Proof complexity and games

Pavel Pudlák[1]

Mathematical Institute, Academy of Sciences, Prague

Olomouc, June 21, 2017

[1]author supported by the ERC grant "FEALORA"

Based on results of Allan Skelley and Neil Thapen, *The Provably Total Search Problems of Bounded Arithmetic* and P.P. and Neil Thapen, *Parity Games and Propositional Proofs*

Standard finite games

Two players – P1, P2

DAG with one source, every node is assigned either to P1 or to P2

The assignment to terminal nodes determines whose winning position it is.

The graph is also called the protocol.

Standard finite games

Two players – P1, P2

DAG with one source, every node is assigned either to P1 or to P2

The assignment to terminal nodes determines whose winning position it is.

The graph is also called the protocol.

Theorem (Zermelo)

In every finite game either P1 or P2 has a winning strategy.

Boolean circuits as games

Let C be a Boolean circuit with gates $\vee, \wedge$ and literals $x_i, \bar{x}_i$ on input nodes.

- assign the gates $\vee$ to P1 and gates $\wedge$ to P2
- given a truth assignment $x_i \mapsto \alpha_i \in \{0, 1\}$, assign an input node to P1 if it gets value 1 and to P2 otherwise

Boolean circuits as games

Let C be a Boolean circuit with gates $\vee, \wedge$ and literals $x_i, \bar{x}_i$ on input nodes.

- assign the gates $\vee$ to P1 and gates $\wedge$ to P2
- given a truth assignment $x_i \mapsto \alpha_i \in \{0, 1\}$, assign an input node to P1 if it gets value 1 and to P2 otherwise

Fact

For (C, α), P1 has a winning strategy iff $C(\alpha) = 1$, and P2 has a winning strategy iff $C(\alpha) = 0$. Hence deciding who has a winning strategy is easy.

Boolean circuits as games

Let C be a Boolean circuit with gates $\vee, \wedge$ and literals $x_i, \bar{x}_i$ on input nodes.

- assign the gates $\vee$ to P1 and gates $\wedge$ to P2
- given a truth assignment $x_i \mapsto \alpha_i \in \{0,1\}$, assign an input node to P1 if it gets value 1 and to P2 otherwise

Fact
For (C, α), P1 has a winning strategy iff $C(\alpha) = 1$, and P2 has a winning strategy iff $C(\alpha) = 0$. Hence deciding who has a winning strategy is easy.

NB Formulas are also circuits, so this also holds for formulas in the basis $\vee, \wedge$.

How to make games more difficult

After playing a game G_1

$$a_1 a_2 a_3 \ldots a_m$$

they play another game $G_2[a_1 \ldots a_m]$ that depends on the moves in the first game.

A particular arrangement of the games

G_1 :	a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_{m-i}	$\ldots$	a_m
$G_2[\mathbf{a}]$:	b_m	b_{m-1}	$\ldots$	$\leftarrow$	$\ldots$	b_i	$\ldots$	b_1

The set of legal moves after b_i depends on b_i and a_{m-i}.

this can be repeated

G_1 :	a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
$G_2[\mathbf{a}]$:	b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
$G_3[\mathbf{a}, \mathbf{b}]$:	c_1	c_2	$\dots$	$\rightarrow$	$\dots$	c_{m-i}	$\dots$	c_m

and so on

Cooperative games and communication complexity

Two players want to achieve the same goal.

The complexity of the task is measured by

- the number of bits they need to communicate (communication complexity), or
- the number of steps (versions of communication complexity),
- etc.

Karchmer-Wigderson games

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, and

- P1 has $\alpha \in \{0,1\}^n$ such that $f(\alpha) = 1$,
- P2 has $\beta \in \{0,1\}^n$ such that $f(\beta) = 0$.

Goal: find an i such that $\alpha_i \neq \beta_i$.

Karchmer-Wigderson games

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, and

- P1 has $\alpha \in \{0,1\}^n$ such that $f(\alpha) = 1$,
- P2 has $\beta \in \{0,1\}^n$ such that $f(\beta) = 0$.

Goal: find an i such that $\alpha_i \neq \beta_i$.

Theorem (Karchmer-Wigderson)

The minimum depth of a circuit (formula) computing f is equal to the communication complexity of the game.

