On depth 1 Frege systems

Pavel Pudlák

Mathematical Institute, Czech Academy of Sciences, Prague [1]

Proof Complexity 2020, Banff, January 2020

[1] supported by EPAC, grant 19-27871X of the Czech Grant Agency

Overview

1. Bounded depth Frege systems, the separation problem, and Bounded Arithmetic
2. Canonical and interpolations pairs of bounded depth Frege systems
3. Monotone interpolation by game-schemas
4. Two characterizations of the interpolation pair of depth 1 Frege system
5. Generalized monotone Boolean circuits

Bounded depth Frege systems

- $\mathcal{F}_d$ - depth d Frege system = depth d Sequent Calculus for propositional logic
- literals have depth 0, conjunctions and disjunctions of literals have depth 1, etc.
- a sequent $A_1, \ldots, A_n$ is semantically $A_1 \vee \ldots A_n$
- Resolution = $\mathcal{F}_0$
- in $\mathcal{F}_1$ sequents are *sequences of conjunctions*, semantically DNFs

Canonical and interpolations pairs

[Razborov'94] Let P be a propositional proof system. The canonical pair $\mathcal{C}_P$ of P is the pair of disjoint **NP** sets (A, B) where

$$A = \{(\phi, 1^m) : \phi \text{ is satisfiable}\}$$
$$B = \{(\phi, 1^m) : \phi \text{ has a } P\text{-refutation of size at most } m\}.$$

Canonical and interpolations pairs

[Razborov'94] Let P be a propositional proof system. The canonical pair $\mathcal{C}_P$ of P is the pair of disjoint **NP** sets (A, B) where

$$A = \{(\phi, 1^m) : \phi \text{ is satisfiable}\}$$
$$B = \{(\phi, 1^m) : \phi \text{ has a } P\text{-refutation of size at most } m\}.$$

[P'03] Let Δ_P be the set of triples (ϕ, ψ, π) where ψ and ϕ are propositional formulas in disjoint variables and π is a P-refutation of $\phi \wedge \psi$. The interpolation pair $\mathcal{I}_P$ is the pair of disjoint **NP** sets (A, B) where

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

- polynomial separability of the canonical pair of $P =$ automatability of P
- polynomial separability of the interpolation pair of $P =$ feasible interpolation for P

Proposition

1. *The interpolation pair of $\mathcal{F}_0$ (Resolution) is polynomially separable ($\equiv$ feasible interpolation) [Krajíček, 1994]*
2. *For every $d \geq 0$, the canonical pair of the proof systems $\mathcal{F}_d$ is equivalent to the interpolation pair of $\mathcal{F}_{d+1}$. [BPT'14]*

Problem

Is the canonical pair of $\mathcal{F}_0$ (resolution) polynomially separable, i.e., is Resolution weakly automatable?
Equivalently, is the interpolation pair of $\mathcal{F}_1$ polynomially separable?

Definition (**NP** pairs of combinatorial games)

Let G be a combinatorial 2-player game with a concept of a *positional strategy*. Suppose the concept of a *positional winning strategy is in* **NP**. Then we associate a disjoint **NP** pair (A, B) with G defined by

$$A = \{G : \text{Player 1 has a positional winning strategy}\}$$
$$B = \{G : \text{Player 2 has a positional winning strategy}\}.$$

[2] Moreover, it seems that the characterization can be extended to (unbounded depth) *Frege systems*.

Definition (**NP** pairs of combinatorial games)

Let G be a combinatorial 2-player game with a concept of a *positional strategy*. Suppose the concept of a *positional winning strategy is in* **NP**. Then we associate a disjoint **NP** pair (A, B) with G defined by

$$A = \{G : \text{Player 1 has a positional winning strategy}\}$$
$$B = \{G : \text{Player 2 has a positional winning strategy}\}.$$

- The canonical and interpolation pairs of $\mathcal{F}_d$ can be characterized by the canonical pairs of certain games [P'19].[2]
- The canonical pair of Resolution (= interpolation pair of $\mathcal{F}_1$) is also characterized by the canonical pair of the *point-line game* [BPT'14].

