Distinguishing graphs in Choiceless Polynomial Time and the Extended Polynomial Calculus

Benedikt Pago

CSL 2023

Mathematical Foundations of Computer Science - RWTH Aachen University

Propositional Proof Complexity and Finite Model Theory

- **Proof Complexity:** Studies *proof systems* for refuting the satisfiability of propositional formulas (e.g. resolution).
- **Finite Model Theory:** Studies expressive power of *(fixed-point) logics* on finite structures.
- Given a translation between propositional formulas and finite structures, the two formalisms can simulate each other.
- **Application:** Transferring *lower-bound* results between the two fields.

Old and new connections between proof systems and logics

Theorem (Grädel, Grohe, Pakusa, P. (2019))

- *Existential least fixed-point logic* $\equiv$ *width-k resolution.*
- *Least fixed-point logic* $\equiv$ *Horn resolution.*
- *Fixed-point logic with counting* $\equiv$ *degree-k monomial calculus.*

- Proof search can be implemented in fixed-point logic.
- For any fixed-point sentence ψ, there is a uniform translation from finite structures $\mathfrak{A}$ to propositional formulas Φ such that $\mathfrak{A} \models \psi$ iff Φ has a refutation.

Old and new connections between proof systems and logics

Theorem (Grädel, Grohe, Pakusa, P. (2019))

- *Existential least fixed-point logic* $\equiv$ *width-k resolution.*
- *Least fixed-point logic* $\equiv$ *Horn resolution.*
- *Fixed-point logic with counting* $\equiv$ *degree-k monomial calculus.*

- Proof search can be implemented in fixed-point logic.
- For any fixed-point sentence ψ, there is a uniform translation from finite structures $\mathfrak{A}$ to propositional formulas Φ such that $\mathfrak{A} \models \psi$ iff Φ has a refutation.

Theorem

With respect to the graph isomorphism problem:
Choiceless Polynomial Time $<$ *degree-3 Extended Polynomial Calculus.*

$\Rightarrow$ Lower bounds for Extended Polynomial Calculus translate to CPT.

Choiceless Polynomial Time

CPT = *Fixed-point logic with counting* + construction of polynomial-size isomorphism-invariant *hereditarily finite sets*.

Syntax includes set-theoretic operations:

- $\texttt{Pair}(a, b) := \{a, b\}$.
- $\texttt{Union}(a) := \bigcup a$.
- Comprehension: $\{t \ : \ x \in a \ : \ \varphi\} := \{t(x) \mid x \in a, \mathfrak{A} \models \varphi(x)\}$.
- $\texttt{Card}(a) = |a|$, as a von Neumann ordinal.
- Iteration: Terms can be iterated until a halting-condition is met (similar to fixed-point computation).

CPT = *Fixed-point logic with counting* + construction of polynomial-size isomorphism-invariant *hereditarily finite sets*.

Syntax includes set-theoretic operations:

- $\texttt{Pair}(a, b) := \{a, b\}$.
- $\texttt{Union}(a) := \bigcup a$.
- Comprehension: $\{t \ : \ x \in a \ : \ \varphi\} := \{t(x) \mid x \in a, \mathfrak{A} \models \varphi(x)\}$.
- $\texttt{Card}(a) = |a|$, as a von Neumann ordinal.
- Iteration: Terms can be iterated until a halting-condition is met (similar to fixed-point computation).

Open question

Can every PTIME-decidable class of finite structures be decided by a CPT-sentence?

The **Polynomial Calculus** (PC) is a sound and complete decision procedure for the (complement of the) following problem:

Satisfiability of Polynomial Equation Systems

Input: A set P of multilinear polynomials over a variable set $\mathcal{V}$.
Question: Is there a $\{0, 1\}$-assignment to the variables in $\mathcal{V}$ that is a common zero of all polynomials in P?

There is a PC-derivation of the $\mathbf{1}$-polynomial from P, iff P is unsat.

Proof rules of the Extended Polynomial Calculus

Let $\mathcal{V}$ the set of variables, f, g polynomials.

Linear combination: $$\frac{f \quad g}{a \cdot f + b \cdot g} \qquad a, b \in \mathbb{Q}.$$

Multiplication with variable: $$\frac{f}{Xf} \qquad X \in \mathcal{V}.$$

Extension axioms: $$\frac{}{X_f - f} \qquad X_f \text{ a fresh variable.}$$

Proof rules of the Extended Polynomial Calculus

Let $\mathcal{V}$ the set of variables, f, g polynomials.

