A Finite-Model-Theoretic View on Propositional Proof Complexity

Erich Grädel, Martin Grohe, **Benedikt Pago**, Wied Pakusa

Mathematical Foundations of Computer Science - RWTH Aachen University

April 7, 2021

What does Proof Complexity have to do with 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.

Outline

1. Resolution and least fixed-point logic (LFP).
2. Polynomial Calculus (PC) and fixed-point logic with counting (FPC).
3. Lower-bound applications.

Resolution

Resolution is a sound and complete decision procedure for the following problem:

CNF-Unsatisfiability

Input: A propositional formula ψ in conjunctive normal form.
Question: Is ψ unsatisfiable?

Resolution rule:

$$\frac{(X \vee \bigvee Y_i), \quad (\neg X \vee \bigvee Z_j)}{(\bigvee Y_i \vee \bigvee Z_j)}$$

A CNF-formula ψ is unsat iff the empty clause is derivable from it.
Complexity of a refutation:

- *Size:* Number of clauses in the refutation.
- *Width:* Size of largest clause.

Least fixed-point logic (LFP)

LFP extends first-order logic by fixed-point formulas of the following form:

$$[\mathbf{lfp}\ Rx.\ \varphi(x; R)](y).$$

Second-order fixed-point variable

Update formula

Free variable

Semantics

$\mathfrak{A} \models [\mathbf{lfp}\ Rx.\ \varphi(x; R)](a)$ iff a is in the *least fixed-point* of the following sequence:

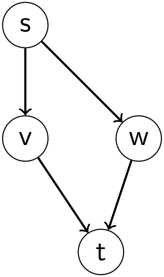
- $R_0 := \emptyset$.
- $R_{i+1} := \{b \in \mathfrak{A} \mid \mathfrak{A} \models \varphi(b; R_i)\}$.

Expressive power: $FO \lneq \mathbf{LFP} \lneq PTIME$.

A first example: The Reachability problem

Reachability problem

Input: A directed graph $G = (V, E, s, t)$.
Question: Is there a path from s to t?



$$\varphi := [\textbf{lfp}\ Rx.\ \underbrace{(x = s \vee \exists y(Ry \wedge E\ yx))}_{\text{“Add to } R \text{ each vertex } x \text{ that is } s \text{ or has a predecessor in } R\text{”}}\ ](t).$$

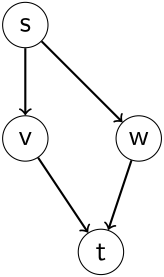
Fixed-point computation:

- $R_0 = \emptyset$.
- $R_1 = \{s\}$.
- $R_2 = \{s, v, w\}$.
- $R_3 = \{s, v, w, t\}$.

A first example: The Reachability problem

Reachability problem

Input: A directed graph $G = (V, E, s, t)$.
Question: Is there a path from s to t?



Set of propositional clauses (UNSAT iff s-t-path exists):

Node clauses:

(X_s) $(\neg X_t)$

Edge clauses:

$(\neg X_s \lor X_v)$
$(\neg X_s \lor X_w)$

$(\neg X_v \lor X_t)$
$(\neg X_w \lor X_t)$

(X_v) (X_w)

(X_t)

$()$

Translating finite structures to CNF-formulas

An *FO-interpretation* $\mathcal{I}$ is an "FO-definable mapping between finite structures".

Main properties:

- Elements of $\mathcal{I}(\mathfrak{A})$ correspond to tuples of elements of $\mathfrak{A}$.
- Relations of $\mathcal{I}(\mathfrak{A})$ are FO-definable in $\mathfrak{A}$.
- For any structure $\mathfrak{A}$, the image $\mathcal{I}(\mathfrak{A})$ can be *computed without recursion/fixed-point induction*.

Simulation of LFP-formula φ in Resolution: The "input structure" $\mathfrak{A}$ for φ is mapped to a *CNF-formula* $\mathcal{I}(\mathfrak{A})$.

Horn-Resolution captures LFP

Theorem

*For every $\varphi \in$ **LFP** there is an FO-interpretation $\mathcal{I}_\varphi$ such that for every finite structure $\mathfrak{A}$:*

$$\mathfrak{A} \models \varphi \text{ iff the Horn-formula represented by } \mathcal{I}_\varphi(\mathfrak{A}) \text{ is unsat.}$$

Proof.

Model-checking games for **LFP** on finite structures are *reachability games*. They can be solved by Resolution similarly as reachability. □

Theorem

*There is an **LFP**-sentence φ_{unsat} such that, for any structure $\mathfrak{A}_\psi$ representing a Horn-formula ψ:*

$$\mathfrak{A}_\psi \models \varphi_{unsat} \text{ iff } \psi \text{ is unsat.}$$

Bounded-width Resolution

Existential LFP (**EFP**): Fixed-point update formulas may not contain universal quantification (**EFP** $\lneq$ LFP).