[2] Moreover, it seems that the characterization can be extended to (unbounded depth) *Frege systems*.

From disjoint **NP** pairs to partial monotone Boolean functions

Suppose that the definition of a game has a parameter $\bar{z} \in \{0,1\}^n$ which may be

- initial position, or
- string that determines the winning positions.

Then we call the same concept with $\bar{z}$ as a variable a *game schema*.

Let $G(\bar{z})$ be a game schema. Then it determines a partial Boolean function:

For $\bar{a} \in \{0,1\}^n$,

$$F(\bar{a}) = 1 \text{ if Player 1 has a positional winning strategy}$$
$$F(\bar{a}) = 0 \text{ if Player 2 has a positional winning strategy}$$

otherwise undefined.

Let $G(\bar{z})$ be a game schema. Then it determines a partial Boolean function:

For $\bar{a} \in \{0,1\}^n$,

$$F(\bar{a}) = 1 \text{ if Player 1 has a positional winning strategy}$$
$$F(\bar{a}) = 0 \text{ if Player 2 has a positional winning strategy}$$

otherwise undefined.

- If 1s in $\bar{a}$ are the winning positions for Player 1, then the function is monotone.
- For the point-line game where $\bar{z}$ determines the initial position, the function is monotone.
- We can compare game schemas using projections.

Basic example: monotone Boolean circuit

Let $C(\bar{z})$ be a monotone Boolean Circuit and $\bar{a} \in \{0,1\}^n$.

1. (C, a) *as a game*
   - players $\bigvee$ and $\bigwedge$
   - $\bigvee$ wants to reach an input with 1, $\bigwedge$ wants 0
2. $C(\bar{z})$ is a *game schema*

Basic example: monotone Boolean circuit

Let $C(\bar{z})$ be a monotone Boolean Circuit and $\bar{a} \in \{0,1\}^n$.

1. (C, a) *as a game*
   - players $\bigvee$ and $\bigwedge$
   - $\bigvee$ wants to reach an input with 1, $\bigwedge$ wants 0
2. $C(\bar{z})$ is a *game schema*

N.B. if a player has a winning strategy then (s)he also has a *positional* winning strategy.

Monotone interpolation by game schemas

Theorem (P'19)

Let $\Phi(\bar{x}, \bar{z})$ and $\Psi(\bar{y}, \bar{z})$ be two CNF formulas whose only common variables are $\bar{z}$ and they occur in Φ only positively and in Ψ only negatively. Let an $\mathcal{F}_d$ refutation of $\Phi(\bar{x}, \bar{z}) \wedge \Psi(\bar{y}, \bar{z})$ be given.

Then it is possible to construct in polynomial time a depth $d + 1$ game schema $S(\bar{z})$ such that for every assignment $\bar{a} : \bar{z} \to \{0, 1\}$,

- *if $\Phi(\bar{x}, \bar{a})$ is satisfiable, then Player I has a positional wining strategy in $S(\bar{a})$ and*
- *if $\Psi(\bar{y}, \bar{a})$ is satisfiable, then Player II has a positional wining strategy in $S(\bar{a})$.*

Depth 2 games and game schemas

Definition (Depth 2 game)

Two players alternate filling a $2 \times m$ matrix

$$\begin{pmatrix} u_1 & u_2 & \dots & u_{m-1} & u_m \\ v_1 & v_2 & \dots & v_{m-1} & v_m \end{pmatrix}$$

in the order $u_1 u_2 \dots u_{m-1} u_m v_m v_{m-1} \dots v_2 v_1$, $u_i, v_j \in A$.

Legal moves (and positional strategies) are

- for u_i, determined by i, u_{i-1},
- for v_i, determined by i, u_i, and v_{i+1}.

Player 1 wins if $v_1 \in W$, otherwise Player 2.

