Lecture 6

- HW 1 posted
- Course project - schedule mtg if you haven't already
- Today: Bdd depth Frege Lower Bounds for PHP

Theorem [P-Beame-Impagliazzo '92, Krajicek-Pudlak-Woods '92]
[Earlier breakthru superpoly LBs Ajtai '88]

Any depth-d Frege proof of PHP^{n+1}_n requires size $2^{n^{\varepsilon_d}}$, $\varepsilon_d \sim \frac{1}{6^d}$

High Level Idea Mirrors AC^0_d-circuit lower Bounds:

Theorem [Ajtai, FSS, Hastad]

$Parity_n$ requires $2^{n^{\varepsilon_d}}$ size AC^0_d-circuits, $\varepsilon_d \sim \frac{1}{2d}$

Proof high Level

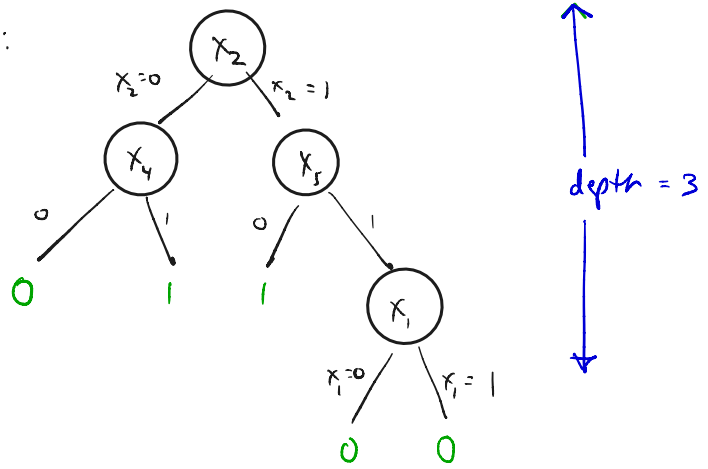
- A restriction $\rho : \{x_1, \dots x_n\} \longrightarrow \{0, 1, *\}$ is a partial assignment that sets some of the underlying variables to 0 or 1.
- Assume for sake of contradiction C is an AC^0_d-circuit of poly size computing Parity over $x_1 \dots x_n$
- Repeatly apply restrictions $\rho_1, \dots, \rho_d$ to successively shrink C to circuits $\underbrace{C_1 = C|_{\rho_1}}_{\text{depth } d-1}$, $\underbrace{C_2 = C|_{\rho_1 \rho_2}}_{\text{depth } d-2}$ $\dots$ $C_d = C|_{\rho_1 \dots \rho_{d-1}}$

← Switching Lemma

In end: C_d is a trivial circuit that cannot compute parity on remaining unset variables

Switching Lemma (for PARITY Lower Bound)

Defn A decision tree T over $x_1 \dots x_n$:



Defn: t-DNF is a disjunction of terms, where each term has max size t

Switching Lemma (for PARITY Lower Bound)

Defn Let f be a t-DNF, ρ a partial restriction

The canonical decision tree for f is defined as follows:

- If $f = 0$, $T(f|_\rho)$: • 0
- If $f = 1$, $T(f|_\rho$: • 1
- If first term of f is C_1, query all vars of C_1

  Each leaf i is associated with a restriction σ_i which sets vars(C_1) according to path from root to leaf i

  Inductively for each leaf i, replace leaf i by the canonical tree for $f|_{\sigma_i}$

Switching Lemma (for PARITY Lower Bound)

Defn Let f be a t-DNF, ρ a partial restriction

The canonical decision tree for f is defined as follows:

- If $f = 0$, $T(f)$ is the decision tree of size 1 labelled 0 • 0
- If $f = 1$, $T(f)$ is " " " " " " " 1 • 1
- If first term of f is C_1, query all vars of C_1

