Lecture 13 Algebraic Proof Systems

Oct 15

Cutting Planes – "semi-algebraic" – inequalities over reals with polynomials

Resolution – "boolean" – standard boolean logic

Today: Nullstellensatz proof system

"algebraic" := manipulates polynomial equalities over a field.

How do we encode CNFs as polynomial equalities?

ex) $C = x_1 \vee x_2 \vee \overline{x_3} \rightsquigarrow \underbrace{(1-x_1)(1-x_2)x_3}_{p(C)=} = 0$

constrain $x_i \in \{0,1\}$ by adding

$x_i^2 - x_i = 0$ for each i.

Given clause C, let $p(C)$ denote it's polynomial encoding.

Defn Let $F = C_1 \wedge \cdots \wedge C_m$ is an unsat CNF over n variables. Let $\mathbb{F}$ be any field. Then a Nullstellensatz refutation of F is a set of polynomials

$$g_1, g_2, \cdots, g_m, h_1, h_2, \cdots, h_n$$

(Generalization: Polynomial calculus)

over $\mathbb{F}$ such that

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

Why is this a refutation?

Suppose that F had a solution! Then plugging in we get $0=1$! Contradiction.

ex) $C = x_1 \wedge (\overline{x}_1 \vee x_2) \wedge (\overline{x}_2 \vee x_3) \wedge \overline{x_3}$

$p(\cdot)\downarrow$ $\qquad\downarrow\qquad\downarrow\qquad\downarrow$

$(1-x_1) \qquad x_1(1-x_2) \qquad x_2(1-x_3) \qquad x_3$

also $\quad x_1^2 - x_1 \qquad x_2^2 - x_2 \qquad x_3^2 - x_3$

C satisfiable iff $\exists$ 0/1 assign setting each poly to 0.

$$(1-x_1) + x_1(1-x_2) + \underbrace{x_1}_{g_i =} x_2(1-x_3) + \underbrace{x_1 x_2}_{g_j =} x_3$$

$$= (1-x_1) + x_1(1-x_2) + x_1 x_2$$

$$= (1-x_1) + x_1 \quad = 1$$

We've argued soundness: if there is a refutation then F is unsatisfiable.

Completeness follows from Q3 on the assignment!

Where does this come from?

Answer: Page 2 of any algebraic geometry textbook.

Name comes from a theorem by Hilbert called Hilbert's Nullstellensatz.

Hilbert wanted to link

Semantics (Model) – solutions to a system of polynomial equations with

Syntactic (Proof) – the set of all polynomial equations derivable from the system.

ex) Pick $x^2 - 4 = 0$ $x \in \mathbb{R}$
$x + 200 = 0$

Not simultaneously satisfiable!

Given poly eqns we can easily deduce new ones!

(multiply by x)

$$x^2 - 4 = 0 \implies x^3 - 4x = 0$$
$$\implies x^{2+i} - 4x^i = 0$$

(addition)

$$x^2 - 4 = 0 \text{ and } x + 200 = 0 \implies x^2 + x + 196 = 0 \text{ !}$$

Define the ideal of a system of polynomial eqns to be the set of all polynomial eqns derivable in this way!

Hilbert's Nullstellensatz

Let $\mathbb{F}$ be any algebraically closed field* and let $\mathcal{F}$ be any system of polynomials over $\mathbb{F}$. Then

$$\{ f = 0 \mid f \in \mathcal{F} \}$$

has no solution in $\mathbb{F}$ iff the ideal contains 1.

Complexity Measures

Let $F = C_1 \wedge \cdots \wedge C_m$ be our CNF formula, on variables $x_1 \cdots x_n$

Let $\Pi = \{g_i\}_{i=1}^{m} \cup \{h_i\}_{i=1}^{n}$ be an NS refutation over $\mathbb{F}$.

$$\deg_{NS}(\Pi) = \max \{\deg(g_i p(C_i))\}_{i=1}^{m} \cup \{\deg(h_i(x_i^2 - x_i))\}_{i=1}^{n}$$

i.e. expand all products and take the maximum degree.

