PRFCMPLX
⟨17-1-2014;1⟩

Best lowerbound for Frege Systems

There are formulas φ_n, st $|\varphi_n| = O(n)$ & the shortest $\mathcal{F}$-proofs of φ_n are size $\Omega(n^2)$

let: $\top$ abbreviate $x_1 \vee \neg x_1$
$\bot$ abbreviate $x_1 \wedge \neg x_1$

$$\varphi_n := \underbrace{\bot \vee (\bot \vee (\bot \vee \ldots\ldots \bot \vee (\bot \vee \top)) \ldots\ldots)}_{n \text{ levels of nesting}}$$

start by proving $\top$, then $\bot \vee \top$, then $(\bot \vee \top) \vee \bot$

$\dfrac{\varphi,\ \varphi \to \psi}{\psi}$, How do we prove this proof is optimal?

Fix n large, let $\mathcal{P}$ be a $\mathcal{F}$-proof of φ_n, $|\mathcal{P}| \ll n$
We say φ_i is active in $\mathcal{P}$, if some axiom of $\mathcal{P}$ uses φ_i in a top-level formula.

φ_i is $\bot \vee \varphi_{i-1}$

φ_i if this $\vee$ is one of the distinguished $\vee$'s in these axioms:

Now it suffices to prove for each φ_i, $1 \leq i \leq n$, is active in $\mathcal{P}$ because:

$$|\mathcal{P}| \geq \sum_{\varphi_i \text{ active}} |\varphi_i| \geq n^2/2$$

Suppose φ_i not active for max i: replace every occurance of $\varphi_i \in \mathcal{P}$ as a subformula with $\bot$.

PRFCMPLX

<17-1-2014;2> This gives a valid $\mathcal{F}$-proof of:

$\bot \vee (\bot \vee (\bot \vee \ldots \vee \bot))$, which is a contradiction. ▨

"Mention every subformula of the thing we're proving" -- these are our only super-linear Frege lower bounds.

So we'll have to go to weaker systems to get lower bounds.

<u>def</u>: Extended Frege Systems (equiv to Extended Resolution) [Tseitn '68]

Don't want to keep repeating same formula: allow <u>abbreviation</u>.

<u>Resolution</u>
Davis-Putnam late 50's
early 60's
John Robinson '63
Resolution for FO

<u>Extention Rule</u>: $x \leftrightarrow \psi$

where: x does not appear in ψ

x does not appear earlier in the proof

x does not appear in the last line of the proof

$x \leftrightarrow \psi \leftrightarrow$
$(x \rightarrow \psi) \wedge (\psi \rightarrow x)$

x must be a truly <u>new</u> symbol.

an extended Frege proof is a Frege proof ($e\mathcal{F}$-proof) allowing the extention ~~rule~~ rule.

Is this cheating? Do we just trade verification time for proof size?

each line: axiom, MP, extention rule can still check efficiently. so, $e\mathcal{F}$ is an abstract proof system.

<u>Open</u>: does $\mathcal{F}$ simulate $e\mathcal{F}$?

Because, extention rule could cause exponential blowup to expand out into a $\mathcal{F}$-proof....

<u>Observe</u>: if we have $e\mathcal{F} \vdash^{m \text{ lines}} \varphi$, then $\Rightarrow$ $\mathcal{F} \vdash^{O(m) \text{ lines}} \varphi$, just by expanding out each use of extentions.

<u>Notations</u>: $\mathcal{F} \vdash^{n} \varphi$ means φ has a proof of $\leq n$ symbols

<u>Thm</u>: If $\mathcal{F} \vdash^{m \text{ line}} \varphi$, then $e\mathcal{F} \vdash^{O(m + |\varphi|^2)} \varphi$
[Statan '73]

<u>idea</u>: above some threshold of formula size, use extention so that all our formulas are "small"

<u>proof</u>: let P be an m-line $\mathcal{F}$-proof of φ

"active" := ① subformula of φ

② is one of the <u>topmost</u> formulas of either an axiom or a use of MP

"topmost"

MP: $\dfrac{\varphi,\ \varphi \to \psi}{\psi}$, is φ, $\varphi \to \psi$, and ψ: all subformulas above the line, but not <u>their</u> subformulas

$(\varphi \to \chi) \to (\psi \to \chi) \to (\varphi \vee \psi \to \chi)$

enumerate all active formulas as $\chi_1, \chi_2, \chi_3 \ldots \chi_{m'}$
$m' = O(m)$

PRFCMPLX
⟨17-1-2014; 4⟩

Intuition: want $z_i \leftrightarrow \chi_i$

Instead: for $\chi_i \approx \neg\varphi,\ \varphi \vee \psi,\ \varphi \wedge \psi,\ \varphi \to \chi,\ ,\ x$

add these extention axioms:

$$z_{\chi_i} \leftrightarrow \neg z_\varphi \qquad z_{\chi_i} \leftrightarrow z_\varphi \vee z_\psi$$

$$z_{\chi_i} \leftrightarrow z_\varphi \wedge z_\psi \qquad z_{\chi_i} \leftrightarrow (z_\varphi \to z_\chi)$$

$$z_x \leftrightarrow x$$

for non-active φ, ψ: use them directly

for each line ψ in $\mathcal{P}$, prove z_ψ

say ψ is inferred from MP $\dfrac{\varphi_1 \quad , \varphi_1 \to \psi}{\psi}$

by ind. hyp, we already proved z_{φ_1} and $z_{\varphi_1 \to \psi}$

so instead of MP, we use the extention line:

$$z_{\varphi_1 \to \psi} \leftrightarrow (z_{\varphi_1} \to z_\psi)$$

$$z_{\varphi_1} \to (z_{\varphi_1 \to x} \leftrightarrow (z_{\varphi_1} \to z_\psi)) \to z_\psi$$ // this is a tautology w/ a constant-sized proof, so we can obtain z_ψ from the proof of z_{φ_1} and $z_{\varphi_1 \to \psi}$ in constant-length

