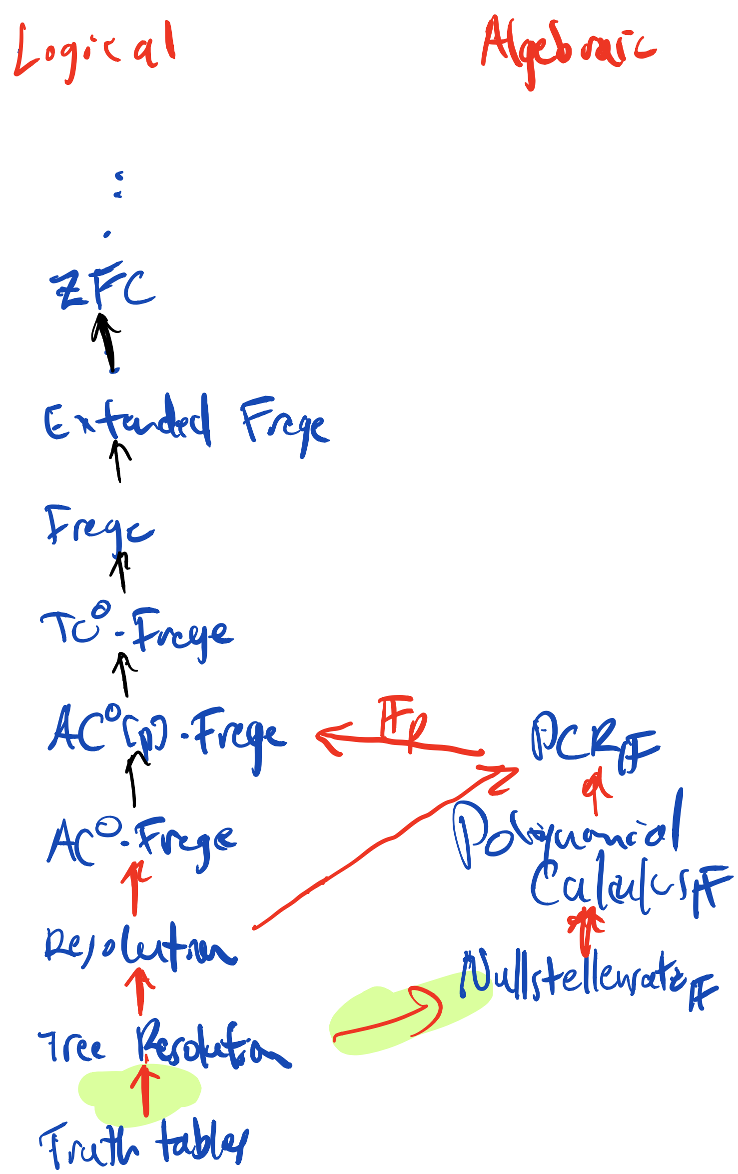
CSE 599S Proof Complexity

Lecture 3

Hierarchy of Proof systems

— simulation → simulation & separation ⇢ separation



Proving CNF $F = C_1 \wedge \cdots \wedge C_m$ in vars $x_1 \cdots x_n$ is UNSAT using algebra

Clause

$C = x \vee \bar{y} \vee z \Rightarrow$

Polynomial

$p_C = (1-x)y(1-z) = 0$

Ideal $I = \{x_1^2 - x_1, \ldots, x_n^2 - x_n\}$

Nullstellensatz Proof. Polynomials $g_1, \ldots, g_m$ s.t.

$$\sum_{i=1}^{m} f_i g_i \equiv_I 1$$

where $f_i = p_{C_i}$

degree $= \max_i (\deg(f_i g_i))$

size $= \sum_i \#\text{monomials}(f_i g_i)$

bitsize $= \#$ bits to represent in total

field $\mathbb{F}$ is $\mathbb{R}$, $\mathbb{F}_2$, $\mathbb{F}_p$

Annoyance: Clause

$x_1 \vee x_2 \vee \cdots \vee x_n$

$p_C = (1-x_1)(1-x_2)\cdots(1-x_n)$

# of monomials $= 2^n$

solution dual variables

x $\quad$ $x, \bar{x}$

$x + \bar{x} - 1 = 0$

C $\quad$ $1 - x - \bar{x} = 0$

$x \vee \bar{y} \vee z \quad \overline{P_C} = \bar{x} \cdot y \cdot \bar{z} = 0$

New ideal I' $\quad$ $x_i^2 - x_i = 0$

$x_i + \bar{x}_i - 1 = 0$

$\Downarrow$

$\bar{x}_i^2 - \bar{x}_i = 0$

F $\quad$ C $\quad$ $\overline{P_C}$

$\sum_i \overline{P_{C_i}} \cdot q_i \equiv_{I'} 1$

doesn't change degree but reduced # monomials

Find Nullstellensatz proofs
of degree d

$$\sum_{i=1}^{m} f_i \underbrace{g_i}_{\text{unknown}} =_I 1$$

# of coefficients of degree $\le d$

multilinear polynomials

monomial = subset of $\{x_1 \ldots x_n\}$

$\binom{n}{\le d}$

linear equations for coefficients of the g_i

RHS constant coeff $= 1$

all others $= 0$

$d \le n$

dimension

$$\begin{bmatrix} f_1 & \cdots & f_m \end{bmatrix} \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

solve in time

$\binom{n}{\le d}^3 \approx n^{O(d)}$

Nullstellensatz proofs are static

NS PF

Polynomial Calculus

lines, axioms, rules of inference

line: polynomial p ($p = 0$)

axioms: $x_i^2 - x_i$

P_{C_i} input axioms

Polynomial Calculus ($PC_{\mathbb{F}}$)

