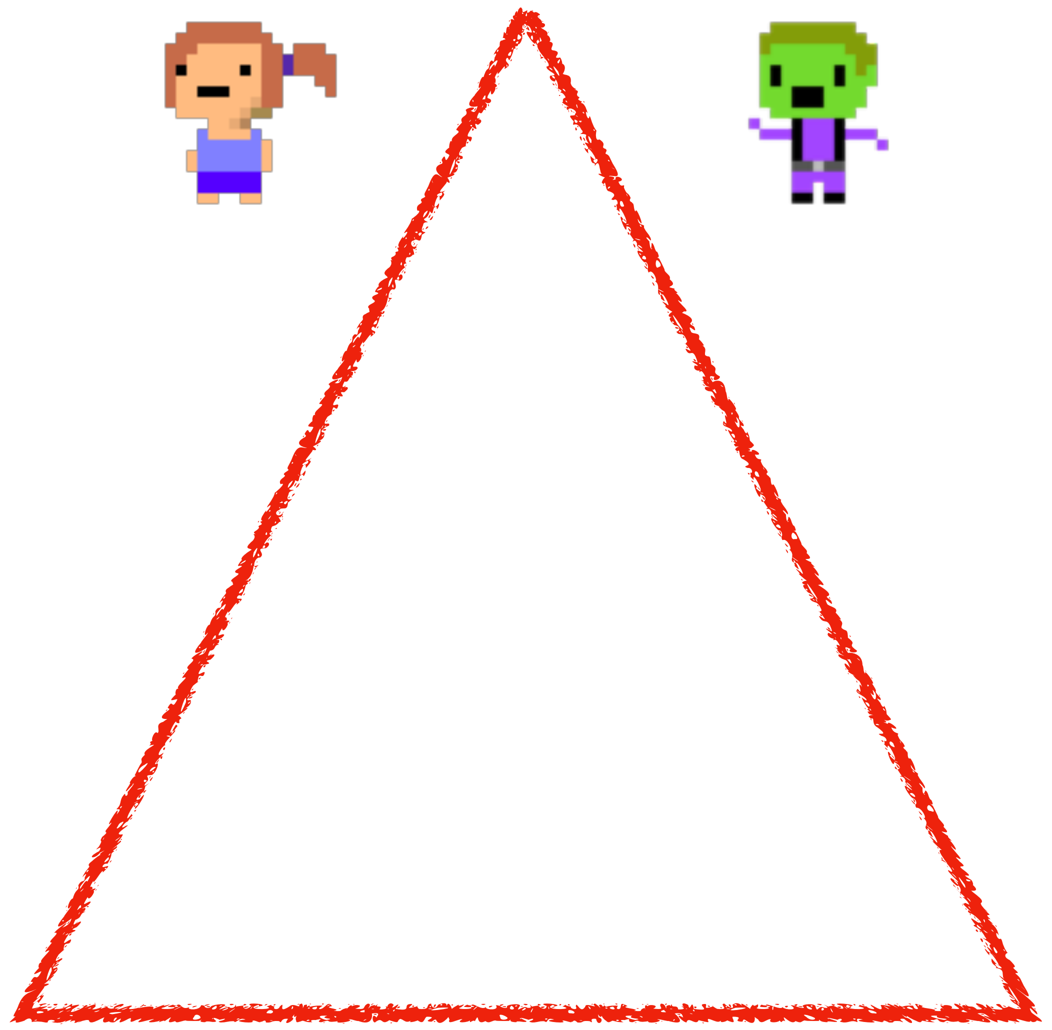
Query Model

Protocol simulates Query

Communication Model







For “complex” g
this is **best** strategy!

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

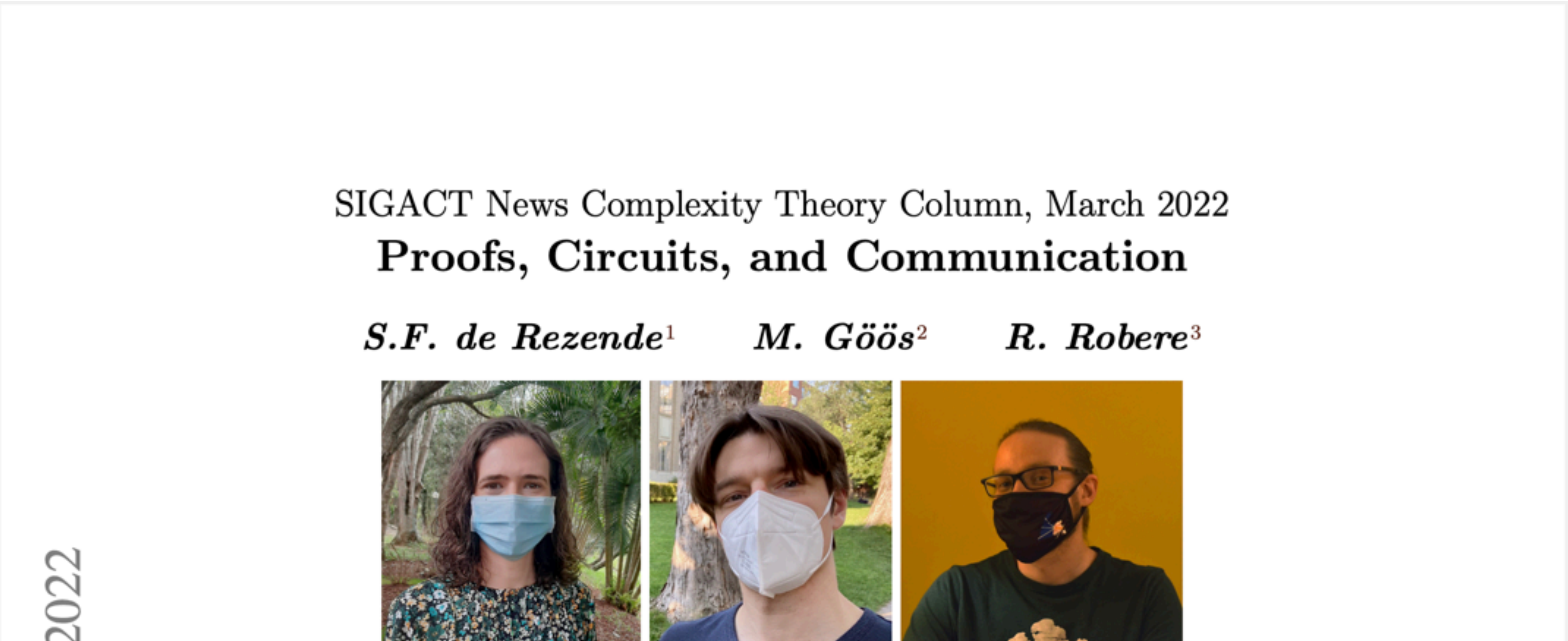
$f \circ g^n : X^n \times Y^n \to \{0,1\}$

$g : X \times Y \to \{0,1\}$ is a “complex gadget”

Complexity Preserving Simulations!

What This Talk Is About

- **Query-to-communication** lifting theorems for **search problems** $S \subseteq \mathcal{I} \times \mathcal{O}$
- Survey some basic ideas from lifting theorems for tree-like and dag-like models, motivate "why" the connection should hold.
- Connections to other areas, like TFNP.
- Based on recent SIGACT Complexity Column:


SIGACT News Complexity Theory Column, March 2022

Proofs, Circuits, and Communication

S.F. de Rezende[1] *M. Göös*[2] *R. Robere*[3]

2022

Part 1

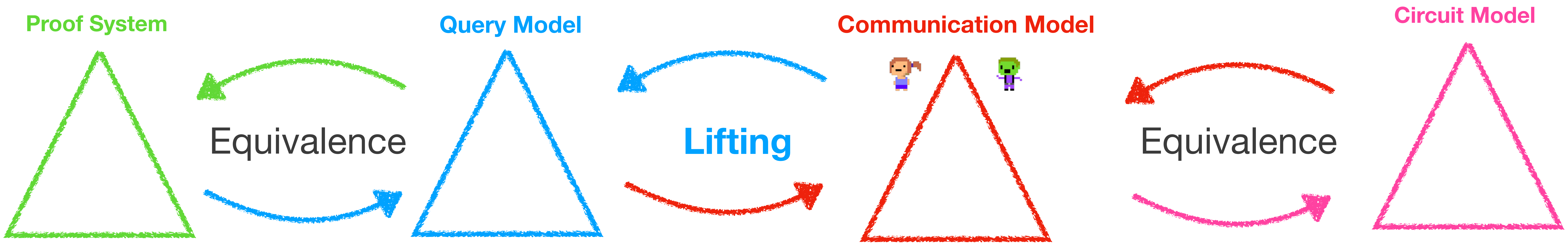
Total Search Problems

and

Concrete Complexity

Lifting Schema

All equivalences are “complexity preserving”



$F = C_1 \wedge \cdots \wedge C_m$

F is an unsatisfiable CNF

e.g. **Tree-like Resolution**

$S(F) \subseteq \{0,1\}^n \times \mathcal{O}$

e.g. **Decision Trees**

$S(F) \circ g^n : X^n \times Y^n \to \mathcal{O}$

$g : X \times Y \to \{0,1\}$ is a “complex gadget”

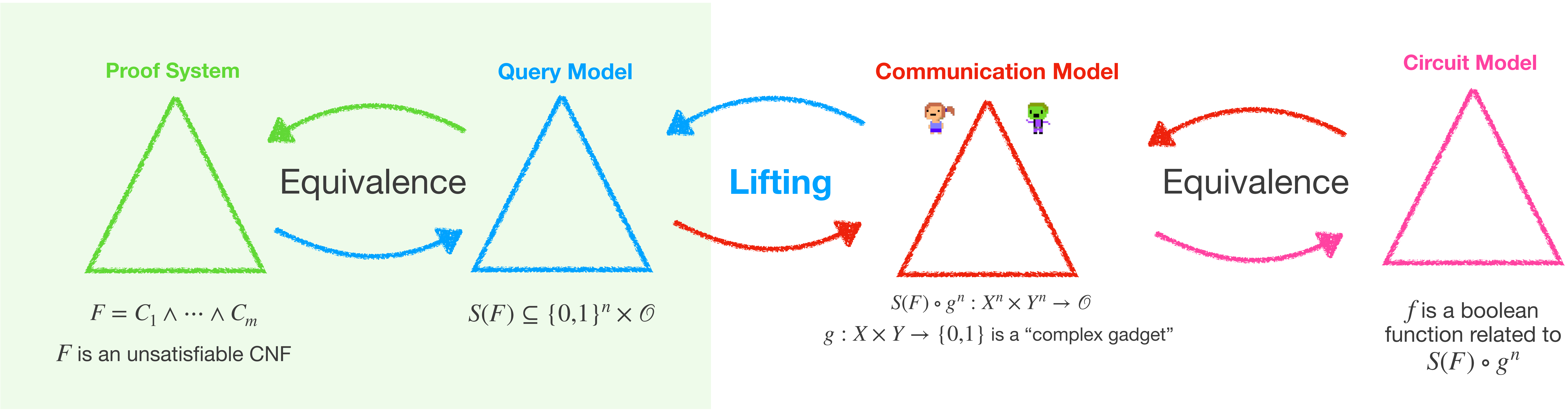
e.g. **Communication Protocols**

f is a boolean function related to $S(F) \circ g^n$

e.g. **Monotone Boolean Formulas**

Lifting Schema

All equivalences are “complexity preserving”



Total Search Problems

- $S \subseteq I \times O$ is a **total search problem** if for all $x \in I$ there is an $o \in O$ such that $(x, o) \in S$.
  - For any $x \in I$ let $S(x) := \{o \in O : (x, o) \in S\}$
- Study total search problems with **verifiable solutions** in various algorithmic models.
- **Classical** TFNP

  Verify $(x, o) \in S$ using polynomial time Turing Machines
- **Black-Box** TFNP^{dt}

  Verify $(x, o) \in S$ using $\log^{O(1)} n$-depth decision trees
- **Communication** TFNP^{cc}

  Verify $(x, o) \in S$ using $\log^{O(1)} n$-depth communication protocols

Black-Box TFNP

- $\mathcal{S} = \{S_n \subseteq \{0,1\}^n \times O_n\}_{n\in\mathbb{N}}$ sequence of total search problems
  - O_n finite, reasonably bounded in size (e.g. $|O_n| = n^{O(1)}$).
- $\mathcal{S} \in \mathsf{TFNP}^{dt}$ if for every n, $o \in O_n$ there is a decision tree T_o of depth $\log^{O(1)} n$ that, given query access to $x \in \{0,1\}^n$ verifies if $(x, o) \in S_n$
- **Canonical Example:** Unsatisfiable $\log^{O(1)} n$-width CNF $F = C_1 \wedge \cdots \wedge C_m$, define

$$S(F) \subseteq \{0,1\}^n \times [m]$$

Given $x \in \{0,1\}^n$, *find* $i \in [m]$ *such that* $C_i(x) = 0$.

False Clause Search Problem

$$S(F) \subseteq \{0,1\}^n \times [m]$$

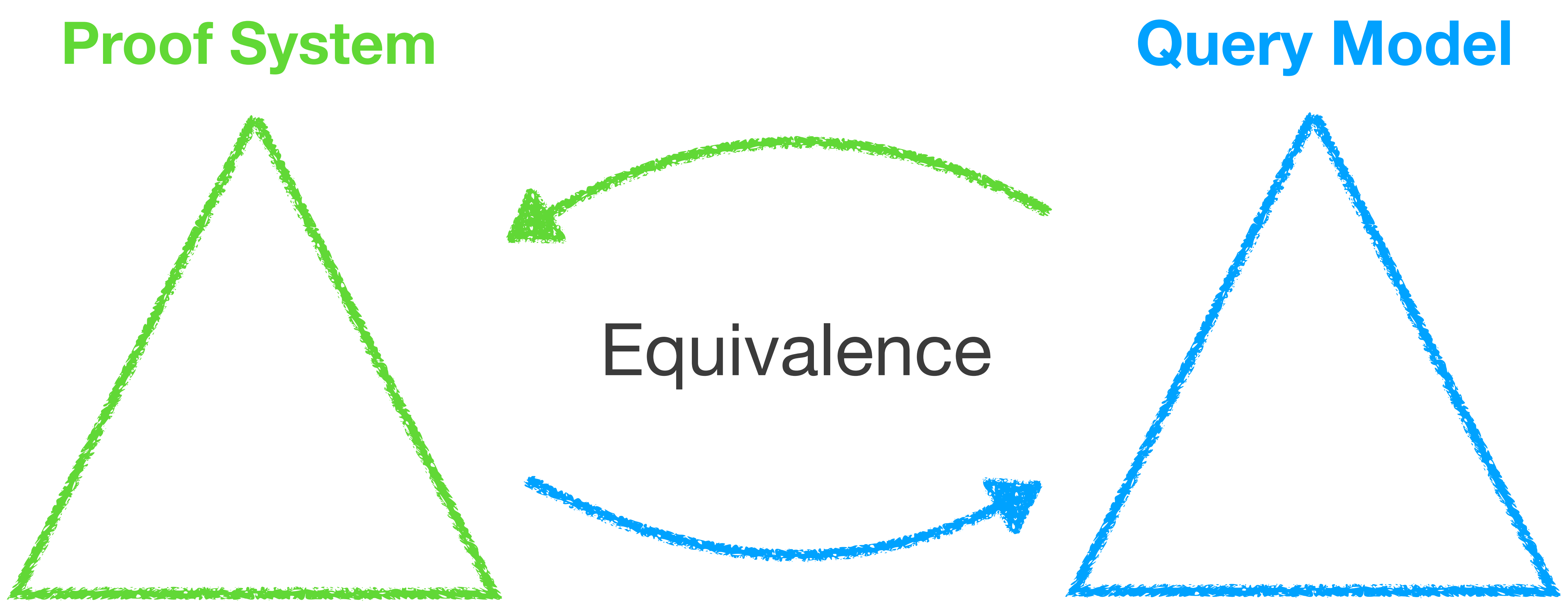
Given $x \in \{0,1\}^n$*, find* $i \in [m]$ *such that* $C_i(x) = 0$*.*

- If $S \subseteq \{0,1\}^n \times O_n$ then define (written as CNF)

$$F_S(x) = \bigwedge_{o \in O_n} \neg T_o(x) = \text{“}x \text{ has no solution”}$$

- T_o is low-depth decision tree so F_S is bounded-width CNF
- Not hard to see that $S(F)$ is essentially the same as $S(F_S)$
- Thus can redefine TFNP$^{dt} = \{\{S(F_n)\}_{n\in\mathbb{N}} : F_n$ is unsat and bounded width$\}$

False Clause Search and Proof Complexity



$F = C_1 \wedge \cdots \wedge C_m$ $\qquad$ $S(F) \subseteq \{0,1\}^n \times \mathcal{O}$

F is an unsatisfiable CNF

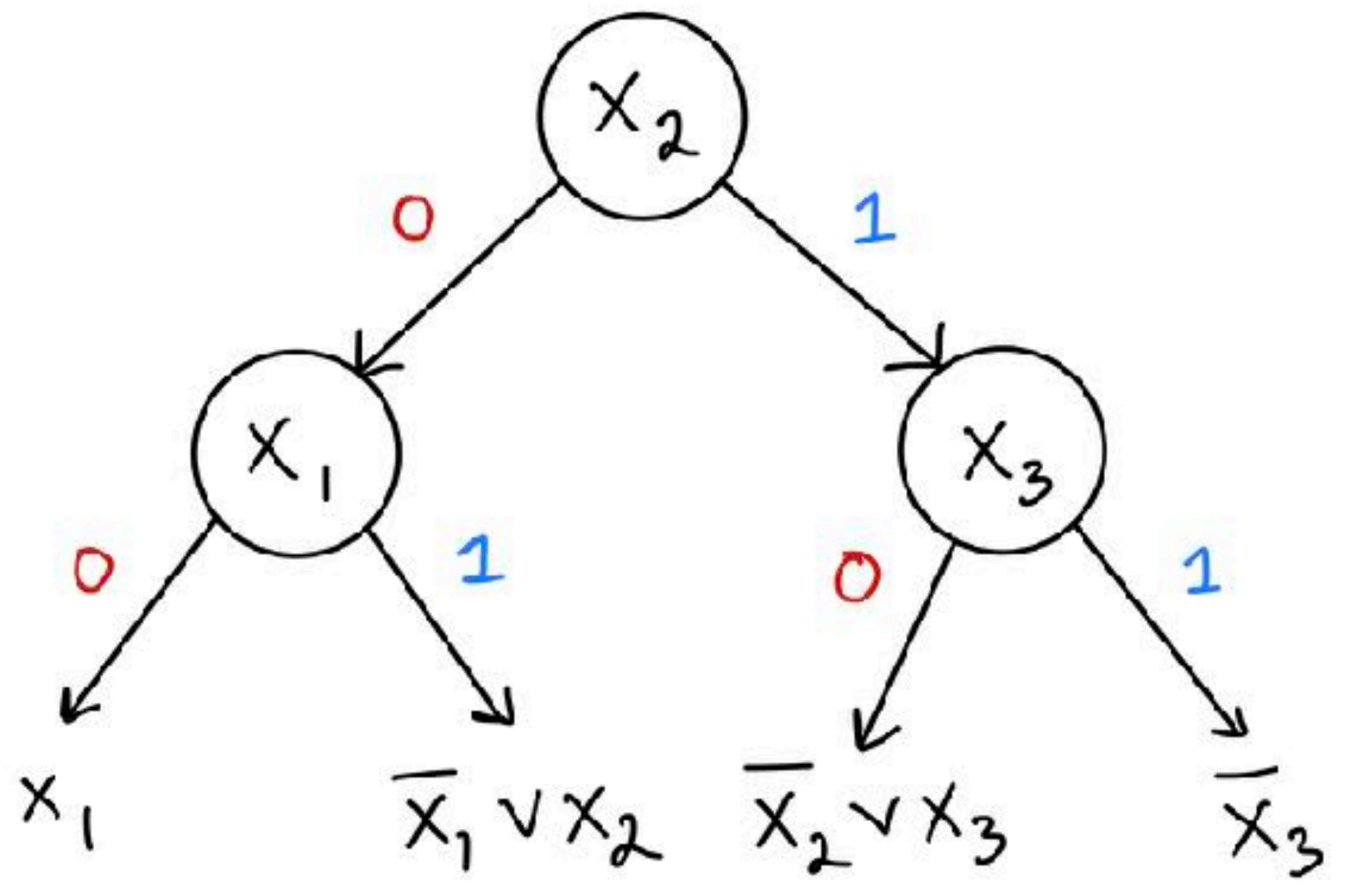
- Query complexity of $S(F)$ is very closely related to the complexity of refuting F
- Let's quickly review one example: **decision trees** and **tree-like Resolution**
- Can be generalized to **rectangle dags** and **Resolution**

Decision Trees for $S(F)$

- **Size**: Number of nodes
- **Depth**: Length of longest path
- Given boolean assignment, follow unique path consistent with that assignment, output violated clause.
- Decision tree for $S(F)$ is essentially the **DPLL method** for solving SAT.

