Proof Complexity Lower Bounds from Algebraic Circuit Complexity

Michael A. Forbes
Princeton University

Amir Shpilka
Tel Aviv University

Iddo Tzameret
Royal Holloway, University of London

Avi Wigderson
Institute for Advanced Study

June 8, 2016

Talk overview

- Very short introduction to proof complexity
- Nullstellensatz proof system
- Models of algebraic computations
- Ideal Proof System (IPS)
- Our results
- Some proofs

Refuting CNFs

Question (3SAT)

Given a 3CNF $\phi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ prove there is **no** *satisfying assignment to ϕ.*

Question is coNP-hard
NP $\neq$ coNP $\implies$ any proof must be long

holy grail: prove *unconditional* lower bounds on lengths of proofs in every proof system.

note: potentially harder than proving P $\neq$ NP

goal: prove *unconditional* lower bounds on lengths of proofs in strong proof systems

Frege Proof System

Example (Hilbert Propositional Calculus)

Axioms:

$$\phi \to (\psi \to \phi)$$

$$((\phi \to (\psi \to \zeta)) \to ((\phi \to \psi) \to (\phi \to \zeta)))$$

$$(\phi \to \psi) \to (\neg\psi \to \neg\phi)$$

Derivation rules:

$$\textit{Modus ponens:} \qquad \frac{\phi, (\phi \to \psi)}{\psi}$$

Frege proof systems capture the way we write proofs
goal: lower bounds on lengths of proofs in *Frege proof system*
known: lower bounds for *restricted* versions of Frege
this talk: algebraic proof systems

Subset Sum

Question (Subset Sum)

Given $a_1, \ldots, a_n, b \in \mathbb{C}$, *prove there is* **no** *subset* $S \subseteq [n]$ *such that* $\sum_{i \in S} a_i = b$.
Equivalently, prove there are **no** *solutions to*

$$x_1^2 - x_1 = \cdots = x_n^2 - x_n = 0,$$

$$a_1 x_1 + \cdots + a_n x_n - b = 0 \ .$$

Question is coNP-hard
NP $\neq$ coNP $\implies$ any proof must be long

goal: prove *unconditional* lower bounds on lengths of proofs in strong **algebraic** proof systems.

Nullstellensatz Proofs (i)

Let $\overline{f} := (f_1, \ldots, f_m)$ be a system of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$.

Theorem (Hilbert's Nullstellensatz)

The system $f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0$ *has no solution iff there are* $g_1, \ldots, g_m \in \mathbb{C}[\overline{x}]$ *such that*

$$g_1(\overline{x}) \cdot f_1(\overline{x}) + \cdots + g_m(\overline{x}) \cdot f_m(\overline{x}) = 1 \ .$$

Gives a *sound* and *complete* proof system for unsatisfiability.
complexity: simple unsatisfiable $\overline{f}$ can require $\deg \overline{g} \geq \exp(m)$.
but: coNP-statements concern $\overline{x} \in \{0,1\}^n$ — polynomials over $\{0,1\}^n$ are degree $\leq n$.

Nullstellensatz Proofs (ii)

$\overline{f} := (f_1, \ldots, f_m)$, $\overline{x}^2 - \overline{x} := (x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

Theorem (Boolean Nullstellensatz)

The system $\overline{f} = \overline{0}$ has no solution over $\overline{x} \in \{0,1\}^n$
$\Leftrightarrow$ *the system $\overline{f}, \overline{x}^2 - \overline{x}$ is unsatisfiable*
$\Leftrightarrow$ *there are $g_1, \ldots, g_m, h_1, \ldots, h_n \in \mathbb{C}[\overline{x}]$ such that*

$$\sum_j g_j(\overline{x}) \cdot f_j(\overline{x}) + \sum_i h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1 \, .$$

complexity: $\deg \overline{g}, \overline{h} \leq O(n)$, $\overline{g}, \overline{h}$ have $\leq 2^{O(n)}$ monomials
goal: prove lower bound on the complexity of $\overline{g}, \overline{h}$.
prior work ([BIK+96a, CEI96, BIK+96b, Raz98, Gri98, IPS99, BGIP01, AR01,...]): exhibit simple $\overline{f}$ where

- $\deg \overline{g}, \overline{h} \geq \Omega(n)$
- $\overline{g}, \overline{h}$ require $2^{\Omega(n)}$ monomials

