Proof complexity and arithmetic circuits

Pavel Hrubeš

Institute of Mathematics, Prague

$\mathbb{F}$ a fixed underlying field.

Arithmetic circuit: computes a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$. It starts from variables and field elements and computes f by means of operations $+$ and $\times$.

- It is a directed acyclic graph. Leaves labelled with variables or field elements. Inner nodes have in-degree 2 and are labelled with $+, \times$.
- *Size* - number of operations.
- *Depth* - the length of a longest directed path.
- *Formula* - the underlying graph is a tree.

Class VP: polynomials of polynomial size and degree.

Class VNP: Boolean sums over polynomials in VP.

$$\sum_{z \in \{0,1\}^m} f(z, x_1, \ldots, x_n).$$

I. Polynomial Identity Testing

Polynomial Identity Testing: given an arithmetic circuit F, accept iff F computes the zero polynomial.

- Typically, $\mathbb{F}$ is $\mathbb{Q}$ or a finite field.
- PIT $\in$ coRP. (Schwarz-Zippel lemma)
- Not known to be in P or even NSUBEXP.
- If PIT has non-deterministic subexponential algorithm then we have new circuit lower bounds [Kabanetz & Impagliazzo'04]
- Deterministic poly-time algorithm for non-commutative formulas [Raz & Shpilka'05].
- Deterministic poly-time algorithm for $\Sigma\Pi\Sigma$-circuits with constant top fan-in [Dvir&Shpilka'05, Kayal& Saxena'07,...]

Question: is PIT in NP?

We want a polynomial-size witness (or, a proof) that F equals zero.

Question: can we efficiently prove that $F = 0$ by means of syntactic manipulations?

Example of a syntactic algorithm:

Open all brackets in F and see if everything cancels.

The DS algorithm

A $\Sigma\Pi\Sigma$-circuit:

$$F = F_1 + \cdots + F_k \,,$$

where $F_i = \prod_{j=1}^{d} L_{ij}$ and L_{ij} are linear.

- F is *simple* if no L_{ij} divides every F_i.
- F is *minimal* if no proper subset of F_i sums to 0.
- *Rank of F*:= the rank of L_{ij}'s in F.

Theorem (Dvir & Shpilka'07).

Assume that F computes the zero polynomial and F is simple and minimal. Then rank of F is $\leq 2^{O(k^2)}(\log d)^{k-2}$.

Note: speaker reminded that stronger bounds are nowadays known.

The DS algorithm: find a basis of the L_{ij}'s and then open the brackets.

The PI system [H&Tzameret] called $\mathbb{P}_f(\mathbb{F})$

- A proof-line is an equation $F = G$ where F, G are arithmetic formulas.
- The inference rules are

$$\frac{F = G}{G = F}\,, \quad \frac{F = G\,,\ G = H}{F = H}\,, \quad \frac{F_1 = G_1\,,\ F_2 = G_2}{F_1 \star F_2 = G_1 \star G_2}\,, \text{ where } \star = +, \cdot$$

- The axioms are

$$\begin{array}{ll}
F = F & F + G = G + F \\
F + (G + H) = (F + G) + H & F \cdot G = G \cdot F, \\
F \cdot (G \cdot H) = (F \cdot G) \cdot H & F \cdot (G + H) = F \cdot G + F \cdot H \\
F + 0 = F & F \cdot 0 = 0 \\
F \cdot 1 = F & \\
a = b + c\,, a' = b' \cdot c'\,, & \text{if true in } \mathbb{F}.
\end{array}$$

circuit-PI system: work with formulas instead of circuits.

- Both systems are sound and complete: $F = G$ has a proof iff F and G compute the same polynomial.
- PI system is an arithmetic analogy of Frege and circuit-PI of Extended Frege.
- Over GF(2), Frege resp. Extended Frege are equivalent to the PI systems with axioms $x_1^2 = x_1, \ldots, x_n^2 = x_n$.
- The PI-system can simulate the DS algorithm.

Open problem: Is the PI or circuit-PI system polynomially bounded?

The PI systems can simulate classical results in arithmetic circuit complexity.