$S(F) \subseteq \{0,1\}^n \times [m]$

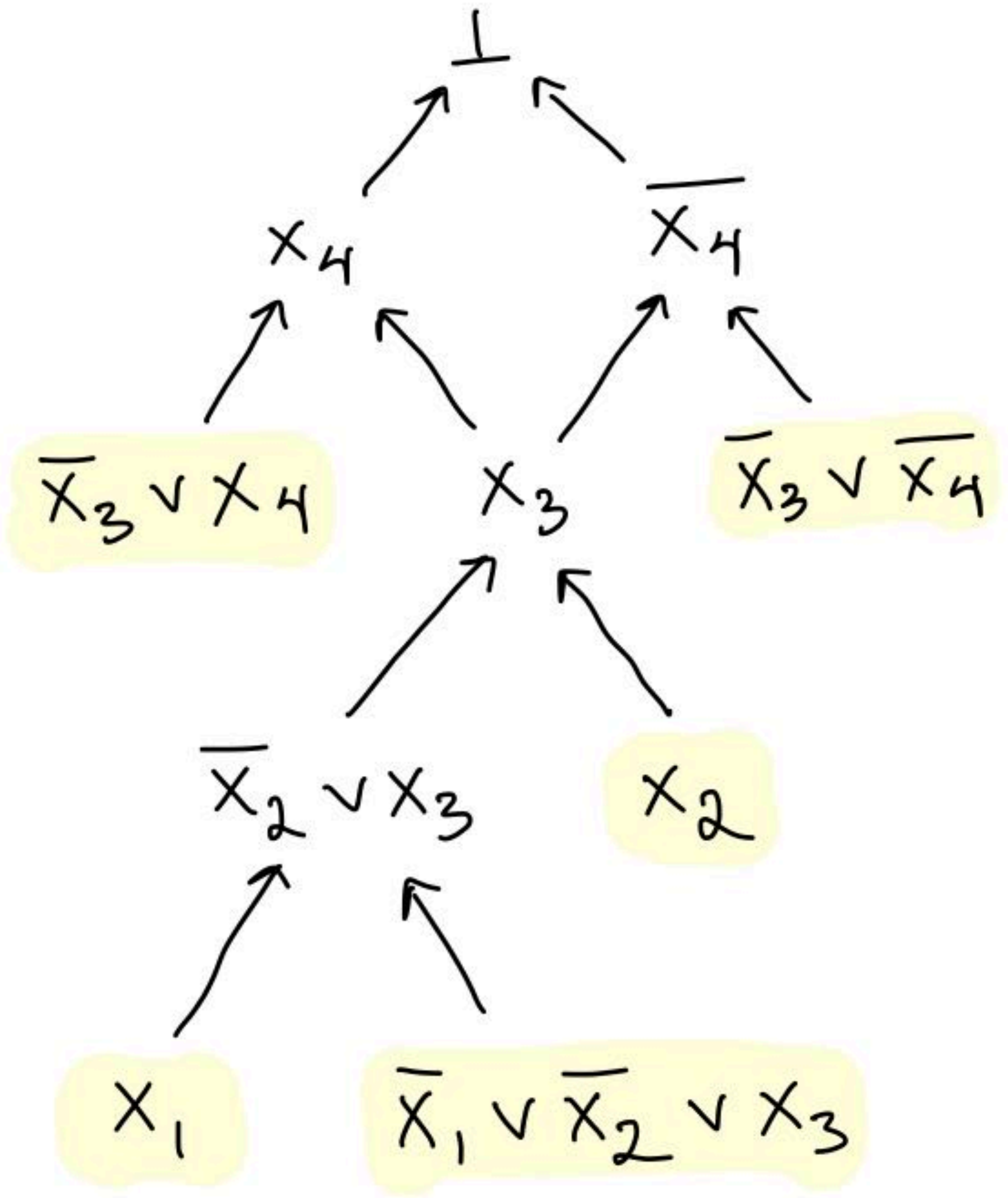
Given $x \in \{0,1\}^n$, *find* $i \in [m]$ *such that* $C_i(x) = 0$.



$$F = x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$$

Resolution Proofs

- Lines are **clauses**.
- New lines deduced using
  - **Resolution Rule**: $C \vee x, D \vee \bar{x} \vdash C \vee D$
  - **Weakening**: $C \vdash C \vee D$
- **Length**: Number of lines.
- **Depth**: Length of longest path.
- Proof is **tree-like** if each clause is used at most once.
  - Input clauses can be copied any number of times

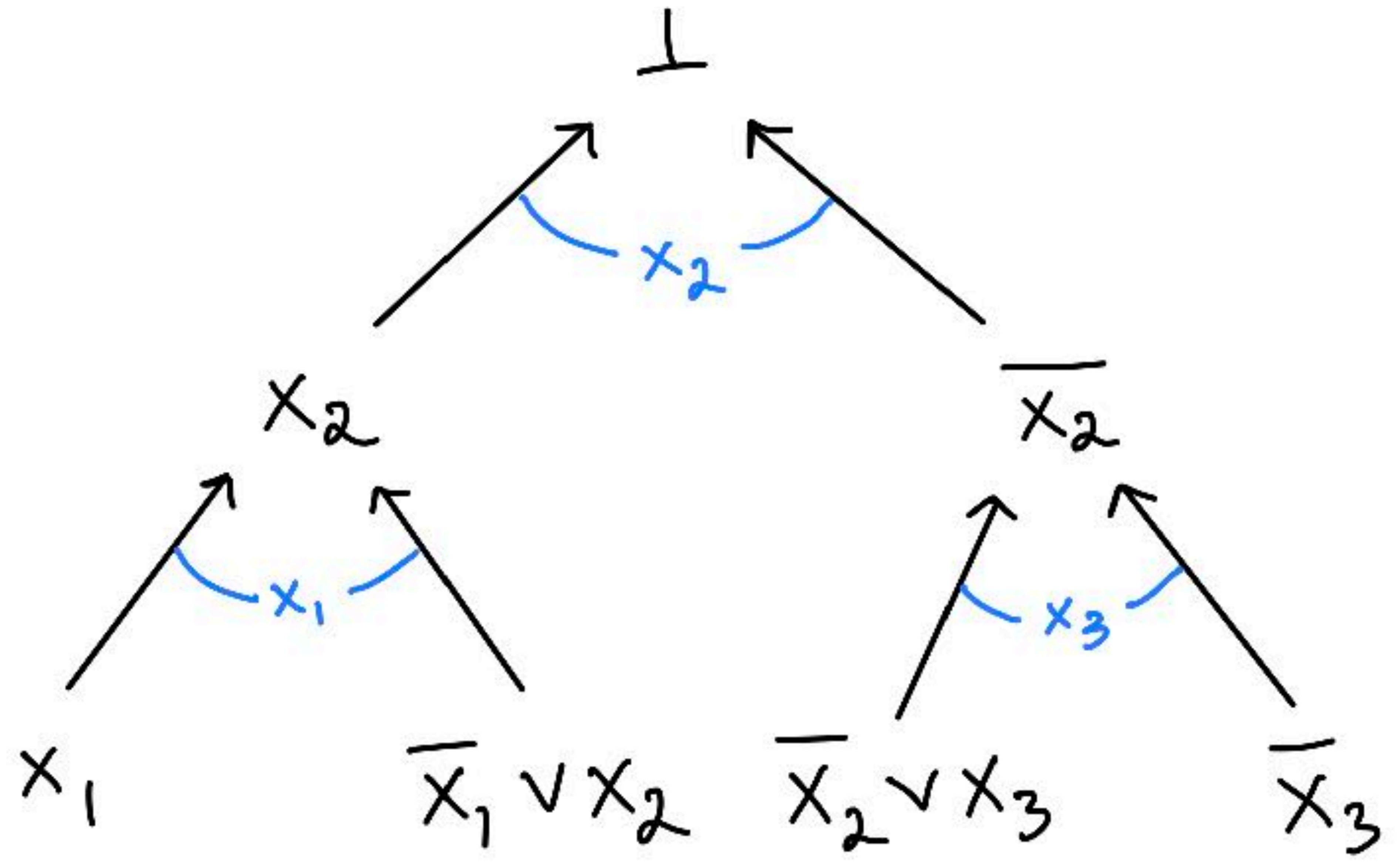


Example. $F = x_1 \wedge x_2 \wedge (\bar{x}_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_3 \vee x_4) \wedge (\bar{x}_3 \vee \bar{x}_4)$

