# Lecture 13: "The Pigeonhole principle is hard for bounded depth Frege"

In this and the next two lectures we are going to prove that the pigeonhole principle is hard for bounded depth Frege. Those lectures are based on

Urquhart, Fu "<u>Simplified</u> Lower Bounds for Propositional Proofs", 1996.
$\longrightarrow$ the original proof is due to [Beame, Impagliazzo, Krajíček, Pitassi, Pudlák, Woods - 1992]

— PRELIMINARIES —

Consider fixed two disjoint sets $P$ and $H$ respectively of size $n+1$ and $n$. $P$ for "pigeons" and $H$ for "holes". Let $K(P,H)$ be the complete bipartite graph with bipartition $(P,H)$. We consider the language $\mathcal{L}_n$ built from the variables $\{x_e : e \in K(P,H)\}$, the constants $0$ and $1$, and the connectives

- $\neg$ (NOT, unary operator), $\vee$ (OR, as a binary operator).

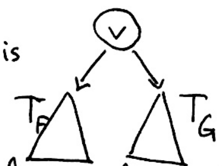
- In this language we can express the (onto functional) pigeonhole principle as a tautology, this will be the negation of the usual $OFPHP_n^{n+1}$ but for clarity let's write it explicitly:

$$\neg OFPHP_n^{n+1} = \bigvee_{i \in P}\Big(\neg \bigvee_{j\in H} x_{ij}\Big) \vee \bigvee_{\substack{j \in H\\ i \neq i' \in P}} \big(\neg(\neg x_{ij} \vee \neg x_{i'j})\big) \vee \bigvee_{j\in H}\Big(\neg \bigvee_{i \in P} x_{ij}\Big) \vee \bigvee_{\substack{i\in P\\ j\neq j' \in H}}\big(\neg(\neg x_{ij} \vee \neg x_{ij'})\big)$$

Technically speaking all the unbounded ORs above should be expanded using the binary $\vee$, e.g. $A \vee B \vee C$ should be expanded as $(A\vee B)\vee C$.
This is not really crucial and indeed it is useful to introduce those unbounded

- ORs as a notation, the <u>merged form</u>, given a disjunction $F$, the merged form of $F$ is $\bigvee_{i\in I} F_i$, where the $F_i$ are the subformulas of $F$ that are not disjunctions but every proper subformula of $F$ containing $F_i$ is a disjunction.

- To every formula $F$ in the language $\mathcal{L}_n$ we can associate its formation tree $T_F$ as follows: $T_{x_{ij}}$ is $x_{ij}$ ; $T_{\neg F}$ is  ;

$T_{F\vee G}$ is 

$\boxed{\text{make small example in class}}$

The <u>logical depth</u>, or just depth, of a formula $F$ is the maximum number of alternations between $\vee$ and $\neg$ in any path of the formation tree of $F$.
¿what is the logical depth of $\neg OFPHP_n^{n+1}$?

We are going to see now a proof system to prove tautologies (instead of refuting contradictions).

The Shoenfield' system $S$ is a sound and implicationally complete Frege system over the connectives $\neg$ and $\vee$ (binary) with the following inference rules:

$$\frac{}{A \vee \neg A} \text{ (excluded middle)} \qquad \frac{A}{A \vee B} \text{ (expansion)} \qquad \frac{A \vee A}{A} \text{ (contraction)}$$

$$\frac{(A \vee B) \vee C}{A \vee (B \vee C)} \text{ (associativity)}$$ and last but not least, the cut rule:

$$\frac{A \vee B \qquad \neg B \vee C}{A \vee C}.$$ A, B, C are place holders for formulas over $\{\vee, \neg\}$.

Unlike Res or Res(k) this proof system is a proof system that proves tautologies (instead of refuting contradictions) and since it is implicationally complete, that is

- whenever $F_1, \dots, F_m \models F_0$ then there is a derivation of $F_0$ from $F_1, \dots, F_m$ using the rules of $S$, then $S$ proves $\neg OFPHP_n^{n+1}$ from an empty set of premises.
- Let $\Pi$ be a proof in $S$, the depth of $\Pi$ is the maximum logical depth of a formula in $\Pi$; the size of $\Pi$ is the number of subformulas in $\Pi$, which is roughly the number of symbols in $\Pi$.

$S$ restricted only on derivations of formulas of depth 1 is morally p-equivalent to Resolution. $S$ restricted only on derivations of formulas of depth 2 is much stronger than Res(k) for any k for example constant.

## – THE MAIN THEOREM –

- In this and the next two lectures we are going to prove the following theorem.

> **Thm1:** Let $S$ be the Shoenfield's system above and let $d > 3$. For sufficiently large $n$, every depth $d$ proof of $\neg OFPHP_n^{n+1}$ in $S$ must have size $2^{n^\delta}$ for $0 < \delta < \left(\frac{1}{5}\right)^d$.

This result actually holds for any Frege system over $\{\vee, \neg\}$ with rules of bounded size, e.g. the cut rule in $S$ has size 7 since taken as atomic A, B, C it involves only 7 distinct formulas. For simplicity let's stick with $S$.

