CSE 599S Proof Complexity & Applications

Lecture 20   9 Dec 2020

How hard is it to find short proofs if they exist?

F constant size clauses

	Size	width/degree	Find
Tree-resolution proof	S	$O(\log S)$	$n^{O(\log S)}$
Resolution	S	$O(\sqrt{n \log S})$	$n^{O(\sqrt{n \log S})}$
PC	S	$O(\sqrt{n \log S})$	$=$
SOS	S	$O(\sqrt{n \log S})$	$2^{\tilde{O}(\sqrt{n \log S})}$

$\Downarrow$ if S is $n^{O(1)}$ algorithm is $2^{\tilde{O}(n^{1/2})}$

Best paper FOCS 2019 Atserias & Müller

NP-hard to do much better for Resolution

$F \overset{3\text{-CNF}}{\longmapsto} F'$ s.t.
φ polytime

if F is SAT then F' has a short ($n^{O(1)}$) resolution refutation

F is unSAT then F' requires a $2^{\Omega(n^{1/5})}$ resolution refutation

What is F'?

"F has a size n^3 trivial (tree) resolution refutation"

~~Vars~~ Vars for each clause in purported proof, vars to say which clauses are derived from which, etc

If F is SAT then w/ a satisfying assignment it is easy to refute F'

If F is not SAT then can find F' to encode PHP^{n+1}_n

hard for resolution

extended to

NS

Cutting Planes

SA

Regular Resolution

Ordered Resolution

PHP easy

lifted PHP

like Clique-Coloring

Open: SOS

PHP hard

lifted PHP is easy ~~for~~ SOS

Proofs in Practice of SAT solving

SAT solver fails to find an asst.
Is it • a failure of the solver?
• a true proof?

SAT competition: Complete solvers now required to produce $\underbrace{\text{proofs}}_{\text{easily checkable}}$ not just Yes/No.

DRAT proofs

Proof looks like: Γ set of formulae maintained

$\Gamma \leftarrow$ {clauses of F}
$\Gamma \leftarrow \Gamma \cup \{C\}$
C is derived from Γ

AT derivation from Γ of a clause C
"reverse unit propagation" RUP

Def'n C is an AT consequence of Γ iff
$\Gamma, \overline{C}$ unit propagates $\bot$

all negated literals of C

e.g. $\overline{C}$ are decision vars on a branch leading to $\bot$

easy to check

exactly the typical learned clause if we got a contradiction following decision of $\overline{C}$

$\bot$

This means $\Gamma \models C$
logically entails

Def^n C is an **RAT consequence of Γ**
iff
there is a literal $\ell \in C$
s.t. $\forall$ clauses $\bar{\ell} \vee D \in \Gamma$
$\Gamma, \bar{C}, \bar{D}$ unit propagates $\perp$
i.e. $C \vee D$ is an AT consequence of Γ

Also easy to check in terms of $|\Gamma|$

many make it harder to add C if Γ is bigger

Claim Γ is SAT $\Rightarrow$ $\Gamma \cup \{C\}$ is SAT.

Proof Suppose α is a truth ass^t satisfying Γ

If $\alpha(C) = 1$ then we are done ✓
If $\alpha(C) = 0$ then $\alpha(\ell) = 0$
define $\alpha' = \alpha$ with value $\alpha'(\ell) = 1$

as only flip

- $\alpha'(C) = 1$ ✓
- why is $\alpha'(\Gamma) = 1$?

Consider a clause $\bar{\ell} \vee D \in \Gamma$

claim: $\alpha'(\bar{\ell} \vee D) = 1$
i.e. $\alpha'(D) = 1$

note $\alpha'(D) = \alpha(D)$

clauses of Γ that don't contain $\bar{\ell}$ still true under α'

by * $\Gamma \models C \vee D$
$\alpha(\Gamma) = 1$ so $\alpha(C \vee D) = 1$
but $\alpha(C) = 0$ $\therefore \alpha(D) = 1$

Special case / Blocked clause addition

$(\ell \vee C)$ $(\bar{\ell} \vee D)$

cut through literal resolution would produce tautology.

DRAT : RAT derivation rule
+ can delete a clause at any time

Boolean Pythagorean Triple Problem

can you 2-color $\mathbb{N}$ to avoid all $a^2 = b^2 + c^2$ ~~of~~ the same color

2016 no: can't do it for [1, ..., 7825]

