Lecture 14 Nullstellensatz Oct 20

Last time we introduced NS proofs "algebraic"
polynomial eqns

- Encode CNFs as systems of polynomials

$$C = x_1 \vee \bar{x}_2 \vee x_3 \longrightarrow \overbrace{(1-x_1)x_2(1-x_3)}^{p(C)=} = 0 \qquad x_i^3 = x_i^2 = x_i \ \cdots$$

encode $x_i \in \{0,1\}$ $\quad x_i^2 - x_i = 0$

$x_i^2 = x_i$

NS Refutation over field $\mathbb{F}$ for an unsat CNF $F = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ is a list of polynomials

$$g_1, \cdots, g_m, h_1, \cdots, h_n$$

$x_i x_j x_k^3 = x_i x_j x_k$

satisfying

$$\sum_{i=1}^{m} g_i p(C_i) + \sum_{i=1}^{n} h_i (x_i^2 - x_i) = 1$$

Proof is given "statically" in one-shot, rather than "dynamically" generating new lines like Resolution.

Last time: Nullstellensatz can be weaker than resolution.

"Pebbling formulas" (which are horn) are very easy for Resolution but hard NS.

Today: Show that Tseitin contradictions are easy for NS over $\mathbb{F} = GF(2)$.

Let $G=(V,E)$ be a graph, $|V|$ be odd. Then $\mathrm{Tsei}_G$ is the following system of constraints:

$$\forall v \in V \qquad \sum_{uv \in E} x_{uv} = 1 \pmod 2$$

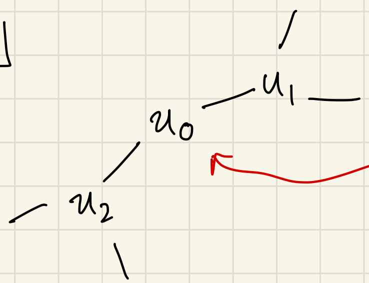
encoded in CNF!

Prove easy even using the CNF encoding!

First: observe $\displaystyle\sum_{v\in V}\sum_{uv\in E} x_{uv} = \sum_{v\in V} 1$

$$\Rightarrow \underbrace{0}_{\text{handshaking (every edge appears twice)}} = \underbrace{1}_{|V| \text{ odd}}$$

<u>ex</u>




$x_{01} + x_{02} = 1 \pmod 2$

$\Updownarrow$

$x_{01} \vee x_{02} \qquad \overline{x_{01}} \vee \overline{x_{02}}$

$\Updownarrow$

$(1-x_{01})(1-x_{02})=0 \qquad x_{01}x_{02}=0$

$x_{01}^2 - x_{01} = 0 \qquad x_{02}^2 - x_{02} = 0$

$(1-x_{01})(1-x_{02})$

$= 1 + x_{01} + x_{02} + x_{01}x_{02} \pmod 2$

observe: $(1-x_{01})(1-x_{02}) + x_{01}x_{02} = 1 + x_{01} + x_{02}$

i.e. can recover the original linear equations efficiently!

"Claim": Summing all polynomial equations in the CNF encoding of a vertex constraint for $v$, you get the polynomial

(Not actually true)

$$1 + \sum_{uv \in E} x_{uv}$$

<u>Lemma</u> Let $b \in \{0,1\}$, let $d$ be a positive integer. Let

$$\mathcal{E}_{d,b} := \left\{ \prod_{i \in S} (1+x_i) \prod_{i \notin S} x_i \;\middle|\; S \subseteq [d],\ |S| \equiv b \pmod 2 \right\}$$

Then $$\sum_{p \in \mathcal{E}_{d,b}} p = \sum_{i=1}^{d} x_i + b + d + 1 \pmod 2$$

(in the above case: $d=2$, $b=0$, so we recover it)

Pf Exercise — induction on $d$!