- Strassen's elimination of divisions.
- Homogenization.
- Balancing.

[VSBR'83]: *If a polynomial of degree d has circuit of size s then it has circuit of size poly(s, d) and depth $O(\log s(\log s + \log d))$.*

Theorem.
Assume that $F = 0$ has a circuit-PI proof of size s and F has depth k and (syntactic) degree d. Then $F = 0$ has a proof of size poly(s, d) in which every circuit has depth $O(k + \log s(\log s + \log d))$.

- Hence, PI quasi-polynomially simulates circuit-PI.
- Applied to construct quasi-polynomial PI (and hence Frege) proofs of linear algebra based tautologies.

$$AB = I_n \rightarrow BA = I_n\,, \text{ for } A, B \in M_{n\times n}(\mathbb{F})\,.$$

II. Ideal membership problems

General setting

Let $f, f_1, \ldots, f_k$ be polynomials such that $f \in I(f_1, \ldots, f_k)$. I.e., there exist $g_1, \ldots, g_k$ with

$$f = f_1 g_1 + \ldots f_k g_k \,. \tag{1}$$

What can we say about the complexity of $g_1, \ldots, g_k$?

- $g_1, \ldots, g_k$ is *a certificate* for $f \in I(f_1, \ldots, f_k)$
- define $\mathrm{IC}(f \mid\mid f_1, \ldots, f_k)$ as the smallest s so that there exists $g_1, \ldots, g_k$ satisfying (1) which can be (simultaneously) computed by an arithmetic circuit of size s.

1. Effective nullstellensatz

Nullstellensatz. *Let* $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$. *If* $f_1 = 0, \ldots, f_k = 0$ *have no common solution in* $\bar{\mathbb{F}}$ *then there exist* $g_1, \ldots, g_k \in \mathbb{F}[x_1, \ldots, x_n]$ *such that*

$$1 = f_1 g_1 + \cdots + f_k g_k \,.$$

- One can view $g_1, \ldots, g_k$ as a *proof* that $f_1, \ldots f_k = 0$ has no solution.

Strong nullstellensatz. *If every solution to* $f_1, \ldots, f_k = 0$ *satisfies* $f = 0$ *then there exists* $r \in \mathbb{N}$ *and polynomials* $g_1, \ldots, g_k$ *with*

$$f^r = f_1 g_1 + \cdots + f_k g_k \,.$$

Nullstellensatz. *Let* $f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$*. If* $f_1 = 0, \ldots, f_k = 0$ *have no common solution in* $\bar{\mathbb{F}}$ *then there exist* $g_1, \ldots, g_k \in \mathbb{F}[x_1, \ldots, x_n]$ *such that*

$$1 = f_1 g_1 + \cdots + f_k g_k \,.$$

- For every i,

  $$\deg(f_i g_i) \leq \max(d, 3)^{\min(n,k)} \,,$$

  where d is the maximum degree of f_i. [Kollár'88, Brownawell' 87,...]
- This is tight if $d \geq 3$: there exist $f_1, \ldots f_n$ of degree d such that

  $$\max \deg(f_i g_i) \geq d^n \,.$$

  [Maser& Philippon]

$\mathrm{IC}(1 \parallel f_1, \ldots, f_k)$ is the smallest circuit complexity of $g_1, \ldots, g_k$ with $1 = \sum_{i=1}^{k} f_i g_i$.

Open question: can we find $f_1, \ldots, f_k$ with $1 \in I(f_1, \ldots, f_k)$ so that $\mathrm{IC}(1 \parallel f_1, \ldots, f_k)$ is super-polynomial in the circuit complexity of $f_1, \ldots, f_k$?

- Expect ”yes", unless $\mathrm{coNP} \subseteq \mathrm{NP}^{\mathrm{PIT}}$.

Observation: If measuring *formula* size, the answer is "yes".

Proof.
Exponential degree. $\square$

Nullstellensatz as a decision problem: given $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$, decide if $f_1 = 0, \ldots, f_k = 0$ has a solution in $\mathbb{C}^n$.