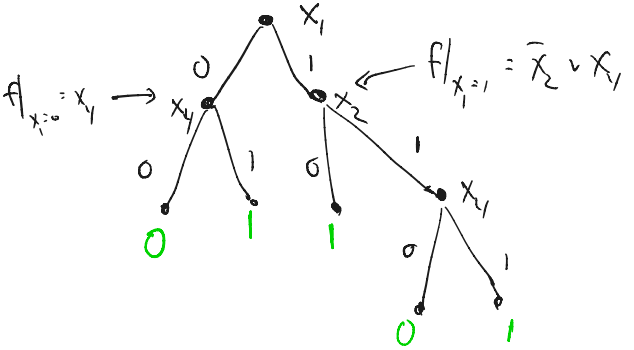
  Each leaf i is associated with a restriction σ_i which sets vars(C_1) according to path from root to leaf i

  Inductively for each leaf i, replace leaf i by the canonical tree for $f|_{\sigma_i}$

Example

$f = x_1\bar{x}_2 \vee x_4$

$t_1 \quad t_2$



Switching Lemma (for PARITY Lower Bound)

Random Restrictions $\mathcal{R}_n^p$: set of all restrictions ρ on domain $x_1 \dots x_n$ where exactly $n - pn$ variables are set to 0/1 and remaining pn variables are set to $*$.

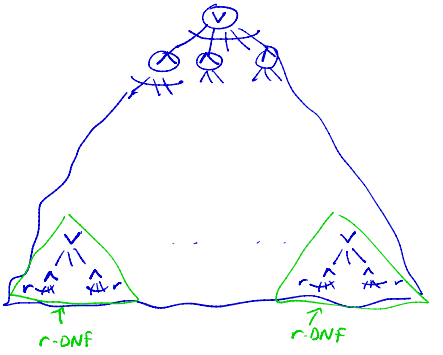
Lemma (Hastad)

Let f be an r-DNF over $x_1 \dots x_n$, $p \leq \frac{1}{4}$

then $\Pr_{\rho \sim \mathcal{R}_n^p} [\, T(f|_\rho) \text{ has depth } \geq s \,] \leq (4pr)^s$

$AC^0[d]$ Lower Bound for PARITY

Lemma (Hastad)
Let f be an r-DNF over $x_1 \dots x_n$. $p \le \frac{1}{4}$
Then $\Pr_{\rho \sim R^p_n}[\, T(f|_\rho) \text{ has depth} \ge s \,] \le (4pr)^s$



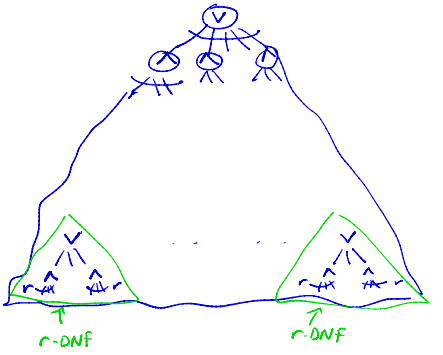
- Assume for contradiction C is a size Δ $AC^0[d]$ formula for Parity_n. Assume w.l.o.g, bottom level of C consists of rDNFs.
- Since C has size $\le \Delta$ at most Δ rDNFs at bottom.
- By Hastad lemma and union bound (assuming $\Delta < \frac{1}{(4pr)^s}$, and setting $r = s$)
  $\exists \rho_1 \in R^p_n$ such that for every bottom-level rDNF f, $T(f|_{\rho_1})$ has depth $\le s$ (since $r = s$)
- Apply ρ_1 to entire circuit — each rDNF under ρ_1 is also an rCNF (since $r = s$)
  so $C|_{\rho_1}$ has depth $d-1$ (merge 2-levels of ANDs at bottom)
- Repeat d times to get $\rho_1 \dots \rho_d$ s.t. $C|_{\rho_1 \dots \rho_d}$ is a depth $\le r$ decision tree
  for $\text{Parity}_{n'}$ where n' = number of variables unset by $\rho_1 \rho_2 \dots \rho_d$