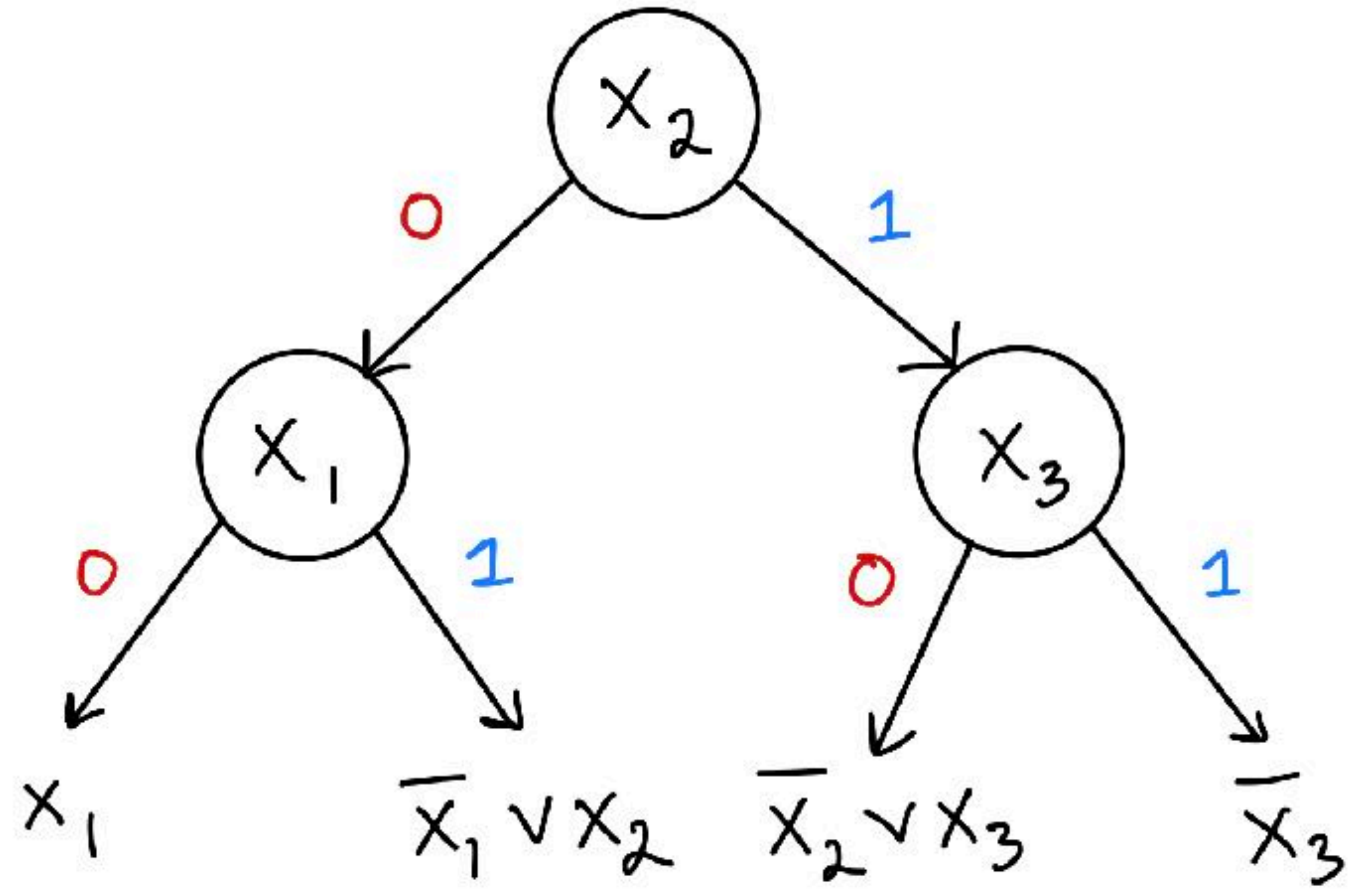
Length: 10, **Depth:** 4

Tree-Like Resolution $\equiv$ Decision Trees

Tree-Like Resolution of F



Decision Tree for $S(F)$

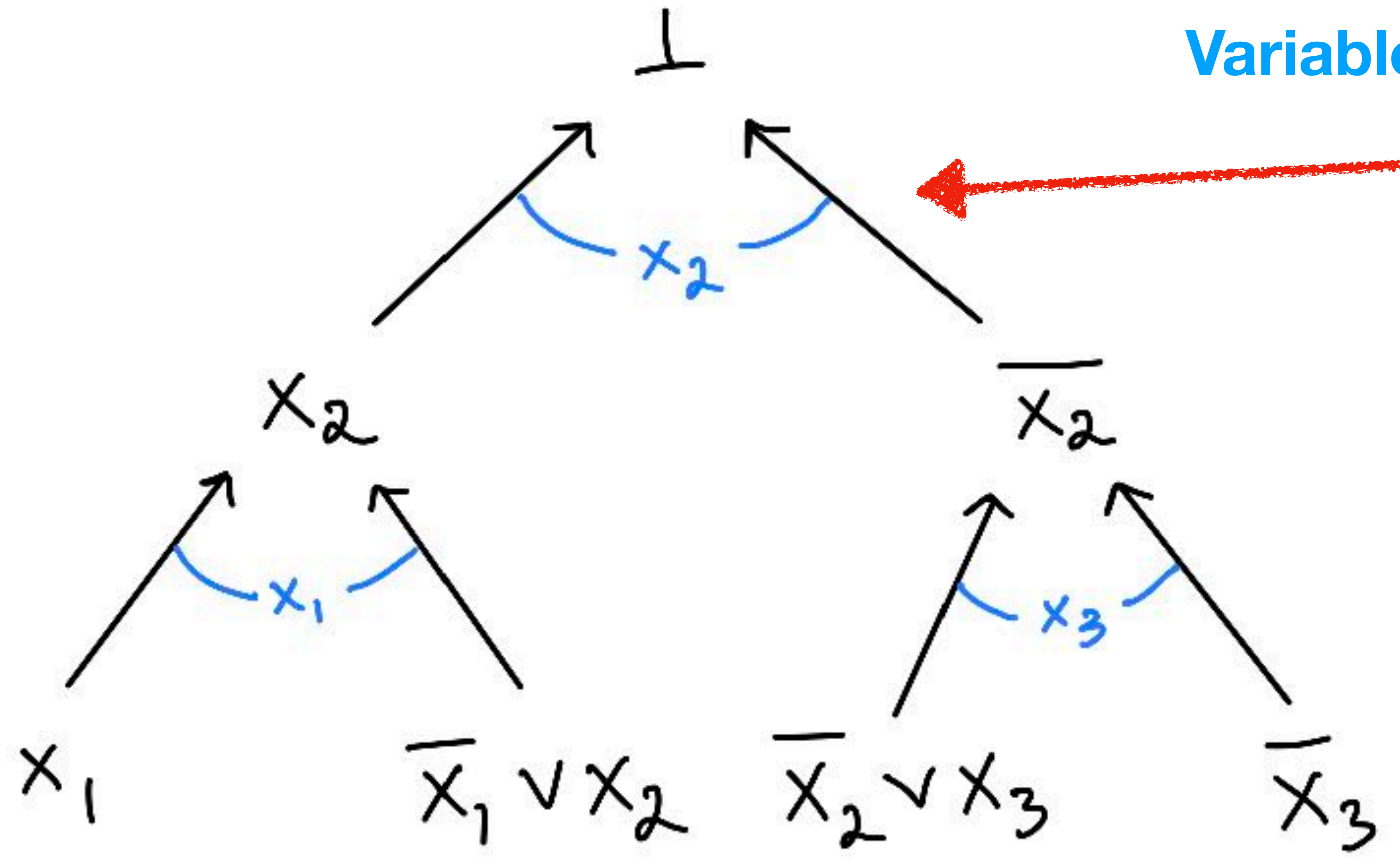


$$F = x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$$

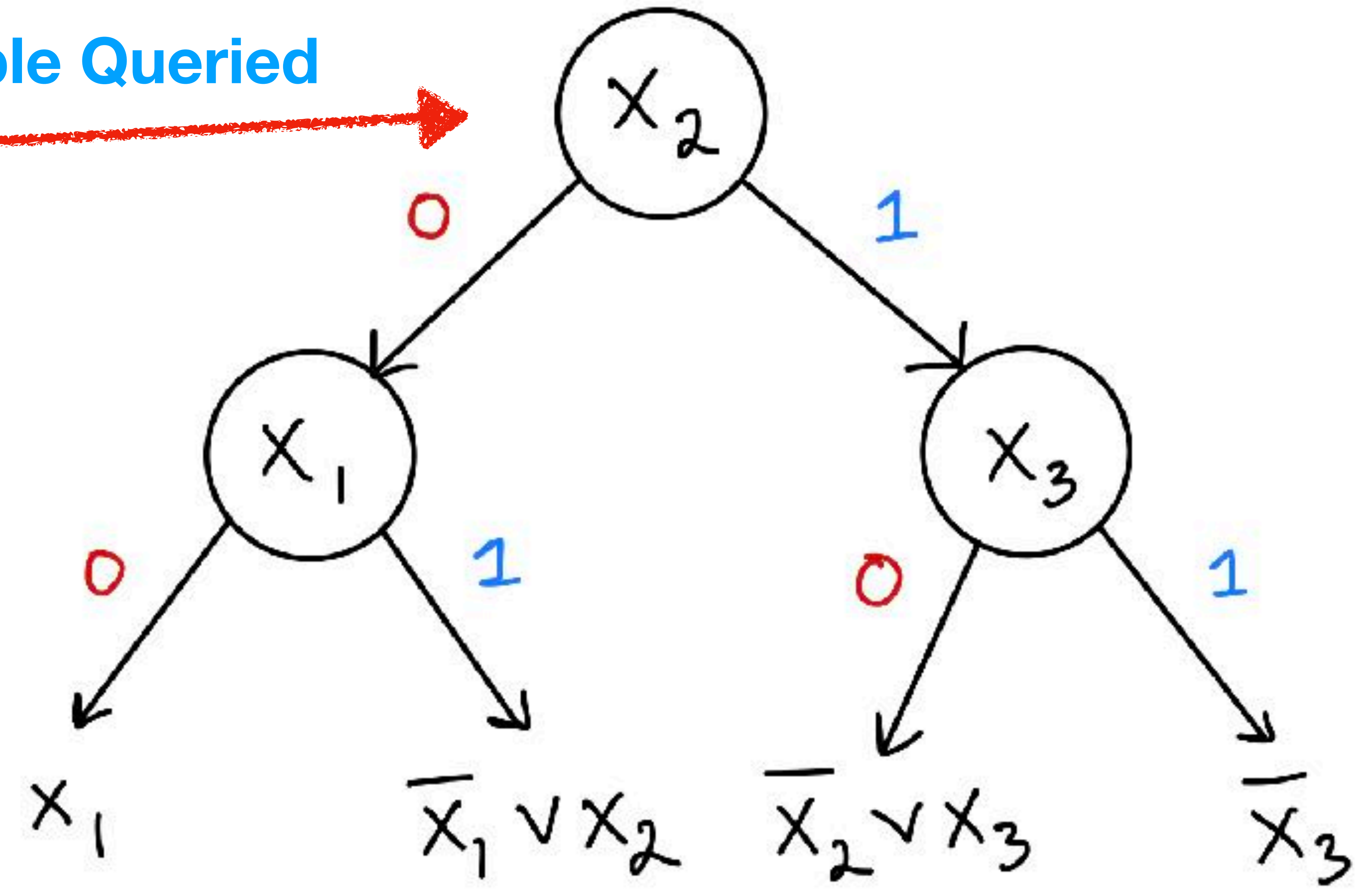
Tree-Like Resolution ≡ Decision Trees

Tree-Like Resolution of F

Decision Tree for $S(F)$



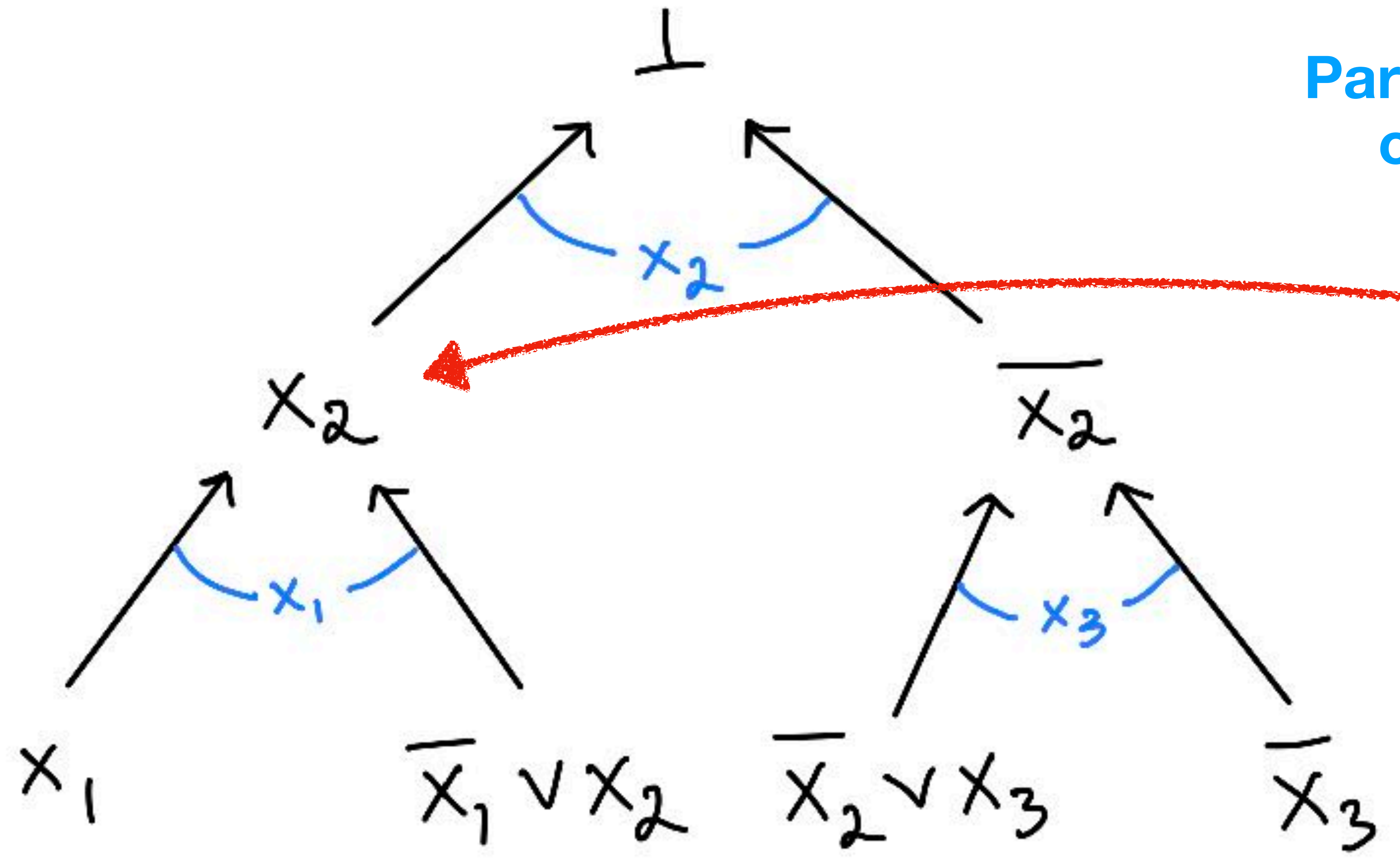
Variable Resolved ≡ Variable Queried



$$F = x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$$

Tree-Like Resolution ≡ Decision Trees

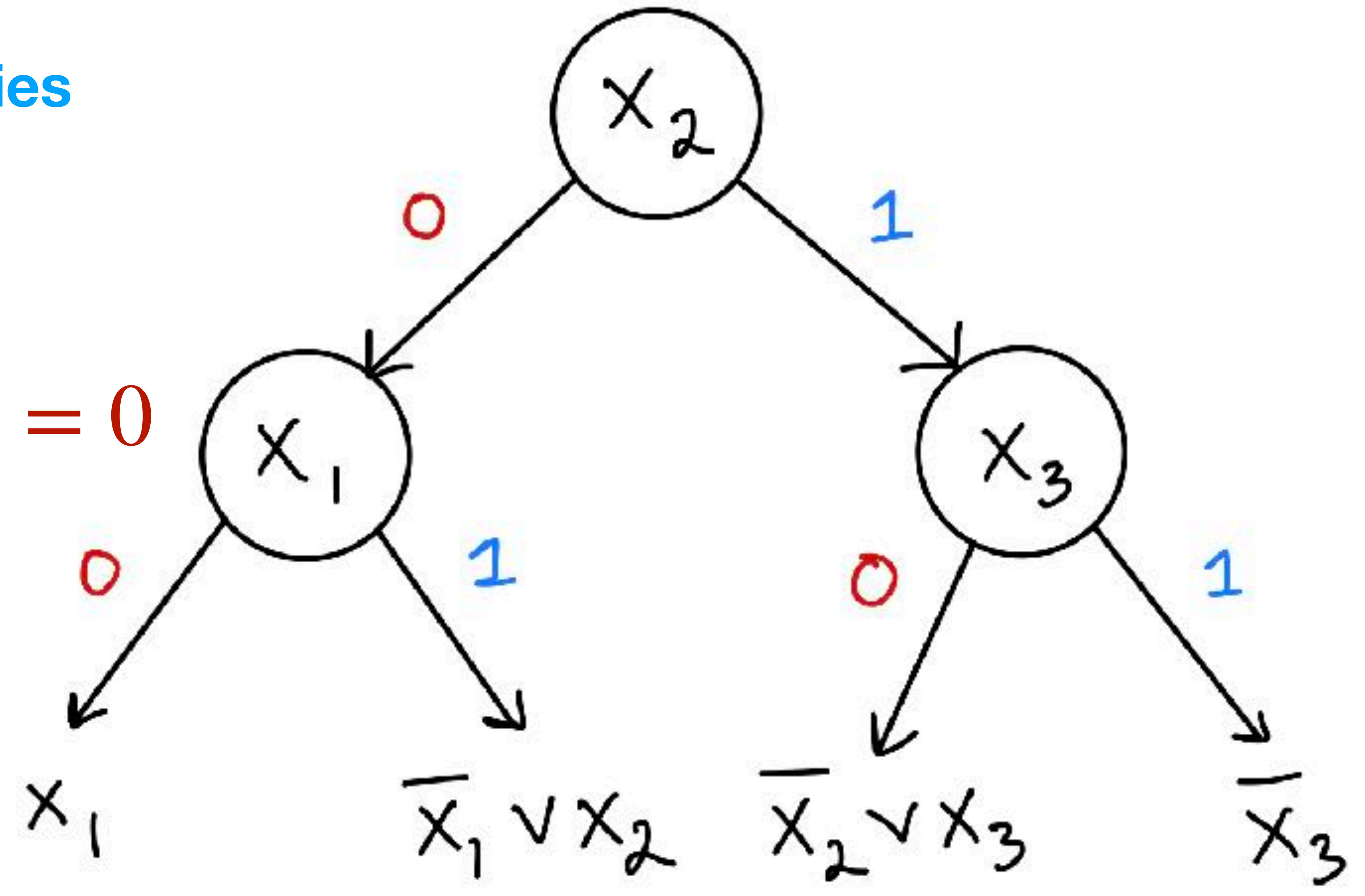
Tree-Like Resolution of F



Partial assignment falsifies corresponding clause

Decision Tree for $S(F)$

$x_2 = 0$

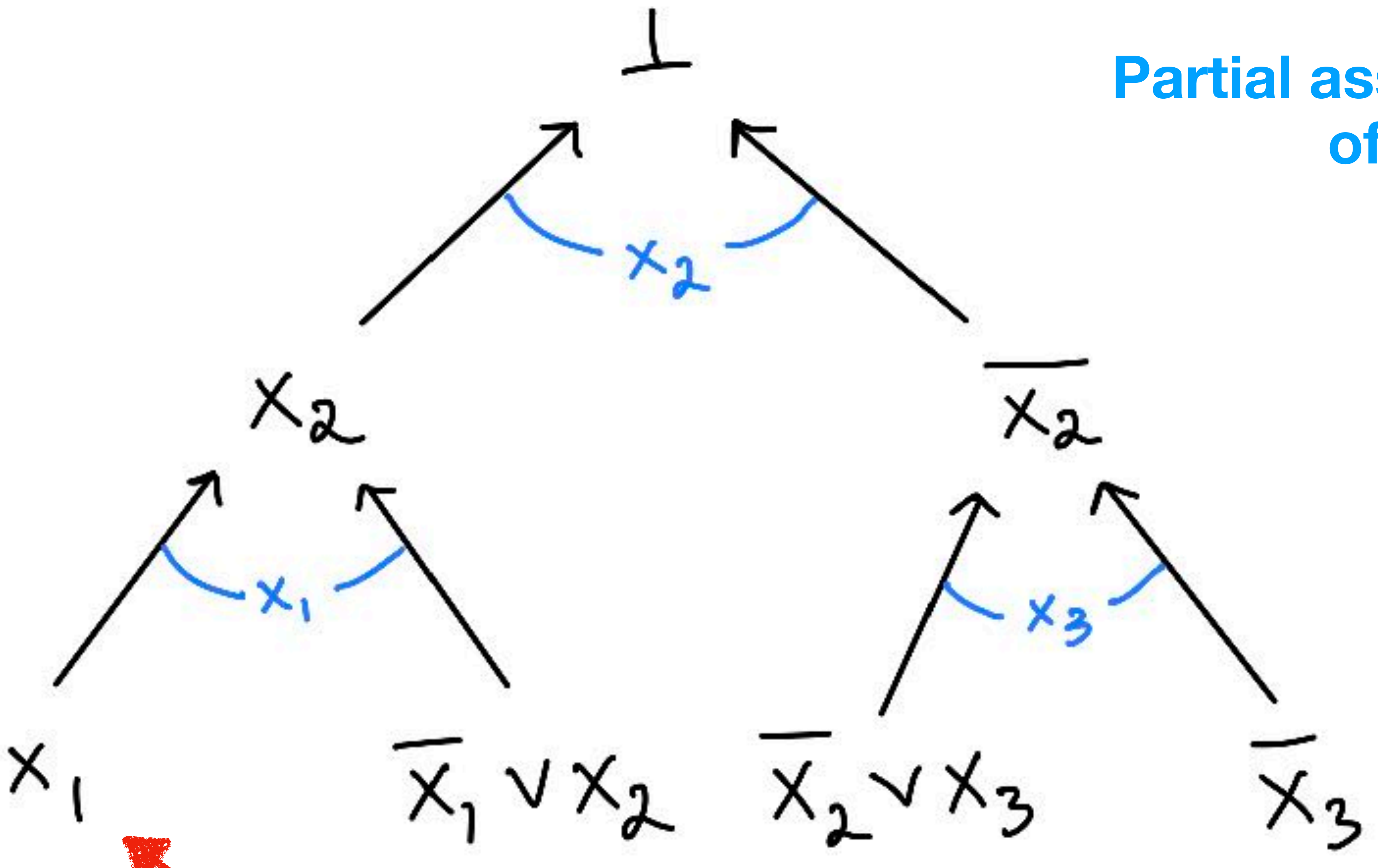


$$F = x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$$

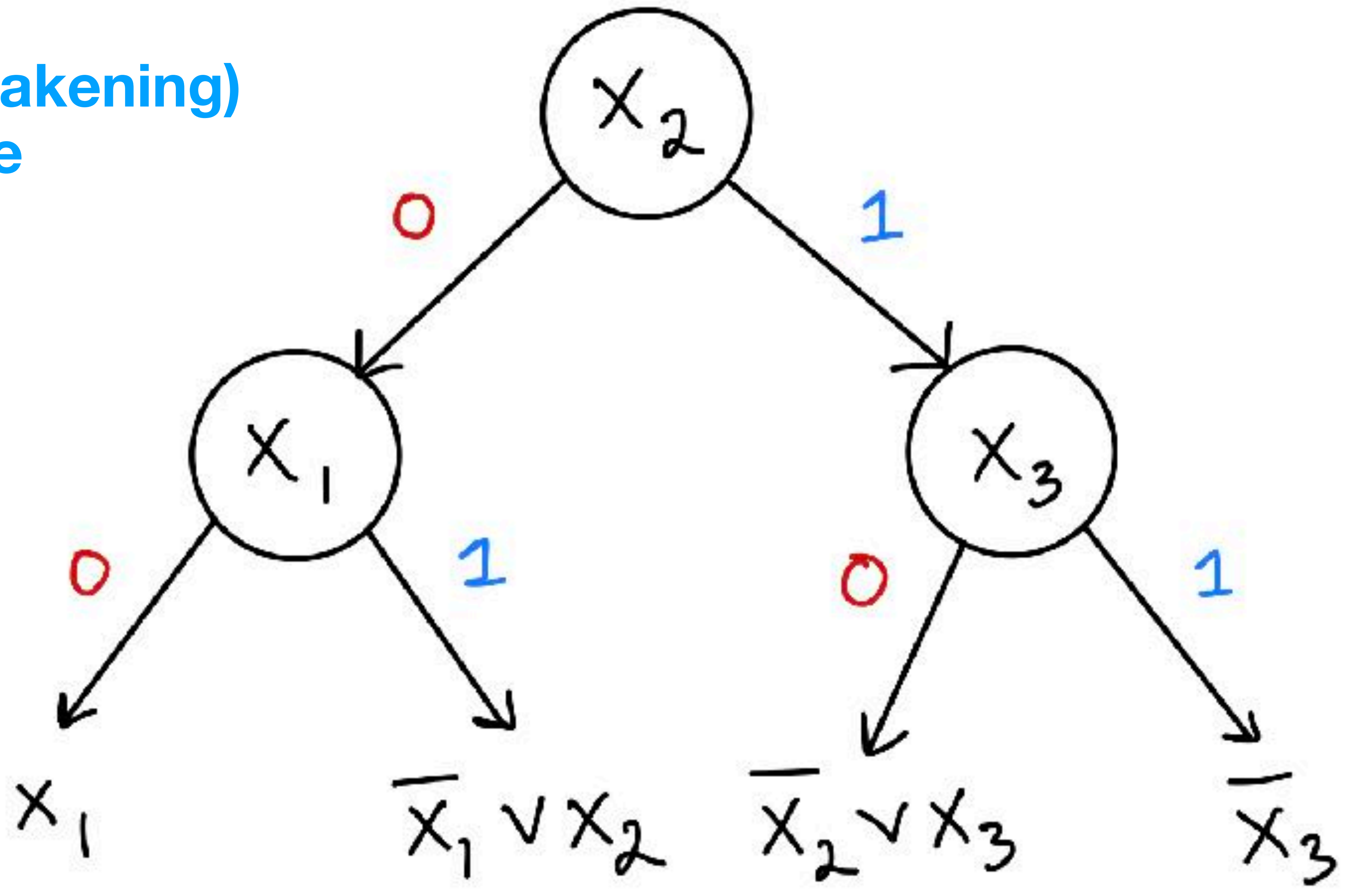
Tree-Like Resolution $\equiv$ Decision Trees

Tree-Like Resolution of F

Decision Tree for $S(F)$



Partial assignment falsifies (weakening) of corresponding clause



$x_1 = 0,\ x_2 = 0$

$$F = x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (\bar{x}_2 \vee x_3) \wedge \bar{x}_3$$

Tree-Like Resolution $\equiv$ Decision Trees

Theorem. Let F be an unsatisfiable CNF formula. Then

Size $O(s)$, depth $O(d)$ Tree-like Res. refutation of F

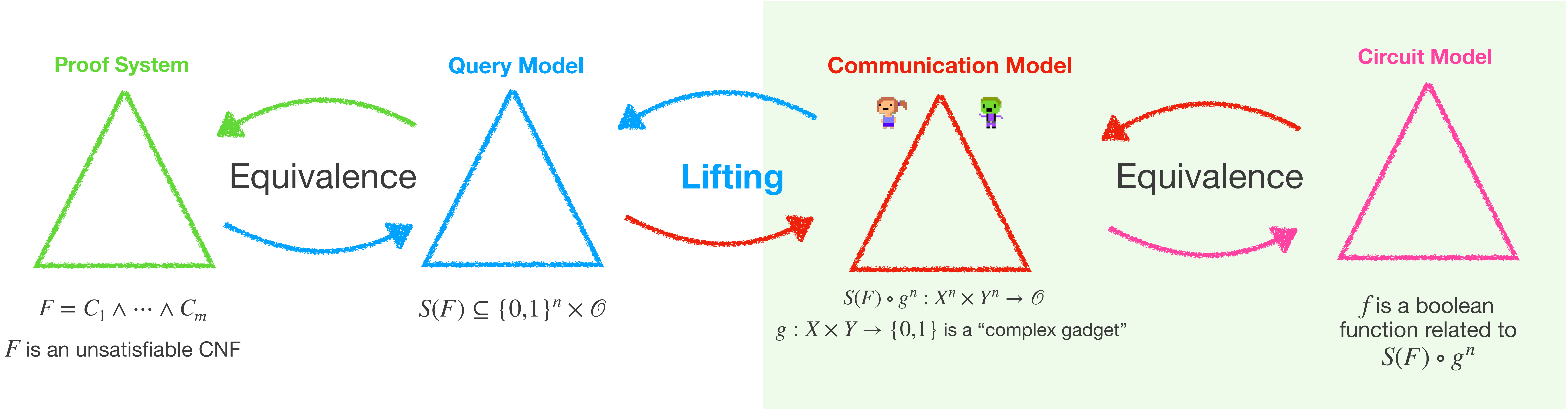
if and only if

Size $O(s)$, depth $O(d)$ Decision Tree for $S(F)$

Correspondence is stronger: essentially the same object!

Lifting Schema

All equivalences are “complexity preserving”



Communication TFNP

- $\mathcal{S} = \{S_n \subseteq (X^n \times Y^n) \times O_n\}_{n \in \mathbb{N}}$ sequence of communication total search problems
  - X, Y, O_n finite, O_n reasonably bounded in size (e.g. $|O_n| = n^{O(1)}$).
- $\mathcal{S} \in \mathrm{TFNP}^{cc}$ if for every n there is a **monochromatic rectangle cover** $\mathcal{R}$ of S_n of at most quasipolynomial size (equiv. polylogarithmic non-deterministic protocols)

  This means $\bigcup_{R \in \mathcal{R}} R = X^n \times Y^n$ and $\forall R \in \mathcal{R}\, \exists o \in O_n$ s.t. o is valid for all $(x, y) \in R$

- **Canonical Example:** Given $f : \{0,1\}^n \to \{0,1,*\}$, define the **KW-Game** [KW90]:

$$\mathrm{KW}(f) \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$$

Given $x \in f^{-1}(1), y \in f^{-1}(0)$, *find* $i \in [n]$ *such that* $x_i \neq y_i$

Karchmer-Wigderson Games

- Let $f : \{0,1\}^n \to \{0,1,*\}$
  - (Total) f **monotone** if $x \leq y$ (coordinate-wise) implies $f(x) \leq f(y)$
  - (Partial) f **monotone** if it has a total monotone extension
- f has an associated **total search problem** [KW 90]

$$\mathrm{KW}(f) \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$$

Given $x \in f^{-1}(1), y \in f^{-1}(0)$, *find* $i \in [n]$ *such that* $x_i \neq y_i$

Circuit Complexity of f $\equiv$ **Communication Complexity** of $\mathrm{KW}(f)$

Karchmer-Wigderson Games

- Let $f : \{0,1\}^n \to \{0,1,*\}$
  - (Total) f **monotone** if $x \leq y$ (coordinate-wise) implies $f(x) \leq f(y)$
  - (Partial) f **monotone** if it has a total monotone extension
- **Monotone** f has an associated **total search problem** [KW 90]

$$\text{mKW}(f) \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$$

Given $x \in f^{-1}(1), y \in f^{-1}(0)$, *find* $i \in [n]$ *such that* $x_i > y_i$

Mon. Circuit Complexity of f $\equiv$ **Mon. Communication Complexity** of $\text{KW}(f)$

Monotone KW-Games are Canonical

$$\text{mKW}(f) \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$$

Given $x \in f^{-1}(1), y \in f^{-1}(0)$*, find* $i \in [n]$ *such that* $x_i > y_i$

- Every $\mathcal{S} \in \text{TFNP}^{cc}$ is a mKW game in disguise!
- If $S \subseteq U \times V \times O$ with rect. cover $\mathcal{R} = \{U_i \times V_i\}_{i=1}^r$ then let $f : \{0,1\}^r \to \{0,1\}$:
  - $f(x) = 1$ if there is a $u \in X^n$ s.t. for all $i \in [r]$, $x_i = 1 \iff u \in U_i$
  - $f(x) = 0$ if there is a $v \in Y^n$ s.t. for all $i \in [r]$, $x_i = 0 \iff v \in V_i$
  - $f(x) = *$ otherwise
- Well defined since if x satisfies both conditions then (u, v) is not covered by $\mathcal{R}$!