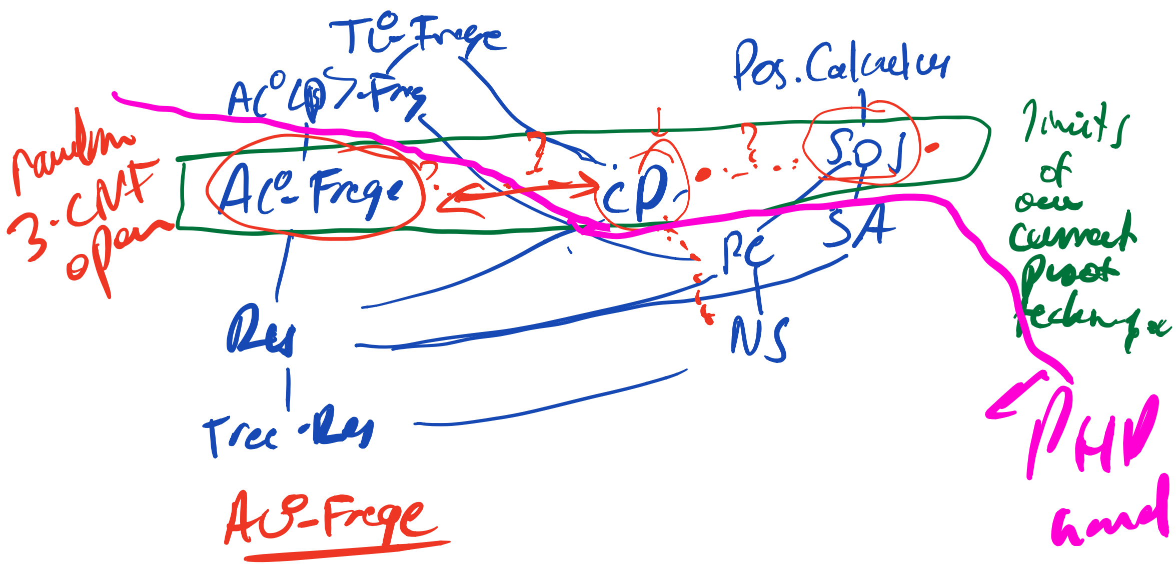
Heule Kullmann

Proof: DRAT proof found using parallel SAT solving

original 200TB proof reduced to ~90MB checked

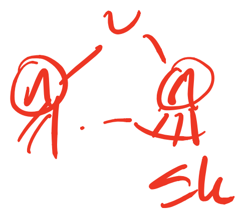
$F \mapsto F^{(\wedge 2)}$

Cause Proof size DRAT



AC^0-Frege

special case $Res(k)$



lines k-DNF

depth d

each line a circuit of depth d or formula

PHP_n^{n+1} requires size $2^{n^{\Omega(1/5^d)}}$

i.e. polysize requires depth $d = \Omega(\log\log n)$

Method random restriction method used for AC^0 circuits

Ajtai, FSS, Hastad

Parity $\notin AC^0$

ρ randomly set all but p fraction of vars to 0, 1

$\text{Parity}^n|_\rho \equiv \text{Parity}^{pn}$

set all but p fresh randomly

probably constant 0.

parity $2^{\Omega(n^{1/d})}$

$p = \frac{1}{\log S}$

$\frac{n}{\log S} \quad \frac{n}{\log^2 S} \quad \cdots \quad \frac{n}{\log^d S}$

Proofs: (don't think of refutation system) where each axiom is a tautology

$F_1, F_2, \ldots, F_S = F$ proof

$F_1 \equiv 1, \quad F_2 \equiv 1, \quad \ldots, \quad F_S \equiv 1$

not interesting to apply restriction and keep original full memory

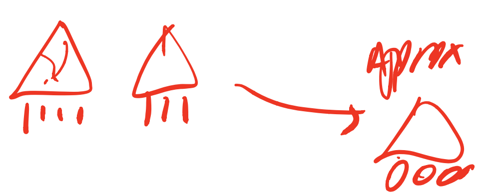
Instead Apply restriction and then locally approximate

e.g. PHP^{n+1}_n

set all but $\sqrt{n}$ vars.

$n \to \sqrt{n} \to n^{1/4} \to n^{1/8} \cdots$

only interested in truth assignments that look like partial matching



Approx of

recent Tseitin $2^{n^{\Omega(1/d)}}$ lower bound

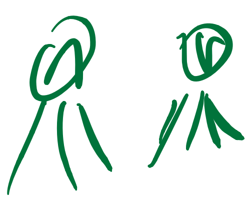
$\Omega(\log n / \log\log n)$ depth

PHP^m_n is hard for resolution even when $m = 2^{n^{1/3}/\log n}$

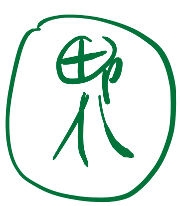
"Resolution cannot prove $P \neq NP$"

Open: Can SOS simulate CP efficiently for clause inputs?
(knapsack easy for CP but not clauses)

$AC^0(p)$-Frege
why can't we get lower bounds?
we already circuit lower bds for $AC^0(p)$ circuits



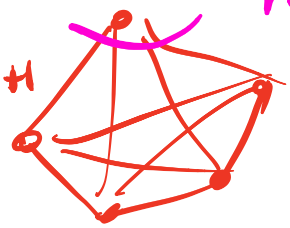
– current technique
we approx of $\oplus_p$
by low degree polys
no analogue of restrictions that we did for AC^0



Key next case

RES(LIN$_2$)
talk Monday Oliver

Open: Parity principle (CP vs pos. code)

K_{2n+1}  deg 1

no perfect match

LS

trivial for SOS

requires deg $\Omega(n)$ SOS

LS (Lovasz-Schrijver) — semi-alg, deg 2, each $p(x) \geq 0$

deg 2

each line: linear $\cdot (1-x)$ + linear $\cdot x$

d.

$x^2 \to x$

Open CP vs. CP*

Open Good hard examples for TC^0-Frege

candidate

$$\boxed{\text{Square matrices } A, B \in \{0,1\}^{n \times n} \qquad A \cdot B = I \to B \cdot A = I}$$

$\Updownarrow$ $\Updownarrow$

quasi-poly upper bound $n^{\log^c n}$

Fixed parameter complexity

k-CLIQUE $n^{O(k)}$ alg

Suppose G does not have a k-clique

G vars refute by formula saying that it does!

k

$2^k n$

$2^{\Omega(k)}$ lower bound

$n^{\Omega(k)}$ regular resolution

open for general resolution

Exactly clarity powers

- of DRAT and related proofs
- CDCL without restarts.