  } since $C|_\rho$ still computes Parity or $\neg$Parity on unset vars

- This contradicts the following (easy) claim, as long as $n' > r$

Claim No depth q decision tree computes Parity on $\ge q+1$ variables

$AC^0[d]$ Lower Bound for PARITY



- Assume for contradiction C is a size ℓ $AC^0[d]$ formula for $Parity_n$. Assume w.l.o.g, bottom level of C consists of rDNFs.
- Since C has size $\le \ell$ at most ℓ rDNFs at bottom.
- By Hastad lemma and union bound (assuming $\ell < \frac{1}{(4pr)^s}$, and setting $r=s$)
  $\exists \rho_1 \in R^p_n$ such that for every bottom-level rDNF f, $T(f|_{\rho_1})$ has depth $\le s$ (since $r=s$)
- Apply ρ_1 to entire circuit — each rDNF under ρ_1 is also an rCNF (since $r=s$)
  so $C|_{\rho_1}$ has depth $d-1$ (merge 2-levels of ANDs at bottom)
- Repeat $d-1$ times to get $\rho_1 \cdots \rho_{d-1}$ s.t. $C|_{\rho_1 \cdots \rho_{d-1}}$ is a depth $\le r$ decision tree
  for $Parity_{n'}$ where n' = number of variables unset by $\rho_1 \rho_2 \cdots \rho_{d-1}$
  } since $C|_\rho$ still computes Parity or $\neg$Parity on unset vars
- This contradicts the following (easy) claim, as long as $n' > r$

Claim No depth q decision tree computes Parity on $\ge q+1$ variables

Parameter settings: the number of unset variables after applying $\rho_1 \cdots \rho_{d-1}$ is $n' = p^{d-1} n$

set $p = \frac{1}{8r}$ so prob. SL fails for a random ρ is $\le \frac{1}{2^s} = \frac{1}{2^r}$

Set $\ell < 2^r$ so $\forall i = 1, \ldots, d-1$, by union bound $\exists \rho_i$ that is good in round i.

For base case claim, need $n' = p^{d-1} n > r \Rightarrow n > (8r)^{d-1} \cdot r$. Set $r = n^{1/2d}$ works.

this gives LB $\ell \ge 2^{n^{\Omega(\frac{1}{2d})}}$

AC^0_d-Frege Lower Bounds for PHP^{n+1}_n

Recall an AC^0_d Frege proof of PHP^{n+1}_n is a sequence of AC^0_d formulas $F_1, F_2, \ldots, F_m$ such that each F_i is either an axiom, or follows from one or two previous lines by a valid Frege rule, and $F_m = PHP^{n+1}_n$.

Assume (for contradiction) we have a size s AC^0_d-Frege proof Π for PHP^{n+1}_n

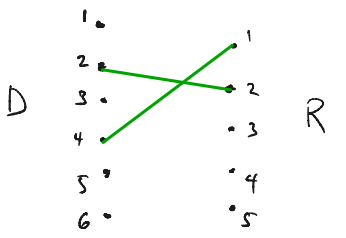
We want to apply a sequence of restrictions to reduce the depth of Π until eventually it has depth 1, and then get a direct contradiction

* Problem: every line in Π is a tautology so each line is already equivalent to a depth-1 trivial formula.

* New Idea: we need to differentiate between a complicated depth-d formula that is equivalent to "1" and a simple formula equiv. to 1.

Imagine instead that n is infinite.
Then there is a 1-1 map from $n+1 \to n$ (for n infinite)
We will define a family of partial restrictions that does not violate PHP, and carry out a similar depth reduction, replacing "equivalent" with "locally consistent"

Matching Disjunctions & Matching Decision Trees



Matching restrictions ρ over $\{P_{i,j}, i \in D, j \in R\}$:

$\rho \in Q_n^\rho$ is a partial 1-1 mapping of size $n-\ell$

corresponding restriction:

If ρ maps $i \to j$ then $\begin{cases} P_{ij} = 1 \\ P_{ij'} = 0 & \forall j' \neq j \\ P_{i'j} = 0 & \forall i' \neq i \end{cases}$

$\rho \in R_4^2$ $n=5$, $\ell = 3$ matching size is $n-\ell$

Matching-disjunctions

A matching disjunction is an OR of matching terms, where a matching term corresponds to a partial 1-1 mapping. An r-disjunction an OR of size $\leq r$ matching terms

Example: $P_{1,2}P_{3,4} \vee P_{3,2}P_{4,1} \vee P_{2,3}$ is a 2-disjunction

Restriction of an r-disjunction f an r-disjunction, ρ a matching restriction

defines $f|_\rho$ in natural way

Example $P_{12}P_{34} \vee P_{32}P_{41} \vee P_{2,3} \Big|_{1\to 3, 4\to 1} = P_{32}$