- The problem is in PSPACE
- Assuming GRH, it is in AM ($\subseteq \Pi_2$) [Koiran'96].

2. Ideal membership

Theorem[Hermann'26]. *Assume that* $f \in I(f_1, \ldots, f_k)$ *where* $f, f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$ *and* $\deg f_1, \ldots, \deg f_k \leq d$*. Then there exist* $g_1, \ldots, g_k$ *with*

$$f = f_1 g_1 + \cdots + f_k g_k$$

having degree at most $\deg(f) + (kd)^{2^n}$*.*

- This is asymptotically tight [Mayr& Mayer' 82].
- The *Ideal Membership Problem*: given $f, f_!, \ldots, f_k$, decide if $f \in I(f_1, \ldots, f_k)$. Is EXPSPACE hard.

Question: can we find $f, f_1, \ldots, f_k$ so that $f \in I(f_1, \ldots, f_k)$ and $\mathrm{IC}(f \mid\mid f_1, \ldots, f_k)$ is exponential in the circuit complexity of $f, f_1, \ldots, f_k$?

Answer: yes.

Proof.
Doubly-exponential degree. $\square$

Open question: Can we prove this if there exist witnesses $g_1, \ldots, g_k$ of degree polynomial in the maximum degree of $f, f_1, \ldots, f_k$?

Toy example.
$f \in I(f_1)$. $f = f_1 g_1$, and hence $g_1 = f/f_1$.

- If a polynomial g of degree d can be computed by a circuit of size s using *division gates* then it can be computed by circuit of size $s \cdot \mathrm{poly}(d)$ *without* division gates. [Strassen]
- Hence, $\mathrm{IC}(f \mid\mid f_1)$ is polynomial in $\deg(f) - \deg(f_1)$ and the circuit size of f, f_1.

Open question: In Strassen's elimination algorithm, can we replace $s \cdot \mathrm{poly}(d)$ by $\mathrm{poly}(s, \log d)$?

Monomial ideals.

$$f := (x_{11}z_1 + \cdots + x_{1n}z_n)(x_{21}z_1 + \cdots + x_{2n}z_n)\cdots(x_{n1}z_1 + \cdots + x_{nn}z_n)\,.$$

Let Z be the set of $n+1$ monomials

$$\prod_{i=1}^{n} z_i\,,\quad z_1^2, \ldots, z_n^2\,.$$

$$\mathrm{perm}_n = \sum_{\pi \in S_n} \left(x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)}\right).$$

Proposition 1.
$f \in I(Z)$. $IC(f \parallel Z)$ is at least the circuit complexity of perm_n.

$$f = (x_{11}z_1+\cdots+x_{1n}z_n)(x_{21}z_1+\cdots+x_{2n}z_n)\cdots(x_{n1}z_1+\cdots+x_{nn}z_n)\,.$$

$$Z = \{\prod_{i=1}^{n} z_i\,,\ z_1^2,\ldots,z_n^2\}\,.$$

- $$f \in I(Z): \qquad f - \mathrm{perm}_n \cdot (\prod_{i=1}^{n} z_i) \in I(z_1^2,\ldots,z_n^2)\,.$$

- $$\text{Assume} \qquad f - g \cdot (\prod_{i=1}^{n} z_i) \in I(z_1^2,\ldots,z_n^2)\,.$$

  Write $g = g_0 + h$ with $g_0 := g(z_1,\ldots,z_n/0)$ and $h \in I(z_1,\ldots,z_n)$.

  $$(g_0 + h - \mathrm{perm}_n)\cdot \prod_i z_i \in I(z_1^2,\ldots,z_n^2)\,,$$

  $$(g_0 - \mathrm{perm}_n)\cdot \prod z_i \in I(z_1^2,\ldots,z_n^2) \ \text{ and } g_0 = \mathrm{perm}_n\,.$$

3. Polynomial calculus

Nullstellensatz as a proof system

View $g_1, \dots, g_k$ with

$$1 = g_1 f_1 + \cdots + g_1 f_k$$

as a proof of unsatisfiability of $f_1, \dots, f_k = 0$.