Depth 2 games and game schemas

Definition (Depth 2 game)

Two players alternate filling a $2 \times m$ matrix

$$\begin{pmatrix} u_1 & u_2 & \dots & u_{m-1} & u_m \\ v_1 & v_2 & \dots & v_{m-1} & v_m \end{pmatrix}$$

in the order $u_1 u_2 \dots u_{m-1} u_m v_m v_{m-1} \dots v_2 v_1$, $u_i, v_j \in A$.

Legal moves (and positional strategies) are

- for u_i, determined by i, u_{i-1},
- for v_i, determined by i, u_i, and v_{i+1}.

Player 1 wins if $v_1 \in W$, otherwise Player 2.

Definition (depth 2 game schema)

same, except W is not fixed.

equivalent definition

1. In the 1st round players alternate constructing a monotone Boolean circuit C.
2. In the 2nd round they play the game determined by C and an input $a \in \{0,1\}^n$.

equivalent definition

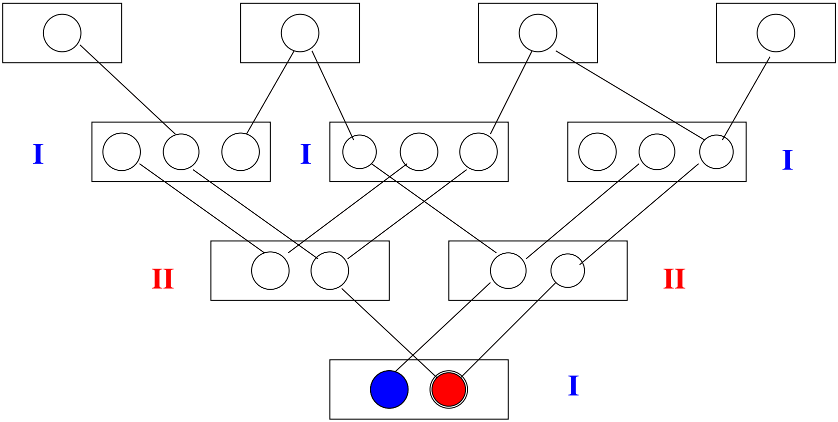
1. In the 1st round players alternate constructing a monotone Boolean circuit C.
2. In the 2nd round they play the game determined by C and an input $a \in \{0,1\}^n$.