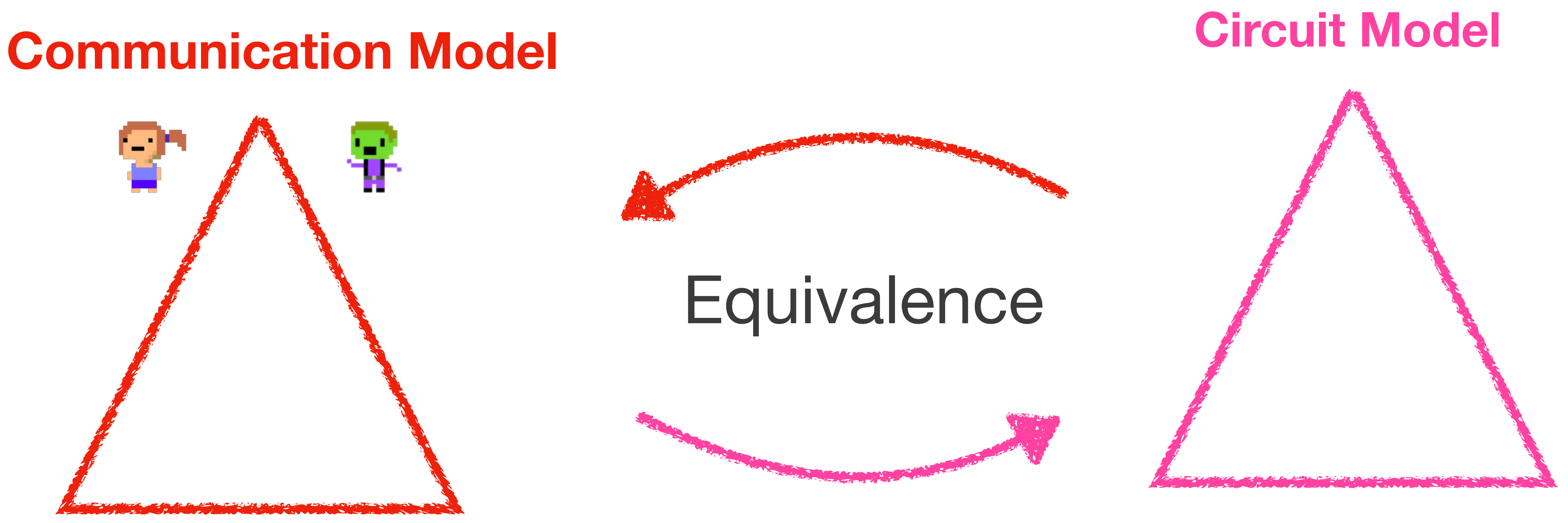
Monotone KW-Games are Canonical

$$\mathsf{mKW}(f) \subseteq f^{-1}(1) \times f^{-1}(0) \times [n]$$

Given $x \in f^{-1}(1), y \in f^{-1}(0)$, *find* $i \in [n]$ *such that* $x_i > y_i$

- Every $\mathcal{S} \in \mathsf{TFNP}^{cc}$ is a mKW game in disguise!
- If $S \subseteq U \times V \times O$ with rect. cover $\mathcal{R} = \{U_i \times V_i\}_{i=1}^r$ then let $f : \{0,1\}^r \to \{0,1\}$:
  - $f(x) = 1$ if there is a $u \in X^n$ s.t. for all $i \in [r]$, $x_i = 1 \iff u \in U_i$
  - $f(x) = 0$ if there is a $v \in Y^n$ s.t. for all $i \in [r]$, $x_i = 0 \iff v \in V_i$
  - $f(x) = *$ otherwise
- With this definition, $\mathsf{mKW}(f)$ is equivalent to S!

KW Games and Circuit Complexity



$S(F) \circ g^n : X^n \times Y^n \to \mathcal{O}$

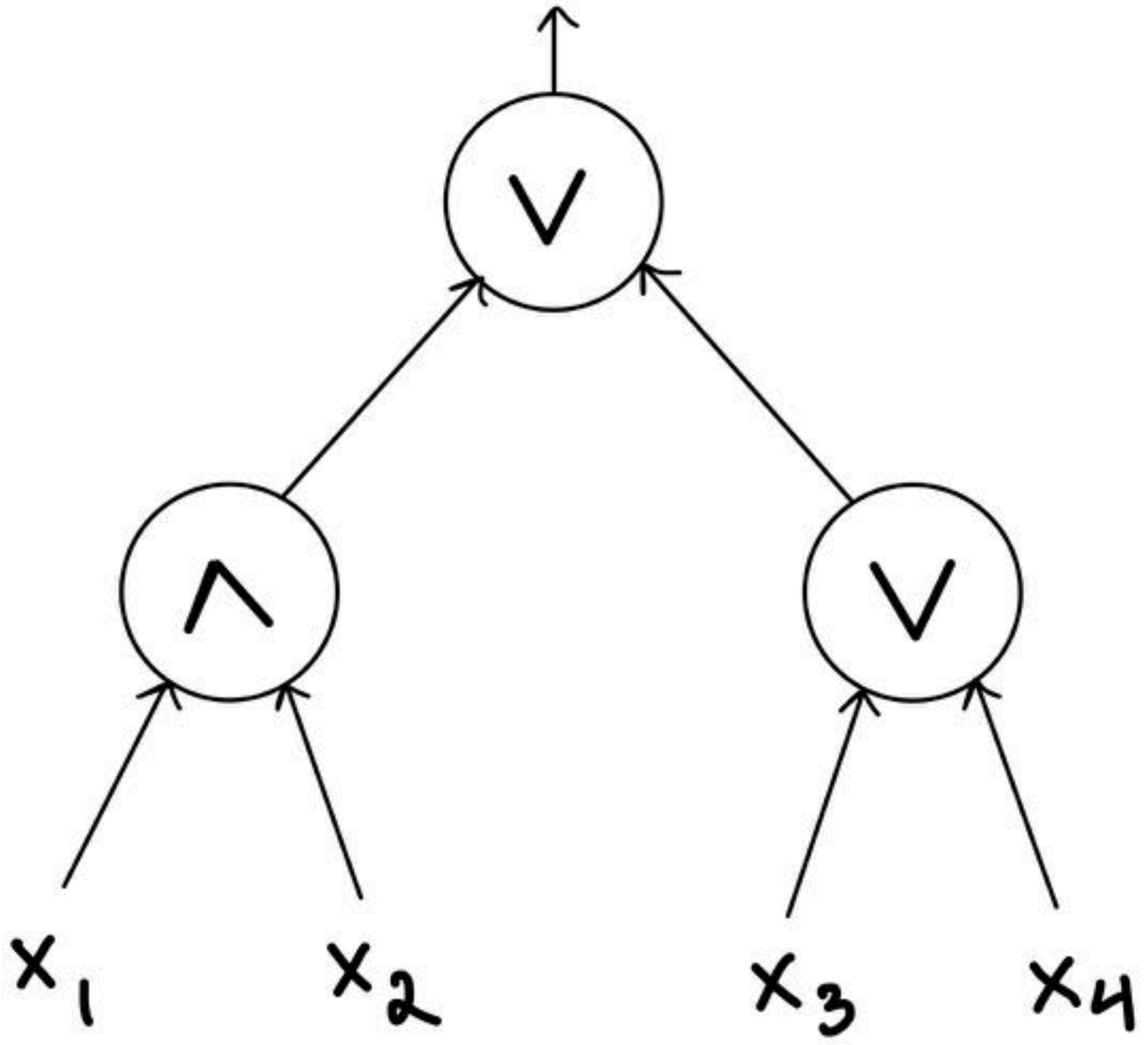
$g : X \times Y \to \{0,1\}$ is a "complex gadget"

f is a boolean function related to $S(F) \circ g^n$

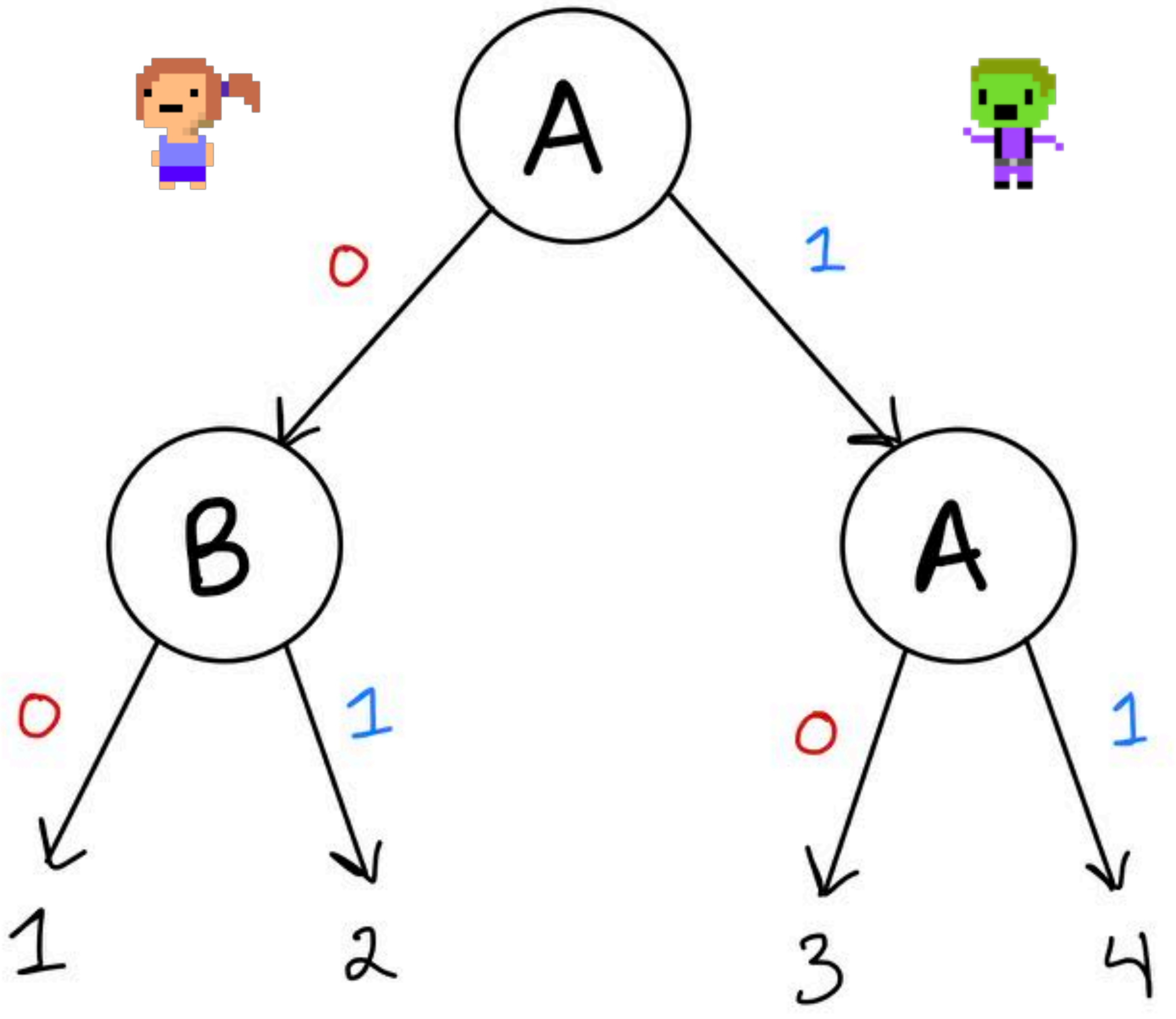
- Karchmer and Wigderson famously showed that the **deterministic communication complexity** of (m)KW(f) captures (monotone) **circuit depth** [KW 90]
- Razborov later showed that PLS^{cc} captures (monotone) **circuit size**! [Razb 95]

Formulas $\equiv$ Communication

Boolean Formula for f



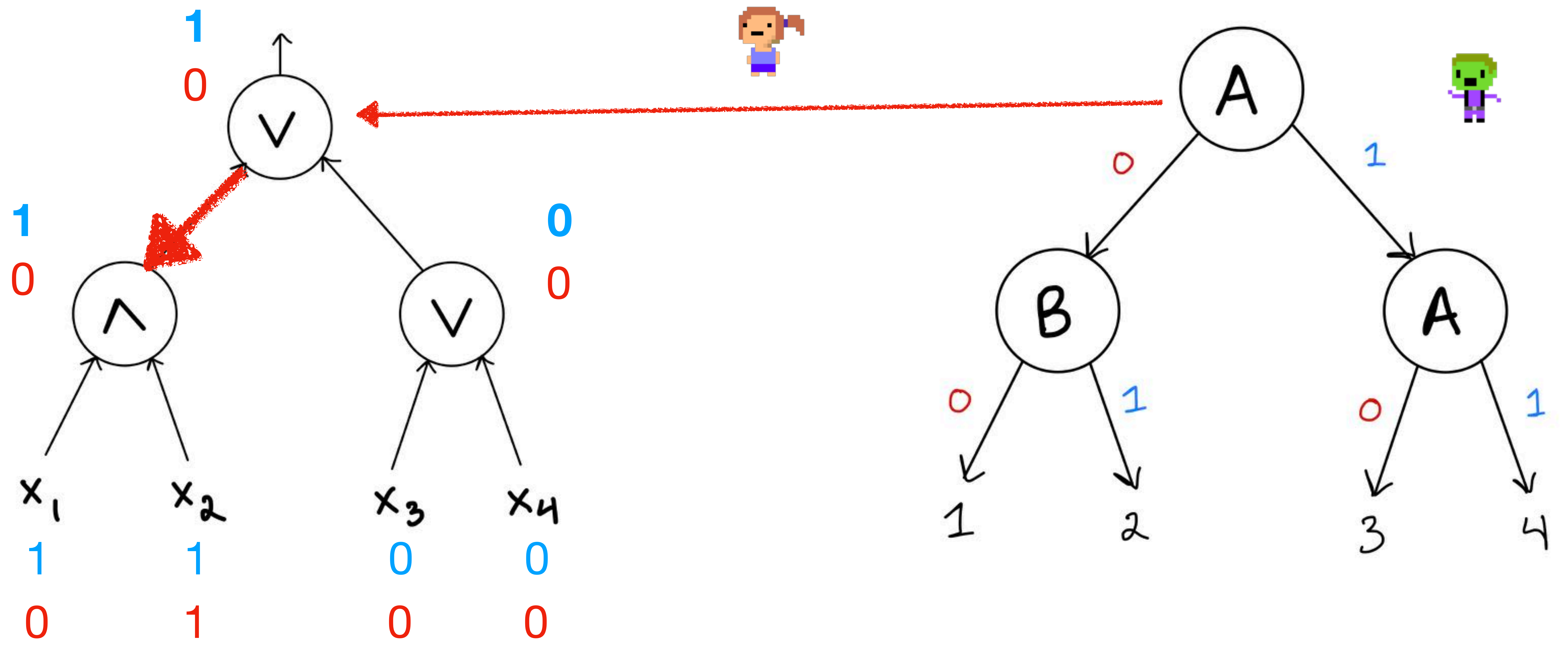
Protocol for $\mathsf{KW}(f)$



$$f = (x_1 \wedge x_2) \vee x_3 \vee x_4$$

Formulas $\equiv$ Communication

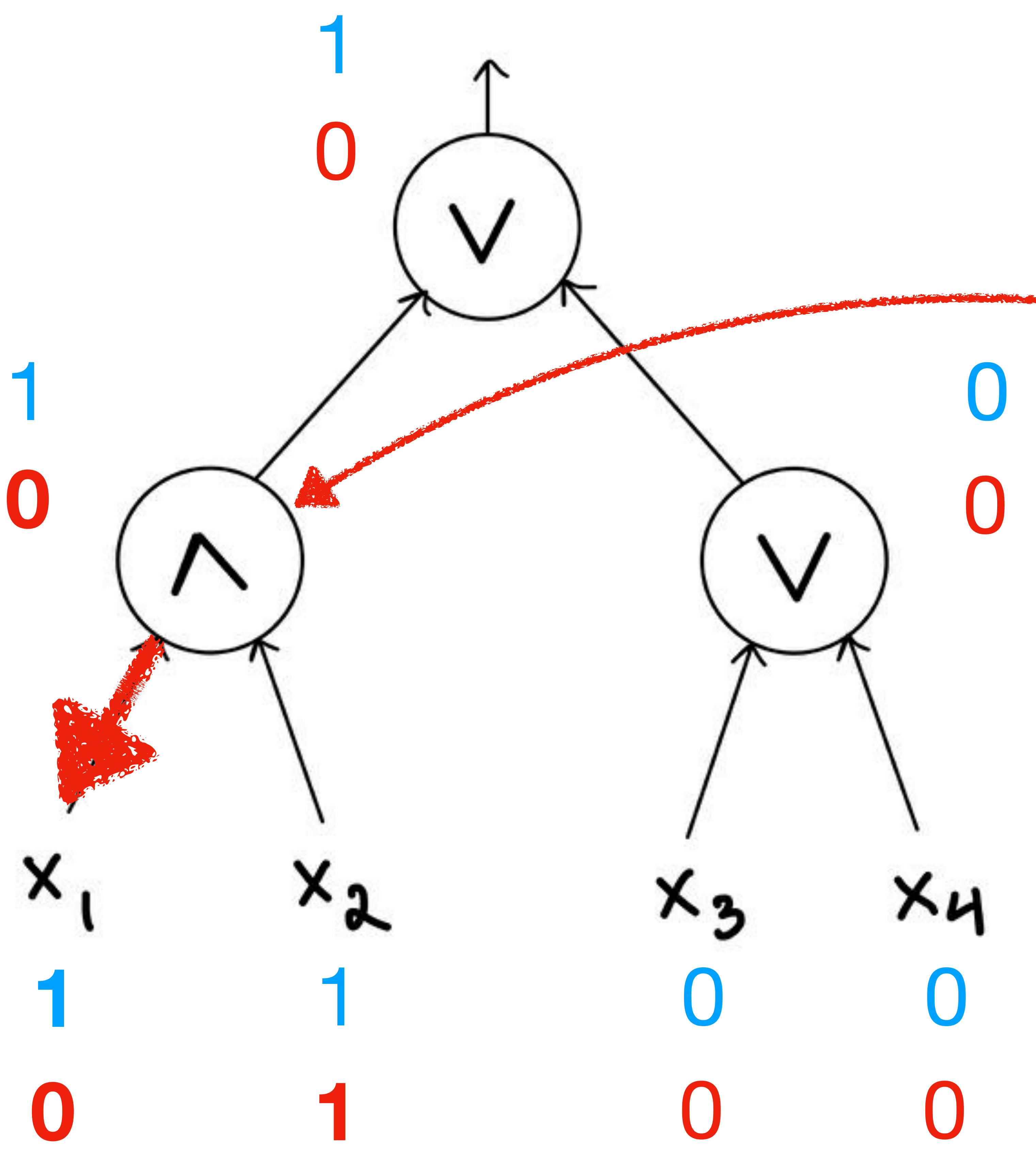
Boolean Formula for f | Protocol for $\mathrm{KW}(f)$