- $f_1, \dots, f_k$ include Boolean axioms $x_1^2 - x_1, \dots, x_n^2 - x_n$ and typically have constant degree. E.g., translation of a 3CNF.
- Complexity measured as the degree of $g_1, \dots, g_k$ or the number of monomials.

Polynomial Calculus [Clegg, Edmonds & Impagliazzo'96]

We want to show that $f_1, \dots, f_k = 0$ has no solution by deriving 1 from $f_1, \dots, f_k$. The rules are

$$\frac{f}{xf}, x \text{ a variable} \quad , \qquad \frac{f \,,\; g}{af + bg} \quad a, b \in \mathbb{F}\,.$$

- Complexity is measured as the maximum degree of a line in the refutation.
- PC is strictly stronger than Nullstellensatz.

The Pigeon Hole Principle $\neg\mathrm{PHP}_n^m$: variables x_{ij}, $i \in [m]$, $j \in [n]$

$$\sum_{j\in[n]} x_{ij} - 1\,,\ \ i \in [m]$$

$$x_{i_1 j} x_{i_2 j}\,,\ i_1 \neq i_2 \in [m], j \in [n]\,,$$
$$x_{ij_1} x_{ij_2}\,,\ i \in [m], j_1 \neq j_2 \in [m]\,.$$

- Polynomials in $\neg\mathrm{PHP}_n^m$ do not have a common zero if $m > n$.

Theorem (Razborov'98).

Every Polynomial Calculus refutation of $\neg PHP_n^m$ with $m > n$ (including the polynomials $x_{ij}^2 - x_{ij}$) has degree at least $n/2 + 1$.

- Lower bound on number of monomials in PC [Impagliazzo & al.'99].
  - PHP refutation requires $2^{\Omega(n)}$ monomials.
  - In general, a refutation with few monomials can be converted to a low-degree refutation.
- Random $k - CNF$'s require large degree. [Ben-Sasson& Impagliazzo'99, Alekhnovich& Razborov'03]
- Polynomial Calculus with Resolution [Alekhnovich & al.'02]
- ...

Proposition 2.

Assume that $f_1 = 0, \ldots, f_k = 0$ *has PC refutation with s lines. Then there exist* $g_1, \ldots, g_k$ *with*

$$1 = f_1 g_1 + \cdots + f_k g_k$$

such that every g_i *has circuit of size* $O(s)$ *and degree* $\leq s$*.*

- Hence, *without the boolean axioms*, there exist n equations of degree 2 which require PC refutation with 2^n lines.

4. The Boolean ideal

Consider the ideal $I(x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

Boolean Nullstellensatz. *Assume that* $f \in \mathbb{F}[x_1, \dots, x_n]$ *vanishes on* $\{0,1\}^n$. *Then* $f \in I(x_1^2 - x_1, \dots, x_n^2 - x_n)$. *Moreover, there exist* $g_1, \dots, g_n$ *of degree at most* $\deg f - 2$ *such that* $f = \sum_{i=1}^n f_i g_i$.

- Special case of the so-called Combinatorial Nullstellensatz [Alon].

Boolean Nullstellensatz. *If f vanishes on $\{0,1\}^n$ then $f \in I(x_1^2 - x_1, \ldots, x_n^2 - x_n)$.*

Proof.

Define $\hat{f}_0, \hat{f}_1, \ldots, \hat{f}_n$, $g_1, \ldots, g_n$ as follows:
$\hat{f}_0 := f$. For $0 \le i < n$, $\hat{f}_i$ and g_i are the polynomials satisfying

$$\hat{f}_{i-1} = g_i \cdot (x_i^2 - x_i) + \hat{f}_i\,,\ \deg_{x_i} \hat{f}_i \le 1.$$

Hence,

$$\begin{aligned} f =&(\hat{f}_0 - \hat{f}_1) + (\hat{f}_1 - \hat{f}_2) + \cdots + (\hat{f}_{n-1} - \hat{f}_n) + \hat{f}_n = \\ =&g_1 \cdot (x_1^2 - x_1) + g_2 \cdot (x_2^2 - x_2) + \cdots + g_n \cdot (x_n^2 - x_n) + \hat{f}_n \end{aligned}$$