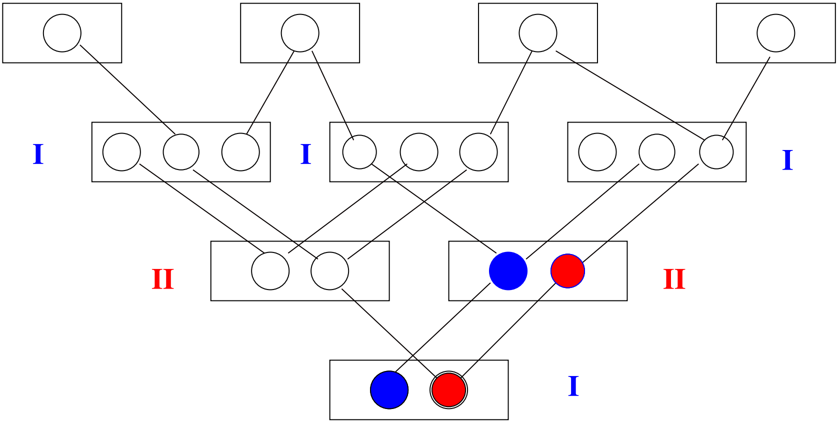
In more detail

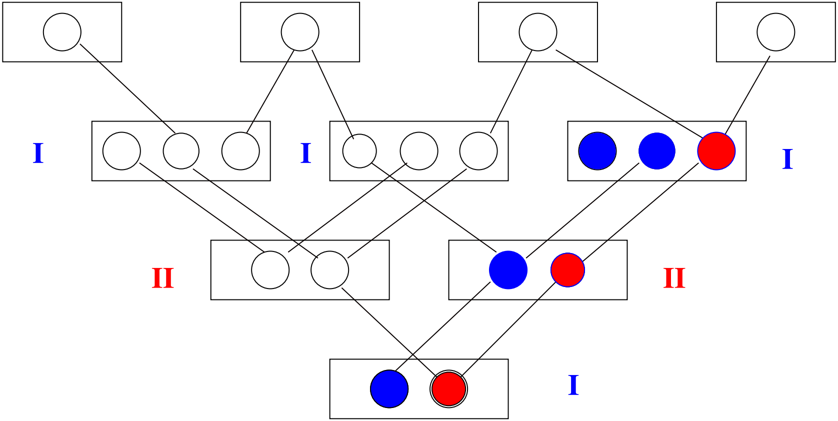
- the circuit they construct will be a *straight-line program*
- at step i, the player can choose an instruction from some fixed set I_i (e.g., I_i can be $\{y_k := x_l \wedge y_p, \quad y_k := y_q \vee y_r\}$)
- they construct the program in the *reverse order*.

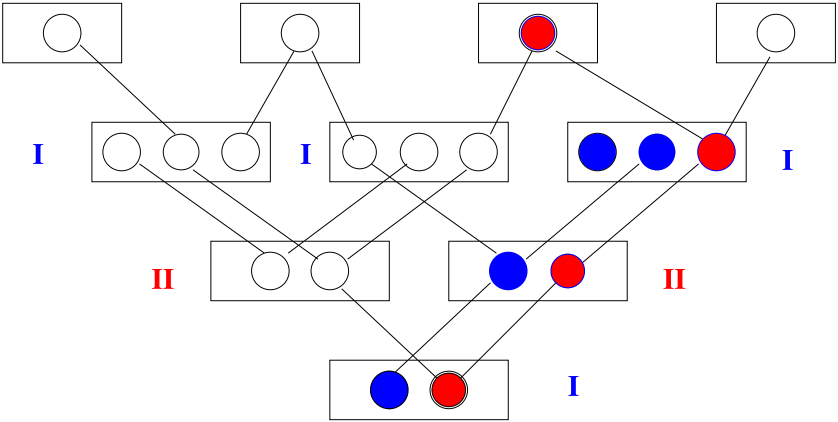
The point-line game

- DAG (G, E) (nodes and arrows)
- nodes labeled B and W (the players)
- for every node A, a set P_A (points of A)
- for every arrow $A \to B$, a partial matching between P_A and P_B (lines)
- one source
- each sink has exactly one point
- game starts with black and white pebbles on the points of the source
- players pick arrows and move pebbles along the lines
- the winner is whose pebble ends up in a sink


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 different way of playing the point-line game

- do not move pebbles, only construct the path
- after reaching a leaf, determine the color by following the lines back

Proposition

Point-line game schemas and depth 2 game schemas are reducible to each other using projections and at most polynomial increase of the size of the games.

Proof (only the easy direction - simulation of point-line games by depth 2 games).

We will use the definition of depth 2 games based on circuits.

Let a point-line game G be given. Think of the points as variables. When a player decides to go from node P to node Q where $p_1 \to q_1, \ldots, p_k \to q_k$ is the matching of lines, then in the depth 2 game the player will play

$$q_1 := p_1, \ldots, q_k := p_k$$

Furthermore, we may assume w.l.o.g. that there is a unique sink in the point-line game. The variable assigned to the point y in it will be the output variable of the constructed circuit.

The resulting circuit will contain instructions

$$r_2 := r_1, r_3 := r_2, \ldots, y := r_{m-1},$$

where $r_1, \ldots, r_{m-1}, y$ is the path from point r_1 in the input node to y, the point in the sink.

Generalized monotone Boolean circuits

Monotone Boolean circuits as a calculus

Axioms: $0, 1, x_1, x_2, \ldots$

Rules:

$$\frac{f \quad g}{f \wedge g} \qquad \frac{f \quad g}{f \vee g}$$

Generalized monotone Boolean circuits

Monotone Boolean circuits as a calculus

Axioms: $0, 1, x_1, x_2, \ldots$

Rules:

$$\frac{f \quad g}{f \wedge g} \qquad \frac{f \quad g}{f \vee g}$$

Generalized monotone Boolean circuits as a calculus

$+$ substitution rule:

$$\frac{f(y_1, \ldots, y_r)}{f(z_1, \ldots, z_r)}$$

where $y_1, \ldots, y_r$ are distinct variables and $z_1, \ldots, z_r$ are variables or constants.