Linear combination: $$\frac{f \quad g}{a \cdot f + b \cdot g} \qquad a, b \in \mathbb{Q}.$$

Multiplication with variable: $$\frac{f}{Xf} \qquad X \in \mathcal{V}.$$

Extension axioms: $$\frac{}{X_f - f} \qquad X_f \text{ a fresh variable.}$$

Polynomial calculus without extension axioms is a complete proof system.
But: *Extension axioms* may allow for *shorter proofs*.
For unbounded degree, extension axioms make the PC *exponentially stronger*.

Distinguishing graphs in the (extended) polynomial calculus

Let G, H be graphs. The *existence of an isomorphism* is expressed by the polynomials $P_{\text{iso}}(G, H)$:

$\sum_{v \in V(G)} X_{vw} - 1$	for all $w \in V(H)$.
$\sum_{w \in V(H)} X_{vw} - 1$	for all $v \in V(G)$.
$X_{vw} X_{v'w'}$	for all $v, v' \in V(G), w, w' \in V(H)$ such that $(v, v') \mapsto (w, w')$ is not a local isomorphism.

A proof system $\mathcal{P}$ distinguishes G and H if $P_{\text{iso}}(G, H)$ has a $\mathcal{P}$-refutation.

Definition

Let $\mathcal{K}$ be a class of graphs. CPT distinguishes all graphs in $\mathcal{K}$ if there exists a polynomial $p(n)$ such that for every pair of *non-isomorphic* graphs $G_1, G_2 \in \mathcal{K}$, *there exists* a CPT-sentence Π with a bounded number of variables such that

$$G_1 \models \Pi \text{ and } G_2 \not\models \Pi$$

and the h.f. sets constructed by Π have size $\leq p(|G_i|)$.

The main result

Theorem

If CPT *distinguishes all graphs in a class $\mathcal{K}$, then the degree-3 extended polynomial calculus* (EPC$_3$) *distinguishes all graphs in $\mathcal{K}$ with refutations of polynomial size.*

The main result

Theorem

If CPT *distinguishes all graphs in a class* $\mathcal{K}$*, then the degree-3 extended polynomial calculus* (EPC_3) *distinguishes all graphs in* $\mathcal{K}$ *with refutations of polynomial size.*

Corollary

Let $\mathcal{K}$ *be a graph class such that:*

- *The graph isomorphism problem on* $\mathcal{K}$ *is in* PTIME.
- *Distinguishing graphs in* $\mathcal{K}$ *in* EPC_3 *requires refutations of super-polynomial size.*

Then CPT $\neq$ PTIME.

An exponential lower bound for EPC is known (not for graph isomorphism) [Alekseev, 2020].

A consequence for proof complexity

Corollary

There exist non-isomorphic graphs $(G_n, H_n)_{n\in\mathbb{N}}$ which are distinguishable in EPC_3 but not in degree-k polynomial calculus, for any $k \in \mathbb{N}$.

Proof. Certain families of Cai-Fürer-Immerman graphs are distinguishable in CPT [Dawar, Richerby, Rossman; 2008], but not in bounded-degree PC [Berkholz, Grohe; 2015].

Proof of the main result

CPT distinguishes all graphs in $\mathcal{K}$.

$\Downarrow$

Fix any $G, H \in \mathcal{K}, G \not\cong H$.

$\Downarrow$

There exists $\Pi \in$ CPT with $G \models \Pi$ and $H \not\models \Pi$,
constructing h.f. sets of polynomial size.

$\Downarrow$

Turn the constructed sets into an EPC_3-refutation of $P_{\text{iso}}(G, H)$.

Proof of the main result

CPT distinguishes all graphs in $\mathcal{K}$.

$\Downarrow$

Fix any $G, H \in \mathcal{K}, G \not\cong H$.

$\Downarrow$

There exists $\Pi \in$ CPT with $G \models \Pi$ and $H \not\models \Pi$, constructing h.f. sets of polynomial size.

$\Downarrow$

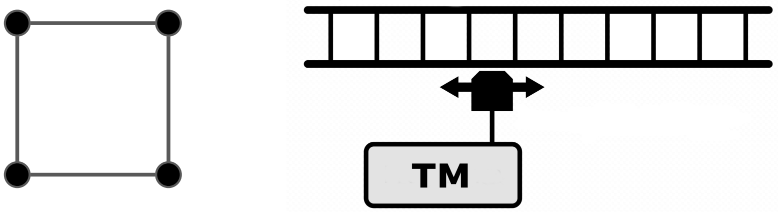
There exists a polynomial time *Deep Weisfeiler Leman* algorithm distinguishing G and H.

