Logic and Complexity

Pavel Pudlák[1]

Mathematical Institute, Czech Academy of Sciences, Prague

St. Petersburg, May 2018

[1] author supported by the ERC advanced grant “FEALORA”

Overview

1. Reflection principles and canonical **NP**-pairs
2. Why we are interested in canonical **NP**-pairs
3. Games for bounded depth Frege systems
4. A proof system
5. Games from proofs

Reflection principles and canonical **NP**-pairs

Reflection principle for T

$$Pr_T(\phi) \to \phi.$$

Equivalently, the following sets are disjoint:

$$\{\phi \mid Pr_T(\phi)\} \text{ and } \{\phi \mid Sat(\neg\phi)\}.$$

Definition (Cook)

1. Let Σ be a finite alphabet and *Taut* a set of tautologies. A function F is called a proof system if

1. F is polynomial time computable,
2. $F : \Sigma^* \rightarrow \mathit{Taut}$ (soundness),
3. F is onto *Taut* (completeness).

Definition (Cook)

1. Let Σ be a finite alphabet and *Taut* a set of tautologies. A function F is called a proof system if

  1. F is polynomial time computable,
  2. $F : \Sigma^* \to \mathit{Taut}$ (soundness),
  3. F is onto *Taut* (completeness).

2. A proof system F_2 polynomially simulates a proof system F_1, if there exists a polynomial time computable function g such that

$$F_1(w) = F_2(g(w)).$$

$w \in \Sigma^*$ is a P-proof of the tautology $F(w)$.

Frege systems are systems based on axiom schemas and rules.

depth d Frege system is a Frege system in the de Morgan basis in which only formulas of depth d (number of alternations of $\wedge, \vee$) are allowed.

In this talk: Resolution will be depth 1 Frege system.

Definition (Razborov)

The canonical disjoint **NP** *pair* of the proof system P is the pair of sets

$$\{(\phi, 0^n) \mid \exists w,\ w \text{ is a } P\text{-proof of } \phi \text{ of length} \leq n\},$$

$$\{(\phi, 0^n) \mid \ \neg\phi \text{ is satisfiable}\}.$$

Here 0^n denotes padding that ensures that the sets are in **NP**.

4 reasons for studying canonical pairs

(1) The canonical pair (A, B) of a proof system P gives us a computational complexity problem:

> *How difficult is it to decide whether ϕ is in A or in B, provided that it is in one the sets?*

Definition

Let $A, B \in \mathbf{NP}$ be disjoint. (A, B) is reducible to (C, D) if there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.

Definition

Let $A, B \in \mathbf{NP}$ be disjoint. (A, B) is reducible to (C, D) if there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.

Conjectures

- There exists a disjoint **NP** pair that is not separable by a set in **P**. (True if $P \neq \mathbf{NP} \cap \mathbf{coNP}$.)
- There is no complete disjoint **NP** pair.

Proposition

Let (A, B) be the canonical pair of a proof system P and (C, D) be the canonical pair of Q. If a proof system Q polynomially simulates P, then (A, B) is polynomially reducible to (C, D).

(2) Proof search

Question. Let P be a proof system. Let a tautology ϕ and a number n be given. Is it possible to find a P proof of length n in polynomial time in n and $|\phi|$?

(2) Proof search

Question. Let P be a proof system. Let a tautology ϕ and a number n be given. Is it possible to find a P proof of length n in polynomial time in n and $|\phi|$?

If it is, then the canonical pair of P can be separated by a set in **P**.

(2) Proof search

Question. Let P be a proof system. Let a tautology ϕ and a number n be given. Is it possible to find a P proof of length n in polynomial time in n and $|\phi|$?

If it is, then the canonical pair of P can be separated by a set in **P**.

No nontrivial proof system is known for which proof search is in **P**.

(3) Feasible interpolation.

[2] i.e., by polynomial size Boolean circuits

(3) Feasible interpolation.

Let ϕ and ψ have disjoint sets of propositional variables. By Craig's Interpolation Theorem, if $\vdash \phi \to \psi$, then

$$\phi \to \bot \to \psi \quad \text{or} \quad \phi \to \top \to \psi.$$

Problem. Given a proof *w* of $\vdash \phi \to \psi$, decide which of the two $\bot, \top$ is an interpolant.

