There are formulas $\varphi_n$, s.t. $|\varphi_n| = O(n)$ & the shortest $S$-proofs of $\varphi_n$ are size $\Omega(n^2)$

let: $T$ abbreviate $x, v \rightarrow x$
  $I$ abbreviate $x, \top \rightarrow x$

$\varphi_n := \underbrace{\top \lor (\top \lor (\top \lor \ldots \top \lor \top \lor T)) \ldots}$

$n$ levels of nesting

start by proving $T$, then $\top \lor T$, then $(\top \lor T) \lor \top$

$\varphi_n \vdash \varphi_n$, How do we prove this proof is optimal?

Fix $n$ large, let $P$ be a $F$-proof of $\varphi_n$, $|P| \leq n$

We say $\varphi_i$ is active in $P$, if some axiom of $P$ uses $\varphi_i$ in a top-level formula.

$\varphi_i$ is $\top \lor \varphi_{i-1}$

$\varphi_i$ if this $v$ is one of the distinguished $v$'s in these axioms:

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

$|P| \geq \sum |\varphi_i| \geq \Omega(n^{\frac{3}{2}})$

$\varphi_i$ active

Suppose $\varphi_i$ not active for max $i$: replace every occurrence of $\varphi_i \in P$ as a subformula with $\top$.
This gives a valid \( \mathcal{F} \)-proof of:

\[ \neg v (\neg v (\neg v \ldots \, \neg v \, \neg 1)) \text{, which is a contradiction.} \]

"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.

**def:** Extended Frege Systems (equiv to Extended Resolution [Tseitin '68]

Don't want to keep repeating same formula: allow abbreviation.

**Resolution**

<table>
<thead>
<tr>
<th>Davis-Putnam late '50s</th>
<th>Extention Rule: (x \rightarrow \psi)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early '60s</td>
<td>where: (x) does not appear in (\psi)</td>
</tr>
<tr>
<td>John Robinson '63</td>
<td>(x) does not appear earlier</td>
</tr>
<tr>
<td>Resolution for FO</td>
<td>in the proof</td>
</tr>
<tr>
<td></td>
<td>(x) does not appear in the last line of the proof</td>
</tr>
</tbody>
</table>

\[ x \leftrightarrow \psi \leftrightarrow (x \rightarrow \psi) \land (\psi \rightarrow x) \]

\(x\) must be a truly new symbol.

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

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

Each line: axiom, MP, extension rule can still check efficiently. So, e\(\mathcal{F}\) is an abstract proof system.
Open: does \( F \) simulate \( eF \)?

Because, extension rule could cause exponential blowup to expand out into a \( F \)-proof...

Observe: if we have \( F \mid m \text{ lines } \psi \), then \( F \mid o(m) \text{ lines } \psi \), just by expanding out each use of extensions.

Notations: \( \bar{F} \mid n \psi \) means \( \psi \) has a proof of \( \leq n \) symbols

Thm: If \( F \mid m \text{ line } \psi \), then \( eF \mid O(m + 19m^2) \psi \)

[Statan '73]
idea: above some threshold of formula size, use extension so that all our formulas are "small"

proof: let \( P \) be an \( m \)-line \( F \)-proof of \( \psi \)

"active" := \( \exists \) subformula of \( \psi \)

\( \exists \) is one of the topmost formulas of either an axiom or a use of MP

"topmost" of MP

\( MP: \psi, \psi \rightarrow \psi \rightarrow \psi \), is \( \psi, \psi \rightarrow \psi, \) and \( \forall \): all subformulas above the line, but not their subformulas

\( (\psi \rightarrow x) \rightarrow (\psi \rightarrow x) \rightarrow (\psi \psi \rightarrow x) \)

enumerate all active formulas as \( x_1, x_2, x_3, \ldots x_m \)

\( m' = O(m) \)
PRFCMPLX
(17-1-2014; 4)