Matching Disjunctions & Matching Decision Trees

Matching Decision Trees A matching decision tree over $D \cup R$ is a rooted directed tree where:

- Internal nodes labelled by elements of $D \cup R$
- Leaves labelled by 0 or 1
- If the root of T is labelled by $i \in D$, then $\forall j \in R$ there is one outedge from root labelled $i \to j$
- If root of T is labelled by $j \in R$, then $\forall i \in D$, there is one outedge labelled $i \to j$
- Let $T^{[i \to j]}$ be the tree whose root is the node connected to root of T by edge $i \to j$

  Then $T^{[i \to j]}$ is a matching decision tree over $D' \cup R'$, $D' = D \setminus \{i\}$, $R' = R \setminus \{j\}$.

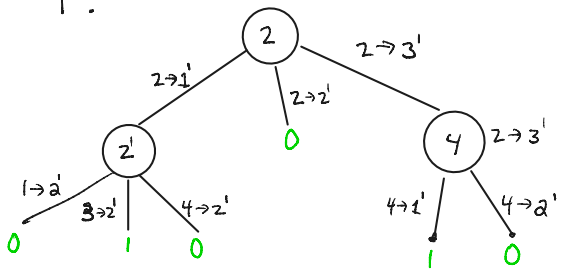
Example

$D = \{1, 2, 3, 4\}$

$R = \{1', 2', 3'\}$

D $\begin{bmatrix} 1 \bullet & \\ 2 \bullet & \bullet 1' \\ 3 \bullet & \bullet 2' \\ 4 \bullet & \bullet 3' \end{bmatrix}$ R

T:



T represents the matching disjunction

$$\text{Disj}(T) = P_{2,1'} P_{3,2'} \vee P_{2,3'} P_{4,1'}$$

(the OR of all 1-paths in T)

Matching Disjunctions & Matching Decision Trees

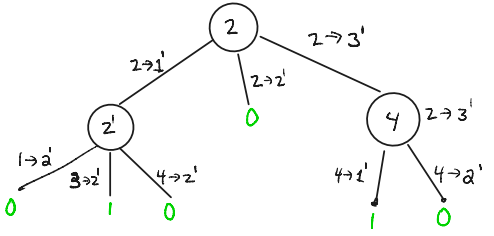
Let ρ be a matching restriction and T a matching decision tree
We define $T|_\rho$ inductively:

1. If T consists of a single node $T|_\rho = T$
2. If T consists of > one node & root of T is labelled with vertex i
   (a) if ρ maps $\{i,j\}$ for some j,
   $T|_\rho = T'|_\rho$ where T' is subtree at root labelled with $\{i,j\}$
   (b) if ρ doesn't map anything to/from i, $T|_\rho$ has root labelled by i with subtrees $T'|_\rho$ where T' is attached to the root by an edge labelled $\{i,k\}$ where k not mapped/fixed by ρ

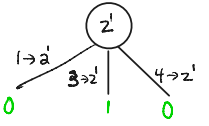
Example

$D = \{1,2,3,4\}$
$R = \{1',2',3'\}$

D $\begin{bmatrix} 1 & \bullet & & \\ 2 & \bullet & & \bullet\, 1' \\ 3 & \bullet & & \bullet\, 2' \\ 4 & \bullet & & \bullet\, 3' \end{bmatrix}$ R



$\rho : 2 \to 1'$



Matching Disjunctions & Matching Decision Trees

Defn Let T be a matching decision tree over variables of PHP_n^{n+1} of depth $< n$, Let f be a matching disjunction. T represents f if: $\forall$ paths in T with associated partial matching restriction σ, $f|_\sigma$ = leaf value of path σ

Lemma Let T be a matching dec. tree, ρ a matching restriction. Then:

1. $Disj(T) \equiv Disj(T|_\rho)$
2. If T is complete over $D^{n+1} \cup R^n$, then $T|_\rho$ is complete over $D^{n+1}|_\rho$, $R^n|_\rho$
3. $(T|_\rho)^c = T^c|_\rho$ where "c" toggles all leaf values of tree
4. If ℓ is a leaf in $T|_\rho$, then $\exists$ leaf ℓ' in T with same label as ℓ so that $\underbrace{\pi(\ell')}_{\substack{\text{partial matching associated} \\ \text{with path in } T \\ \text{from root to } \ell'}} \leq \pi(\ell) \cup \rho$
5. If T represents the matching disjunction F, then $T|_\rho$ represents $F|_\rho$

Switching Lemma (for PHP)

Defn Let f be an r-disjunction, $\rho \in Q_n^p$ a matching restriction

The canonical matching decision tree for f, $T(f)$, is defined as follows:

- If $f = 0$, $T(f|_\rho)$: • 0
- If $f = 1$, $T(f|_\rho$: • 1
- Otherwise Let t_1 be the first matching term of f.

  Create the complete matching decision tree over the set $S' \subseteq D \cup R$ of pigeons/holes mentioned in C_1 (can stop early if t_1 forced to 0 or 1)

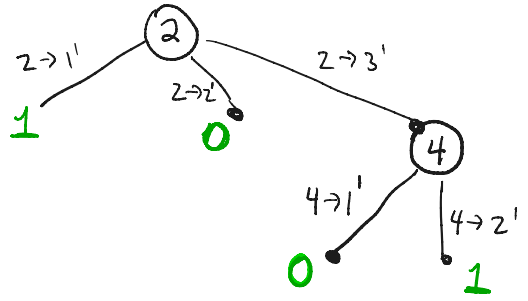
  Each leaf i is associated with a matching restriction σ_i

  Inductively for each leaf i, replace leaf i by the canonical matching decision tree $T(f|_{\sigma_i})$

Switching Lemma (for PHP)

Example $f = \underbrace{p_{2'}}_{t_1} \vee \underbrace{p_{23'} p_{42'}}_{t_2}$

$D = \{1,2,3,4\} \quad R = \{1',2',3'\}$



Query vars (t_1)

Query vars (t_2)

Switching Lemma (for PHP)

Random Restrictions $\mathcal{Q}_n^p$: set of all matching restrictions ρ over $D = [n+1]$, $R = [n]$ such that ρ leaves $pn+1$ pigeons, pn holes unset

Lemma (PHP Switching Lemma)
Let f be an r-disjunction

$$\Pr_{\rho \sim \mathcal{Q}_n^p} [\, T(f|_\rho) \text{ has depth} \geq s \,] \leq (11p^4 n^3 r)^s$$

Switching Lemma (for PHP)

Random Restrictions $\mathcal{Q}_n^\rho$: set of all matching restrictions ρ over $D=[n+1]$, $R=[n]$ such that ρ leaves $pn+1$ pigeons, pn holes unset

Lemma (PHP Switching Lemma)
Let f be an r-disjunction

Then $\Pr_{\rho\sim\mathcal{Q}_n^\rho}[T(f|_\rho) \text{ has depth } \geq s] \leq (16p^4n^3r)^s$ ← worse bound than before but still good enough to get LB $\sim \exp(n^{1/6^d})$

Parameter settings Let $n_0=n$, n_i = number of unset holes after round i. $n_{i+1}=p_{i+1}n_i$, $n_0=n$

Set $p_{i+1}=n_i^{-5/6}$, $r_i=s_i<n_i^{1/6}$ so prob. SL fails for a random ρ is $\sim (n_i^{-\frac{20}{6}} n_i^3 n_i^{1/6})^r = (n_i^{-\frac{20}{6}+\frac{18}{6}+\frac{1}{6}})^r < (\frac{1}{2})^r$

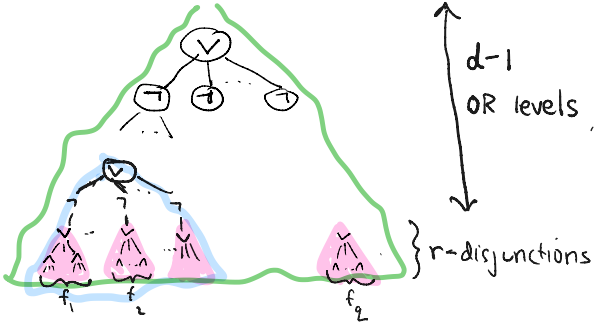
(Note at stage i, $r_i \approx n_i^{1/6}$, where $n_i \sim n_{i-1}^{1/6}$)