Karchmer-Wigderson games

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, and

- P1 has $\alpha \in \{0,1\}^n$ such that $f(\alpha) = 1$,
- P2 has $\beta \in \{0,1\}^n$ such that $f(\beta) = 0$.

Goal: find an i such that $\alpha_i \neq \beta_i$.

Theorem (Karchmer-Wigderson)

The minimum depth of a circuit (formula) computing f is equal to the communication complexity of the game.

Proof: ($\Leftarrow$) The circuit is essentially the protocol. ($\Rightarrow$) To get the circuit, remove superfluous parts of the protocol.

When enemies become friends, and vice versa

Let C be a circuit

1. given $\alpha \in \{0,1\}^n$
   - P1 has a strategy to reach a satisfied input literal iff $C(\alpha) = 1$,
   - P2 has a strategy to reach a falsified input literal iff $C(\alpha) = 0$
2. - P1 has $\alpha \in \{0,1\}^n$ such that $C(\alpha) = 1$, and
   - P2 has $\beta \in \{0,1\}^n$ such that $C(\beta) = 0$,

   then they have a strategy to find a literal p such that
   - $p[\alpha] = 1$,
   - $p[\beta] = 0$.

1. from adversarial to cooperative:
   - Both players have winning strategies, hence games must be different. Find the difference!
2. from cooperative to adversarial
   - One player is cheating, therefore must loose.

A symmetric calculus

Idea: A calculus for general formulas, yet it looks like Resolution.

A symmetric calculus

Idea: A calculus for general formulas, yet it looks like Resolution.

Our calculus is a streamlined and symmetric version of a calculus of Skelley and Thapen.

Language: $\vee, \wedge, \top, \bot$, literals $x_i, \bar{x}_i$, no negation, except in literals.
We will tacitly assume that $\vee, \wedge$ are associative and commutative, or equivalently that conjunctions and disjunctions are *multisets.*

[2] Recall that A does not contain negations.

Language: $\vee, \wedge, \top, \bot$, literals $x_i, \bar{x}_i$, no negation, except in literals. We will tacitly assume that $\vee, \wedge$ are associative and commutative, or equivalently that conjunctions and disjunctions are *multisets.*

A proof of $A \vdash B$ is a sequence of formulas $A = \Phi_1, \ldots, \Phi_m = B$ where Φ_{i+1} follows from Φ_i by an application of a deduction rule.

A proof of A is a proof of $\top \vdash A$.
A refutation of A is a proof of $A \vdash \bot$.

[2] Recall that A does not contain negations.

Language: $\vee, \wedge, \top, \bot$, literals $x_i, \bar{x}_i$, no negation, except in literals. We will tacitly assume that $\vee, \wedge$ are associative and commutative, or equivalently that conjunctions and disjunctions are *multisets.*

A proof of $A \vdash B$ is a sequence of formulas $A = \Phi_1, \dots, \Phi_m = B$ where Φ_{i+1} follows from Φ_i by an application of a deduction rule.

A proof of A is a proof of $\top \vdash A$.
A refutation of A is a proof of $A \vdash \bot$.

Deep inferences (of course!)

$$\frac{A[\dots B \dots]}{A[\dots C \dots]}$$

where $B \vdash C$ is a deduction rule. [2]

[2] Recall that A does not contain negations.

Deduction rules:

contraction/expansion

$$\frac{A \vee A}{A} \qquad \frac{A}{A \wedge A}$$

weakenings

$$\frac{A}{A \vee B} \qquad \frac{A \wedge B}{A}$$

truth constants

$$\frac{A \vee \bot}{A} \qquad \frac{A}{A \wedge \top}$$

Deduction rules:

contraction/expansion

$$\frac{A \vee A}{A} \qquad \frac{A}{A \wedge A}$$

weakenings

$$\frac{A}{A \vee B} \qquad \frac{A \wedge B}{A}$$

truth constants

$$\frac{A \vee \bot}{A} \qquad \frac{A}{A \wedge \top}$$

resolution/dual resolution

$$\frac{(A \vee p) \wedge (B \vee \bar{p})}{A \vee B} \qquad \frac{A \wedge B}{(A \wedge p) \vee (B \wedge \bar{p})}$$

E.G.

$$\frac{\dfrac{(A \wedge (B \vee p)) \wedge C}{(A \wedge (B \vee p) \wedge \bar{p}) \vee (p \wedge C)}}{(A \wedge B) \vee (p \wedge C)}$$

Padding

We are interested in proofs of bounded depth, i.e., where each formula has at most k alternation of $\vee$ and $\wedge$ for some constant k.