Algebraic Complexity Measures

Degree and number of monomials are *weak* measures for complexity

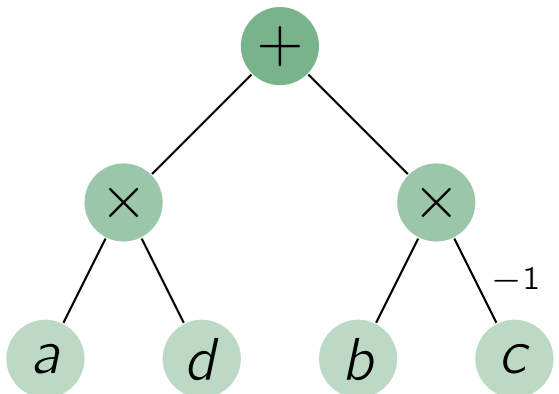
More interesting measure: size of representation in interesting algebraic models

this talk: study Ideal Proof System (IPS) that looks at more interesting measures of complexity

next: Algebraic models and Grochow-Pitassi IPS proof system

Algebraic Formulas

Algebraic formulas are a succinct model of computation for polynomials, e.g. $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ can be given by



size: number of edges
depth: length of longest input-output path
known: [Kalorkoti85] $\Omega(n^2)$ lower bound for algebraic formulas

The Ideal Proof System (IPS) (i)

$\overline{f} := (f_1, \ldots, f_m)$, $\overline{x}^2 - \overline{x} := (x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

Definition ([GrochowPitassi14])

A *formula*-IPS proof of $\overline{f}, \overline{x}^2 - \overline{x}$ is a pair $(\overline{g}, \overline{h})$ such that

- $\sum g_j f_j + \sum h_i \cdot (x_i^2 - x_i) = 1$
- the size of the proof is the formula size of g_j, h_i

- proof verification: via *Polynomial Identity Testing*, only randomized algorithms known in general.

goal: prove lower bounds for interesting $\overline{f}$

How realistic is this goal?

The Ideal Proof System (IPS) (ii)

Theorem ([GrochowPitassi14])

Let CNF $C = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ be unsatisfiable and encoded by the equations $f_1, \ldots, f_m, \overline{x}^2 - \overline{x}$. Then there are $\overline{g}, \overline{h}$ such that

$$\sum_j g_j \cdot f_j + \sum_i h_i \cdot (x_i^2 - x_i) = 1, \quad \textit{where}$$

- *If there is a size-s Frege proof that C is unsatisfiable, then there are $\overline{g}, \overline{h}$ with $\mathrm{poly}(n, m, s)$-size algebraic formulas.*
- *There are $\overline{g}, \overline{h}$ in $\mathsf{VNP} \approx \{$explicit polynomials$\}$.*

Corollary

- *formula-IPS as powerful as Frege*
- *lower bounds for CNFs $\Longrightarrow$ lower bounds for the permanent*

goal: prove lower bounds for restricted, yet interesting and powerful, algebraic models

The Ideal Proof System (IPS) (iii)

$\overline{f} := (f_1, \ldots, f_m)$, $\overline{x}^2 - \overline{x} := (x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

Definition ([GrochowPitassi14])

For an algebraic model $\mathcal{C}$, a $\mathcal{C}$-IPS proof of $\overline{f}, \overline{x}^2 - \overline{x}$ is a pair $(\overline{g}, \overline{h})$ such that

- $\sum g_j f_j + \sum h_i \cdot (x_i^2 - x_i) = 1$
- the size of the proof is the maximum size of the g_j, h_i as $\mathcal{C}$-computations.

goal: prove lower bounds for $\mathcal{C}$-IPS for interesting $\mathcal{C}$

Multilinear Formulas

Definition

A polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ is **multilinear** if the individual degree of each variable x_i is at most 1, that is