Set $d < 2^{r_{d-1}}$ so $\forall i=1\ldots d-1$, by union bound $\exists \rho_i$ that is good at round i

For base case, need $n^{1/6^{d-1}} > r_{d-1}$ which holds when $r_i=s_i << n_i^{1/6}$

This gives lower bound: $d > 2^{n^{r_{d-1}}} \sim 2^{n^{1/6^d}}$

Reducing a depth d formula L by $\rho_1, \ldots, \rho_{d-1}$

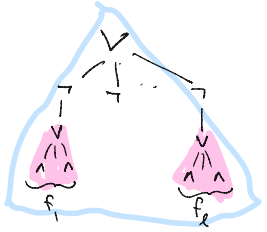


1. Without loss of generality:
   - L is depth d formula over basis $\neg, \bigvee$
     $\left(\bigwedge(F_1, \ldots, F_k) \equiv \neg \bigvee(\neg F_1, \ldots, \neg F_k)\right)$
   - Bottom 2 layers are r-disjunctions

2. Let $\rho_1 \in Q_r^p$ be matching restriction such that $\forall i$ $\mathcal{T}(f_i|_{\rho_1})$ has depth $\leq r$
   (ρ_1 guaranteed to exist by PHP SL)

3. Define $L|_{\rho_1}$: For all bottom-level depth 3 subformulas (Light blue)
   - Convert $\neg f_i|_{\rho_1} \to \neg \mathcal{T}(f_i|_{\rho_1}) \to \mathcal{T}^c(f_i|_{\rho_1})$
   - Convert $\bigvee_{i=1}^{q}(\neg f_i|_{\rho_1}, \ldots, \neg f_i|_{\rho_1}) \to \bigvee_{i=1}^{q} \bigvee_{t \text{ a 1path in } \mathcal{T}(f_i|_{\rho_1})} t$

bottom subformula of L



converts under ρ_1

r-disjunction

Reducing a depth d formula L by $\rho_1, \ldots, \rho_{d-1}$

After step 3, $L|_{\rho_1}$ converted to new formula of OR-depth $d-2$ at top, with r-disjunctions at leaves

Repeat step 3 $d-1$ times so that $L|_{\rho_1 \cdots \rho_{d-1}}$ converts to a single matching decision tree of height $\leq r$

AC^0_d-Frege Lower Bound for PHP^{n+1}_n

- Let Π be an alleged size $< \delta$ AC^0_d-Frege proof of PHP^{n+1}_n. $\Pi = \{L_1, \ldots, L_m\}$.

- So far we have the following "PHP" switching lemma, which (usin parameter settings we gave) can be applied iteratively $d-1$ times to obtain a good sequence of restrictions $\rho_1, \ldots, \rho_{d-1}$ such that under $\rho = \rho_1 \circ \cdots \rho_{d-1}$, we can convert $\Pi = \{L_1, \ldots, L_m\}$ into another sequence of formulas $\Pi^* = \{L_1^* \ldots L_m^*\}$, where L_i^* are depth $\leq r$ matching decision trees obtained by successively applying $\rho_1, \ldots, \rho_{d-1}$ to obtain $L_i', \ldots, L_i^{d-1} = L_i^*$ (as described in last slide).