To this end we allow one element disjunctions and conjunctions. In particular, literals can be interpreted as formulas of any given depth.

Interpreting proofs as games I.

Let

$$A = \Phi_1, \dots, \Phi_m = B$$

be a proof. Suppose, for example, that

$$\Phi_i = \bigvee_j \bigwedge_k \bigvee_l p_{ijkl}$$

where p_{ijkl} are literals.

P1 conjunctions:	a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
P2 disjunctions:	b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1

$a_i = \bigwedge_k \bigvee_l p_{ij_i kl}$
$b_i = \bigvee_l p_{ij_i k_i l}$

Finally, P1 picks $p_{1 j_1 k_1 l_1}$.

$A \vdash B$ by a proof $A = \Phi_1, \ldots, \Phi_m = B$, $\Phi_i = \bigvee_j \bigwedge_k \bigvee_l p_{ijkl}$

P1 conjunctions:	a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_{m-i}	$\ldots$	a_m
P2 disjunctions:	b_m	b_{m-1}	$\ldots$	$\leftarrow$	$\ldots$	b_i	$\ldots$	b_1

Furthermore, truth assignment $\alpha \in \{0,1\}^n$ is given.

$A \vdash B$ by a proof $A = \Phi_1, \ldots, \Phi_m = B$, $\Phi_i = \bigvee_j \bigwedge_k \bigvee_l p_{ijkl}$

P1 conjunctions:	a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_{m-i}	$\ldots$	a_m
P2 disjunctions:	b_m	b_{m-1}	$\ldots$	$\leftarrow$	$\ldots$	b_i	$\ldots$	b_1

Furthermore, truth assignment $\alpha \in \{0,1\}^n$ is given.

The goals of the players:

P1 claims $A[\alpha] = 1$.
P2 claims $B[\alpha] = 0$.

P1 looses if $p[\alpha] = 0$ for a literal that he claims to be true.
P2 looses if $p[\alpha] = 1$ for a literal that he claims to be false.

Actions of players

Let $\Phi_i \vdash \Phi_{i+1}$ by dual resolution.

$\Phi_i = \cdots \vee (C \wedge D) \vee \ldots$ and P1 played $C \wedge D$.
$\Phi_{i+1} = \cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$.

Then P1 must play

- $C \wedge p$, if p is true, or
- $C \wedge \bar{p}$, if $\bar{p}$ is true.

Actions of players

Let $\Phi_i \vdash \Phi_{i+1}$ by dual resolution.

$\Phi_i = \cdots \vee (C \wedge D) \vee \ldots$ and P1 played $C \wedge D$.
$\Phi_{i+1} = \cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$.

Then P1 must play

- $C \wedge p$, if p is true, or
- $C \wedge \bar{p}$, if $\bar{p}$ is true.

For the other rules, the action is also uniquely determined (in fact, without using the assignment).

Actions of players

Let $\Phi_i \vdash \Phi_{i+1}$ by dual resolution.

$\Phi_i = \cdots \vee (C \wedge D) \vee \ldots$ and P1 played $C \wedge D$.
$\Phi_{i+1} = \cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$.

Then P1 must play

- $C \wedge p$, if p is true, or
- $C \wedge \bar{p}$, if $\bar{p}$ is true.

For the other rules, the action is also uniquely determined (in fact, without using the assignment).

The actions of P2 are dual.

E.G.

$$\cdots \vee (C \wedge D) \vee \ldots$$

$$\cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$$

$$\vdots$$

$$\cdots \vee (p \wedge (q \vee \bar{p})) \vee \ldots$$

$$\cdots \vee q \vee \ldots$$

E.G.

$$\cdots \vee (C \wedge D) \vee \ldots$$

$$\cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$$

$$\vdots$$

$$\cdots \vee (p \wedge (q \vee \bar{p})) \vee \ldots$$

$$\cdots \vee q \vee \ldots$$

E.G.

$$\cdots \vee (C \wedge D) \vee \ldots$$

$$\cdots \vee (C \wedge p) \vee (D \wedge \bar{p}) \vee \ldots$$

$$\vdots$$

$$\cdots \vee (p \wedge (q \vee \bar{p})) \vee \ldots$$

$$\cdots \vee q \vee \ldots$$

Interpreting proofs as games II.