$$f(\overline{x}) = \sum_{S \subseteq [n]} \alpha_S \prod_{i \in S} x_i$$

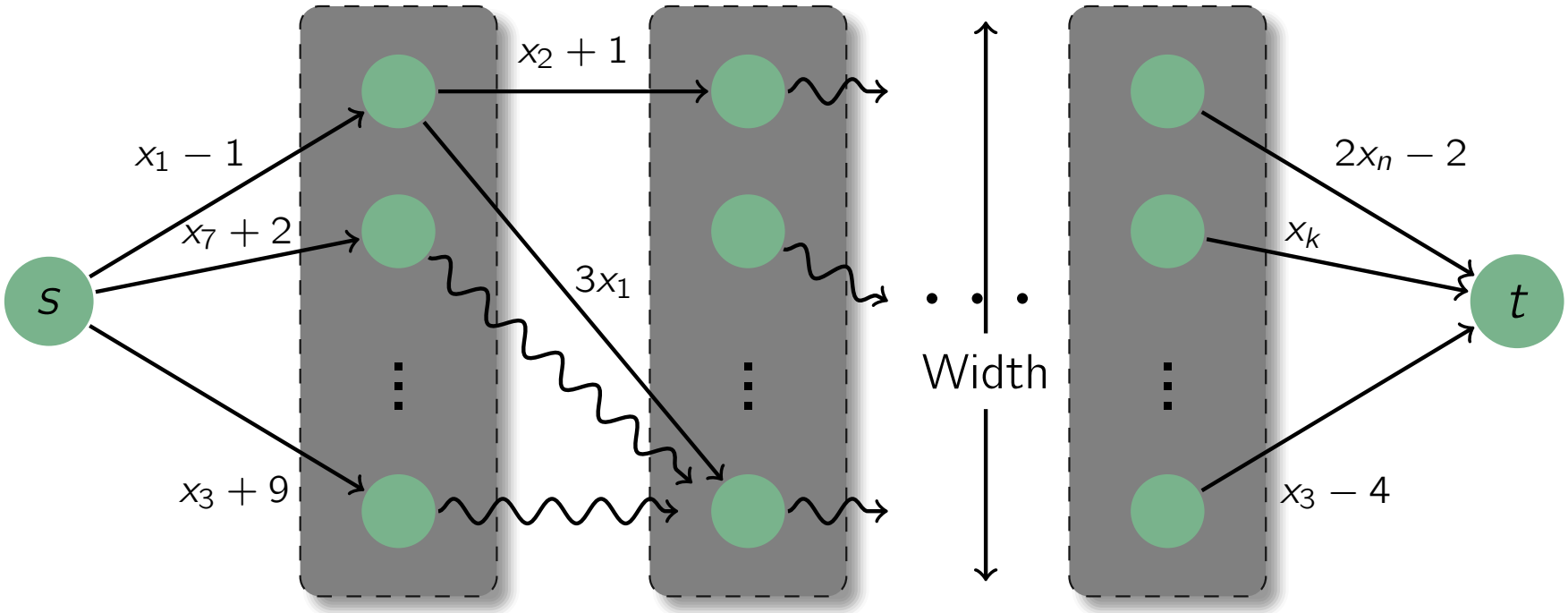
A formula is multilinear if each gate is multilinear

- multilinear polynomials uniquely determined by evaluations over $\{0,1\}^n$

known: [Raz04,RY09]: permanent and determinant require $n^{\Omega(\lg n)}$-size multilinear formulas, $2^{n^{\Omega(1)}}$-size constant-depth multilinear formulas