- To finish the lower bound we need to reach a contradiction by showing that if the proof Π is sound, then Π' is also a "locally" sound proof of $PHP^{n'+1}_{n'}$ on the remaining $n'+1$ unset pigeons, and n' unset holes

AC^0_d-Frege Lower Bound for PHP^{n+1}_n

Defn (k-evaluation)

Let Γ be a set of formulas closed under subformulas, over $D^{n+1} \cup R^n$

A k-evaluation for Γ is an assignment of complete matching decision Trees $\mathcal{T}(A)$ to all formulas A in Γ such that:

(1) $\mathcal{T}(A)$ has depth $\leq k$ $\forall A$

(2) $\mathcal{T}(1)$ is the tree with a single node labelled 1
$\mathcal{T}(0)$ " " " " " " " " 0

(3) $\mathcal{T}(P_{ij})$ is the full matching tree over $D^{n+1} \cup R^n$ with leaf ℓ labelled 1 if $\pi(\ell)$ contains $\{i,j\}$, and 0 ow

(4) If A is a matching disjunction then $\mathcal{T}(A)$ represents $\bigvee_i \mathrm{Disj}(\mathcal{T}(A_i))$

AC^0_d-Frege Lower Bound for PHP^{n+1}_n

Defn (k-evaluation)

Let Γ be a set of formulas closed under subformulas, over $D^{n+1} \cup R^n$. A k-evaluation for Γ is an assignment of complete matching decision trees $\mathcal{T}(A)$ to all subformulas A in Γ such that:

(1) $\mathcal{T}(A)$ has depth $\leq k$ $\forall A$

(2) $\mathcal{T}(1)$ is the tree with a single node labelled 1
$\mathcal{T}(0)$ " " " " " " " " 0

(3) $\mathcal{T}(P_{ij})$ is the full matching tree over $D^{n+1} \cup R^n$ with leaf ℓ labelled 1 if $\pi(\ell)$ contains $\{i,j\}$, and 0 ow

(4) If A is a matching disjunction then $\mathcal{T}(A)$ represents $\bigvee_i Disj(\mathcal{T}(A_i))$

Lemma (obtaining a k-evaluation)

Let Π be a size S depth-d Frege proof of PHP^{n+1}_n. Let $\rho_1, \rho_2, \ldots \rho_{d-1}$ be the good restrictions guaranteed to exist by PHP switching Lemma. Then:

there exists a k-evaluation for $\Gamma = \{$all subformulas occurring in $\Pi|_{\rho_1 \cdots \rho_{d-1}}\}$ over $D^{n+1} \cup R^n$

Proof of (*) omitted, but given inductively on depth d

[Let F_i = all subformulas occurring in Π, & have depth $\leq i$
Then after stage i, we have a k-evaluation for the formulas $F_i|_{\rho_1 \cdots \rho_i}$
$k \leq r_i$]

Base Case Let $\Pi = \{L_1, \ldots, L_m\}$ be alleged proof of PHP_n^{n+1}

It is left to argue that if we have a k-evaluation $\tilde{\gamma}$ for all subformulas of $\Pi|_\rho$ over $D^{n+1} \cup R^{n'}$ where $k << n'$, then we reach a contradiction.

Why?

On the one hand we can show:

(A) All axioms of $\Pi|_\rho$ convert to all-1 trees and the Frege rules preserve 1-trees, so every formula in $\Pi|_\rho$ converts to a 1-tree

On the other hand:

(B) The last line $L_m|_\rho$ converts to an all 0-tree

(B): $\forall n > 1$, PHP_n^{n+1} converts to a 0-tree under $\mathcal{T}$

PHP_n^{n+1} consists of the disjunction of the following formula

(1) $\neg(\neg P_{i,k} \vee \neg P_{j,k})$ $\quad \forall i \neq j \leq n+1,\ k \leq n$

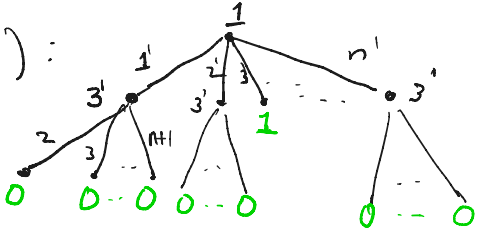
(2) $\neg(P_{i1} \vee P_{i2} \vee \dots \vee P_{in})$ $\quad \forall i \leq n+1$