Karchmer-Wigderson type game

Interpreting proofs as games II.

Karchmer-Wigderson type game

P1 has α such that $A[\alpha] = 1$.
P2 has β such that $B[\beta] = 0$.

Goal: find a literal p such that $p[\alpha] = 1$ and $p[\beta] = 0$.

Interpreting proofs as games II.

Karchmer-Wigderson type game

P1 has α such that $A[\alpha] = 1$.
P2 has β such that $B[\beta] = 0$.

Goal: find a literal p such that $p[\alpha] = 1$ and $p[\beta] = 0$.

The players follow the schedule

P1:	a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
P2:	b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
etc.	$\dots$							

Interpreting proofs as games II.

Karchmer-Wigderson type game

P1 has α such that $A[\alpha] = 1$.
P2 has β such that $B[\beta] = 0$.

Goal: find a literal p such that $p[\alpha] = 1$ and $p[\beta] = 0$.

The players follow the schedule

P1:	a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
P2:	b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
etc.	$\dots$							

The literal p can be found

- either at the ends Φ_1, Φ_m,
- or at some application of resolution or dual resolution

Interpreting proofs as games III.

Fact

Suppose $var(A) \cap var(B) = \emptyset$ and $A \vdash B$. Then

1. *either $A \vdash \bot \vdash B$, i.e., A is unsatisfiable,*
2. *or $A \vdash \top \vdash B$, i.e., B is a tautology.*

We want to "decide" which is true by means of a game.

[3] w.r.t. polynomial time reductions

Interpreting proofs as games III.

Fact

Suppose $var(A) \cap var(B) = \emptyset$ and $A \vdash B$. Then

1. *either $A \vdash \bot \vdash B$, i.e., A is unsatisfiable,*
2. *or $A \vdash \top \vdash B$, i.e., B is a tautology.*

We want to "decide" which is true by means of a game.

We now assign P1 to variables of A, and P2 to variables of B.
Thus they have to alternate in the rows.

[3] w.r.t. polynomial time reductions

Interpreting proofs as games III.

Fact

Suppose $var(A) \cap var(B) = \emptyset$ *and* $A \vdash B$. *Then*

1. *either* $A \vdash \bot \vdash B$, *i.e.,* A *is unsatisfiable,*
2. *or* $A \vdash \top \vdash B$, *i.e.,* B *is a tautology.*

We want to "decide" which is true by means of a game.

We now assign P1 to variables of A, and P2 to variables of B.
Thus they have to alternate in the rows.

Conjecture (stated very informally)

The problem of deciding 1. or 2. is equivalent[3] *to the existence of certain winning strategies in a suitable game.*

[3] w.r.t. polynomial time reductions

Interlude—so what?

Question: *Why are we trying to characterize provability of sentences of certain complexity in certain systems by combinatorial principles?*

Interlude—so what?

Question: *Why are we trying to characterize provability of sentences of certain complexity in certain systems by combinatorial principles?*

Answer 1. Look at Peano Arithmetic.

Problem

Find a combinatorial interpretation of the sentence $Con(PA)$.

Interlude—so what?

Question: *Why are we trying to characterize provability of sentences of certain complexity in certain systems by combinatorial principles?*

Answer 1. Look at Peano Arithmetic.

Problem

Find a combinatorial interpretation of the sentence $Con(PA)$.

Theorem (Paris-Harrington)

The Σ_1-reflection principle for PA is equivalent to the PH sentence.

Answer 2. Look at computational complexity.

Complexity classes are often characterized by (many) concrete computational problems.

The corresponding concepts in proof complexity are first order theories/proof systems and mathematical/combinatorial principles.

Answer 2. Look at computational complexity.