<u>finally</u>: we've proved z_φ, from this we need to prove φ, so prove $z_x \leftrightarrow x$ $\forall x$ subformulas of φ

total cost: $O(\sum |x|) = O(|\varphi|^2)$

basically, in $e\mathcal{F}$, lines of proof can be compressed down.

Note that earlier lowerbound still works for $e\mathcal{F}$... can't lose that $|\varphi|^2$ factor at the end unless you're happy stopping at z_φ.

<u>Central Example</u>: PHP, the pigeonhole principal

" $\neg f : [n+1] \xrightarrow{1:1,\ onto} [n]$ " , $[n] = \{0, \dots, n-1\}$

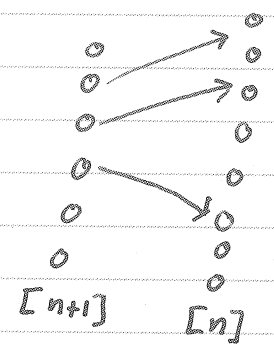
$$PHP_n^{n+1}\left(\bigwedge_{i=0}^{n} \bigvee_{j=0}^{n-1} x_{ij}\right) \to \bigvee_{i=0}^{n} \bigvee_{i'=i+1}^{n} \bigvee_{j=0}^{n-1} (x_{ij} \wedge x_{i'j})$$

$|PHP_n^{n+1}| = O(n^3)$ $\qquad$ x_{ij} means "$f(i) = j$"

so the above says there is at least one collision, and is a TAUTOLOGY

[CR '79] $e\mathcal{F} \vdash^{n^{O(1)}} PHP_n^{n+1}$

<u>proof idea</u>:



(bipartite showing f)

x_{ij} = edges

use extention to introduce vars x_{ij}^{ℓ}, $\ell = n, \dots, 1$

so we will show: $\qquad i \leq \ell,\ j < \ell$

$\neg PHP_\ell^{\ell+1} \to \neg PHP_{\ell-1}^{\ell}$

then get $\neg PHP_n^{n+1} \to \neg PHP_1^2$, but we can prove PHP_1^2

PRFCMPLX

(17-1-2014; 6) Extentions: $x^n_{ij} \leftrightarrow x_{ij}$

$$x^{\ell-1}_{ij} \leftrightarrow \left(x^{\ell}_{ij} \vee \left(x^{\ell}_{i,\ell-1} \wedge x^{\ell}_{\ell,j} \right)\right)$$

from here there is a straightforward proof of:

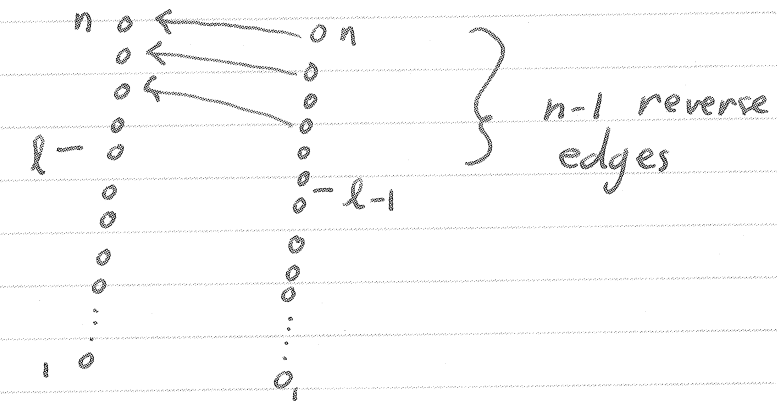
$$\neg PHP^{\ell+1}_{\ell}(\bar{x}^{\ell}) \to \neg PHP^{\ell}_{\ell-1}(\bar{x}^{\ell-1})$$

then we get: $\neg PHP^{n+1}_{n}(\vec{x}) \to \neg PHP^{2}_{1}(\vec{x}^{1})$

<u>Thm</u>: [Buss 86] $\mathcal{F} \vdash^{poly} PHP^{n+1}_{n}$

<u>proof</u>: formalizing counting in $\mathcal{F}$

<u>Thm</u>: [Buss, 1/10/2014] CR79 can be adapted to show $\mathcal{F} \vdash^{quasi\text{-}poly} PHP^{n+1}_{n}$



x^{ℓ}_{ij} - "there is a directed path in this graph from i to j" $\in NC^2$, so quasipoly formulas!

So PHP can't separate $e\mathcal{F}$ from $\mathcal{F}$....

"partial consistency" complete for $e\mathcal{F}$

no other candidates to separate $e\mathcal{F}$ from $\mathcal{F}$...