Definition (Krajíček)

A proof system *P* has *feasible interpolation property* if the problem above is decidable in nonuniform polynomial time.[2]

[2] i.e., by polynomial size Boolean circuits

Feasible interpolation is used to prove lower bounds on some (weak) proof systems.

For proof systems P stronger than resolution, the question whether P has feasible interpolation is often equivalent to separation of the canonical pair by a set in **P**.

Feasible interpolation is used to prove lower bounds on some (weak) proof systems.

For proof systems P stronger than resolution, the question whether P has feasible interpolation is often equivalent to separation of the canonical pair by a set in $\mathbf{P}$.

Question: Which proof systems have the feasible interpolation property?

(4) Combinatorial games.

For some games, e.g., *parity games, simple stochastic games, mean payoff games*, one can define *positional strategies* and prove that if a player has a winning strategy, then it has a winning positional strategy.

(4) Combinatorial games.

For some games, e.g., *parity games, simple stochastic games, mean payoff games,* one can define *positional strategies* and prove that if a player has a winning strategy, then it has a winning positional strategy.

A positional strategy has a feasible description, i.e., description of polynomial size that can be checked in polynomial time. Hence,

- the condition that a player has a winning strategy is in **NP**,
- only one player can have a winning strategy.

(4) Combinatorial games.

For some games, e.g., *parity games, simple stochastic games, mean payoff games,* one can define *positional strategies* and prove that if a player has a winning strategy, then it has a winning positional strategy.

A positional strategy has a feasible description, i.e., description of polynomial size that can be checked in polynomial time. Hence,

- the condition that a player has a winning strategy is in **NP**,
- only one player can have a winning strategy.

Thus we also have disjoint **NP** pairs (in fact, sets in $\mathbf{NP} \cap \mathbf{coNP}$ for (some) combinatorial games.

It is possible to polynomially reduce the **NP** pair to the canonical pair of a proof system by proving its disjointness in the proof system.
For example:

Theorem

1. *The pair of the Parity Game is polynomially reducible to the canonical pair of Resolution, [Beckmann,P.,Thapen 2014].*
2. *The pair of the Simple Stochastic Game is polynomially reducible to the canonical pair of depth-2 Frege, [Atserias,Maneva 2004,Huang,Pitassi 2011,BPT 2014].*

It is possible to polynomially reduce the **NP** pair to the canonical pair of a proof system by proving its disjointness in the proof system.
For example:

Theorem

1. *The pair of the Parity Game is polynomially reducible to the canonical pair of Resolution, [Beckmann,P.,Thapen 2014].*
2. *The pair of the Simple Stochastic Game is polynomially reducible to the canonical pair of depth-2 Frege, [Atserias,Maneva 2004,Huang,Pitassi 2011,BPT 2014].*

Since in the two combinatorial games the existence of winning strategies is equivalent to the existence of winning *positional* strategies, this means that the decision problem of which player has a winning strategy is reduced to the canonical pairs.

Games for bounded depth Frege systems

We want to characterize the canonical pairs of bounded depth Frege systems by positional strategies in certain games.

[3] depth 1 is Resolution, etc.

Games for bounded depth Frege systems

We want to characterize the canonical pairs of bounded depth Frege systems by positional strategies in certain games.

We define 2-player games parametrized by numbers d, called *rounds*, and *positional winning strategies.*

Theorem

For $d \geq 1$,[3] the canonical pairs of the depth d Frege system is polynomially equivalent to the pair (A^1_{d+1}, A^2_{d+1}), where

$$A^i_d := \{G \mid G \textit{ is a } d\textit{-round game in which } \textit{Player } i \textit{ has a positional winning strategy}\}.$$

[3] depth 1 is Resolution, etc.

Corollary

1. *The pair of the Parity Game is polynomially reducible to the pair of depth 2 game.*
2. *The pair of the Simple Stochastic Game is polynomially reducible to the depth 3 game.*

The game

Players alternate and fill in a $d \times m$ square grid with symbols from an alphabet A in a zig-zag way. We will assume that the size of A is polynomial in m.

E.g., $d = 3$

a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
c_1	c_2	$\dots$	$\rightarrow$	$\dots$	c_{m-i}	$\dots$	c_m

The game

Players alternate and fill in a $d \times m$ square grid with symbols from an alphabet A in a zig-zag way. We will assume that the size of A is polynomial in m.

E.g., $d = 3$

a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
c_1	c_2	$\dots$	$\rightarrow$	$\dots$	c_{m-i}	$\dots$	c_m

What is a legal move depends only on the entries in the previous column.

