Lecture 15 Survey of Strong Algebraic Proof Systems Oct 22

Nullstellensatz Proofs $\sum g_i p(C_i) + \sum h_i (x_i^2 - x_i) = 1$

for unsat CNF formula $F = C_1 \wedge \cdots \wedge C_m$.

- **degree** of NS refutation is $\max\{\deg(g_i p(C_i)), \deg(h_i(x_i^2 - x_i))\}$
- **size** is total number of monomials obtained by multiplying out the proof before cancellation.

ex) $C = x_1 \vee x_2 \vee \cdots \vee x_n \rightsquigarrow p(C) = (1-x_1)(1-x_2)\cdots(1-x_n)$
2^n monomials!

Polynomial Calculus ("Dynamic Nullstellensatz")

Def Let $P = \{p_1 = 0, p_2 = 0, \cdots, p_m = 0\}$ be a set of polynomial equations over field $\mathbb{F}$.

A **Polynomial Calculus** proof of poly h from P is given by a sequence of polynomials

$$h_1, h_2, \cdots, h_s = h$$

s.t.

- Each h_i is either in P or deduced from earlier h_is by one of two rules

$$\frac{p \quad q}{p+q} \qquad \frac{p}{p \cdot q} \text{ for any poly. } q$$

A Polynomial Calculus **refutation** of P is a proof of 1.

- The degree of a PC refutation is the maximal degree of any polynomial in the proof.
- The size of a PC refutation is the size of all polynomials in the proof, when expanded as monomials.

$\deg_{PC}(F)$:= min degree of any PC refutation of F

$S_{PC}(F)$:= — size —

<u>Fact</u> $\deg_{PC}(F) \le \deg_{NS}(F)$
$S_{PC}(F) \le S_{NS}(F)^{O(1)}$

Clearly NS proofs can be simulated by PC.

<u>Claim</u> Peb_G have $O(1)$, short proofs in PC if the degree of the graph is small!

<u>Pf Idea.</u> Locally simulate Resolution using PC!

$$\frac{C \vee x \quad \bar{x} \vee D}{C \vee D} \rightsquigarrow \frac{\dfrac{p(C)(1-x)}{p(D)p(C)(1-x)} + \dfrac{p(D)x}{p(C)p(D)x}}{p(D)p(C)}$$

$\square$

To solve the "$(1-x_1)(1-x_2)\cdots(1-x_n)$" problem, define

PCR (Polynomial Calculus Resolution)

Just change encoding of clauses to polynomials!

Now: for every variable x introduce two variables

x, x' with the equations $x^2 - x = 0$, $(x')^2 - x' = 0$, $x + x' = 1$

Now: translate "$x = 1 - x'$"

$C = x_1 \vee \overline{x_2} \vee x_3 \rightsquigarrow p^+(C) = x_1 \, x_2' \, x_3$

<u>Fact</u> PCR can size and degree - simulate resolution!

Lower Bounds:

<u>Thm</u> [CEI 96]

The exact same width-size relationship! as Resolution

For any unsat CNF F,

$$S_{PC}(F) \geq 2^{\Omega\left(\frac{(\deg_{PC}(F) - \deg(F))^2}{n}\right)}$$

So: degree lower bounds imply size lower bounds!

<u>Thm</u> [Razborov 98, AR 01, BCEIP 98]

true if $\mathrm{char}(\mathbb{F}) \neq 2$

$\deg_{PC}(PHP^{n+1}_{n}) \geq \frac{n}{2} + 1$, $\deg_{PC}(Tsei_G) = \Omega(n)$

$\deg_{PC}(\text{random } k\text{-CNFs}) \geq \Omega(n)$

Ideal Proof System [Grochow-Pitassi 14]

Let $P = \{p_1 = 0, p_2 = 0, \cdots, p_m = 0\}$ be a set of polys.

<u>Defn</u> An IPS certificate for P is another polynomial

$$C(\underbrace{x_1, x_2, \cdots, x_n}^{\text{shared by } p_i\text{s}}, y_1, \cdots, y_m)$$

on $n+m$ variables that satisfies

(1) $C(x_1, x_2, \cdots, x_n, 0, 0, \cdots, 0) = 0$

(2) $C(x_1, x_2, \cdots, x_n, p_1, p_2, \cdots, p_m) = 1$

So any such C witnesses P is unsatisfiable!

The size of C is the size of the smallest algebraic circuit computing C.

- inputs are variables $x_1 \cdots x_n, y_1 \cdots y_m$
- output is C
- gates are $+, \cdot$

Test conditions (1) and (2) using Polynomial Identity Testing (i.e. evaluate C on a bunch of random points in $\mathbb{F}$).

<u>Lem [Schwarz-Zippel]</u> If p is a polynomial with n variables over a field $\mathbb{F}$, and $S \subseteq \mathbb{F}$ is finite, and $r_1, r_2, \cdots, r_n$ are chosen uniformly at random from S, then

$$\Pr\left[p(r_1, \dots, r_n) = 0\right] \le \frac{d}{|S|}$$

So: IPS proofs are not "formal" propositional proof systems unless $PIT \in P$.

"Thm" [Grochow-Pitassi 14]

Polynomial Identity Testing

There are a set of "PIT axioms" that encode the correctness of PIT.

If a proof system P can

- simulate polynomial evaluation and
- can prove the PIT axioms

then P can efficiently simulate IPS!

IPS is in the intersection of

- Algebra
- Proof Complexity
- Derandomization