$\Downarrow$

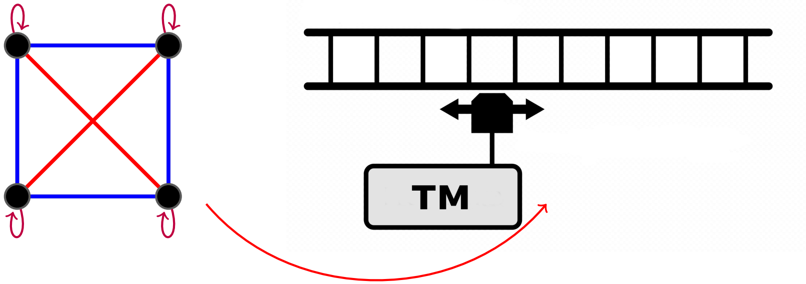
Turn the constructed sets into an EPC_3-refutation of $P_{\mathrm{iso}}(G, H)$.

Deep Weisfeiler Leman (Grohe, Schweitzer, Wiebking; 2021)

A Deep Weisfeiler Leman algorithm is a Turing machine whose input is a graph to which it has limited access.



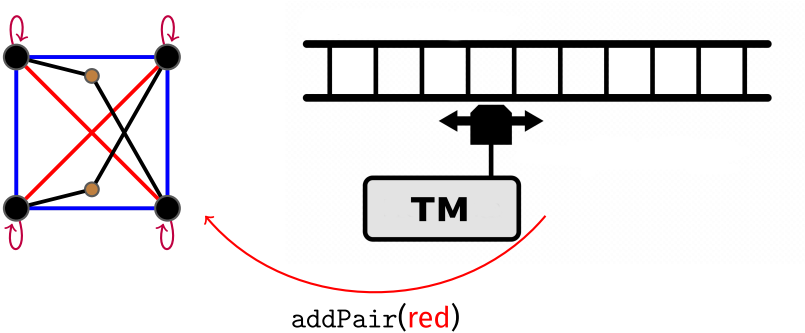
A Deep Weisfeiler Leman algorithm is a Turing machine whose input is a graph to which it has limited access.



2-dimensional Weisfeiler Leman colouring

Deep Weisfeiler Leman (Grohe, Schweitzer, Wiebking; 2021)

A Deep Weisfeiler Leman algorithm is a Turing machine whose input is a graph to which it has limited access.



Proof continued

- Deep Weisfeiler Leman (DWL) is an isomorphism-invariant computation model *equivalent to* CPT [Grohe, Schweitzer, Wiebking; 2021].
- DWL is "2-dimensional Weisfeiler Leman + construction of new vertices".
- The *2-dimensional Weisfeiler Leman* algorithm can be simulated in the *degree-3 polynomial calculus* [Berkholz, Grohe; 2015].
- $\Rightarrow$ These facts together allow to construct an EPC_3-refutation of $P_{iso}(G, H)$.

Outlook: Symmetric proof systems

Stronger version of the result:

Theorem

If CPT distinguishes all graphs in a class $\mathcal{K}$, then the degree-3 extended polynomial calculus (EPC_3) distinguishes all graphs in $\mathcal{K}$ with symmetric refutations of polynomial size.

- Extension axioms in the refutation of $P_{\mathrm{iso}}(G, H)$ are closed under $\mathbf{Aut}(G) \times \mathbf{Aut}(H)$.
- **Question:** What is the right notion of a *symmetric proof system*?
- Aim: Use symmetry-dependent proof techniques from finite model theory against symmetric proof systems.

Stronger version of the result:

Theorem

If CPT *distinguishes all graphs in a class $\mathcal{K}$, then the degree-*3 *extended polynomial calculus* (EPC_3) *distinguishes all graphs in $\mathcal{K}$ with symmetric refutations of polynomial size.*

- Extension axioms in the refutation of $P_{\text{iso}}(G, H)$ are closed under $\mathbf{Aut}(G) \times \mathbf{Aut}(H)$.
- **Question:** What is the right notion of a *symmetric proof system*?
- Aim: Use symmetry-dependent proof techniques from finite model theory against symmetric proof systems.

Thank you!