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 1, 2016

Subset Sum

Question (Subset Sum)

Given $\alpha_1, \ldots, \alpha_n, \beta \in \mathbb{C}$*, prove there is* **no** *subset* $S \subseteq [n]$ *with the sum* $\sum_{i \in S} \alpha_i = \beta$*? Equivalently, prove there are* **no** *solutions to*

$$0 = x_1^2 - x_1 = \cdots = x_n^2 - x_n = \alpha_1 x_1 + \cdots + \alpha_n x_n - \beta \ .$$

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

Theorem (Hilbert's Nullstellensatz)

The system $f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0$ *has no solution iff there are* $g_1, \dots, g_m \in \mathbb{C}[\overline{x}]$ *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: only weak bounds for $\overline{g}$ in general, ex: 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 $\overline{x} \in \{0,1\}^n$ iff the system $\overline{f}, \overline{x}^2 - \overline{x}$ is unsatisfiable iff 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 at most $2^{O(n)}$ monomials

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

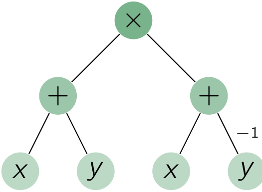
Nullstellensatz Proofs (iii)

Theorem ([GrochowPitassi14])

Let CNF $C = C_1 \wedge \cdots \wedge C_m$ be unsatisfiable and be encoded by the equations $f_1, \ldots, f_m, \overline{x}^2 - \overline{x}$. Then there are $\overline{g}, \overline{h}$ such that $\sum_j g_j \cdot f_j + \sum_i h_i \cdot (x_i^2 - x_i) = 1$, where

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

Algebraic formulas are a succinct model of computation for polynomials, e.g. $x^2 - y^2 = (x + y)(x - y)$ can be given by



The Ideal Proof System (IPS)

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

Definition ([GrochowPitassi14])

A size-s **(linear) Ideal Proof System (IPS)** proof of unsatisfiability of $\overline{f}, \overline{x}^2 - \overline{x}$ using $\mathcal{C}$-computations is $\overline{g}, \overline{h}$ where

- $\sum_j g_j(\overline{x}) \cdot f_j(\overline{x}) + \sum_i h_i(\overline{x}) \cdot (x_i^2 - x_i) = 1$.
- each g_j, h_i is size-s $\mathcal{C}$-formula.

- proof verification: via *Polynomial Identity Testing*, only randomized algorithms known in general.
- [GP14]: formula-IPS is as powerful as Frege.
- [GP14]: lower bounds for $\mathcal{C}$-proofs of CNFs $\implies$ lower bounds for $\mathcal{C}$-computations of the permanent
- [FTL15]: *non-commutative* formula-IPS is equivalent to Frege.

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.

- A multilinear polynomial is uniquely determined by evaluations over $\{0,1\}^n$.
- [Raz04,RY09]: permanent and determinant require $n^{\Omega(\lg n)}$-size multilinear formulas, $2^{n^{\Omega(1)}}$-size constant-depth multilinear formulas
- [RT08]: defined proof system based on multilinear formulas, short proofs for pigeonhole principle, etc.

goal: prove lower bounds for multilinear-formula-IPS.

Our Results

$x_1 + \cdots + x_n + 1, \overline{x}^2 - \overline{x}$, 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* $\mathrm{poly}(n)$*-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 (ii)

Theorem (Lower Bounds for Subset-Sum Variants)

$\sum_{i<j} z_{i,j}x_ix_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$ 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

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

$$\begin{aligned} g(\overline{x}) \cdot f(\overline{x}) &= 1, & \overline{x} &\in \{0,1\}^n \\ g(\overline{x}) &= 1/f(\overline{x}), & \overline{x} &\in \{0,1\}^n \end{aligned}$$

$\implies$ g unique as a *function* or as *multilinear* polynomial.

goal: find *easy* $f(\overline{x})$ so <u>any</u> g with $g|_{\{0,1\}^n} = \frac{1}{f}|_{\{0,1\}^n}$ is *hard*.
A type of *functional lower bound* [GR00,**F**KS15].

Our Results (iii)

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

$f \in \mathbb{C}[\overline{x}]$. *If*

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

then $\deg f \geq n$.

Tight. Strengthens prior $\deg f \geq {}^{n}/_{2}$ [IPS99].

Proof.

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

Evaluation Dimension

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

Definition ([Nis91,Sap12,FS13b])

The **set of evaluations** of f is

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

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

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

- multilinear formulas [Raz04,RY09,...]
- non-commutative ABPs, roABPs [Nisan91,**F**S13b,...]
- depth-3 powering formulas [Saxena08,**F**S13b,...]

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

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

Proof.

- $\mathbf{Eval}_{\overline{x}|\overline{y}}(f) = \{f(\overline{x}, \overline{\beta})\}_{\overline{\beta} \in \{0,1\}^n}$.
- For $\overline{x} \in \{0,1\}^n$, $f(\overline{x}, \overline{\beta}) = \frac{1}{\sum_i x_i \beta_i + 1} \overset{\overline{\beta} \leftrightarrow S}{=} \frac{1}{\sum_{i \in S} x_i + 1}$
- $\mathrm{ml}(f(\overline{x}, S))$ has degree $\leq |S|$, $\geq |S| \implies$ $\mathrm{ml}(f(\overline{x}, S)) = \prod_{i \in S} x_i + (\text{lower terms})$.
- $\mathrm{ml}(f(\overline{x}, S))$ triangular system $\implies$ linearly independent.

$$\dim \mathbf{Eval}_{\overline{x}|\overline{y}}(f) \geq \dim \mathrm{ml}(\mathbf{Eval}_{\overline{x}|\overline{y}}(f)) = \dim \{\mathrm{ml}(f(\overline{x}, S))\}_{S \subseteq [n]}$$

$$= \dim \left\{ \prod_{i \in S} x_i + (\text{lower terms}) \right\}_S = 2^n . \qquad \square$$

Our Results (iv)

Theorem (Lower Bounds for Subset-Sum Variants)

$\sum_{i<j} z_{i,j}x_ix_j + 1, \overline{x}^2 - \overline{x}, \overline{z}^2 - \overline{z}$ 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.

- 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 $\frac{1}{\sum_i x_i y_i + 1}$
- symmetrize to get functional lower bound for $\frac{1}{\sum_{i<j} z_{i,j}x_ix_j + 1}$
- invoking existing relations to restricted circuit classes
- convert functional lower bound to IPS lower bound □

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 (in every order)

Other results:

- "non-linear" IPS = "linear" IPS
- lower bounds for multiples: if f requires large formulas, does $g \cdot f$ for every non-zero g?

Open Questions:

- Lower bounds for unsatisfiability of $f_1, \ldots, f_m, \overline{x}^2 - \overline{x}$ with $m > 1$?