Theorem

On finite structures, EFP can be simulated by width-3 Resolution.
For any $k \in \mathbb{N}$, width-k Resolution can be simulated in EFP.

Part II: The Polynomial Calculus and Fixed-point logic with counting.

Fixed-point logic with counting

Fixed-point logic with counting (**FPC**) extends LFP by *counting terms*:

$$\#x[\varphi(x)]$$

$$= \text{"the number of elements } x \text{ that satisfy } \varphi\text{"}$$

Expressive power:

LFP $\lneq$ **FPC** $\lneq$ PTIME.

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 $\mathcal{P}$ 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 $\mathcal{P}$?

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

Proof rules of the Polynomial Calculus

Let $\mathbb{F}$ be a field, $\mathcal{V}$ the set of variables, f, g polynomials.

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

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

Example

Let $\mathcal{P} = \{(XY - 1), X\}$. No common zero exists.

Proof:

1. Derive XY from X (*multiplication with variable*).
2. Derive 1 from $(XY - 1)$ and XY (*linear combination*).

Complexity of Polynomial Calculus

Complexity measures for PC-refutations:

- *Size:* Number of polynomials in the refutation.
- *Degree:* Maximum degree of a polynomial in the refutation.
- (Field: The characteristic of the underlying field $\mathbb{F}$ affects the complexity, too).

Theorem (Clegg, Edmonds, Impagliazzo)

For any constant k, exhaustive proof search for the k-degree PC can be done in PTIME.

Proof.

There are only poly. many monomials.
Hence, the derivable polynomials form a *vector space* of poly. dimension, which can be computed with the *Gröbner basis algorithm*. □

PC = FPC

Theorem

On finite structures, FPC can be simulated by degree-2 Polynomial Calculus over $\mathbb{Q}$ (w.r.t. FO^+-interpretations).

Conversely, for any $k \in \mathbb{N}$, there is an FPC-sentence that decides the existence of a degree-k PC-refutation over $\mathbb{Q}$.

Proof.

FPC $\Rightarrow$ PC: Solve model-checking games involving counting.
PC $\Rightarrow$ FPC: Implement Gröbner-basis algorithm in FPC (linear algebra over $\mathbb{Q}$ is feasible in FPC). $\square$

Results in summary

$$
\begin{tikzcd}
\mathsf{EFP} \arrow[r, leftrightarrow, "="] \arrow[d, phantom, "\lneq" rotate=-90] & k\text{-Resolution} \\
\mathsf{LFP} \arrow[r, leftrightarrow, "="] \arrow[d, phantom, "\lneq" rotate=-90] & \text{Horn-Resolution} \\
\mathsf{FPC} \arrow[r, leftrightarrow, "="] & k\text{-PC}
\end{tikzcd}
$$

Application: Lower bounds

- **Goal:** Transfer lower bounds from finite model theory to proof complexity.
- **A complexity measure for finite structures:** "*Number of first-order variables* required to identify a structure up to isomorphism".
- For structures $\mathfrak{A}$ and $\mathfrak{B}$, "$\mathfrak{A} \equiv^k \mathfrak{B}$" means: $\mathfrak{A}$ and $\mathfrak{B}$ cannot be distinguished by any k-variable sentence.
- **Idea:** If $\mathfrak{A} \equiv^k \mathfrak{B}$, and $\mathcal{I}$ an FO-interpretation, then $\mathcal{I}(\mathfrak{A})$ and $\mathcal{I}(\mathfrak{B})$ are indistuingishable in k-Resolution/k-PC.

Lower bounds for Graph Isomorphism

- **Fact** ("CFI-construction"): There are sequences of *non-isomorphic* graphs $(\mathfrak{A}_n)_{n\in\mathbb{N}}, (\mathfrak{B}_n)_{n\in\mathbb{N}}$ of size $\mathcal{O}(n)$ with $\mathfrak{A}_n \equiv^{\Omega(n)} \mathfrak{B}_n$.
- Let $\mathcal{I}_{\mathsf{Iso}}$ be any FO-interpretation that maps pairs of graphs to propositional formulas/polynomials expressing the *existence of an isomorphism*.
- $\Rightarrow$ The resolution-*width*/PC-*degree* required to refute $\mathcal{I}_{\mathsf{Iso}}(\mathfrak{A}_n, \mathfrak{B}_n)$ is at least *linear*.
- $\Rightarrow$ The proof *size* is *exponential* (well-known relationship between width/degree and size).
- This is not new, but now more independent of the concrete encoding of graph isomorphism.
- Exponential resolution lower-bounds for *pigeonhole principle* and *three-colourability* can be reproved this way.