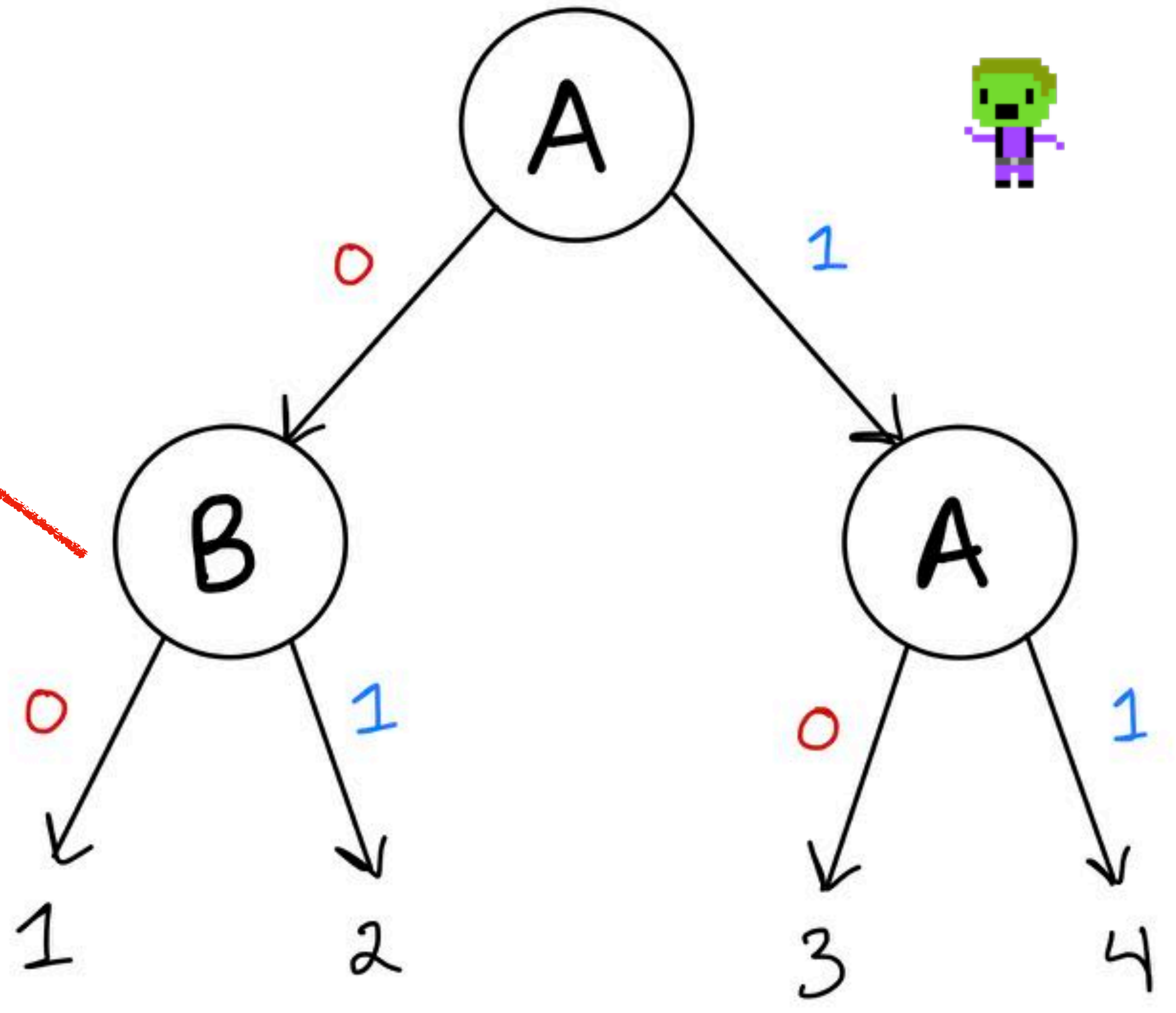
$$f = (x_1 \wedge x_2) \vee x_3 \vee x_4$$

Formulas $\equiv$ Communication

Boolean Formula for f



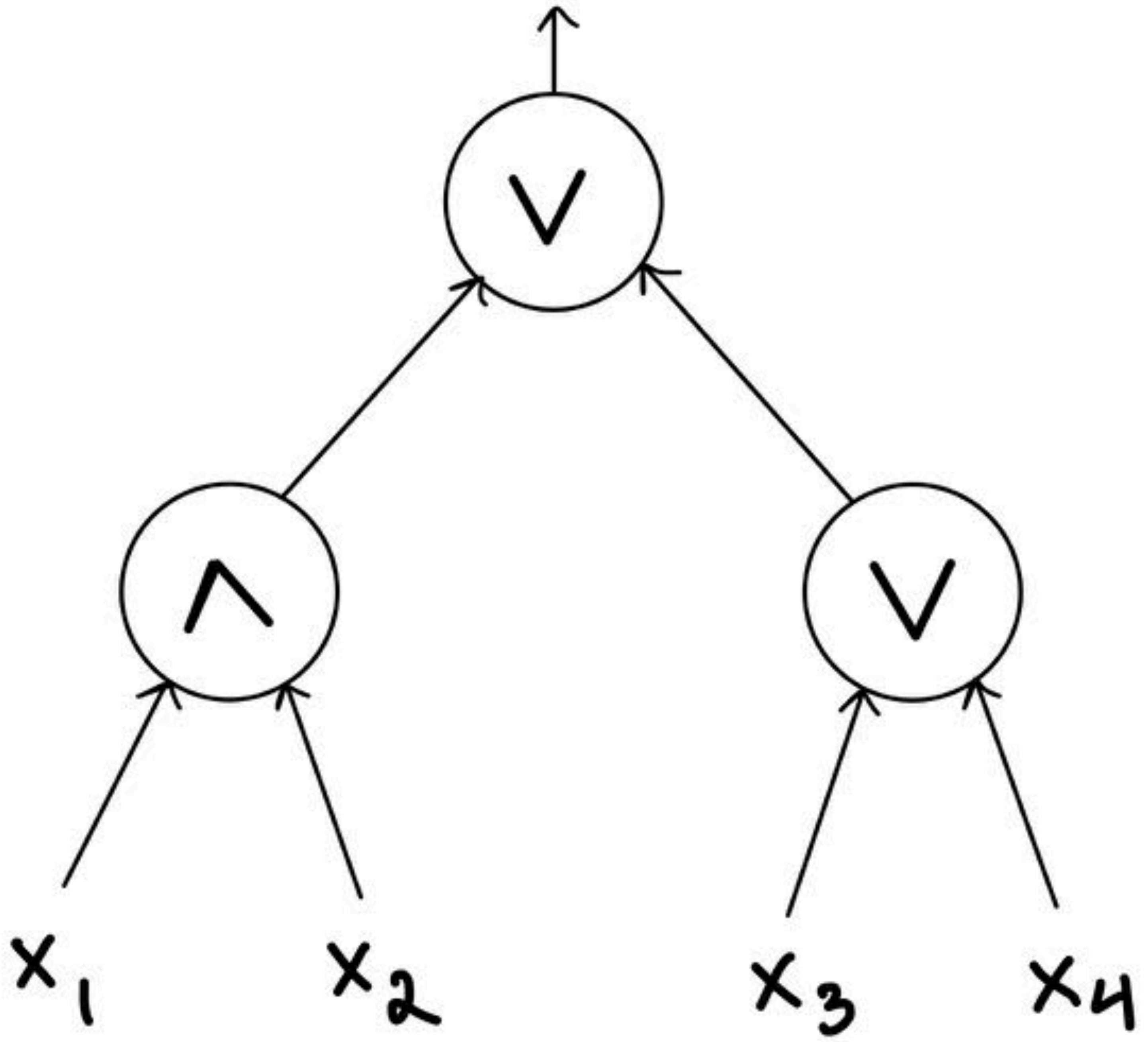
Protocol for $\mathrm{KW}(f)$



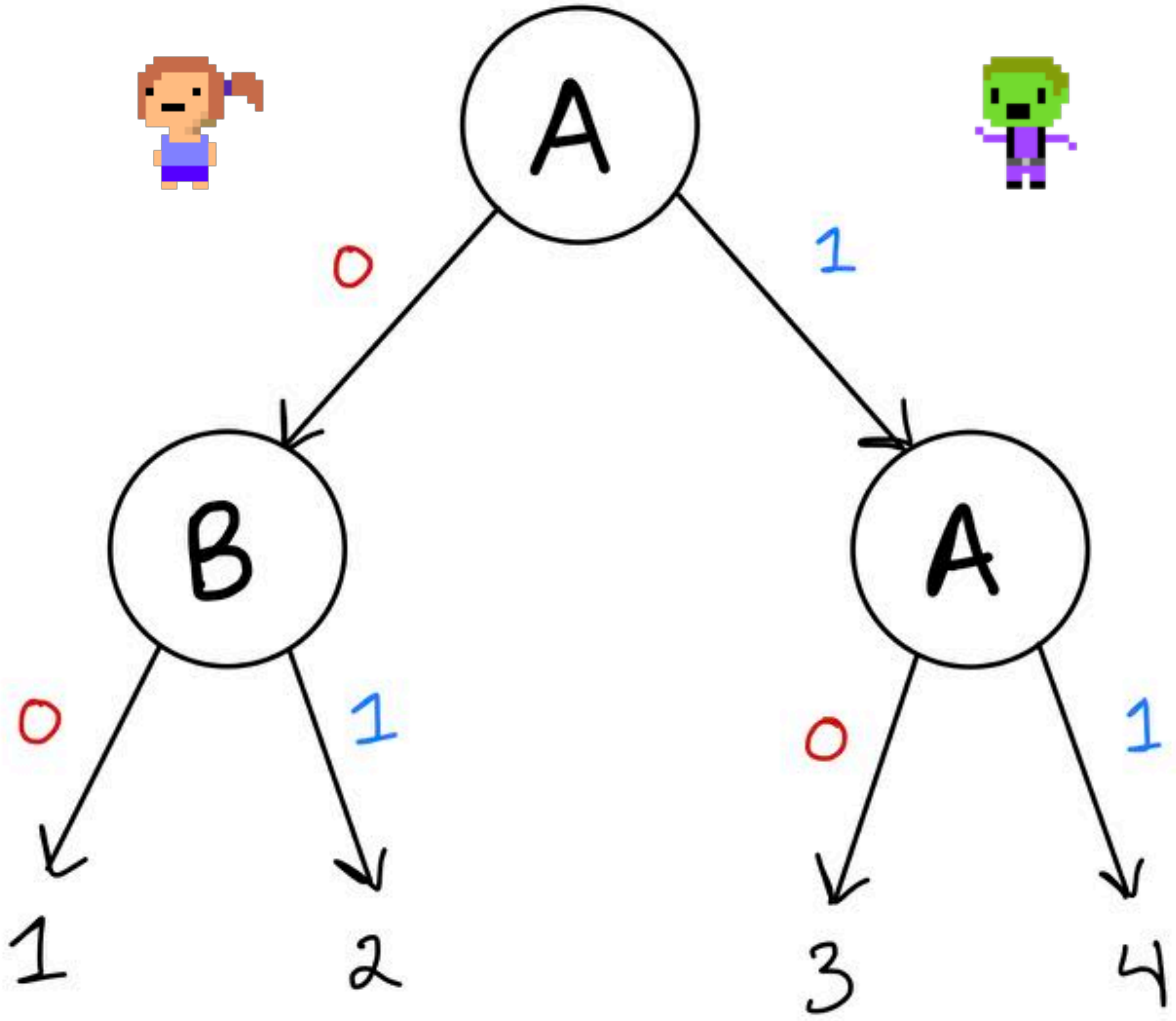
$$f = (x_1 \wedge x_2) \vee x_3 \vee x_4$$

Formulas ≡ Communication

Boolean Formula for f



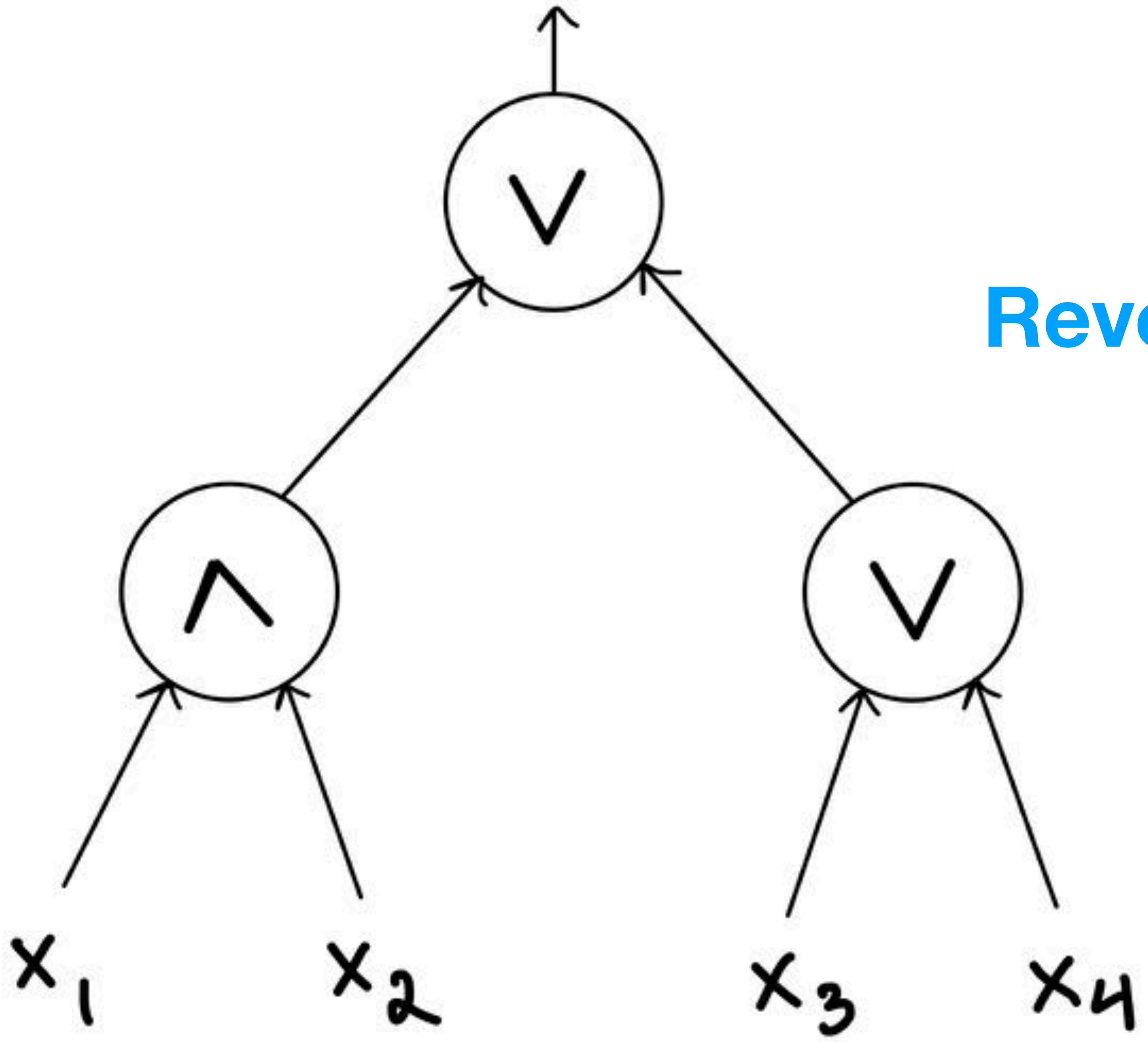
Protocol for $\mathsf{KW}(f)$



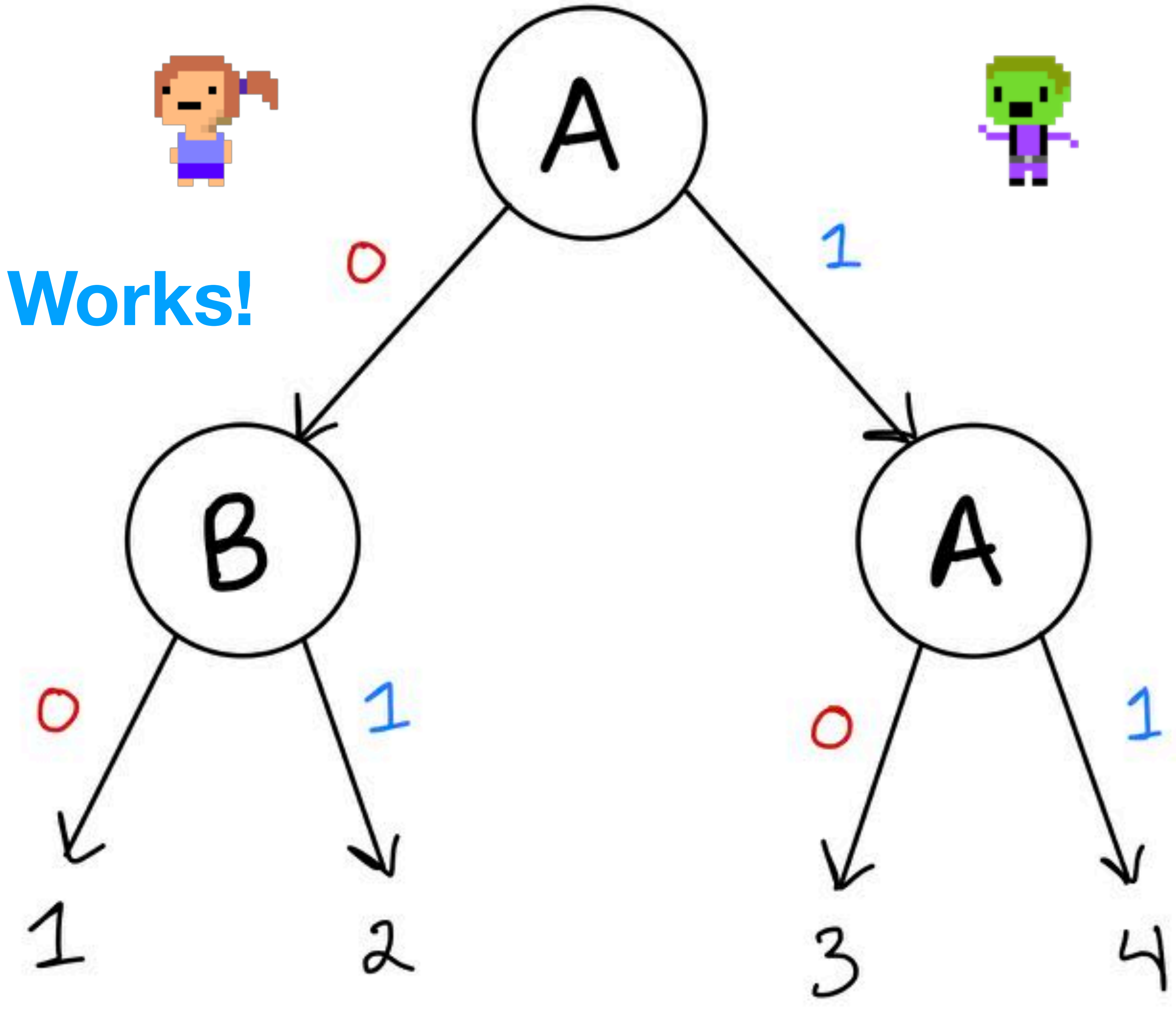
$$f = (x_1 \wedge x_2) \vee x_3 \vee x_4$$

Formulas $\equiv$ Communication

Boolean Formula for f



Protocol for $\mathrm{KW}(f)$



Reverse Direction Also Works!

$$f = (x_1 \wedge x_2) \vee x_3 \vee x_4$$

Formulas $\equiv$ Communication

Theorem.

Let $f : \{0,1\}^n \to \{0,1,*\}$ be a partial boolean function. Then

Size $O(s)$, depth $O(d)$ Boolean formula for f

if and only if

Size $O(s)$, depth $O(d)$ communication protocol for $\mathsf{KW}(f)$

Correspondence is stronger: essentially the same object!

Formulas $\equiv$ Communication

Theorem.