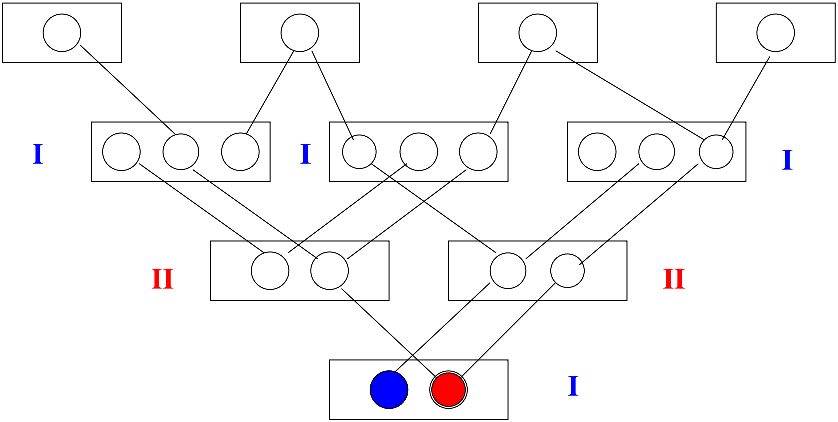
Complexity classes are often characterized by (many) concrete computational problems.

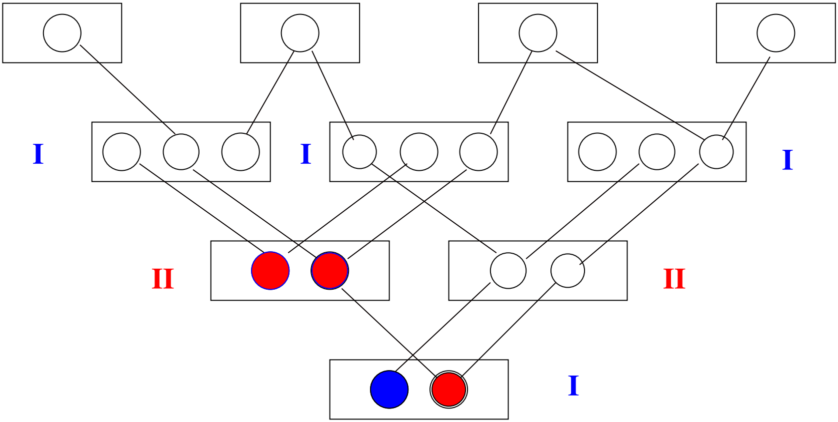
The corresponding concepts in proof complexity are first order theories/proof systems and mathematical/combinatorial principles.

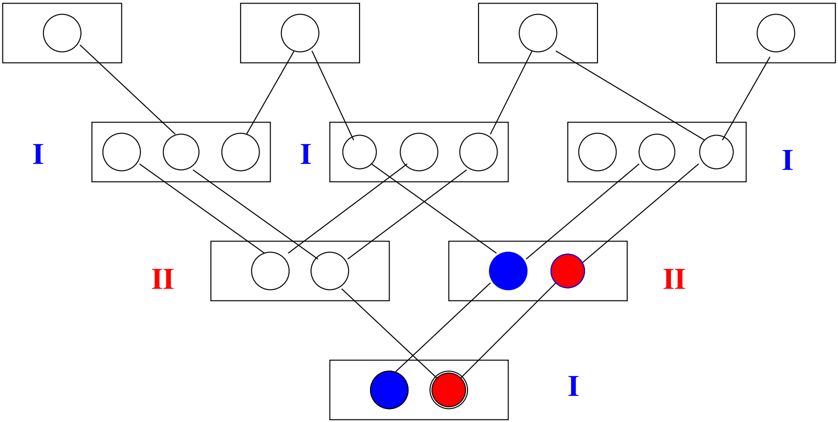
Answer 3. Because we want to prove, or to argue that they are not provable in weaker systems.