The game

Players alternate and fill in a $d \times m$ square grid with symbols from an alphabet A in a zig-zag way. We will assume that the size of A is polynomial in m.

E.g., $d = 3$

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
c_1	c_2	$\ldots$	$\rightarrow$	$\ldots$	c_{m-i}	$\ldots$	c_m

What is a legal move depends only on the entries in the previous column.

What is a winning situation for Player 1, or 2 depends only on the entries in the current column.

a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_i	?	

a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
			$\leftarrow$	?	b_i	$\dots$	b_1

a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m
b_m	b_{m-1}	$\dots$	$\leftarrow$	$\dots$	b_i	$\dots$	b_1
c_1	c_2	$\dots$	$\rightarrow$	$\dots$	c_{m-i}	?	

Positional strategies

Definition

A position is a partially filled column.

Positional strategies

Definition

A position is a partially filled column.

In particular, we can talk about winning/loosing positions.

A positional strategy is a strategy in which the next move only depends on the entries in the previous column.

List of legal moves and positional strategies are objects of size polynomial in the size of the game.

Proposition

Given a positional strategy, it is possible to decide in polynomial time if it is a winning strategy for the given player.

List of legal moves and positional strategies are objects of size polynomial in the size of the game.

Proposition

Given a positional strategy, it is possible to decide in polynomial time if it is a winning strategy for the given player.

Proof-idea:
1. Given a strategy σ, inductively define positions that are reachable when the player plays σ.
2. Check that there is no loosing position for the player among them.

□

special cases: $d = 1$ and 2

$\mathbf{d = 1}$

a_1	a_2	$\ldots$	$\rightarrow$	$\ldots$	a_{m-i}	$\ldots$	a_m

We can decide who has a winning strategy by "dynamic programming" - computing the set of winning positions starting from the last square and going back to the first.

special cases: $d = 1$ and 2

d = 1

a_1	a_2	$\dots$	$\rightarrow$	$\dots$	a_{m-i}	$\dots$	a_m

We can decide who has a winning strategy by "dynamic programming" - computing the set of winning positions starting from the last square and going back to the first.

d = 2

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

After finishing the first row, the game reduces to the case of $d = 1$. So the players "know who must win".

If we let the players compute the winning positions in the second row as they play in the first row, we get the point-line game of BPT.

The interpolation pair

Definition

Let P be a proof system. Let Δ_P be the set of triples (ϕ, ψ, w) where ψ and ϕ are propositional formulas in disjoint variables and w is a P-refutation of $\phi \wedge \psi$. The interpolation pair $\mathcal{I}_P$ is the pair of disjoint **NP** sets (A, B) where

$$A = \{(\phi, \psi, w) \in \Delta_{\mathcal{P}} : \ \phi \text{ is satisfiable}\}$$
$$B = \{(\phi, \psi, w) \in \Delta_{\mathcal{P}} : \ \psi \text{ is satisfiable}\}.$$

The interpolation pair

Definition

Let P be a proof system. Let Δ_P be the set of triples (ϕ, ψ, w) where ψ and ϕ are propositional formulas in disjoint variables and w is a P-refutation of $\phi \wedge \psi$. The interpolation pair $\mathcal{I}_P$ is the pair of disjoint **NP** sets (A, B) where

$$A = \{(\phi, \psi, w) \in \Delta_{\mathcal{P}} : \ \phi \text{ is satisfiable}\}$$
$$B = \{(\phi, \psi, w) \in \Delta_{\mathcal{P}} : \ \psi \text{ is satisfiable}\}.$$

Proposition

The canonical pair of the depth d Frege system is polynomially equivalent to the interpolation pair of the depth $d + 1$ Frege system.

Proof of the characterization

To show that the games characterize the interpolation pairs of bounded depth Frege systems we need:

(1) given a game G, to construct in polynomial time a bounded depth Frege proof of

" for every pair of positional strategies σ, ρ for the two players, either σ is not winning, or ρ is not winning"

Proof of the characterization

To show that the games characterize the interpolation pairs of bounded depth Frege systems we need:

(1) given a game G, to construct in polynomial time a bounded depth Frege proof of

" for every pair of positional strategies σ, ρ for the two players, either σ is not winning, or ρ is not winning"

(2) given a refutation of a CNF formula $\phi(x) \wedge \psi(y)$, where x and y are disjoint sets of variables, to construct in polynomial time a game G such that