Let $f : \{0,1\}^n \to \{0,1,*\}$ be a partial **monotone** boolean function. Then

Size $O(s)$, depth $O(d)$ **monotone** Boolean formula for f

if and only if

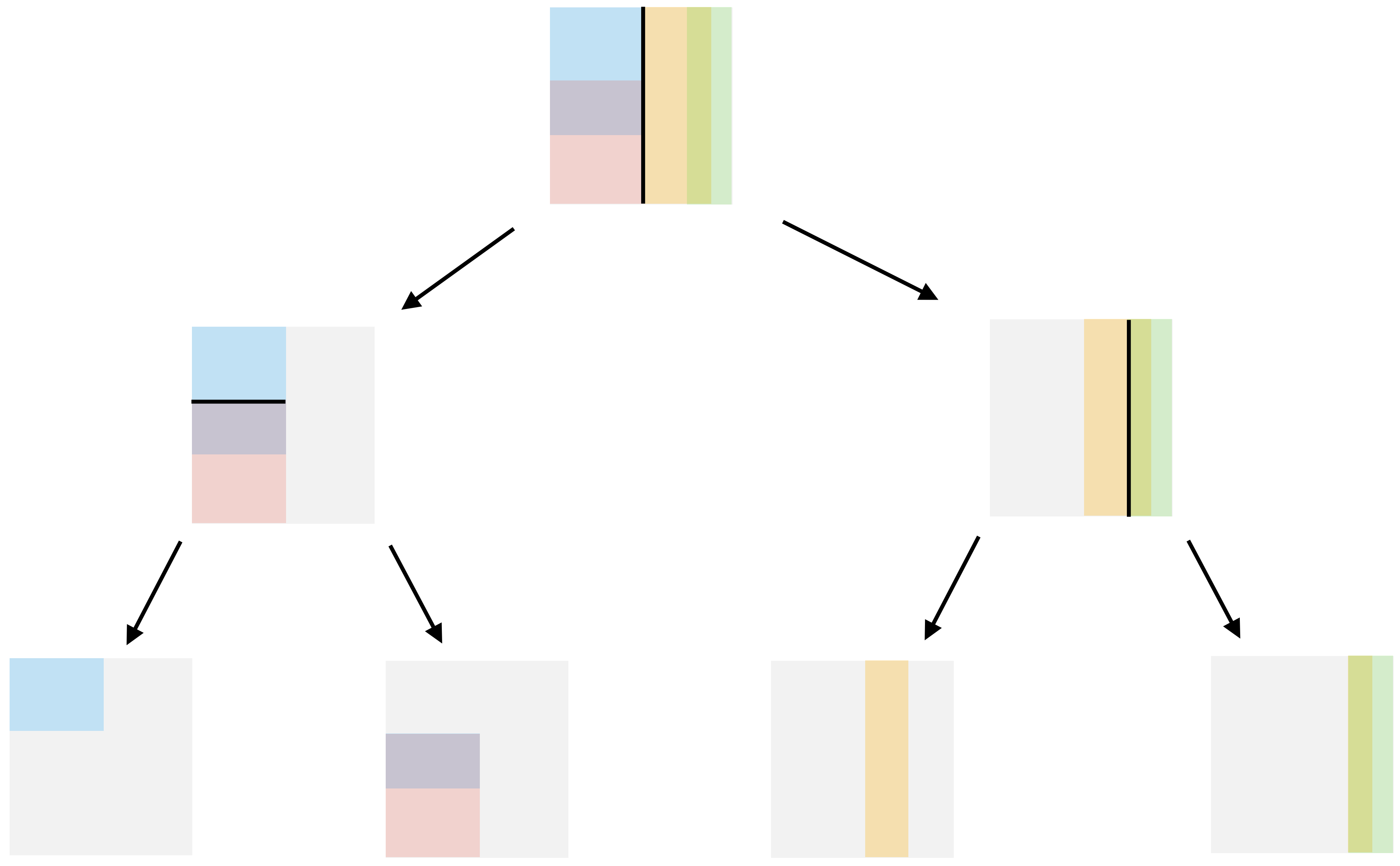
Size $O(s)$, depth $O(d)$ communication protocol for $\mathrm{mKW}(f)$

Correspondence is stronger: essentially the same object!

Alternate Perspective: Rectangle DAGs

- Let $S \subseteq X^n \times Y^n \times O$ be a total search problem

- A **rectangle DAG** for S is a directed acyclic graph $G = (V, E)$ with a unique root node such that
  - Every vertex is a rectangle in $X^n \times Y^n$
  - Root is $X^n \times Y^n$
  - Leaves are **monochrome** (consistent with one solution)
  - If R has children $R_1, R_2 \Rightarrow R \subseteq R_1 \cup R_2$



Rectangle DAGs vs KW-Games

Let $\mathrm{mF}(f)$ denote the minimum size of any monotone formula computing f.

Theorem [KW90]. Rectangle **Tree** Size of $\mathrm{mKW}_f = \Theta(\mathrm{mF}(f))$

Let $\mathrm{mC}(f)$ denote the minimum size of any monotone circuit computing f.

Theorem [R95, S16, GGKS17]. Rectangle **DAG** Size of $\mathrm{mKW}_f = \Theta(\mathrm{mC}(f))$

- *Rectangle DAG:*
  - Root is $X \times Y$
  - Leaves are monochrome (consistent with one solution)
  - If R has children $R_1, R_2 \Rightarrow R \subseteq R_1 \cup R_2$

Query Models and Communication Models

Bottom-up models (proofs, circuits)

are captured by

Top-down algorithms (decision trees, comm. protocols)

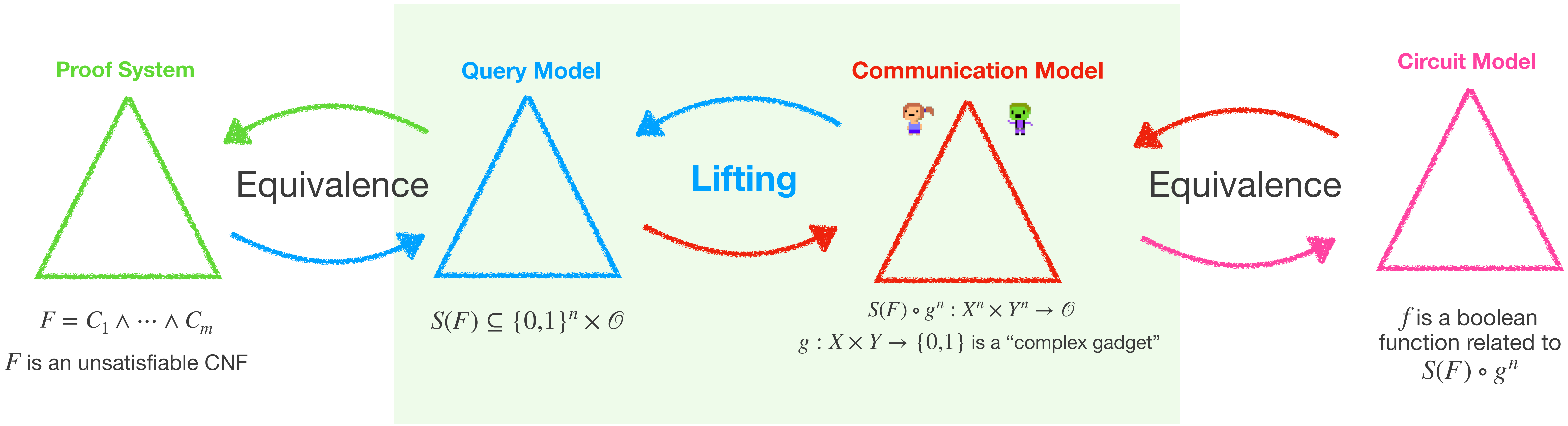
$\mathsf{Search}(F)$ and $\mathsf{mKW}(\mathsf{f})$

- **Capture** the complexity of these processes
- Are **canonical** examples of their respective TFNP classes

Part 2

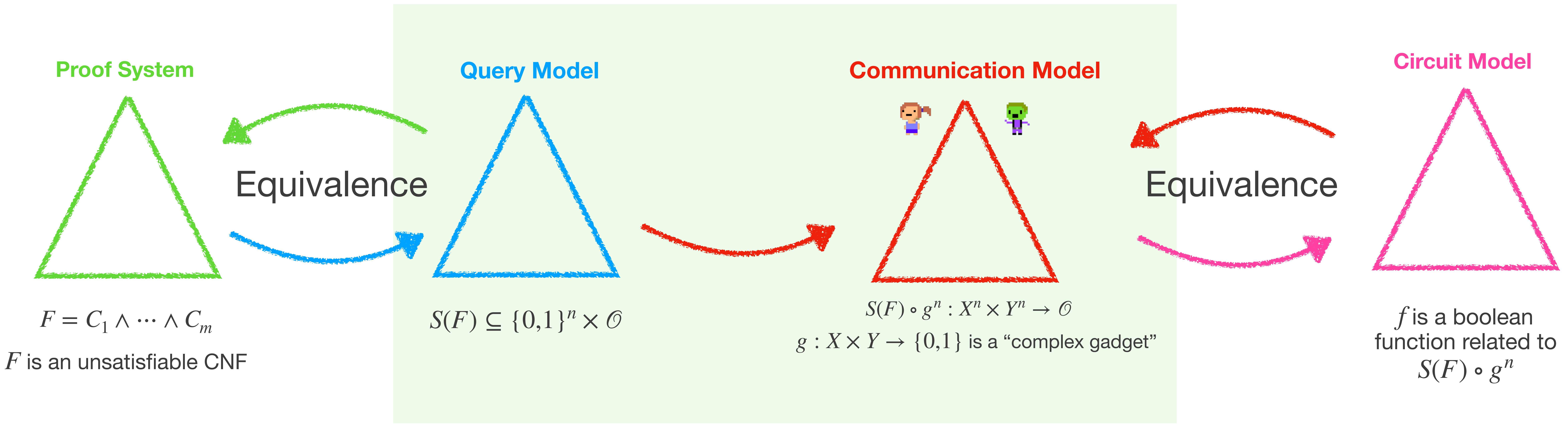
Relating Query to Communication

Lifting Schema



First, we need to discuss how to relate $S(F)$ for unsatisfiable F with communication search problems.

Lifting Schema



First, we need to discuss how to relate $S(F)$ for unsatisfiable F with communication search problems.

“Feasible Interpolation”

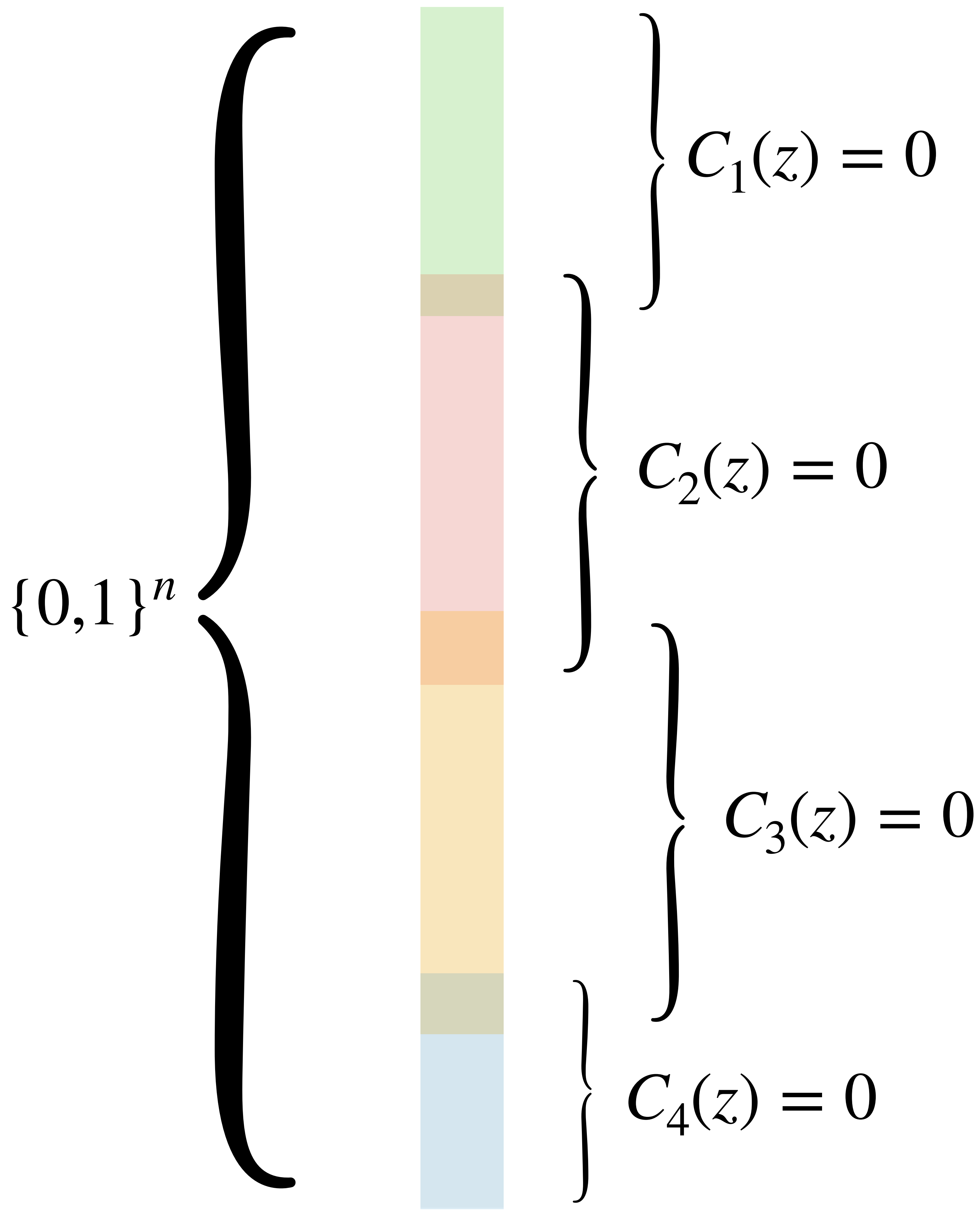
- Many interesting results from **relating** two worlds
- Here is the simplest way to turn a query problem into a communication problem.
- If $\mathcal{S} \subseteq \{0,1\}^n \times O$ is a **query** search problem, let $[n] = X \cup Y$ be variable partition
- Define $\mathcal{S}^{X,Y} \subseteq \{0,1\}^X \times \{0,1\}^Y \times O$ as a **communication** problem, so
  - Alice gets $x \in \{0,1\}^X$, Bob gets $y \in \{0,1\}^Y$, solutions are $\mathcal{S}^{X,Y}(x,y) = \mathcal{S}(xy)$
- Translates **circuit lower bounds** to **proof lower bounds**
  - Closely related to classical **feasible interpolation** results [K97, P97, BPR00,…]
  - Construction underlies Cutting Planes lbs for random CNFs [FPPR 16, HP16]

From Proofs to Communication

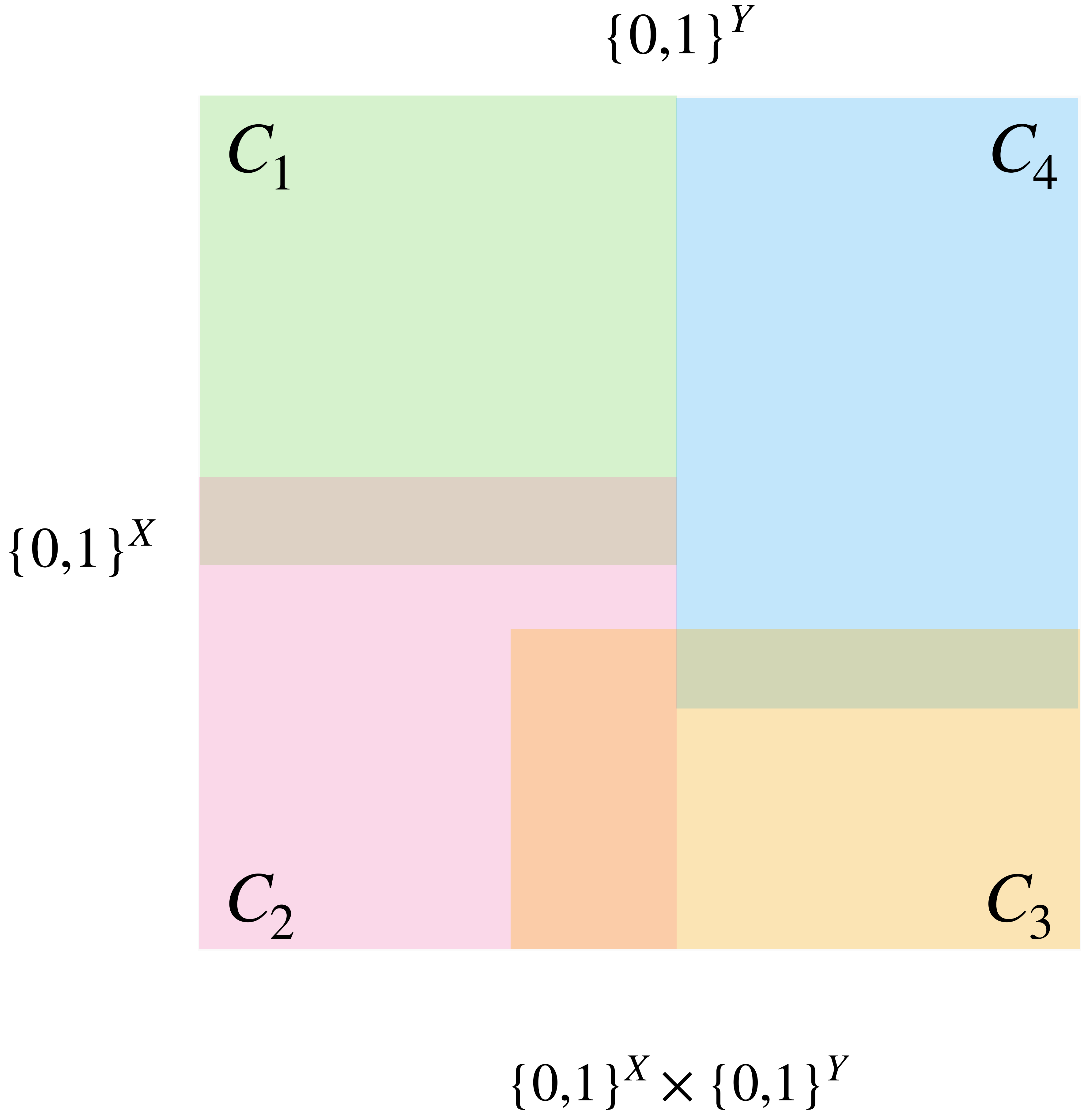
Search$(F) \subseteq \{0,1\}^n \times [m]$

$F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$
unsatisfiable CNF

Search$_{X,Y}(F) \subseteq \{0,1\}^X \times \{0,1\}^Y \times [m]$



partition
$[n] = X \cup Y$



From Proofs to Communication

- Let $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ be an unsatisfiable CNF on variables $z_1, \ldots, z_n$.
- $S(F)$: Given $z \in \{0,1\}^n$, find $i \in [m]$ such that $C_i(z) = 0$.
- For any partition $X \cup Y = [n]$, $S_{X,Y}(F) \subseteq \{0,1\}^X \times \{0,1\}^Y \times [m]$:
  - Given $x \in \{0,1\}^X$, $y \in \{0,1\}^Y$, find $i \in [m]$ such that $C_i(xy) = 0$.
- **Observation:** Since C_i is a clause, the set

Combinatorial Rectangle!

$$R_i = \{(x,y) \in \{0,1\}^X \times \{0,1\}^Y : C_i(xy) = 0\}$$

$$= \{x \in \{0,1\}^X : C_i^X(x) = 0\} \times \{y \in \{0,1\}^Y : C_i^Y(y) = 0\}$$

- Thus *clauses of* F yield a *rectangle covering* of $S_{X,Y}(F)$

mCSP-SAT / Unsatisfiability Certificate

- *Every* communication total search problem is equivalent to mKW_f for some partial monotone boolean function $f : \{0,1\}^n \to \{0,1,*\}$
- What is the boolean function corresponding to $S_{X,Y}(F)$?
- [FPPR 17, HP 17] Gave independent (essentially equivalent) answers.
  - [FPPR 17] $\mathrm{mCSPSAT}$:= *monotone generalization of SAT*
    - ($\mathrm{mCSPSAT}$ appears in many works on lifting [GP12, GPW14, O15,…])
  - [HP 17] cert_F := *unsatisfiability certificate of* F

Unsatisfiability Certificate [HP 17]

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ unsat. CNF, $X \cup Y = [n]$ partition of variables
- Let $C_i = C_i^X \vee C_i^Y$ (partition clauses according to X, Y)
- Define $\mathrm{cert}_F = \mathrm{cert}_F^{X,Y} : \{0,1\}^m \to \{0,1\}$ by

$$\mathrm{cert}_F(z) = \begin{cases} 1 & \bigwedge_{i : z_i = 0} C_i^X \text{ is satisfiable} \\ 0 & \bigwedge_{i : z_i = 1} C_i^Y \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Unsatisfiability Certificate [HP 17]

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ unsat. CNF, $X \cup Y = [n]$ partition of variables
- Let $C_i = C_i^X \vee C_i^Y$ (partition clauses according to X, Y)
- Define $\mathrm{cert}_F = \mathrm{cert}_F^{X,Y} : \{0,1\}^m \to \{0,1\}$ by

$$\begin{array}{cccc} z_1 & z_2 & z_3 & z_4 \\ (C_1^X \vee C_1^Y) \wedge & (C_2^X \vee C_2^Y) \wedge & (C_3^X \vee C_3^Y) \wedge & (C_4^X \vee C_4^Y) \end{array}$$

$$\mathrm{cert}_F(z) = \begin{cases} 1 & \bigwedge_{i : z_i = 0} C_i^X \text{ is satisfiable} \\ 0 & \bigwedge_{i : z_i = 1} C_i^Y \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Unsatisfiability Certificate [HP 17]

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ unsat. CNF, $X \cup Y = [n]$ partition of variables
- Let $C_i = C_i^X \vee C_i^Y$ (partition clauses according to X, Y)
- Define $\text{cert}_F = \text{cert}_F^{X,Y} : \{0,1\}^m \to \{0,1\}$ by

$$z_1 = 1 \quad z_2 = 0 \quad z_3 = 1 \quad z_4 = 0$$

$$(C_1^X \vee C_1^Y) \wedge (\boxed{C_2^X} \vee C_2^Y) \wedge (C_3^X \vee C_3^Y) \wedge (\boxed{C_4^X} \vee C_4^Y)$$

Satisfiable?

$$\text{cert}_F(z) = \begin{cases} \boxed{1} & \bigwedge_{i : z_i = 0} C_i^X \text{ is satisfiable} \\ 0 & \bigwedge_{i : z_i = 1} C_i^Y \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Unsatisfiability Certificate [HP 17]

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ unsat. CNF, $X \cup Y = [n]$ partition of variables
- Let $C_i = C_i^X \vee C_i^Y$ (partition clauses according to X, Y)
- Define $\mathrm{cert}_F = \mathrm{cert}_F^{X,Y} : \{0,1\}^m \to \{0,1\}$ by

$$\begin{array}{cccc} {\color{red} z_1 = 1} & {\color{blue} z_2 = 0} & {\color{red} z_3 = 1} & {\color{blue} z_4 = 0} \end{array}$$

$$(C_1^X \vee \boxed{C_1^Y}) \wedge (C_2^X \vee C_2^Y) \wedge (C_3^X \vee \boxed{C_3^Y}) \wedge (C_4^X \vee C_4^Y)$$

Satisfiable?

$$\mathrm{cert}_F(z) = \begin{cases} 1 & \bigwedge_{i : z_i = 0} C_i^X \text{ is satisfiable} \\ \boxed{0} & \bigwedge_{i : z_i = 1} C_i^Y \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

Unsatisfiability Certificate [HP 17]

- $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ unsat. CNF, $X \cup Y = [n]$ partition of variables
- Let $C_i = C_i^X \vee C_i^Y$ (partition clauses according to X, Y)
- Define $\mathrm{cert}_F = \mathrm{cert}_F^{X,Y} : \{0,1\}^m \to \{0,1\}$ by

$$z_1 = 1 \qquad z_2 = 0 \qquad z_3 = 1 \qquad z_4 = 0$$

$$(C_1^X \vee \boxed{C_1^Y}) \wedge (\boxed{C_2^X} \vee C_2^Y) \wedge (C_3^X \vee \boxed{C_3^Y}) \wedge (\boxed{C_4^X} \vee C_4^Y)$$

$$\mathrm{cert}_F(z) = \begin{cases} 1 & \bigwedge_{i : z_i = 0} C_i^X \text{ is satisfiable} \\ 0 & \bigwedge_{i : z_i = 1} C_i^Y \text{ is satisfiable} \\ * & \text{otherwise} \end{cases}$$

If both satisfiable then the whole formula is satisfiable!