Hence, $\hat{f}_n$ also vanishes on $\{0,1\}^n$. Since $\hat{f}_n$ is multilinear, it equals zero. $\square$

Recall $\mathrm{IC}(f \mid\mid x_1^2 - x_1, \ldots, x_n^2 - x_n)$ is the smallest circuit complexity of $g_1, \ldots, g_n$ with $f = \sum_i (x_i^2 - x_i) g_i$.
Abbreviation: $\mathbf{x}^2 - \mathbf{x} = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\}$.

Open problem: Is there an f that vanishes on $\{0,1\}^n$ such that $\mathrm{IC}(f \mid\mid \mathbf{x}^2 - \mathbf{x})$ is super-polynomial in the circuit complexity of f?

- Think of $g_1, \ldots, g_n$ as a proof that $f = 0$ over $\{0,1\}^n$.
- Expected answer is "yes", unless unless coNP $\subseteq$ NP$^{\mathrm{PIT}}$.
- Open even assuming VP $\neq$ VNP

[Grochow & Pitassi'15] show *"certain proof complexity lower bounds imply arithmetic circuit lower bounds"*

Major open problem: prove super-polynomial lower bounds on the Frege or Extended Frege proof systems.

- Known for bounded-depth Frege in De Morgan basis [Ajtai'88, Beame & al.'93, ...]
- Open even for bounded-depth Frege with parity gates.

Arithmetic translations of Boolean circuits

Given a Boolean circuit A, define the polynomial A^* as follows: replace $u \wedge v$ by $u \cdot v$, $\neg u$ by $1 - u$, $u \vee v$ by $u + v - u \cdot v$ etc.

- A^* and A have the same circuit size (up to a constant factor)
- They agree on inputs from the boolean cube.
- $\mathrm{IC}({A^*}^2 - A^* \mid\mid \mathbf{x}^2 - \mathbf{x})$ is linear in the size of A.

- If $A = A_1 \wedge A_2 \wedge \cdots \wedge A_k$ then A^* is a product of $A_1^*, \ldots, A_k^*$. E.g., A is a 3-CNF, A^* is a product of polynomials of degree 3.
- A is unsatisfiable iff $A^* \in I(\mathbf{x}^2 - \mathbf{x})$
- Alternatively, A is unsatisfiable iff $1 \in I(A_1^* - 1, \ldots, A_k^* - 1, \mathbf{x}^2 - \mathbf{x})$

Claim. $\mathrm{IC}(\prod_{i=1}^k A_i^* \parallel \mathbf{x}^2 - \mathbf{x})$ and $\mathrm{IC}(1 \parallel A_1^* - 1, \ldots, A_k^* - 1, \mathbf{x}^2 - \mathbf{x})$ differ by at most an additive factor of $O(s)$, where s is the (boolean) complexity of $A_1, \ldots, A_k$.

Proposition 3.

Assume that $\neg A$ has an Extended Frege proof of size s. Then $IC(A^* \mid\mid \mathbf{x}^2 - \mathbf{x})$ is polynomial in s.

- Similarly for Frege when counting arithmetic formula size.
- Hence, lower bounds on arithmetic circuits in IC($\mid\mid$) imply proof complexity lower bounds.

Proposition 4.

Assume that $VP = VNP$. Then for every f vanishing on $\{0,1\}^n$, $IC(f \mid\mid \mathbf{x}^2 - \mathbf{x})$ is polynomial in the arithmetic circuit complexity of f.

- Hence, such lower bounds are *at least* as hard as proving VP $\neq$ VNP.