goal: prove lower bounds for multilinear-formula-IPS

Algebraic Branching Programs



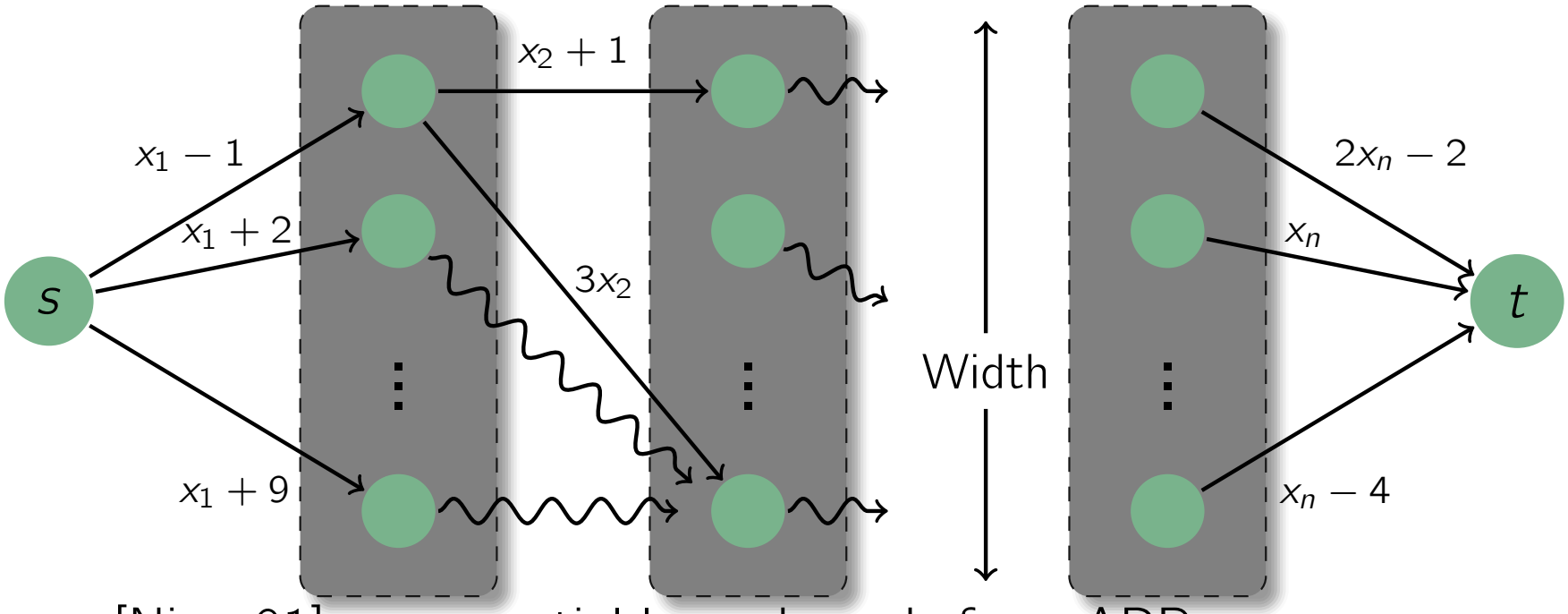
- each $s \to t$ path computes multiplication of edge labels
- program computes the sum of those over all $s \to t$ paths
- output is the $(1,1)$ entry of the matrix product $\prod_{i=1}^{n} M_i(\overline{x})$ (M_i is adjacency matrix of graph on layers $i, i+1$)

goal: prove lower bounds for ABP-IPS

problem: ABPs more expresfull than formulas

Read-Once Oblivious ABPs (i)

read-once oblivious ABP (roABP): every variable appears in one layer



- [Nisan91]: exponential lower bounds for roABPs
- [R**S**05]: polynomial time PIT for roABPs
- [F**S**13,AGKS14,FS**S**14] quasi-poly *black-box* PIT for roABPs

goal: prove lower bounds for roABP-IPS

Recap

Nullstellensatz proof system: proof of unsatisfiability of $\overline{f}, \overline{x}^2 - \overline{x}$ is $\overline{g}, \overline{h}$ such that

$$\sum_j g_j(\overline{x}) \cdot f_j(\overline{x}) + \sum_i h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1$$

IPS: each g_j, h_i has "small" $\mathcal{C}$-computation

Algebraic classes:

- multilinear formulas
- read-once oblivious Algebraic Branching Programs (roABPs)

Next: our results and some proofs

Our Results: Upper Bounds

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$, is unsatisfiable subset-sum instance

Theorem ([ImpagliazzoPudlákSgall99])

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$ *requires Nullstellensatz refutations of*

- *degree* $\geq \Omega(n)$.
- $2^{\Omega(n)}$*-monomials.*

Related to Pigeonhole Principle, well-known "hard" principle

Theorem (Upper Bounds for Subset-Sum)

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$ *has a* poly(n)*-size* $\mathcal{C}$*-IPS proof for* $\mathcal{C} =$

- *depth-3 multilinear formulas*
- *read-once oblivious algebraic branching programs (roABPs)*

Strengthens related upper bounds of [GH03,RT08]

Our Results: Lower Bounds

Theorem (Lower Bounds for Subset-Sum Variants)

$\sum_{i<j} z_{i,j} x_i x_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$ *requires*

- *multilinear-formula-IPS proofs of* $n^{\Omega(\lg n)}$*-size*
- *constant-depth-multilinear-formula-IPS proofs of* $2^{n^{\Omega(1)}}$*-size*
- *roABP-IPS proofs of* $2^{\Omega(n)}$*-size (in every order)*

First such lower bounds, matches much of the frontier of lower bounds in algebraic complexity theory

Proven via *functional lower bounds*.