derivation of $\underline{f = 0}$

from polys $f_1 = 0, \ldots, f_m = 0$

is a sequence

$f_1 \ldots f_m \ldots f_t = f$

where each f_j for $j > m$ is either

- $x_i f_{j'}$ (taken mod I) $j' < j$
- $a f_{j'} + b f_{j''}$ $j', j'' < j$, $a, b \in \mathbb{F}$

deg $= \max_j (\deg f_j)$

size $= \sum_j \#\text{monomials}(f_j)$

bitsize $= \sum_j$ # of bits for represent f_j

PC refutation of $F = \wedge C_i$

$f_i = P_{C_i}$ for $i = 1 \ldots m$

$f = 1$

$PC_{\mathbb{F}}$size$(F) = \min \ldots$

degree$(F) = \min$

$PCR_{\mathbb{F}} = PC_{\mathbb{F}}$ with dual variables mod I^0

$\uparrow$ PC + Resolution

Thm $PCR_{\mathbb{F}}$ efficient simulate resolution

Proof

Resolution:
$$\frac{(a \vee b \vee c \vee \bar{d}) \quad (\bar{a} \vee b \vee c \vee \bar{r})}{b \vee c \vee \bar{d} \vee \bar{r}}$$

PCR given
$$\frac{\begin{array}{c} r \cdot \bar{a}\,\bar{b}\,\bar{c}\,d \\ d \cdot a\,\bar{b}\,\bar{c}\,r \\ \Downarrow \end{array}}{(\bar{a}+a)\,\bar{b}\,\bar{c}\,d\,r}$$
$$\Downarrow$$
$$1\,\bar{b}\,\bar{c}\,d\,r$$
$$= \bar{b}\,\bar{c}\,d\,r$$

$\boxtimes$

Finding PC proofs of degree $\le d$

Notation: $f_1 \dots f_m \vdash_d f$ iff $\exists$ PC derivation of f of deg $\le d$

$V_d = \{ f \mid f$ multilinear s.t. $f_1 \dots f_m \vdash_d f \}$

$\dim(V_d) \le \binom{n}{\le d}$

vector of coefficients

Algorithm: Compute bases $B_0 \dots B_d$ of $V_1 \dots V_d$.

$j = 1, \dots, d$

- View each element f of B_{j-1} as an elt of V_j

$\binom{n}{\le j-1}$

- For any input poly f_i add multilinear(f_i) if it has deg exactly j.

Also add $x_i \cdot f$ for each $i \in [n]$ and each elt f of B_{j-1}

- Use Gaussian elimination to reduce the resulting set of polys to a basis B_j

$\binom{n}{\le j} +$

$\binom{n}{\le d}^{O(1)}$

Runtime $n^{O(d)}$

Gröbner basis alg. rewriting

Lower Bounds & PHP

Pigeonhole Principle: no 1-1 map from m to n for $m > n$ as CNF (unsat) PHP^m_n

x_{ij} $i \in [m], j \in [n]$ "i is mapped to j"

Pigeon — everything is mapped: $x_{i1} \vee x_{i2} \vee \cdots \vee x_{in}$ for all $i \in [m]$

Hole — 1-1: $\bar{x}_{ij} \vee \bar{x}_{i'j}$ $i \neq i' \in [m], j \in [n]$

Unsat

Function: $\bar{x}_{ij} \vee \bar{x}_{ij'}$ $i \in [m], j \neq j' \in [n]$

Onto: $x_{1j} \vee \cdots \vee x_{mj}$ $j \in [n]$

PHP^m_n, funct PHP^m_n, Onto PHP^m_n, bijective PHP^m_n easiest

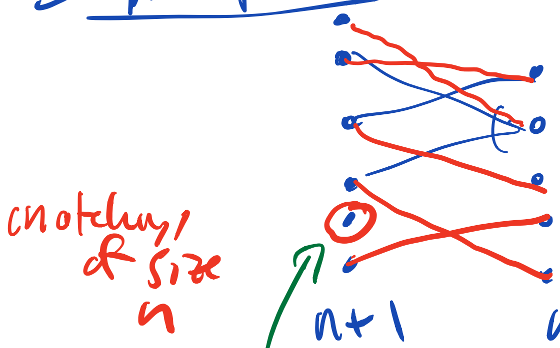
Cook - easy for Extended Res

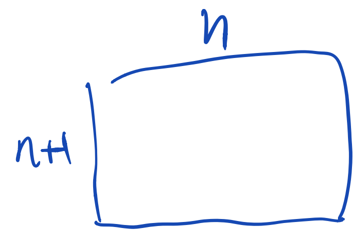
Cook-Karp - suggested as hard problem for Res

Haken 1984 – PHP^{n+1}_{n} is exponentially hard for Res

→ Counting is hard for CDCL, DPLL reasoning

Simpler proof:





left out pigeon

critical truth assts

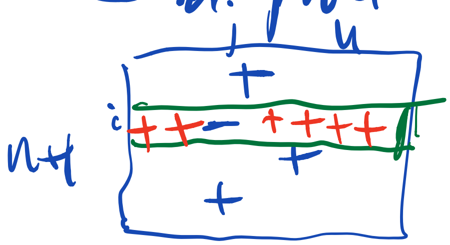
i-critical truth asst

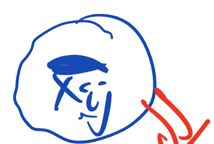
i-cta

if i is the left out pigeon.

Clause C in proof

C





$x_{1j} \vee x_{2j} \vee \dots x_{i-1j} \vee x_{i+1j} \vee \dots x_{n+1n}$

$C \to M(C)$

C and M(C) behave almost the same on cta's