Symmetric Proofs in the Ideal Proof System

Anuj Dawar [2], Erich Grädel [1], Leon Kullmann [1], **Benedikt Pago** [2]

12.08.2025

[1]RWTH Aachen University

[2]University of Cambridge

The Ideal Proof System (IPS)

Definition (Grochow, Pitassi; 2018)

An **IPS certificate** of unsatisfiability of $\mathcal{F} = \{f_1(\vec{x}), \dots, f_m(\vec{x})\} \subseteq \mathbb{F}[X]$ is a polynomial $C(\vec{x}, y_1, \dots, y_m)$ such that:

1. $C(\vec{x}, \vec{0}) = 0$.
2. $C(\vec{x}, \vec{f}) = 1$.

An **IPS refutation** of $\mathcal{F}$ is an *algebraic circuit* that represents $C(\vec{x}, \vec{y})$.
The *size* of a refutation is the number of gates in the circuit.
A certificate $C(\vec{x}, \vec{y})$ is *linear* if it is linear in the $\vec{y}$-variables.

Novelty: We restrict to **symmetric circuits**.

Why symmetry?

1. **Symmetric computation models** (*logics*) are well-studied in finite model theory and have known connections to proof systems like bounded-width resolution, bounded-degree PC [Grädel, Grohe, Pakusa, P. 2019].
2. **Lower bounds** for symmetric algebraic circuits are known: The determinant and *permanent* have an *exponential* complexity gap for symmetric circuits [Dawar, Wilsenach 2020].

Definition

- Let $\mathcal{F} \subseteq \mathbb{F}[X]$ be a set of polynomials.
- Let $\Gamma \leq \mathbf{Sym}(X)$ be a permutation group acting on X.
- Then $\mathcal{F}$ is *Γ-invariant* if for every $\pi \in \Gamma$, $\pi(\mathcal{F}) = \mathcal{F}$.

Example:

$$\text{perm}_n = \sum_{\pi \in \mathbf{Sym}_n} \prod_{i \in [n]} x_{i\pi(i)}$$

is invariant under the action of $(\mathbf{Sym}_n \times \mathbf{Sym}_n)$ on $\{x_{ij} \mid i, j \in [n]\}$, where $(\pi, \sigma)(x_{ij}) = x_{\pi(i)\sigma(j)}$.

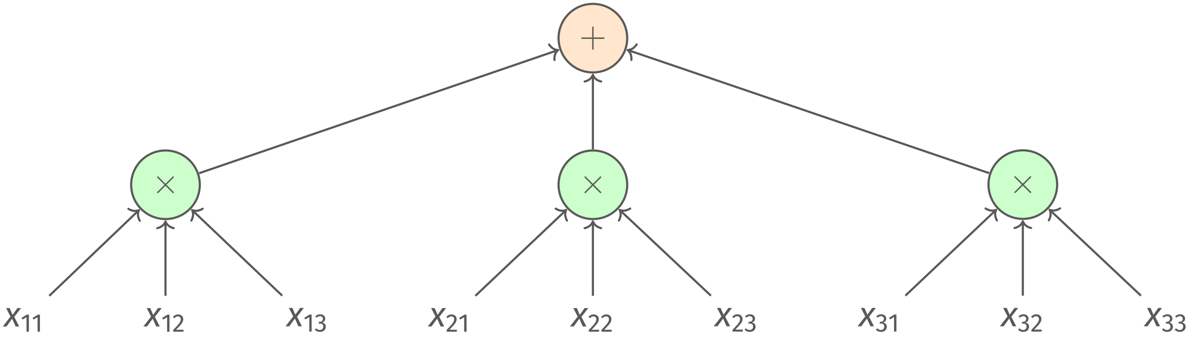
Problem

Input: *A pair* $(\mathcal{F}, \Gamma)$ *where* $\mathcal{F} \subseteq \mathbb{F}[X]$ *and* $\Gamma \leq \mathbf{Sym}(X)$ *is a group under which* $\mathcal{F}$ *is invariant.*
Question: *Is there a common zero of all polynomials in* $\mathcal{F}$*?*

A **sym-IPS refutation** of $(\mathcal{F}, \Gamma)$ is a *Γ-symmetric algebraic circuit* that represents a certificate $C(\vec{x}, \vec{y})$ of unsatisfiability of $\mathcal{F}$.

