Lower bounds for Choiceless Polynomial Time via Symmetric XOR-circuits

Benedikt Pago

Highlights 2023

Mathematical Foundations of Computer Science - RWTH Aachen University

Capturing polynomial time with a logic

Yuri Gurevich (1988): A logic is a set of sentences $\mathcal{L}$ such that:

- $\mathcal{L}$ is **decidable**.
- **Effectiveness:** Given $\psi \in \mathcal{L}$, one can compute a program A_ψ which evaluates ψ in any given structure $\mathfrak{A}$.
- **Isomorphism-invariance:** For any two isomorphic structures $\mathfrak{A}$ and $\mathfrak{B}$, and every $\psi \in \mathcal{L}$, it holds $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$.

Capturing polynomial time with a logic

Yuri Gurevich (1988): A logic is a set of sentences $\mathcal{L}$ such that:

- $\mathcal{L}$ is **decidable**.
- **Effectiveness:** Given $\psi \in \mathcal{L}$, one can compute a program A_ψ which evaluates ψ in any given structure $\mathfrak{A}$.
- **Isomorphism-invariance:** For any two isomorphic structures $\mathfrak{A}$ and $\mathfrak{B}$, and every $\psi \in \mathcal{L}$, it holds $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$.

A logic $\mathcal{L}$ captures PTIME if:

- For every sentence $\psi \in \mathcal{L}$, the *model-checking problem* is *in* PTIME.
- Every PTIME-*decidable class* of structures can be *defined* by a sentence $\psi \in \mathcal{L}$.

Capturing polynomial time with a logic

Yuri Gurevich (1988): A logic is a set of sentences $\mathcal{L}$ such that:

- $\mathcal{L}$ is **decidable**.
- **Effectiveness:** Given $\psi \in \mathcal{L}$, one can compute a program A_ψ which evaluates ψ in any given structure $\mathfrak{A}$.
- **Isomorphism-invariance:** For any two isomorphic structures $\mathfrak{A}$ and $\mathfrak{B}$, and every $\psi \in \mathcal{L}$, it holds $\mathfrak{A} \models \psi \Leftrightarrow \mathfrak{B} \models \psi$.

A logic $\mathcal{L}$ captures PTIME if:

- For every sentence $\psi \in \mathcal{L}$, the *model-checking problem* is *in* PTIME.
- Every PTIME-*decidable class* of structures can be *defined* by a sentence $\psi \in \mathcal{L}$.

Open question: Does there exist a logic that captures PTIME?

Landscape of polynomial time logics

PTIME

$\subsetneq$ $\supseteq$ **(=?)**

Rank logic ⟷ **Choiceless Polynomial Time** (CPT)

$\neq$

$\supsetneq$ $\subsetneq$

Fixed-point logic with counting (FPC)

$\cup\!\!\!\!\,\not{}$

Least fixed-point logic (LFP)

$\cup\!\!\!\!\,\not{}$

First-order logic (FO)

CPT is an extension of fixed-point logic with symmetric *hereditarily finite sets* of polynomial size (Blass, Gurevich, Shelah; 1999).

CPT is an extension of fixed-point logic with symmetric *hereditarily finite sets* of polynomial size (Blass, Gurevich, Shelah; 1999).

Intuitive "definitions":

- Turing machines operating on finite structures, storing sets in their registers, with FOC-definable state updates.

CPT is an extension of fixed-point logic with symmetric *hereditarily finite sets* of polynomial size (Blass, Gurevich, Shelah; 1999).

Intuitive "definitions":

- Turing machines operating on finite structures, storing sets in their registers, with FOC-definable state updates.
- The class of all PTIME "combinatorial" algorithms on graphs (as opposed to, say, algebraic ones).

The problem

Goal: Develop techniques towards proving CPT $\neq$ PTIME.

The problem

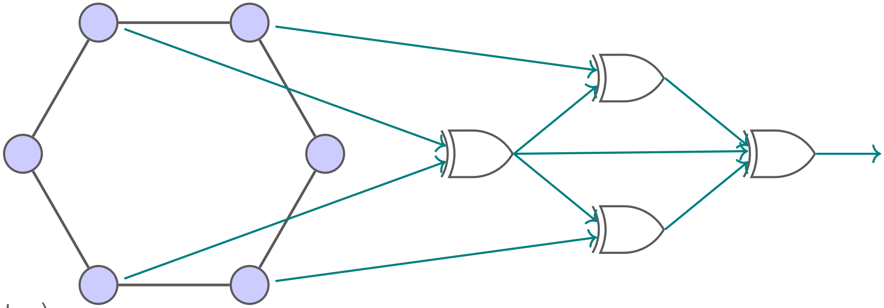
Goal: Develop techniques towards proving CPT $\neq$ PTIME.

Candidate problem: *CFI-query* on unordered base graphs as a “logically hard” PTIME-problem.

Theorem (P., to appear at MFCS 2023)

*The CFI-query on a class $\mathcal{G}$ of base graphs can only be decided by a CPT-algorithm using "**parity summation**" if there exists for each $G \in \mathcal{G}$ a Boolean XOR-circuit C_G satisfying:*

1. *The size of C_G is polynomial in $|G|$.*
2. *C_G has the same **symmetries** as G.*
3. *The fan-in is logarithmic in $|G|$.*
4. *C_G computes the sum mod 2 over (almost) all its inputs.*



Connection with symmetric circuits

Theorem (P., to appear at MFCS 2023)

*The CFI-query on a class $\mathcal{G}$ of base graphs can only be decided by a CPT-algorithm using "**parity summation**" if there exists for each $G \in \mathcal{G}$ a Boolean XOR-circuit C_G satisfying:*

1. *The size of C_G is polynomial in $|G|$.*
2. *C_G has the same **symmetries** as G.*
3. *The fan-in is logarithmic in $|G|$.*
4. *C_G computes the sum mod 2 over (almost) all its inputs.*

Theorem

Let $\mathcal{G}$ be the family of n-dimensional hypercubes. There do not exist circuits as in the above theorem if two of the assumptions are strengthened.

Conclusion

Does CPT capture PTIME?

Can CPT decide the unordered CFI-query?

Answer: If circuit lower bound can be improved, then no parity summation algorithm succeeds.

Conclusion

Does CPT capture PTIME?

Can CPT decide the unordered CFI-query?

Answer: If circuit lower bound can be improved, then no parity summation algorithm succeeds.

Future work: Lift this to *all* CPT-algorithms...