The *size* of the (generalized) circuit is the *length of the derivation* (not counting substitutions).

Proposition

Given a point-line game schema, one can construct a generalized circuit of the same size that computes who has a winning strategy.

Proposition

Given a point-line game schema, one can construct a generalized circuit of the same size that computes who has a winning strategy.

Proof idea.

By induction, construct generalized circuits for all nodes of the given point-line game schema. Nodes of Black (White) will correspond to $\vee$ (to $\wedge$). Substitutions are determined by matchings between the nodes. □

Proposition

Given a point-line game schema, one can construct a generalized circuit of the same size that computes who has a winning strategy.

Proof idea.

By induction, construct generalized circuits for all nodes of the given point-line game schema. Nodes of Black (White) will correspond to $\vee$ (to $\wedge$). Substitutions are determined by matchings between the nodes. □

Problem

Determine for which inputs there is a positional winning strategy.

Proposition

Given a point-line game schema, one can construct a generalized circuit of the same size that computes who has a winning strategy.

Proof idea.

By induction, construct generalized circuits for all nodes of the given point-line game schema. Nodes of Black (White) will correspond to $\vee$ (to $\wedge$). Substitutions are determined by matchings between the nodes. □

Problem

Determine for which inputs there is a positional winning strategy.

Remark. If the graph of the point-line game is a tree, we can eliminate substitutions and get a monotone Boolean formula.

Problems

1. Prove a superpolynomial lower bounds on generalized monotone circuits for explicit functions.

Problems

1. Prove a superpolynomial lower bounds on generalized monotone circuits for explicit functions.
2. Extend the calculus defining generalized monotone circuits to include information about *positional* winning strategies.

Problems

1. Prove a superpolynomial lower bounds on generalized monotone circuits for explicit functions.
2. Extend the calculus defining generalized monotone circuits to include information about *positional* winning strategies.
3. Use 2. to prove a lower bound on point-line game schemas representing a partial monotone function.

WPHP has quasipolynomial $\mathcal{F}_1$ proofs

Corollary

1. *Depth 2 game schemas are exponentially more powerful than monotone Boolean circuits.*
2. *Generalized monotone circuits are exponentially more powerful than monotone Boolean circuits.*

Corollary

For every n, there exists an $m = n^{O(n)}$ and a formula $\phi(\bar{x}, \bar{y})$ where $\bar{x}$ occur negatively in ϕ, $|\bar{x}| = n$, such that every monotone circuit $C(\bar{x})$ such that for every $\bar{a} \in \{0,1\}^n$,

$$C(\bar{a}) = 1 \text{ if } \phi(\bar{a}, y) \text{ has a } \mathcal{F}_1 \text{ refutation of size } \le m$$
$$C(\bar{a}) = 0 \text{ if } \phi(\bar{a}, y) \text{ is satisfiable}$$

has exponential size.

I.e., *$\mathcal{F}_1$ is not weakly automatable by monotone Boolean circuits.*

Corollary

For every n, there exists an $m = n^{O(n)}$ and a formula $\phi(\bar{x}, \bar{y})$ where $\bar{x}$ occur negatively in ϕ, $|\bar{x}| = n$, such that every monotone circuit $C(\bar{x})$ such that for every $\bar{a} \in \{0,1\}^n$,

$$C(\bar{a}) = 1 \text{ if } \phi(\bar{a}, y) \text{ has a } \mathcal{F}_1 \text{ refutation of size } \leq m$$
$$C(\bar{a}) = 0 \text{ if } \phi(\bar{a}, y) \text{ is satisfiable}$$

has exponential size.

I.e., *$\mathcal{F}_1$ is not weakly automatable by monotone Boolean circuits.*

Problem

Can we prove the same for Resolution?

Thank you