– if $\phi(x)$ is satisfiable, then Player 1 has a positional winning strategy, and

– if $\psi(y)$ is satisfiable, then Player 2 has a positional winning strategy

goal (1)

(1) given a game G, to construct in polynomial time a bounded depth Frege proof of

“ *for every pair of positional strategies* σ, ρ *for the two players, either* σ *is not winning, or* ρ *is not winning*”

goal (1)

(1) given a game G, to construct in polynomial time a bounded depth Frege proof of

" for every pair of positional strategies σ, ρ for the two players, either σ is not winning, or ρ is not winning"

- the formalization must include positions reachable when playing the strategies;
- to prove it, use *the game-induction principle* of Skelley and Thapen.

goal (2)

(2) given a refutation of a CNF formula $\phi(x) \wedge \psi(y)$, where x and y are disjoint sets of variables, to construct in polynomial time a game G such that

– if $\phi(x)$ is satisfiable, then Player 1 has a positional winning strategy, and

– if $\psi(y)$ is satisfiable, then Player 2 has a positional winning strategy

A new calculus –

– inspired by the Skelley-Thapen calculus

A new calculus –

– inspired by the Skelley-Thapen calculus

- deep inferences
- a proof of 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.
- in particular, a proof of A is a proof of $\top \vdash A$ and a refutation of A is a proof of $A \vdash \bot$.
- essentially, a term rewriting system

associativity and commutativity of $\vee$ and $\wedge$

contraction/cloning

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

truth constants

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

weakenings

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

dual resolution/resolution

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

where p is a literal

games from proofs

Suppose a proof of $\Phi(x) \wedge \Psi(y)$ is given where x and y are disjoint sets of variables.[4]

Assign x to Player 1 and y to Player 2.

[4] A more natural setting may be a proof of $\Phi(x) \vdash \neg\Psi(y)$.

games from proofs

Suppose a proof of $\Phi(x) \wedge \Psi(y)$ is given where x and y are disjoint sets of variables.[4]
Assign x to Player 1 and y to Player 2.

$\Phi \wedge \Psi$	$\bigwedge$	$\dots$	$\dots$	$\dots$	$\dots$	$\bigwedge$	$\perp$
$\bigvee$	$\bigvee$		$\leftarrow$			$\bigvee$	$\bigvee$
$\bigwedge$	$\bigwedge$		$\rightarrow$			$\bigwedge$	$\bigwedge$
$\bigvee$	$\bigvee$		$\leftarrow$			$\bigvee$	$\bigvee$

[4] A more natural setting may be a proof of $\Phi(x) \vdash \neg\Psi(y)$.

games from proofs

$\{\{\{\bot\}\}\}$	$\wedge$	$\dots$	$\dots$	$\dots$	$\dots$	$\wedge$	Φ
$\{\{\bot\}\}$	$\vee$		$\rightarrow$			$\vee$	$\vee$
$\{\bot\}$	$\wedge$		$\leftarrow$			$\wedge$	$\wedge$
$\bot$	$\vee$		$\rightarrow$			$\vee$	$\vee$

When does a player loose?
Essentially: when he cannot move.

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.

$$\dots \vee (C \wedge D) \vee \dots$$

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

$$\vdots$$

$$\dots \vee (p \wedge (q \vee \bar{p})) \vee \dots$$

$$\dots \vee q \vee \dots$$

E.G.

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

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

$$\vdots$$

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

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

from a satisfying assignment, to a winning strategy

Given an assignment $x := a$, Player 1

- in resolution w.r.t. p, picks the disjunction where p is false,
- in dual resolution w.r.t. p, picks the conjunction where p is true
- in $\Psi(x)$ picks false disjunctions and true conjunctions.[5]

[5] these may actually be just literals

Evidence of hardness

- combinatorial games reducible to the canonical pairs
- cryptographic hard problems (the Diffie-Hellman hard-core bit)
- proof search for Resolution refutations is not in **P** unless **FPT**$=$**W[P]**

Evidence of hardness

- combinatorial games reducible to the canonical pairs
- cryptographic hard problems (the Diffie-Hellman hard-core bit)
- proof search for Resolution refutations is not in **P** unless **FPT**=**W[P]**

Problem Find a polynomial reduction of the canonical pair of Resolution to something else!

Unbounded Frege systems

Problem Characterize the canonical pair of Frege systems.

thank you!