Feasible Interpolation

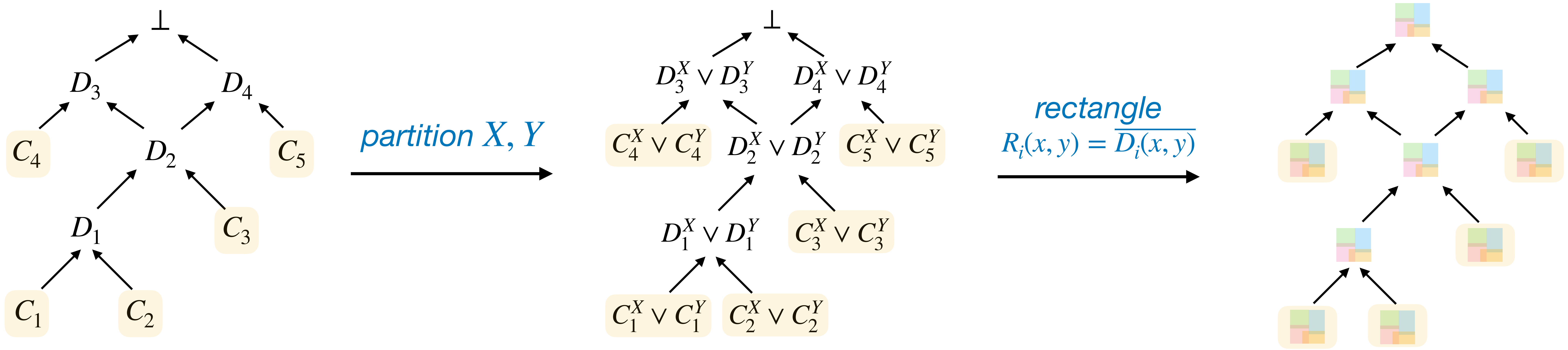
Theorem [HP17]**.** Let F be any unsatisfiable CNF, and let X, Y be any variable partition.

If there is a Resolution refutation of F of size s, then there is a monotone circuit computing $\mathsf{cert}_F = \mathsf{cert}_F^{X,Y}$ of size $O(s)$.

Theorem [HP17]**.** Let F be any unsatisfiable CNF, and let X, Y be any variable partition.

If there is a Resolution refutation of F of size s, then there is a monotone circuit computing $\mathrm{cert}_F = \mathrm{cert}_F^{X,Y}$ of size $O(s)$.

Proof. Given size-s Resolution refutation of F, give size-s Rectangle DAG for $\mathrm{mKW}_{\mathrm{cert}_F}$

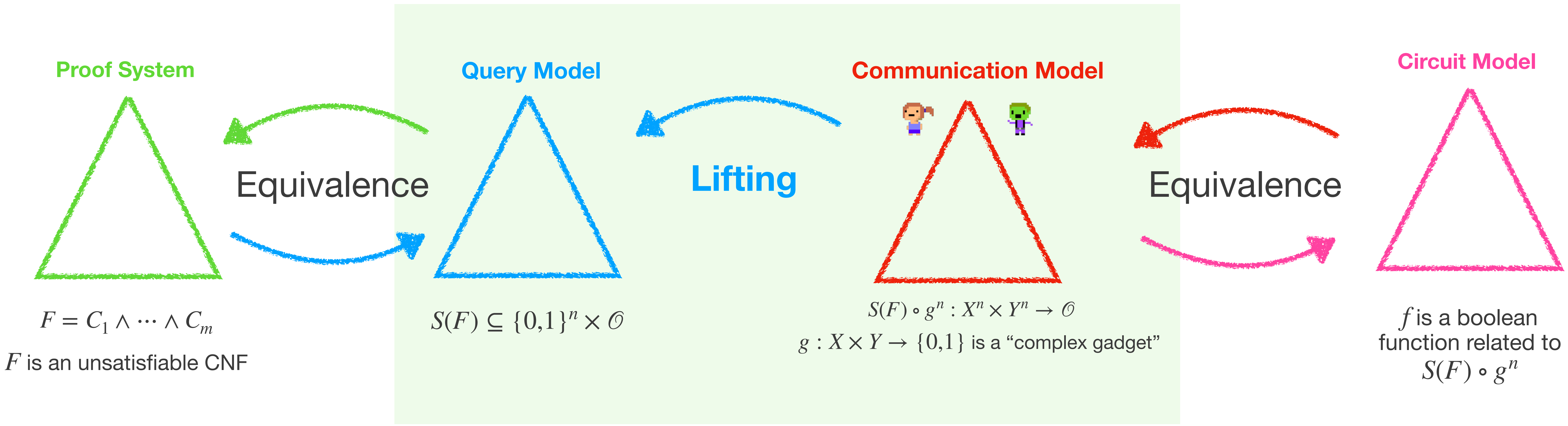


- Root rectangle is $\{0,1\}^X \times \{0,1\}^Y$
- Leaves are defining rectangles for $\mathrm{mKW}_{\mathrm{cert}_F}$
- If D_i deduced from D_j, D_k by resolution, then $R_i \subseteq R_j \cup R_k$
  - Equivalently, if $D_i(x, y) = 0$ then either $D_j(x, y) = 0$ or $D_k(x, y) = 0$.

Monotone Feasible Interpolation

- [HP17] "Standard" feasible interpolation (in [K97] sense) can be deduced from this result.
- [FPPR17, HP17] Key idea enabling Cutting Planes lower bounds for random $\omega(1)$-CNFs.
- Using this idea, one can deduce monotone feasible interpolation results for many proof systems and related monotone circuit models. (*Proof of F size s $\Rightarrow$ Monotone circuit for* cert_F *of size* $s^{O(1)}$)
  - **Resolution $\Rightarrow$ Monotone Circuits** [HP17, prior result K97]
  - **Tree-Like Resolution $\Rightarrow$ Monotone Formulas** [Same as above]
  - **Cutting Planes $\Rightarrow$ Real Monotone Circuits** [HP17b, prior results K97, P97, BPR95]
  - **Nullstellensatz $\Rightarrow$ Monotone Span Programs** [Follows ideas of PR18, prior result PS96]
  - **Sherali-Adams $\Rightarrow$ Weak MLP Gate/Linear Separation Complexity** [FGGR21, prior H20]

Lifting Schema



Lifting Theorems

- **Query-to-communication lifting theorems** give the other direction
- $\mathcal{S} \subseteq \{0,1\}^n \times O$ is a query search problem, $g : X \times Y \to \{0,1\}^n$ is a gadget
- Define $\mathcal{S} \circ g \subseteq X^n \times Y^n \times O$ by $(\mathcal{S} \circ g)(x, y) = \mathcal{S}(g^n(x, y))$
  - Alice gets $x \in X^n$, Bob gets $y \in Y^n$, evaluate $z = g^n(x, y)$ and solve $\mathcal{S}(z)$
- If g "complex" then Alice and Bob's best strategy is to simulate the query strategy

Theorem. [RM 99, GPW 14]

Let $\mathcal{S} \subseteq \{0,1\}^n \times O$ be a search problem, let $\mathrm{Ind}_m : [m] \times \{0,1\}^m \to \{0,1\}$ by $\mathrm{Ind}_m(x, y) = y_x$. If $m = n^{O(1)}$ then

$$\mathrm{FP}^{cc}(\mathcal{S} \circ \mathrm{Ind}_m) = \Theta(\mathrm{FP}^{dt}(\mathcal{S}) \cdot \log m)$$

Lifting?

- By combining this together with the earlier reductions, we get the following theorem:

Theorem [GPW14]**.** Let F be an unsatisfiable CNF formula. There is a function g (*Index*) and a monotone boolean function $f_{F,g}$ such that

$$\mathrm{mF}(f_{F,g}) = 2^{\Omega(D_{\mathrm{Res}}(F)(\log|g|))}$$

- mF denotes **monotone formula size**

- Monotone circuit for $\mathrm{cert}_{F\circ g^n}$ of size $s \implies$ Proof of F with *degree* $O(\log s/\log |g|)$

- Many (*not all*) proof systems have well-defined notions of degree (*depth*, *width*, *polynomial degree*, etc.)

Lower Bounds?

- Is the function that we get from lifting interesting at all?
- Surprisingly, **yes!**
- $f_{F,g} = \text{cert}^{X,Y}_{F \circ g^n}$ depends on the **formula** F and **gadget** $g : X \times Y \to \{0,1\}$
  - **Number of input variables**: $N = O(|F||X|^{w(F)})$
- **Examples**:
  - $F = Ind_n$ then $f_{F,g}$ is **layered st-connectivity** $STCONN$
  - $F = Peb_G$ then $f_{F,g}$ is **generation** GEN
- Changing g modifies the instances of the function produced.

Proof Sketch

Theorem. [RM 99, GPW 14]

Let $\mathcal{S} \subseteq \{0,1\}^n \times O$ be a search problem, let $\mathrm{Ind}_m : [m] \times \{0,1\}^m \to \{0,1\}$ by $\mathrm{Ind}_m(x, y) = y_x$. If $m = n^{O(1)}$ then

$$\mathrm{FP}^{cc}(\mathcal{S} \circ \mathrm{Ind}_m) = \Theta(\mathrm{FP}^{dt}(\mathcal{S}) \cdot \log m)$$

- **Simulation Argument**
  - One direction (query implies communication) is easy.
  - Starting from a communication protocol for $\mathcal{S} \circ \mathrm{Ind}$ of complexity c, extract a query algorithm making $O(c/\log m)$ queries.
  - To do this, we **approximate** an arbitrary rectangle R into "structured" rectangles which are "approximately" of the form $\rho g^{n-d}(x, y)$ for some restriction

Proof ⇒ Circuit Lifting

Proof Complexity Size	Proof Complexity Degree	Circuit Complexity Measure	Gadget	Citation
Tree-Like Resolution Size	Resolution Depth	Monotone Formula Size	Index, Low-Discrepancy	[Folklore, RM99, GPW14, CKFMP19]
Resolution Size	Resolution Width	Monotone Circuit Size	Index	[GGKS17]
Nullstellensatz Monomial Size	Nullstellensatz Degree	Monotone Span Program Size	Any High Rank	[PR18, dRMNPR20]
Sherali-Adams Monomial Size	Sherali-Adams Degree	Linear Extension Complexity	Index, Inner Product*	[GLMW14, CLRS14, KMR17] (Incomplete)
Sums-of-Squares Monomial Size	SOS Degree	Semidefinite Extension Complexity	Index*	[LRS15] (Incomplete)