Proof of Proposition 4. Assume $\mathrm{VP} = \mathrm{VNP}$. Show that $f = \sum_{i=1}^{n}(x_i^2 - x_i)g_i$ with g_i having small circuits.
First, assume that f has a polynomial degree.
$\hat{f}_i(x_1, \ldots, x_n)$ - multilinear in $x_1, \ldots, x_i$ and

$$\hat{f}_i(\mathbf{z}, x_{i+1}, \ldots, x_n) = f(\mathbf{z}, x_{i+1}, \ldots, x_n)\,, \forall \mathbf{z} \in \{0,1\}^i\,.$$

Hence

$$\hat{f}_i = \sum_{\mathbf{z}\in\{0,1\}^i} \left(f(\mathbf{z}, x_{i+1}, \ldots, x_n)\alpha(\mathbf{z}, x_1, \ldots, x_i)\right)\,,$$

where $\alpha(\mathbf{z}, x_1, \ldots, x_i) = \prod_{j=1}^{i}(z_j x_j + (1 - z_j)(1 - x_j))$.
Compute

$$g_i = \frac{\hat{f}_i - \hat{f}_{i-1}}{x_i^2 - x_i}\,.$$

Proof of Proposition 3. View Extended Frege as Frege working with Boolean circuits.

By induction on number of lines show: *if A has proof of size s then $IC(A^* - 1 \mid\mid \mathbf{x}^2 - \mathbf{x})$ is polynomial in s.*

Frege axiom: a constant size tautology $B(y_1, \ldots, y_k)$. Hence, $\mathrm{IC}(B^* - 1 \mid\mid y_1^2 - y_1, \ldots, y_k^2 - y_k)$ is a constant.

$$B^* - 1 = \sum_{j=1}^{k}(y_j^2 - y_j)g_j$$

If $D = B(A_1, \ldots, A_k)$ is a substitution instance then

$$D^* - 1 = \sum_{j=1}^{k}(A_j^{\star 2} - A_j^*)g_j' .$$

We have $A_j^{\star 2} - A_j^\star = \sum_{i=1}^{n}(x_i^2 - x_i)g_{ij}$ and so

$$D^* - 1 = \sum_{i=1}^{n}\left((x_i^2 - x_i)(\sum_{j=1}^{k} g_{ij}g_j')\right) .$$

Modus ponens

$$\frac{A, A \to B}{B}\,.$$

We have

$$A^\star = 1 + \sum_i (x_i^2 - x_i) h_i$$

$$(B^\star - 1) A^\star = \sum_i (x_i^2 - x_i) g_i$$

Hence,

$$(B^\star - 1)(1 + \sum_i (x_i^2 - x_i) h_i) = \sum_i (x_i^2 - x_i) g_i$$

$$B^\star - 1 = \sum_i \Big((x_i^2 - x_i)(g_i - h_i(B^\star - 1)) \Big)\,.$$

Theorem.
Assume that Extended Frege is not polynomially bounded. Then, over $\mathbb{F} = GF(2)$,

1. *$VP \neq VNP$, or*
2. *there exists A such that the polynomial A^* is identically zero but $\neg A$ requires super-polynomial proof in Extended Frege.*

- 2. means that A^* vanishes on $\bar{\mathbb{F}}$ but EF cannot even efficiently prove that it vanishes on $\{0,1\}^n$.
- 2. can be replaced by ”circuit-PI is not poly-bounded".
- Over any field, 2. can be replaced by ”EF cannot prove correctness of a PIT algorithm" [Grochow & Pitassi'15].

Theorem.

Assume that Extended Frege is not polynomially bounded. Then, over $\mathbb{F} = GF(2)$,

1. *$VP \neq VNP$, or*
2. *there exists A such that the polynomial A^* is identically zero but $\neg A$ requires super-polynomial proof in Extended Frege.*

Proof.

Want to refute B. Guess $g_1, \ldots, g_n$ with small circuits such that $B^\star = \sum_i (x_i^2 + x_i) g_i$. Prove the polynomial identity. $\square$

More on [Grochow & Pitassi'15]

Theorem.
A super-polynomial lower bound on number of lines of a Polynomial Calculus refutation of a CNF implies that VNP does not have polynomial size skew arithmetic circuits.

- Skew circuit : = in a product gate, at least one product has degree ≤ 1.
- In PC, one can derive αg from g if α has degree ≤ 1.
- Show that if $g_1, \ldots, g_k$ have a skew circuit of size s and $f = \sum_{i=1}^{k} f_i g_i$ then f has a PC proof with $O(s)$ lines.