$S_{NS}(\Pi)$ = total # of monomials when all products are expanded out before cancellation.

$\deg_{NS_{\mathbb{F}}}(F) :=$ min degree of an NS refutation of F over $\mathbb{F}$

$S_{NS_{\mathbb{F}}}(F) :=$ min size of any NS ref. of F over $\mathbb{F}$.

Compare Nullstellensatz with other proof systems.

Resolution:

- Over $\mathbb{F}_2 = \{0,1\}$, then Nullstellensatz has short proofs of Tsei_G for <u>any</u> G.

- On the other hand: Nullstellensatz has difficulty proving Horn formulas! (These are very easy for Resolution by A1)

We usually use degree as the primary complexity measure for NS. There <u>is</u> a size-degree tradeoff for NS just like resolution (moreover, by a very similar proof).

Q3: $\deg_{NS}(F) \le D_{Res}(F) + w(F)$

<u>Defn</u> Let $G = (V, E)$ be a DAG with a unique sink node t and s.t. every internal node has at most 2 predecessors.

Define Peb_G to be the following unsat. CNF (Horn) formulas:

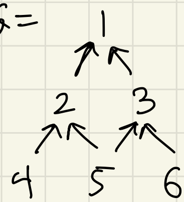
- Variables: x_v for each vertex $v \in V$

- Clauses
  - $\overline{x_t}$ where t is the sink node

  - For every vertex $u \in V$ with predecessors P add the clause

$$x_u \vee \bigvee_{v \in P} \overline{x_v}$$

ex] $G=$



$\rightsquigarrow$ $Peb_G := \overline{x_1},\ x_1 \vee \overline{x_2} \vee \overline{x_3}$

$x_2 \vee \overline{x_4} \vee \overline{x_5},\ x_3 \vee \overline{x_5} \vee \overline{x_6}$

$x_4,\ x_5,\ x_6$

Thm [Buss-Pitassi 98]

Let P_n be the directed path with n vertices:

$$1 \to 2 \to 3 \to \cdots \to n.$$

Then $\deg_{NS_{\mathbb{F}}}(Peb_{P_n}) = \Theta(\log n)$.

Thm [Buresh-Oppenheim et al 00]

For any "good" DAG $G=(V,E)$

$$\deg_{NS_{\mathbb{F}}}(Peb_G) \geq (\text{black pebbling number of } G)$$

combinatorial parameter of G.

There exist graphs with black pebbling number $\Theta(n/\log n)$.

Thm [de Rezende - Meir - Nördstrom - R 18]

For any "good" DAG $G=(V,E)$

$$\deg_{NS_{\mathbb{F}}}(Peb_G) = \text{reversible pebbling number of } G$$

Oct 15

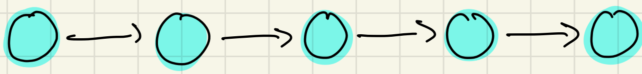
Defn Let $G=(V,E)$ be a good DAG. Consider the following game.

You have a collection of "pebbles". Goal is to place a pebble on the sink vertex of G.

To place pebbles you can make the following "move":

For any vertex v in G, if all predecessors of v have a pebble, then you can place or remove a pebble from v.

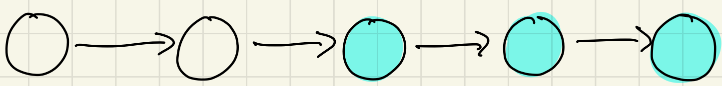
ex)



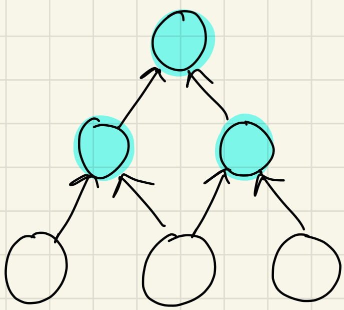
P_5

place pebble here

You can always win by placing $|V|$ pebbles!



Used only 3 pebbles at one time!



Used 4 pebbles

Reversible pebbling number = min # of pebbles