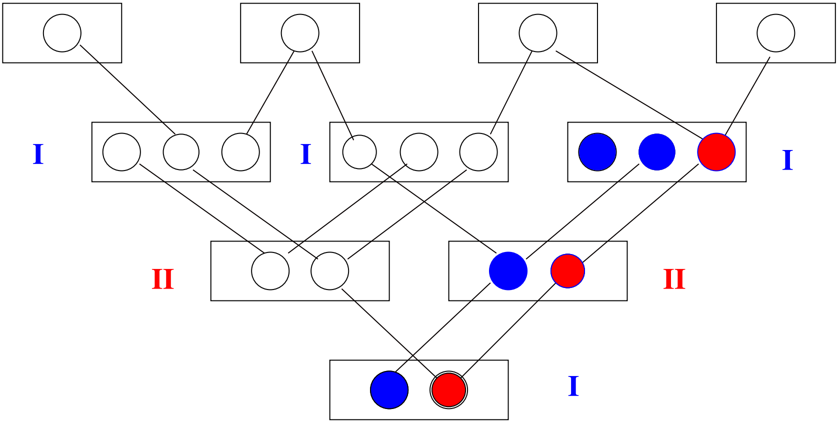
The Point-Line Game

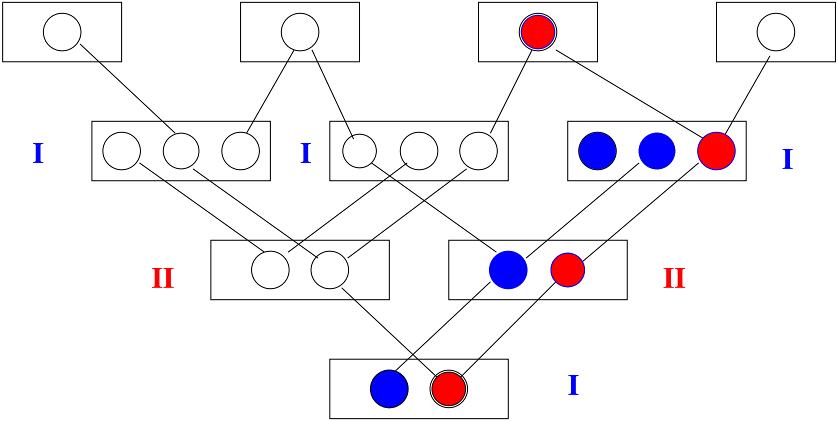
a game for depth 2 Frege proofs

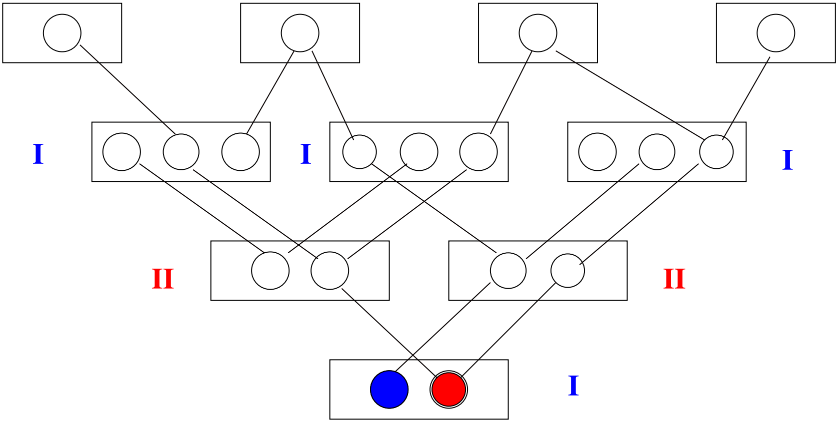

I
I
I
II
II
I

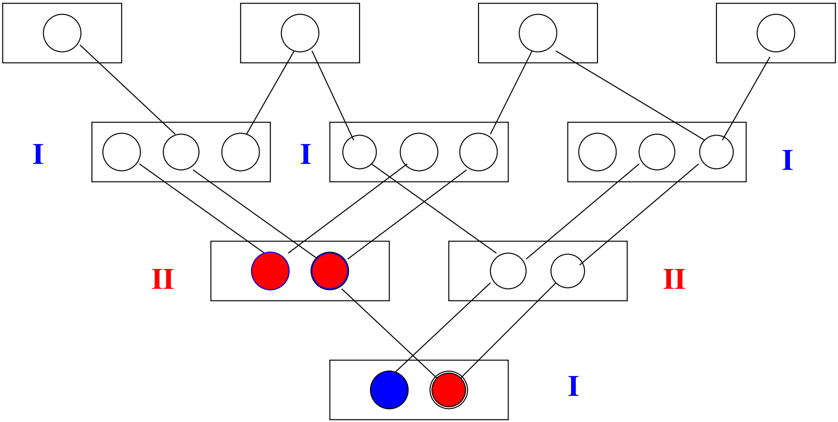

I
I
I
II
II
I

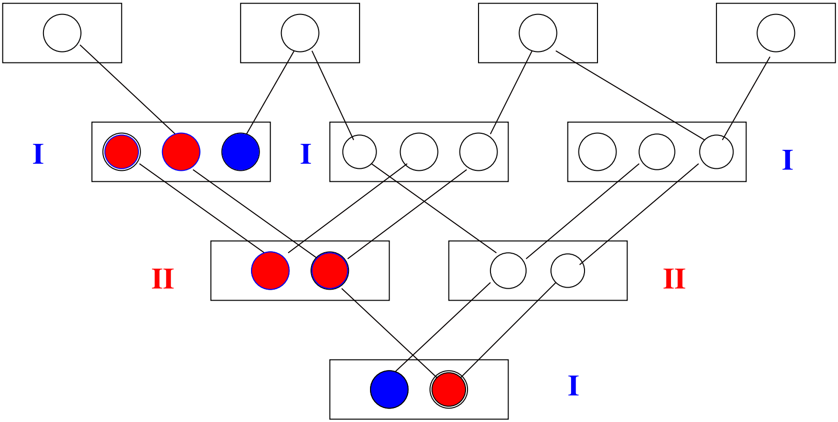

I
I
I
II
II
I


I
I
I
II
II
I

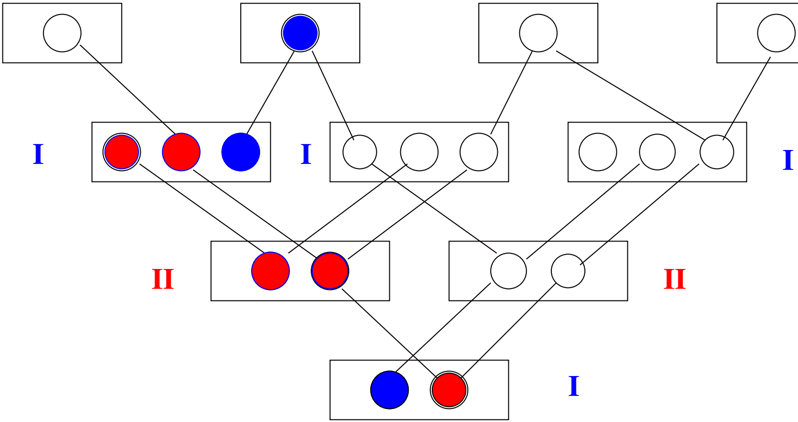

I
I
I
II
II
I


I
I
I
II
II
I


I
I
I
II
II
I



I
I
I
II
II
I


I
I
I
II
II
I

A positional strategy for P1 (P2) is an assignment to his nodes, i.e., a strategy that does not depend on the paths to the nodes.

Whether or not a positional strategy is a winning can be decided in polynomial time.

It is possible that none of the players has a positional winning strategy.

A positional strategy for P1 (P2) is an assignment to his nodes, i.e., a strategy that does not depend on the paths to the nodes.

Whether or not a positional strategy is a winning can be decided in polynomial time.

It is possible that none of the players has a positional winning strategy.

The game can be presented in the form

a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_{m-i}	$\ldots$	a_m
b_m	b_{m-1}	$\ldots$	$\leftarrow$	$\ldots$	b_i	$\ldots$	b_1

where players alternate in the first game and the second game is trivial—*End of the Line*.

Proof search for Resolution

Theorem (Arnold Beckmann, P.P. and Neil Thapen)

The following two problems are polynomially reducible to each other:

1. *Given a CNF formula Φ decide if*
   - *it is satisfiable, or*
   - *it has a resolution refutation of size $|\Phi|^2$,*

   (provided that one of the two is true).
2. *Given a point-line game decide if*
   - *P1 has a positional winning strategy, or*
   - *P1 has a positional winning strategy,*

   (provided that one of the two is true).

Combinatorial games

Theorem (Arnold Beckmann, P.P. and Neil Thapen)

The problem of deciding who has a winning strategy for parity games is reducible to the problem of deciding who has a positional winning strategy in point-line games.

Combinatorial games

Theorem (Arnold Beckmann, P.P. and Neil Thapen)

The problem of deciding who has a winning strategy for parity games is reducible to the problem of deciding who has a positional winning strategy in point-line games.

Proof is based on formalizing parity games in a fragment of bounded arithmetic and translating the proof into depth 2 Frege proofs.

Combinatorial games

Theorem (Arnold Beckmann, P.P. and Neil Thapen)

The problem of deciding who has a winning strategy for parity games is reducible to the problem of deciding who has a positional winning strategy in point-line games.

Proof is based on formalizing parity games in a fragment of bounded arithmetic and translating the proof into depth 2 Frege proofs.

We also formalized simple stochastic games in a theory that gives depth 3 Frege systems.

Thank You