Functional Lower Bounds

circuit complexity: single polynomial requires large formulas
proof complexity: *every* proof requires large formulas
idea: if "*unique*" proof then only study single polynomial

Consider an unsatisfiable system $f(\overline{x}), \overline{x}^2 - \overline{x}$, with proof

$$g(\overline{x}) \cdot f(\overline{x}) + \sum_i h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1$$

This implies

$$g(\overline{x}) \cdot f(\overline{x}) = 1, \qquad \overline{x} \in \{0,1\}^n$$
$$g(\overline{x}) = {}^1\!/\!_{f(\overline{x})}, \qquad \overline{x} \in \{0,1\}^n$$

$\Longrightarrow$ g unique as a *function* over $\{0,1\}^n$ or as *multilinear* polynomial

goal: find *easy* $f(\overline{x})$ so **any** g with $g|_{\{0,1\}^n} = \frac{1}{f}|_{\{0,1\}^n}$ is *hard*
need: proof techniques that works in the functional setting and not just for syntactic polynomials (e.g. partial derivative method)

Structure of Proof

Theorem (Lower Bounds for Subset-Sum Variants)

$\sum_{i<j} z_{i,j} x_i x_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$ *requires*

- *multilinear-formula-IPS proofs of* $n^{\Omega(\lg n)}$*-size*
- *constant-depth-multilinear-formula-IPS proofs of* $2^{n^{\Omega(1)}}$*-size*
- *roABP-IPS proofs of* $2^{\Omega(n)}$*-size (in every order)*

Proof.

- prove functional lower bound for *degree*
- "lift" to functional lower bound for *evaluation dimension*
- conclude functional lower bound for circuit classes via known relations to evaluation dimension
- conclude IPS lower bounds □

Functional Lower Bound — Degree

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$

Proposition

Let $g \in \mathbb{C}[\overline{x}]$ *such that*

$$g(\overline{x}) = \frac{1}{x_1 + \cdots + x_n + 1}, \qquad \overline{x} \in \{0,1\}^n$$

Then $\deg g \geq n$

Tight. Strengthens prior $\deg g \geq n/2$ [IPS99].

Proof.

- multilinearize: $g \mapsto \mathrm{ml}(g)$ with $g|_{\{0,1\}^n} = \mathrm{ml}(g)|_{\{0,1\}^n}$, and $\deg g \geq \deg \mathrm{ml}(g)$
- $\mathrm{ml}(g)$ uniquely determined, compute it explicitly, $\deg \mathrm{ml}(g) = n$ □

Evaluation Dimension

$g \in \mathbb{C}[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Study interaction between $\overline{x}$ and $\overline{y}$

Definition ([Nis91,Sap12,FS**13b])**

The **set of evaluations** of g is

$$\mathbf{Eval}_{\overline{x}|\overline{y}}(g) := \{g(\overline{x}, \overline{b})\}_{\overline{b} \in \{0,1\}^n} \subseteq \mathbb{C}[\overline{x}]$$

The **evaluation dimension** of g is $\dim_{\mathbb{C}} \mathbf{Eval}_{\overline{x}|\overline{y}}(g)$

Well-studied complexity measure, (implicitly) used for many lower bounds:

- multilinear formulas [Raz04,RY09,...]
- non-commutative ABPs, roABPs [Nisan91,F**S**13,...]
- depth-3 powering formulas [Saxena08,F**S**13,...]

Functional Lower Bound — Evaluation Dimension

$\sum_{i=1}^{n} x_i y_i + 1, \overline{x}^2 - \overline{x}, \overline{y}^2 - \overline{y}$

Proposition

$g(\overline{x}, \overline{y}) = \frac{1}{\sum_i x_i y_i + 1}$ *for* $\overline{x}, \overline{y} \in \{0,1\}^n$, *then* $\dim \mathbf{Eval}_{\overline{x}|\overline{y}}(g) \geq 2^n$

Proof.