The IPS system. Let $f_1, \ldots, f_k \in \mathbb{F}[\mathbf{x}]$. An IPS-certificate for unsatisfiability of $f_1 = 0, \ldots, f_k = 0$ is a polynomial $g(\mathbf{x}, y_1, \ldots, y_k)$ such that

- $g(\mathbf{x}, 0, \ldots, 0) = 0$,
- $g(\mathbf{x}, f_1, \ldots, f_k) = 1$.

An IPS proof for unsatisfiability of $f_1 = 0, \ldots, f_k = 0$ is an arithmetic circuit computing some such g.

- If $1 = f_1 g_1 + \cdots + f_k g_k$ then $g = y_1 g_1 + \cdots + y_k g_k$ is an IPS certificate.
- $f_1, \ldots, f_k$ consist of Boolean axioms $x_i^2 - x_i$ and arithmetic translations of clauses from a CNF.

- Super-polynomial lower bounds on IPS-certificates imply VP $\neq$ VNP.
- IPS simulates Extended Frege.
- They are equivalent, if EF can efficiently prove ”correctness of a PIT algorithm".
- Similar statements hold for restricted proofs and models of computation: Frege proofs versus formulas, bounded-depth Frege with mod p gates versus bounded-depth circuits over $GF(p)$.

III. Semi-algebraic proof systems

- Systems based on integer linear programming, intended to prove that a set of linear equalities has no integer solution (or no $0, 1$-solution).
- A CNF can be represented as a set of linear inequalities. A clause $x \vee y \vee \neg z$ as $x + y + (1 - z) \geq 1$

Cutting Planes

- Manipulates linear inequalities with integer coefficients, $a_1 x_1 + \cdots + a_n x_n \geq b$, with $a_1, \ldots, a_n, b \in \mathbb{Z}$
- Given a system $\mathcal{L}$ of linear inequalities with no $0,1$-solution, CP derives the inequality $0 \geq 1$ from $\mathcal{L}$.

Axioms are inequalities in $\mathcal{L}$ and the inequalities

$$x_i \geq 0\,,\;\; x_i \leq 1\,.$$

The rules are:

$$\frac{L \geq b}{cL \geq cb}\,,\;\; \text{if } c \geq 0\,,\;\; \frac{L_1 \geq b_1\,,\;\; L_2 \geq b_2}{L_1 + L_2 \geq b_1 + b_2}\,,$$

$$\frac{a_1 x_1 + \ldots a_n x_n \geq b}{(a_1/c)x_1 + \ldots (a_n/c)x_n \geq \lceil b/c \rceil}\,,\;\; \text{provided } c > 0 \text{ divides every } a_i\,.$$

The Lovász-Schrijver system

- Refutes a set of linear inequalities, but the intermediary steps can have degree 2.
- We can add two inequalities and multiply by a positive number. The additional rules are

$$\frac{L \geq 0}{xL \geq 0}, \quad \frac{L \geq 0}{(1-x)L \geq 0}, \quad x \text{ a variable, } L \text{ degree one.}$$

Degree-d semantic systems

- Intermediate inequalities can have degree $\leq d$.
- Inference rule is *any* valid inference.

$$\frac{L_1 \geq 0, \quad L_2 \geq 0}{L \geq 0},$$

provided every $0, 1$-assignment which satisfies the assumption satisfies the conclusion.

- Exponential lower bound on Cutting Planes [Pudlák'97]
- Works also for the degree-1 semantic system [Filmus& al.'15]
- A lower bound on Lovász-Schrijver system, assuming certain boolean circuit lower bounds [Pudlák'97].
  - Interpolation technique.
- Exponential lower bounds for *tree-like* degree-*d* semantic systems [Beame& al.' 07].
  - Communication lower bounds on randomized multi-party communication complexity of DISJ [Lee& Shraibman'08, Sherstov'12].

Open problem. Prove super-polynomial lower bound on the Lovász-Schrijver system, or the degree-2 semantic system.