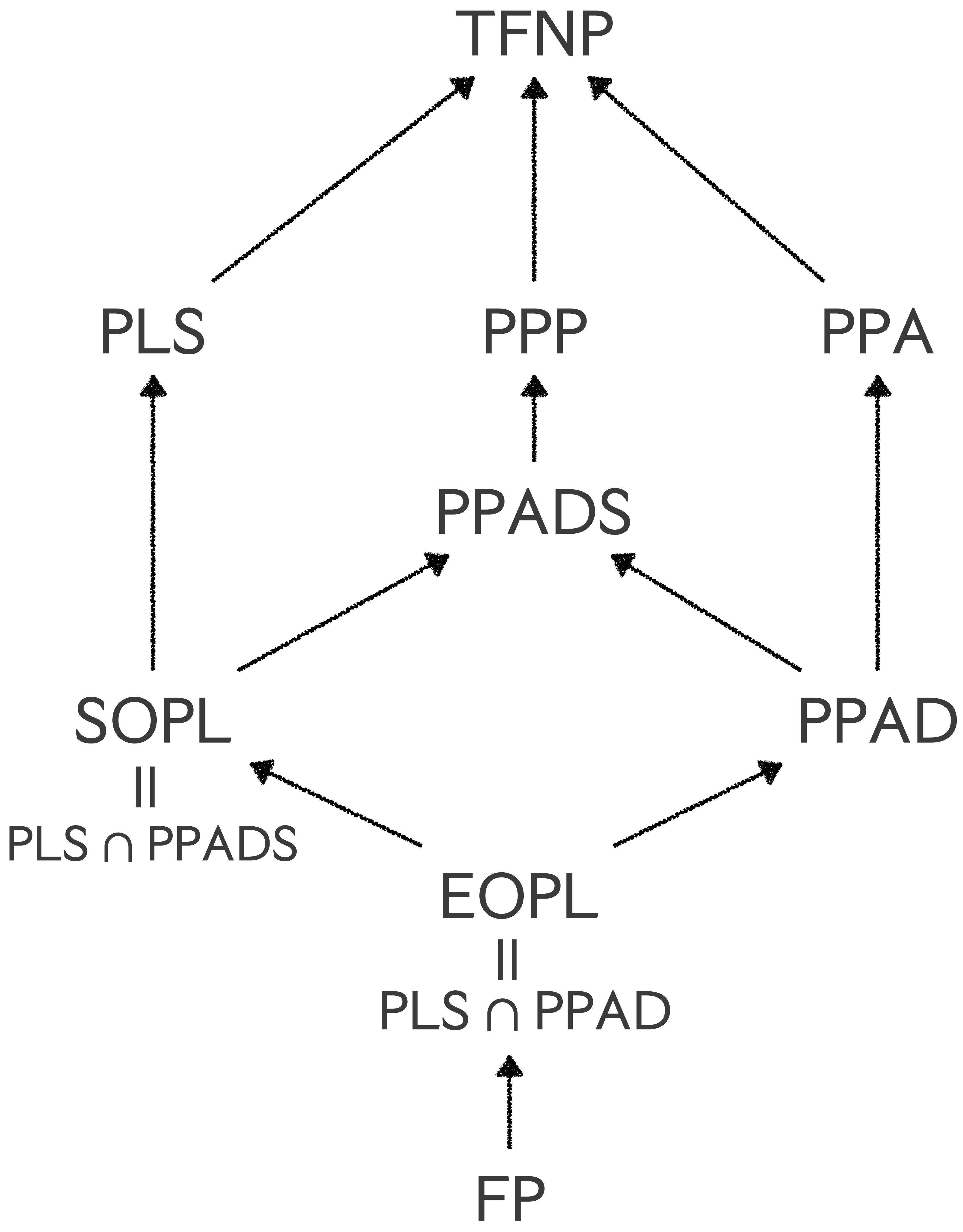
Part 3

TFNP

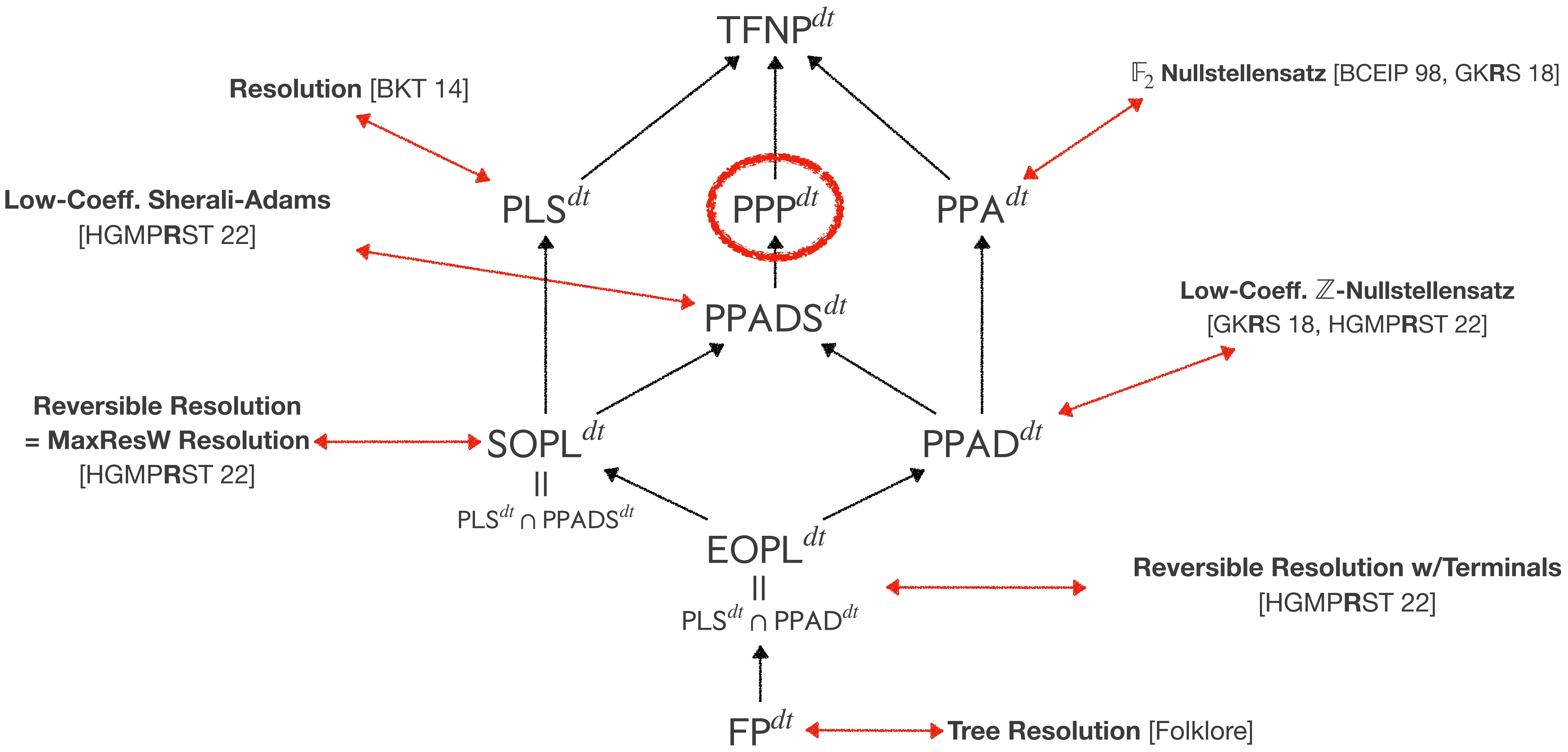
and

Future Directions

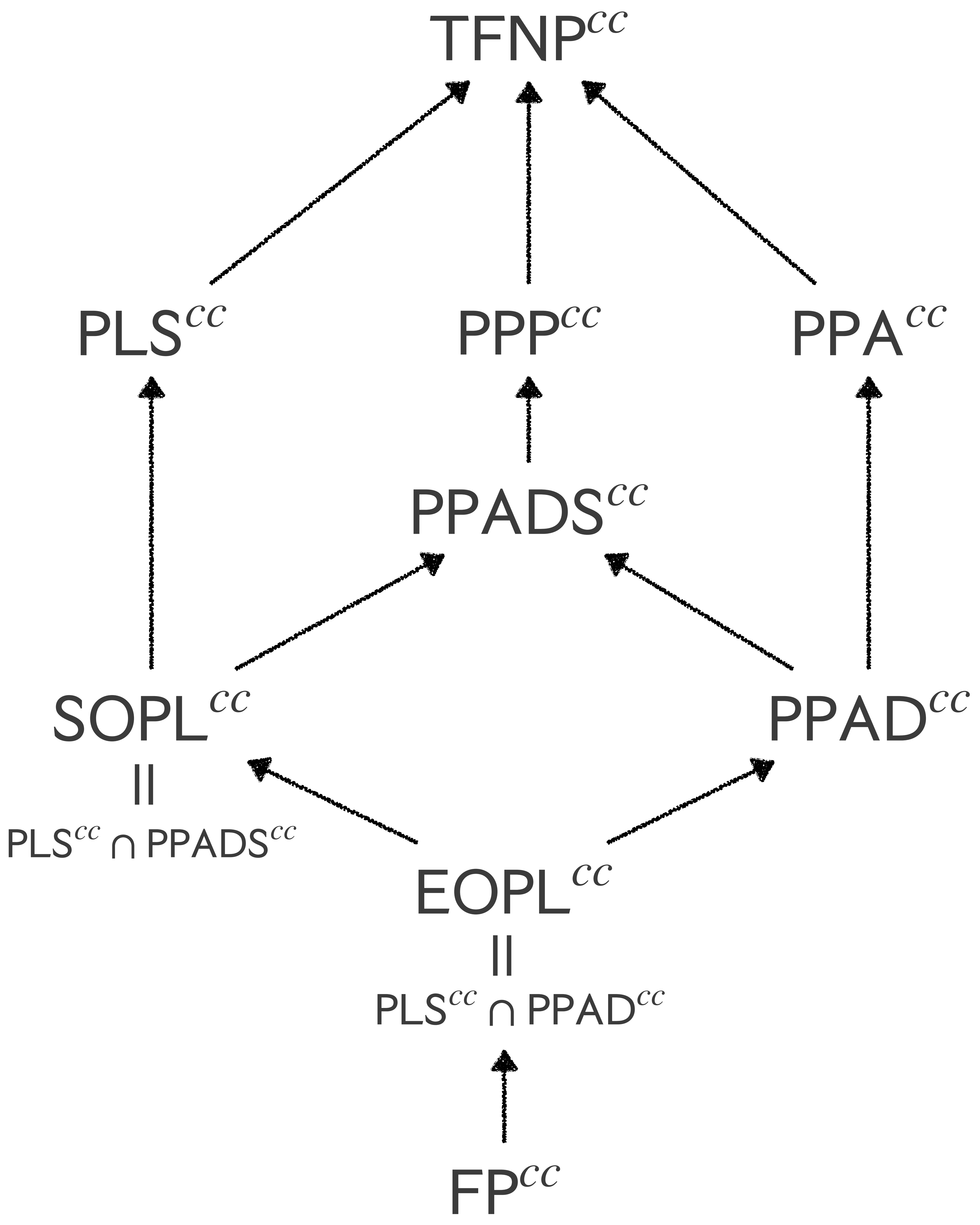
TFNP Classes



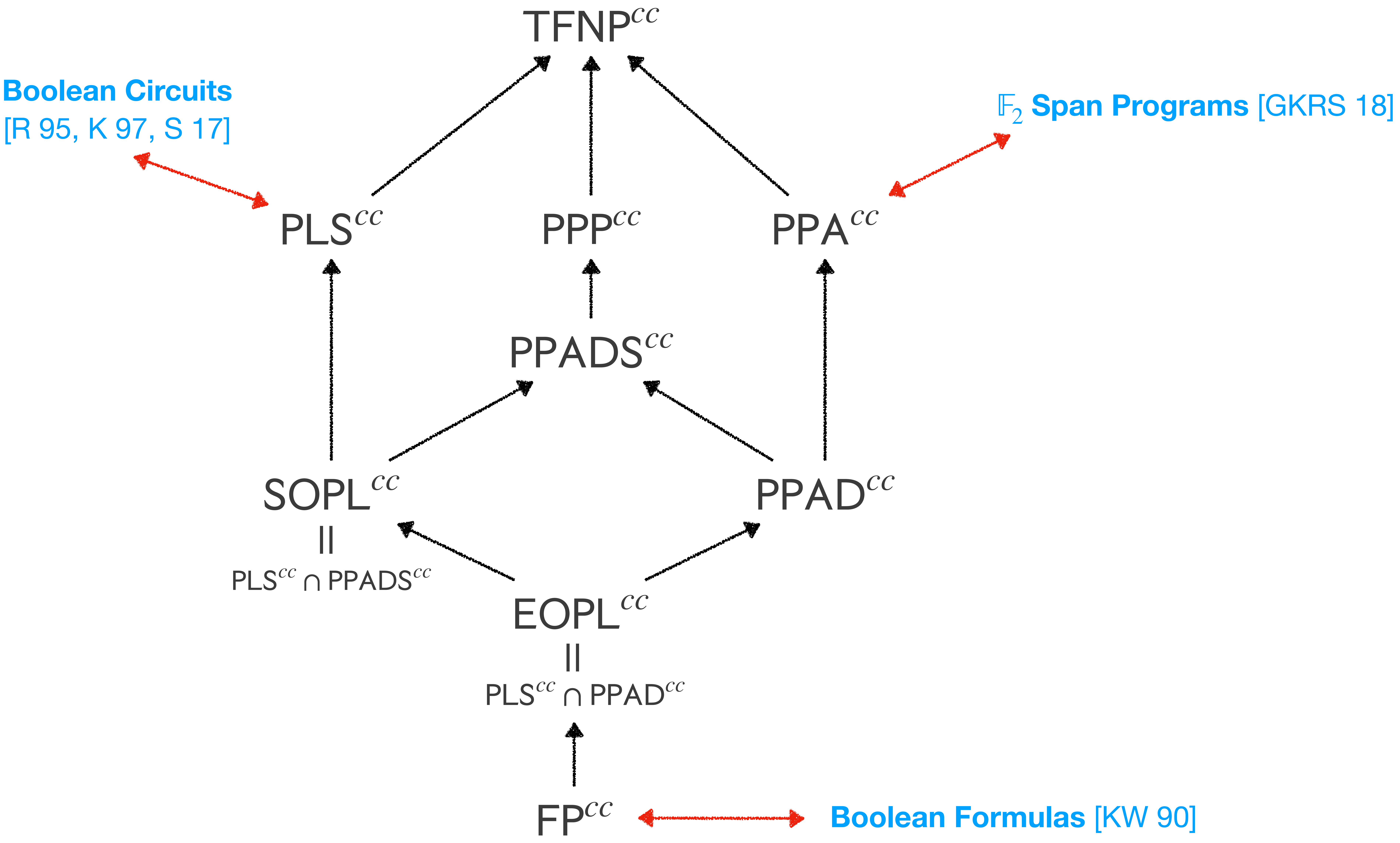
Query TFNP Classes



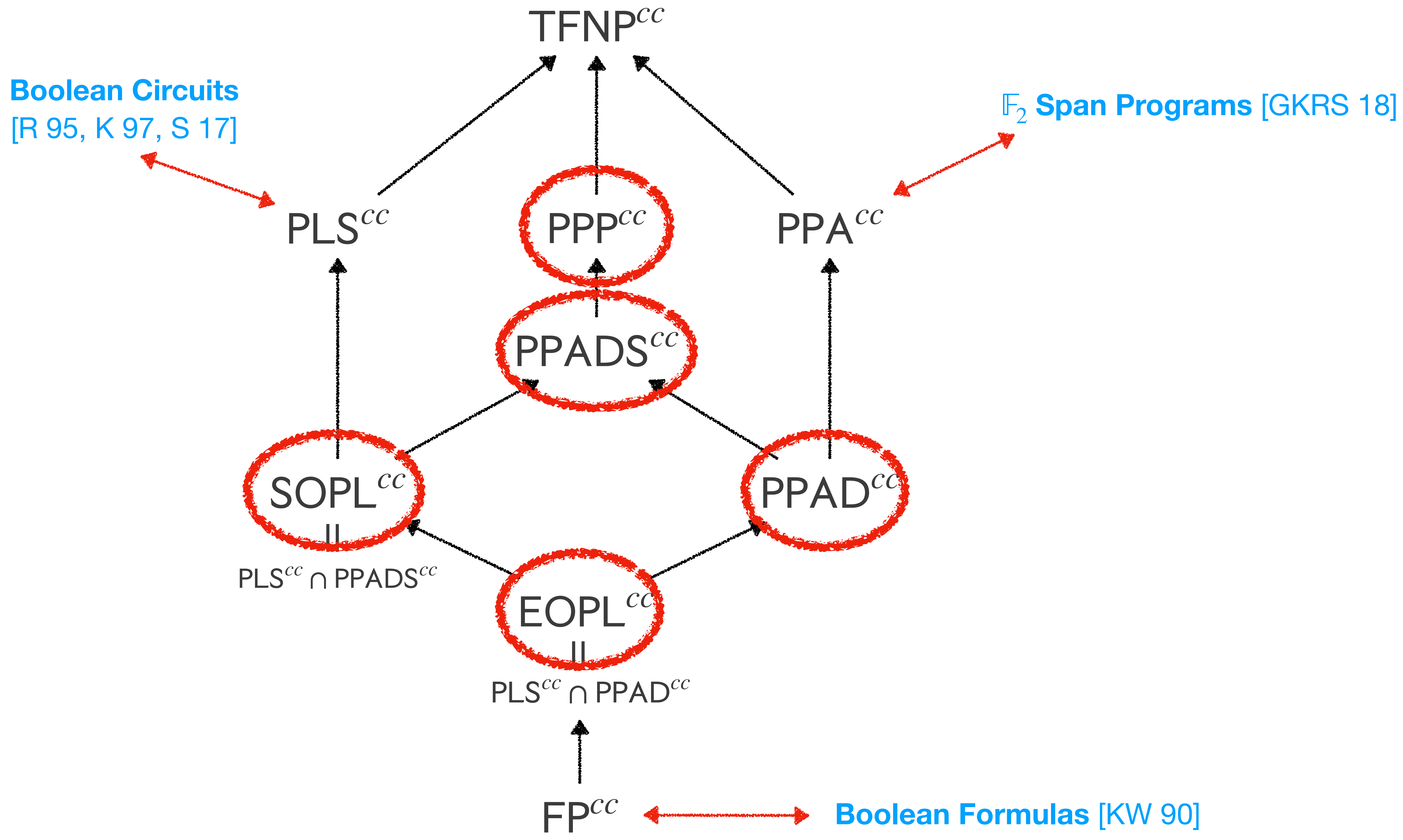
Communication TFNP

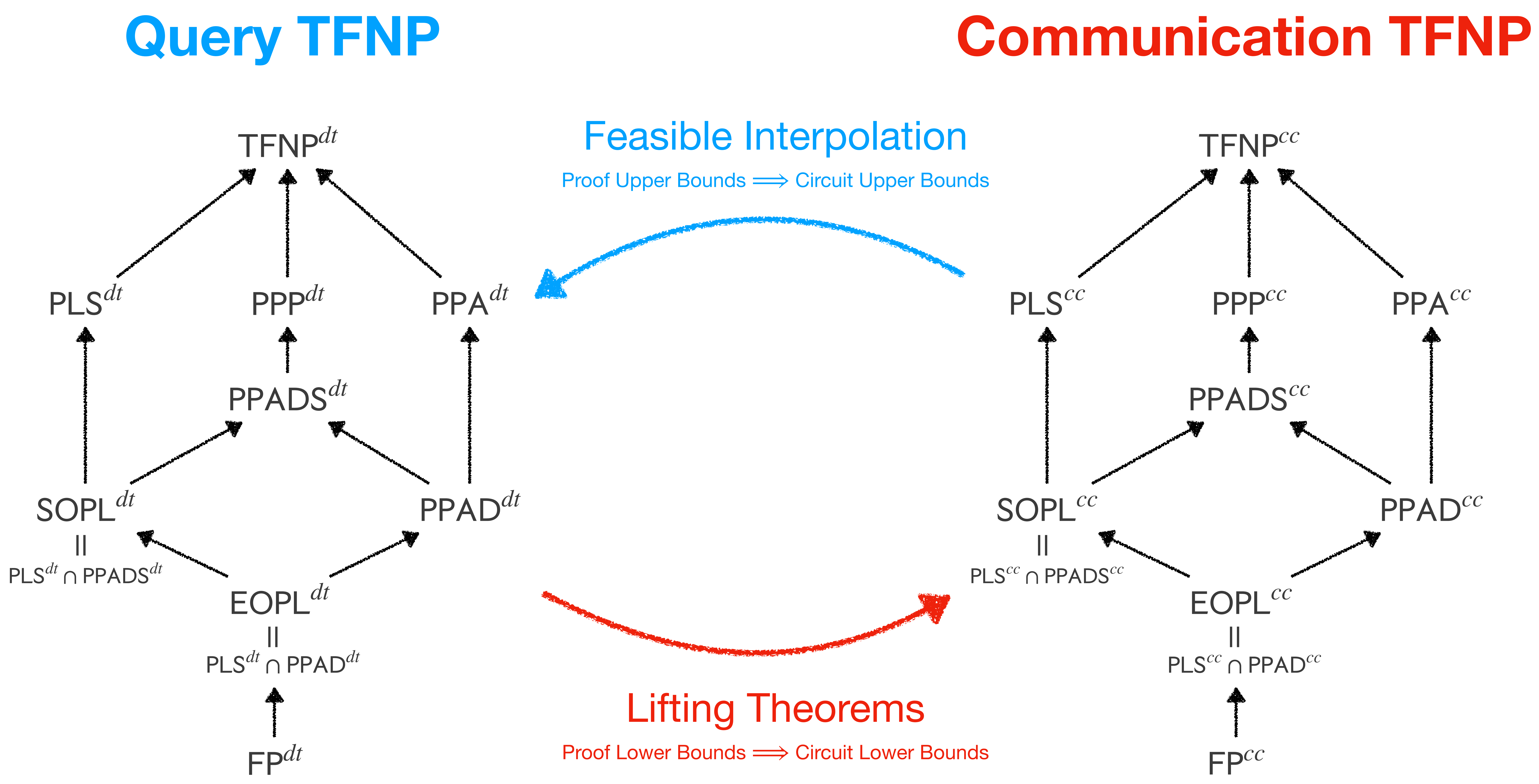


Communication TFNP



Communication TFNP





Query TFNP
Communication TFNP
TFNP^{dt}
PLS^{dt}
PPP^{dt}
PPA^{dt}
PPADS^{dt}
SOPL^{dt}
||
PLS^{dt} ∩ PPADS^{dt}
PPAD^{dt}
EOPL^{dt}
||
PLS^{dt} ∩ PPAD^{dt}
FP^{dt}
Feasible Interpolation
Proof Upper Bounds ⟹ Circuit Upper Bounds
Lifting Theorems
Proof Lower Bounds ⟹ Circuit Lower Bounds
TFNP^{cc}
PLS^{cc}
PPP^{cc}
PPA^{cc}
PPADS^{cc}
SOPL^{cc}
||
PLS^{cc} ∩ PPADS^{cc}
PPAD^{cc}
EOPL^{cc}
||
PLS^{cc} ∩ PPAD^{cc}
FP^{cc}

TFNP Program in Proof and Circuit Complexity

- All in all, this suggests a research program!
- Use TFNP classes to characterize circuit and proof classes.
- Relate these classes by **feasible interpolation** and **lifting theorems**
- Use intuition from one setting to prove results in the other setting.
  - **Many** TFNP classes are not characterized in either setting.
- Intersection theorems are particularly interesting!
  - Reversible Resolution = Resolution ∩ Sherali-Adams* [HGMPRST 22]

Other "Shapes"

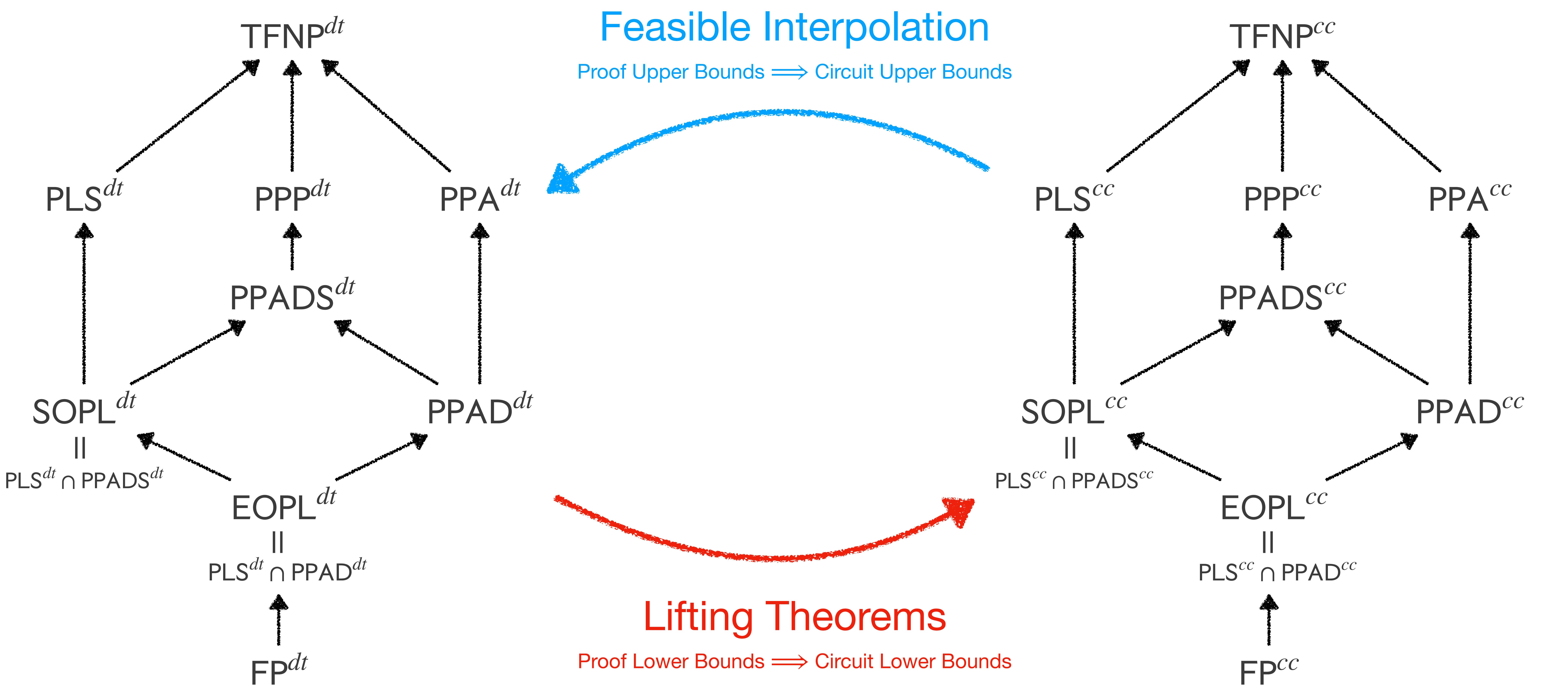
- The TFNP^{cc} classes capture communication reductions to proof systems, but this does not capture **all** proof systems.
- Prominent Example: **Cutting Planes**
  - Pudlak [Pud97], building on Krajicek [Kra97] proved a feasible interpolation theorem for Cutting Planes using **real monotone circuits**, used this to prove the first exponential size lower bounds
  - By lifting to **real communication protocols,** we can prove cutting planes lower bounds [Kra98, BEGJ00, dRNV16, HP18, GGKS20]
- Lifting theorem uses **triangles** instead of **rectangles**

Open Problems

- What TFNP problem captures Sums-of-Squares?
- Characterize the communication variants of other classical classes.
- What about Cutting Planes, Lovasz-Shrijver? (These are somehow different.)
- $\mathsf{Res}(\mathsf{CP})$? Or what about $\mathsf{Res}(\mathsf{Lin})$?
- What about NOF lifting theorems?
- Characterize more circuit and proof classes using TFNP classes.
- Can this approach (communication and query complexity) say anything novel about very powerful proof systems?
- What about non-monotone complexity? Can anything be said?

Query TFNP

Communication TFNP



Thanks for Listening!