Intuition: want $z_i \rightarrow x_i$

Instead: for $x_i \equiv \neg \psi, \psi \lor \psi, \psi \land \psi, \psi \rightarrow x_i$,

add these extension axioms:

\[
\begin{align*}
Z_{x_i} \rightarrow Z \psi & \quad Z_{x_i} \rightarrow Z \psi \lor Z \psi \\
Z_{x_i} \rightarrow Z \psi \land Z \psi & \quad Z_{x_i} \rightarrow (Z \psi \rightarrow Z \psi)
\end{align*}
\]

for non-active $\psi$: use them directly

for each line $\psi$ in $\mathcal{P}$, prove $Z \psi$

say $\psi$ is inferred from MP $\psi_i, \psi \rightarrow \psi$

by ind. hyp., we already proved $Z \psi_i$ and $Z \psi \rightarrow \psi$

so instead of MP, we use the extension line:

\[
Z \psi_i \rightarrow \psi \rightarrow (Z \psi_i \rightarrow Z \psi)
\]

\[
Z \psi_i \rightarrow (Z \psi_i \rightarrow Z \psi_i) \rightarrow Z \psi
\]

with this is a tautology w/ a constant-sized proof, so we can obtain $Z \psi$ from the proof of $Z \psi_i$ and $Z \psi \rightarrow \psi$

in constant-length

finally: we've proved $Z \psi$, from this we need to prove $\psi$, so prove $Z x \rightarrow x$ for subformulas of $\psi$

total cost: $O(\Sigma 1i1) = O(14^2)$
basically, in eF, lines of proof can be compressed down.

Note that earlier lower bound still works for eF... can't lose that LP^2 factor at the end unless you're happy stopping at z_4.

Central Example: PHP, the pigeonhole principal

\[ f : [n+1] \rightarrowtail [n], \quad [n] = \{0, \ldots, n-1\} \]

\[ \text{PHP}^{n+1} \left( \bigwedge_{i=0}^{n} \bigwedge_{j=0}^{n-1} x_{ij} \right) \rightarrow \bigwedge_{i=0}^{n} \bigwedge_{j=0}^{n} \bigwedge_{i'j'}^{n-1} (x_{i'j'} \land x_{ij}) \]

\[ |\text{PHP}^{n+1}| = O(n^3) \quad x_{ij} \text{ means } "f(i) = j" \]

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

\[ [CR'79] \quad e \vdash \sum_{n \in \omega} \text{PHP}^{n+1} \]

proof idea:

(bipartite showing f)

\[ x_{ij} = \text{edges} \]

use extension to introduce vars \( x_{ij}^l \), \( l = n, \ldots \)

so we will show:

\[ \neg \text{PHP}^{l+1} \rightarrow \neg \text{PHP}^l \quad i \leq l, j \leq l \]

then get \( \neg \text{PHP}^{n+1} \rightarrow \neg \text{PHP}^2 \) but we can prove PHP^2.
PRFCMPLX

(17-1-2014; 6)

Extens: \( x_{ij} \to x_{ij} \)

\( x_{ij} \to (x_{ij} \lor (x_{i, l-1} \land x_{l, j})) \)

From here there is a straightforward proof

\( \neg \text{PHP}^{l+1}(\overline{x}^l) \to \neg \text{PHP}^l(\overline{x}^{l-1}) \)

Then we get: \( \neg \text{PHP}^{n+1}(\overline{x}) \to \neg \text{PHP}^2(\overline{x}^1) \)

**Thm:** [Buss86] \( F \vdash \text{poly} \ \text{PHP}^{n+1} \)

**proof:** formalizing counting in \( F \)

**Thm:** [Buss, 11/10/2014] CR79 can be adapted to show \( F \vdash \text{quasi-poly} \ \text{PHP}^{n+1} \)

\[ x_{ij} \quad \text{there is a directed path in the graph from } i \text{ to } j \quad \in \mathcal{N}^2, \text{ so quasi-poly formulas!} \]

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 \( \mathcal{F} \)....