(1) Since $\mathcal{T}(\neg(\neg P_{ik} \vee \neg P_{jk})) = \left[\mathcal{T}(\neg P_{ik} \vee \neg P_{jk})\right]$, (tree for $\neg P_{ik} \vee \neg P_{jk}$ with all leaf values toggled)

to show $\mathcal{T}(\neg(\neg P_{ik} \vee \neg P_{jk}))$ is a 0-tree, want to show $\mathcal{T}(\neg P_{ik} \vee \neg P_{jk})$ is a 1-tree

$$\mathcal{T}(\neg P_{ik} \vee \neg P_{jk}) = \mathcal{T}\left(Disj(\mathcal{T}^c(P_{ik})) \vee Disj(\mathcal{T}^c(P_{jk}))\right)$$

$\mathcal{T}(P_{1,3'})$:

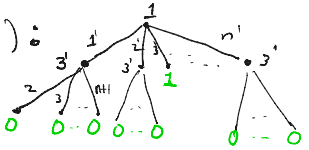


so $\mathcal{T}(\neg P_{1,3'})$: one 0-leaf corresponding to path $1 \to 3'$
all other leaves labelled 1

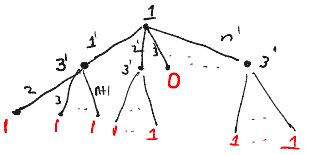
$$\mathcal{T}(\neg P_{ik} \vee \neg P_{jk}) = \mathcal{T}\left(Disj(\mathcal{T}^c(P_{ik})) \vee Disj(\mathcal{T}^c(P_{jk}))\right)$$ ← queries pigeons i, j and hole k

Example $\mathcal{T}(\neg P_{1,3'} \vee \neg P_{2,3'})$

$\mathcal{T}(P_{1,3'})$:

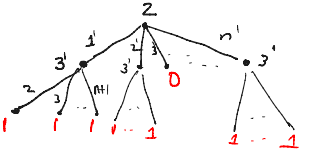


$\mathcal{T}(\neg P_{1,3'})$:



← one 0-leaf corresponding to path $1 \to 3'$

Similarly $\mathcal{T}(\neg P_{2,3'})$:



$$\mathcal{T}(\neg P_{1,3'} \vee \neg P_{2,3'}) = \mathcal{T}\left(\bigvee_{\substack{\text{all 1-paths} \\ G \text{ in } \mathcal{T}(\neg P_{1,3'})}} M_G \vee \bigvee_{\substack{\text{all 1-paths} \\ G' \text{ in} \\ \mathcal{T}(\neg P_{2,3'})}} M_{G'}\right)$$

: Tree queries pigeons 1, 2 and hole 3'.

All leaves labelled by 1

since ever partial matching over $\{2, 1, 3'\}$

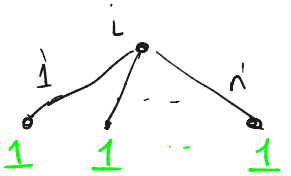
Never maps $2 \to 3'$ and $1 \to 3'$

$$= \text{all 1-tree}$$

(2) show $\mathcal{T}\left(\neg\left(P_{i_1} \vee P_{i_2} \vee \dots \vee P_{i_n}\right)\right) = 0\text{-tree}$

It suffices to show $\mathcal{T}\left(P_{i_1} \vee \dots \vee P_{i_n}\right)$ is a 1-tree:

$\mathcal{T}\left(P_{i_1} \vee \dots \vee P_{i_n}\right)$:



To conclude:

Thm Any AC^0_d-Frege proof of PHP^{n+1}_n requires size $2^{n^{1/6^d}}$.

See [Fu, Urquhart] for omitted lemmas + for a nice presentation of entire argument.

References

① Fu and Urquhart 1996
Simplified Lower Bounds for Propositional Proofs

② Pitassi, Beame, Impagliazzo 1993
Exponential Lower Bounds for the Pigeonhole Principle

③ Krajicek - Pudlak - Woods 1995
Exponential lower bounds to the size of Bounded Depth Frege proofs of the Pigeonhole Principle

④ Ajtai 1988
The complexity of the Pigeonhole Principle

} Streamlined, simplified presentation of ②, ③

} First exponential Lower Bounds $S \geq \exp(n^{\Omega(\frac{1}{d})})$

} First superpoly LB

Followup Paper giving Tighter Lower Bounds:

Hastad, 2023
On small-depth Frege proofs for PHP.

} $S \geq \exp(n^{\Omega(\frac{1}{d})})$ (nearly tight)