- $\mathbf{Eval}_{\overline{x}|\overline{y}}(g) = \{g(\overline{x}, \overline{b})\}_{\overline{b} \in \{0,1\}^n} = \{g(\overline{x}, \mathbb{1}_S)\}_{S \subseteq \{0,1\}^n}$
- For $\overline{x} \in \{0,1\}^n$, $g(\overline{x}, \mathbb{1}_S) = \frac{1}{\sum_{i \in S} x_i + 1}$
- $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))$ has degree $|S|$
- $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S)) = \prod_{i \in S} x_i + (\text{lower terms})$
- $\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))$ linearly independent

$$\dim \mathbf{Eval}_{\overline{x}|\overline{y}}(g) \geq \dim \mathrm{ml}(\mathbf{Eval}_{\overline{x}|\overline{y}}(g)) = \dim \{\mathrm{ml}(g(\overline{x}, \mathbb{1}_S))\}_{S \subseteq [n]}$$
$$= \dim \left\{ \prod_{i \in S} x_i + (\text{lower terms}) \right\}_S = 2^n \qquad \square$$

Lower Bounds for IPS

Theorem (Lower Bounds for Subset-Sum Variants)

$\sum_{i<j} z_{i,j} x_i x_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$ *requires*

- *multilinear-formula-IPS proofs of* $n^{\Omega(\lg n)}$*-size*
- *constant-depth-multilinear-formula-IPS proofs of* $2^{n^{\Omega(1)}}$*-size*
- *roABP-IPS proofs of* $2^{\Omega(n)}$*-size*

Proof.

- degree $\geq n$ functional lower bound for $\frac{1}{\sum_i x_i + 1}$
- $\dim \mathbf{Eval}_{\overline{x}|\overline{y}} \geq 2^n$ functional lower bound for $\frac{1}{\sum_i x_i y_i + 1}$
- $\dim \mathbf{Eval}_{\overline{v}|\overline{u}} \geq 2^{n/2}$ functional lower bounds for $\frac{1}{\sum_{i<j} z_{i,j} x_i x_j + 1}$, for any equipartition $\overline{x} = \overline{v} \cup \overline{u}$
- implies lower bounds for the mentioned circuit classes $\square$

Upper Bounds for IPS (i)

Theorem (Upper Bounds for Subset-Sum)

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$ *has a* poly(n)*-size* $\mathcal{C}$*-IPS proof for* $\mathcal{C} =$

- *depth-3 multilinear formulas*
- *read-once oblivious algebraic branching programs (roABPs)*

Proof.

- Let $p(t) = \prod_{i=0}^{n}(t - i)$
- Then, $p(\sum x_i) = 0$ for $\overline{x} \in \{0,1\}^n$
- Equivalently, $p(\sum x_i) = 0$ modulo $\overline{x}^2 - \overline{x}$
- Note $\frac{p(t)-p(-1)}{t-(-1)} = q(t)$ for some polynomial q
- $q(\sum x_i)(\sum x_i + 1) = p(\sum x_i) - p(-1) \equiv -p(-1) \neq 0$ □

Are we really done?

Upper Bounds for IPS (ii)

Showed that for $p(t) = \prod_{i=0}^{n}(t-i)$ and $q(t) = \frac{p(t)-p(-1)}{t-(-1)}$,

$$q\left(\sum x_i\right)\left(\sum x_i + 1\right) = p\left(\sum x_i\right) - p(-1) \equiv -p(-1) \neq 0$$

To show poly(n)-size $\mathcal{C}$-IPS proofs we need

$$q(\overline{x})\left(\sum x_i + 1\right) + \sum_{i=1}^{n} h_i(\overline{x})(x_i^2 - x_i) = 1 \text{ , where}$$

- $q(\sum x_i)$ has short $\mathcal{C}$-computations
- can efficiently multilinearize $q(\overline{x})\,(\sum x_i + 1)$ in $\mathcal{C}$ (this gives $\overline{h}$)

Proposition

$$q(\sum x_i) = \sum_{i=1}^{\text{poly}(n)} \prod_{j=1}^{n}(a_{i,j}x_j + b_{i,j})$$

Can express this as small roABP and depth-3 multilinear formula and not too difficult to multilinearize □

Conclusions

this talk:

- upper bounds for proving unsatisfiability of $\sum_i x_i + 1, \overline{x}^2 - \overline{x}$
  - depth-3 multilinear formulas
  - read-once oblivious algebraic branching programs (roABPs)
- lower bounds for proving unsatisfiability of $\sum_{i<j} z_{i,j} x_i x_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$
  - multilinear-formula-IPS proofs of $n^{\Omega(\lg n)}$-size
  - constant-depth-multilinear-formula-IPS proofs of $2^{n^{\Omega(1)}}$-size
  - roABP-IPS proofs of $2^{\Omega(n)}$-size

open question:

- lower bounds for unsatisfiability of $f_1, \ldots, f_m, \overline{x}^2 - \overline{x}$ where each f_i depends on $o(n)$ many variables ?

TOC