Symmetric algebraic circuits

- Let X be a set of variables.
- Let Γ be a group acting on X.
- An algebraic circuit C over X is *Γ-symmetric* if the action on X extends to **automorphisms** of C.



Theorem

Sym-IPS *is a complete proof system on all instances* $(\mathcal{F}, \Gamma)$.

Linear sym-IPS *is incomplete over finite fields (if* $|\Gamma|$ *and the field characteristic are not coprime).*

Overview of results

1. Connections with **symmetric computation models** from finite model theory.
2. **Upper bounds** on typical benchmark instances.
3. (Work in progress: Lower bounds).

Theorem

Let $G \not\cong H$, $k \in \mathbb{N}$.

- *G and H k-**WL-distinguishable*** $\Rightarrow$ *"$G \cong H$" has a poly-size* $\deg_k$ sym-IPS *refutation.*
- *G and H **CPT-distinguishable*** $\Rightarrow$ *"$G \cong H$" has a poly-size* *linear* sym-IPS *refutation.*

k-WL: k-dimensional Weisfeiler Leman algorithm

CPT: Choiceless Polynomial Time, a logic/symmetric computation model that distinguishes strictly more graphs than any fixed k-WL.

Summary of upper bounds

Proof System	Graph non-isomorphism	CFI	Subset sum	Pigeonhole principle
$\deg_k$-sym-IPS	$\mathcal{O}(n^c)$ if k-WL-distinguishable	none	none	none
sym-IPS$_{\text{LIN}}$	$\mathcal{O}(n^c)$ if CPT-distinguishable	$\mathcal{O}(2^n)$	$\mathcal{O}(n^c)$	~~$\mathcal{O}(3^n \cdot n)$~~ $\mathcal{O}(n^c)$
sym-IPS	$\mathcal{O}(n^c)$ if CPT-distinguishable	$\mathcal{O}(n^c)$	$\mathcal{O}(n^c)$	~~$\mathcal{O}(3^n \cdot n)$~~ $\mathcal{O}(n^c)$

CFI: System of linear equations over $\mathbb{F}_2$ related to isomorphism of *Cai-Fürer-Immerman* graphs.

Cai-Fürer-Immerman equations: A possible lower bound example?

Fix a connected 3-regular graph $G = (V, E)$ and some distinguished vertex $\tilde{v} \in V$.

Variables: $\{x_i^e \mid e \in E, i \in \mathbb{F}_2\}$. The following is unsatisfiable in $\mathbb{F}_2$.

Cai-Fürer-Immerman

$$x_i^e + x_j^f + x_k^g = i + j + k \quad \text{for each } v \in V \setminus \{\tilde{v}\}, E(v) = \{e, f, g\}, i, j, k \in \mathbb{F}_2.$$

$$x_i^e + x_j^f + x_k^g = i + j + k + 1 \quad \text{for } \tilde{v}, E(\tilde{v}) = \{e, f, g\}, i, j, k \in \mathbb{F}_2.$$

$$x_0^e + x_1^e = 1 \quad \text{for all } e \in E$$

Boolean axioms

Symmetries: Group generated by certain “edge flips” $x_0^e \leftrightsquigarrow x_1^e$.

- **Goal:** Super-polynomial lower bounds for symmetric (linear) IPS.
- **First step:** Consider fragments like symmetric multilinear formula/constant depth IPS.
- Combination of the *functional lower bound method* [Forbes, Shpilka, Tzameret, Wigderson 2021; ...] with symmetry might yield lower bounds for **Boolean CNFs**.
- **Alternative technique:**
  For polynomials expressing graph parameters, small symmetric circuits exist if and only if the parameter is a linear combination of *bounded-treewidth homomorphism counts* [Dawar, P., Seppelt 2025].