CSE 599s Proof Complexity

Lecture 2 5 October 2020

Last time: Proofs and proof systems

Propositional proofs (proof systems for CNF-UNSAT).

Proof complexity

Efficient propositional proofs $\iff$ NP=coNP

Sample proof systems

- Truth tables
- Resolution
- DPLL $\equiv$ Tree resolution.

Davis-Putnam

eliminates vars 1-by-1

resolve away x_1 then x_2

All resolutions on x_1 before those for x_2 etc

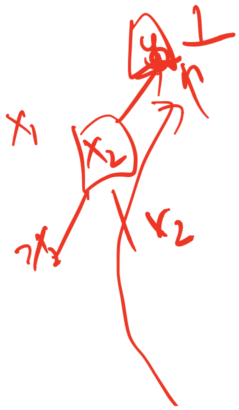
Ordered resolution:

on any path variables resolved are in a fixed order

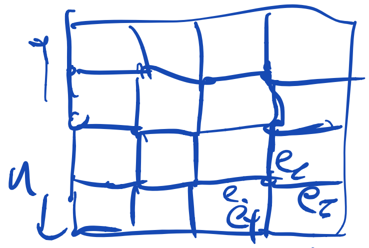
- incomparable to tree resolution

Regular resolution (Tseitin 1968)

- on any path if you've resolved away some var X then never add it back again
- on each path x is resolved on at most once.



Very natural restriction but



Tseitin showed $\exists$ formulas TS_n that required proof size $n^{\Omega(\log n)}$ in regular resolution

G   n odd n^2 vertices odd

variable for each edge in G

For each vertex in G

constraint: parity of incoming edges is odd

$2|E| = \sum_v \deg(v)$

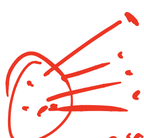
4 edges   8 clauses per vertex

$\neg e_1 \vee \neg e_2 \vee \neg e_3 \vee \neg e_4$

$TS(G, \ell)$ ℓ labelling for $\sum_v \ell(v)$ odd

unsat

later   Galil 1975   expander graph



expander graph

$2^{\Omega(n)}$ lower bound for regular resolution

CDCL $\subseteq$ Resolution

Frege proofs

original Cook-Reckhow paper

axioms: e.g. $A \vee \neg A$

inference rule: e.g. $\dfrac{A,\ A \to B}{\therefore B}$ Modus Ponens

sound, complete

rules used by substitution

$\overline{(x \vee \neg y) \vee \neg(x \vee \neg y)}$

Many different choices of system

Thm (Cook-Reckhow) All Frege systems are p-equivalent

Proof idea

Simulate each rule application in one by several steps of the other (possible by completeness)

$$\frac{A, B}{\therefore C}$$

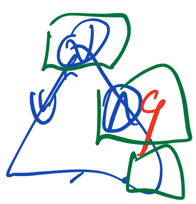
$\therefore (A \wedge B) \to C$ tautology

$\to$ second system can prove it in a constant # of times

- All Frege proofs can be made tree-like without much blow-up in size.

Extended Frege proofs

Can introduce new vars to stand for formulas.



- Extended Resolution New variable

$$(y \leftrightarrow (x_1 \vee \cdots \vee x_n))$$

Add new clauses (for new var y)

$\neg y \vee x_1 \vee \cdots \vee x_n$

$\neg x_1 \vee y$

$\vdots$

$\neg x_n \vee y$

Formula $\Rightarrow$ 3CNF

Extended Resolution $\equiv$ Extended Frege

ZFC   Zermelo-Frankel Set Theory
axiom of choice

$\mathcal{C}$-Frege : $\mathcal{C}$ - complexity class of circuits

$\mathcal{C} = \{$circuits that are polysize and have property $P_{\mathcal{C}}\}$

- clauses   clauses   Resolution
- Constant depth unbounded fan-in $\wedge, \vee, \neg$
- AC^0 - AC^0-Frege
- TC^0 - TC^0-Frege constant depth neural nets
- $AC^0[m]$ - $AC^0[m]$ Frege + mod m gates
- NC^1 - Frege polysize formula log n depth fan-in ~~two~~ 2
- $P/poly$ - Extended Frege polysize circuits

Proof Systems Hierarchy

Algebraic

Logical

ZFC

Extended Frege

Frege

TC^0-Frege

$AC^0[p]$-Frege

AC^0-Frege

Resolution

Tree Resolution

Truth Tables

Algebraic Proofs

Express clause $\bar{x} \vee y \vee z$ C

as a polynomial equation $x(1-y)(1-z)=0$

$p_C = 0$

$F = \bigwedge_i C_i$ $p_{C_1} = 0$

$\vdots$

$p_{C_m} = 0$

Thm (Hilbert) A system of eqns polys. over field $\mathbb{F}$, $f_1 = 0$ $f_2 = 0$ $f_m = 0$

Nullstellensatz

has no solution in the ~~algebraic closure~~ of $\mathbb{F}$ iff $\exists$ polys $g_1 \cdots g_m$ s.t.

$$f_1 \cdot g_1 + \cdots + f_m \cdot g_m \equiv 1$$

Always have equations $x_1^2 - x_1 = 0$, $\ldots$, $x_n^2 - x_n = 0$ } $0,1$

Nullstellensatz proof over field $\mathbb{F}$

set of polys $g_1 \cdots g_m, r_1 \cdots r_n$ s.t.

write out as sums of monomials

$$\sum g_i f_i + \underbrace{\sum r_j (x_j^2 - x_j)}\equiv 1$$

$\sum g_i f_i \equiv_I 1$ Ideal $I \Rightarrow$ multilinear (every has deg 1) degree, size

Thm $\exists$ Nullstellensatz refutation of F of degree $=$ depth of tree resolution refutation of F

x

x^c $(1-x)$

$$\sum\left(\frac{\varphi_i}{x_1}\right)\underbrace{(1-x_1)x_2(1-x_3)}_{f_i} = x_2 - x_2x_3 - x_2x_1 + x_1x_2x_3$$

PC

$x_1^2 \longmapsto x_1$

$x_1^2 x_3^3 x_4^4 \longmapsto x_1 x_2 x_4$