<u>Pf</u> (that Tseitin is easy for NS over $GF(2)$)

Each constraint

$$\sum_{uv \in E} x_{uv} = 1 \pmod 2$$

is transformed into the system of polynomials

$$P_v := \left\{ \prod_{u \in S} (1+x_{uv}) \prod_{u \notin S} x_{uv} \;\middle|\; S \subseteq \mathrm{Nbhd}(v),\ |S| \text{ even} \right\}$$

So:

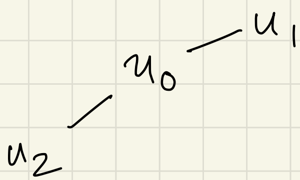
$$\sum_{v} \sum_{p \in P_v} p$$

$$\underset{\text{(lemma)}}{=} \sum_{v} \left[ \sum_{uv \in E} x_{uv} + 0 + \deg(v) + 1 \right] \pmod 2$$

$$= 1 \pmod 2.$$

$\square$

$$P_v := \left\{ \prod_{u \in S} (1 + x_{uv}) \prod_{u \notin S} x_{uv} \;\middle|\; S \subseteq \mathrm{Nbhd}(v),\ |S| \text{ even} \right\}$$




$$x_{01} + x_{01} = 1 \pmod 2$$

$$\rightsquigarrow$$

$$x_{01} \vee x_{02} \qquad \overline{x_{01}} \vee \overline{x_{02}}$$

$$\rightsquigarrow$$

$S = \{u_1, u_2\}$ $\qquad$ $S = \emptyset$

$$(1 + x_{01})(1 + x_{02}) = 0 \qquad x_{01} x_{02} = 0$$

Why is Nullstellensatz studied?

## History

A boolean circuit is $AC^0$ if it has

- $O(1)$ depth
- unbounded-fan-in ANDs, ORs
- NOT gates

Thm [Håstad 86]

Any $AC^0$ circuit computing the XOR of $n$ bits requires exponential-size.

By modifying these techniques ("Switching Lemma") to the proof complexity setting:

Thm [BIKPPW 92] (proof like Resolution with $AC^0$-circuits for lines)

Any $AC^0$-Frege proof of $PHP_n^{n+1}$ requires exponential size!

A circuit is $AC^0[2]$ if it is $AC^0$ and also has XOR gates of unbounded fan-in.

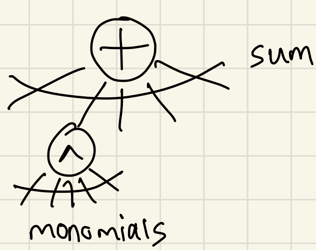
Thm [Razborov 87, Smolensky 87]

Any $AC^0[2]$-circuit computing MAJORITY requires exponential size.

Open Problem

Prove any non-trivial lower bound for $AC^0[2]$-Frege.

Observe that any polynomial $p$ over $GF(2)$ can be represented as




→ This is depth 1 $AC^0[2]$!

i.e. small Nullstellensatz proofs $\Rightarrow$ small $AC^0[2]$-Frege proofs.

small Polynomial Calculus proofs

**Second Motivation**: Span Programs! $F = A(x,y) \wedge B(x,z)$

Span programs are the boolean circuits that feasibly interpolate Nullstellensatz.

Closely related to

- Algebraic Computation

  They capture the computational complexity of Gaussian Elimination

- Cryptography

  Monotone span programs are equivalent to Linear secret sharing schemes

- Quantum Algorithms

  Every quantum algorithm is equivalent to a span program over $\mathbb{C}$.

**Defn** Let $f: \{0,1\}^n \to \{0,1\}$ be a boolean function, let $\mathbb{F}$ be a field. A span program computing $f$ over $\mathbb{F}$ is a matrix $M$ whose rows are labelled with boolean literals.

ex)

$$\begin{array}{c} x_1 \\ x_2 \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$x = 01$, $M_x$

Span program for $\wedge$

On an input $x \in \{0,1\}^n$, let $M_x$ denote the submatrix whose row labels are satisfied by $x$.

Accept input $x$ if $\vec{1} \in$ row-span$(M_x)$, reject otherwise.

Size is the number of rows.

ex)

$$\begin{array}{c} \overline{x_1} \\ x_2 \end{array} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$x = 00$

$\leftarrow$ computes $\overline{x_1}$

Span progs over $\mathbb{C}$ equivalent to Quantum Query Algs.

↑ Proved in a sequence of papers, culminated in [Reichardt 14]

(Nullstellensatz defined in proof complexity by) [BIKPP 94]

?