In Thm 1 we prove something actually slightly stronger, that is that every proof of $\neg OFPHP_n^{n+1}$ in S must contain at least $2^{n^\delta}$ distinct subformulas.

The proof of Thm 1 is quite conceptually involved so let's start with some informal view of what will be going on. The key notion is the concept of <u>K-evaluation</u>.

Another way of seeing this is to see a K-evaluation as **a way of** associating to formulas decision trees representing the formulas seen as Boolean functions <u>BUT</u> in a slightly buggy way...

## — K-EVALUATIONS —

Usually a valuation is a way of assigning a truth value (0/1) to formulas. A K-evaluation does a similar job <u>but</u> associating to formulas sets of partial assignments (represented using some trees) and a value the formula should take on each of those assignments. If the K-evaluation says that all the partial assignments associated to a formula F will give value 1 to F then it is kind of a "tautology". We will be able to show that all the lines in a proof in $\mathcal{S}$ are kind of tautologies but under the K-evaluation we build $\neg OFPHP_n^{n+1}$ will not be "kind of tautology". This contradiction will arise from the fact that in order to build the K-evaluation we will suppose that the proof of $\neg OFPHP_n^{n+1}$ is small, so no such small proof could exists.
Unlike the classical notion of tautology, this notion of "kind of tautology" is not preserved under classically sound inferences so we have to be quite careful in building and handling such concept.

o——o

The partial assignments we consider are naturally associated to matchings in $K(P,H)$, a matching is just a set of vertex-disjoint edges. Let $\mathcal{M}_n$ be the set of all matchings in $K(P,H)$. If $\alpha \in \mathcal{M}_n$ we can associate to it the following partial assignment:

$$\tilde{\alpha}(x_{ij}) = \begin{cases} 1 & \text{if } (i,j) \in \alpha \\ 0 & \text{if } \exists i' \neq i \text{ s.t. } (i',j) \in \alpha \\ 0 & \text{if } \exists j' \neq j \text{ s.t. } (i,j') \in \alpha \\ * & \text{otw.} \end{cases}$$

Given a formula F in $\mathcal{L}_n$ and a matching $\alpha \in \mathcal{M}_n$ we write $F\restriction_\alpha$ instead of $F\restriction_{\tilde{\alpha}}$ just to avoid too heavy notation.

<u>ex.</u> (super easy) given a matching $\alpha \in \mathcal{M}_n$ of size $n-n'$, $\neg OFPHP_n^{n+1}\restriction_\alpha$ is equivalent (up to renaming of variables) to $\neg OFPHP_{n'}^{n'+1}$.

From now on we focus on partial assignments coming from matchings, and on how to represent them.

The main notion needed to define K-evaluations is the notion of Complete Matching Decision Tree (CMDT).

<u>Def:</u> (CMDT) A tree $T$ is a <u>Complete Matching Decision Tree</u> (CMDT) over $P \cup H$ if it has associated a labeling of its vertexes and edges s.t.

(i) no label (either vertex or edge label) is repeated in any branch of T;

(ii) each internal node has as label a vertex in $P \cup H$;

(iii) the edges in $T$ going out a vertex with label $i \in P \cup H$ must have as labels edges adjacent to $i$ in $K(P,H)$;

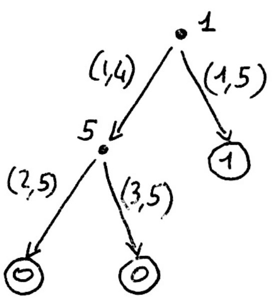
(iv) given a path in $T$, the labels of its edges form a matching in $K(P,H)$;

(v) the leaves have labels either 0 or 1;

(vi) (completeness) the labels of the edges going out from a vertex $i$ must correspond to <u>all</u> the possible ways of extending the matching corresponding to the path in $T$ leading to $i$.

<u>example</u>: $P = \{1,2,3\}$ $H = \{4,5\}$

Let $CMDT_n$ be the set of all CMDT $T$ over $P \cup H$.




is a CMDT.

Let $Br_i(T)$ be the set of paths (identified with the corresponding matching) leading to a leaf in $T$ with label $i$.

A CMDT $T$ (strongly) <u>represents</u> a formula $F$ in the usual way:

if for every $\alpha \in Br_0(T)$ $F\restriction_\alpha \equiv 0$ and

if for every $\alpha \in Br_1(T)$ $F\restriction_\alpha \equiv 1$.

(Recall that $F\restriction_\alpha$ is the formula $F$ restricted with the partial assignment associated with the path and matching given by $\alpha$, and then simplified using the usual rules: $\neg 0 \equiv 1$, $\neg 1 \equiv 0$, $0 \vee A \equiv A$, $A \vee 0 \equiv A$, $(1 \vee A) \equiv 1$, $(A \vee 1) \equiv 1$.)

Given a CMDT $T$ we need to canonically associate to it a DNF, <u>Disj (T)</u>, defined as follows:

$$Disj(T) = \bigvee_{\alpha \in Br_1(T)} \left( \bigwedge_{e \in \alpha} x_e \right).$$

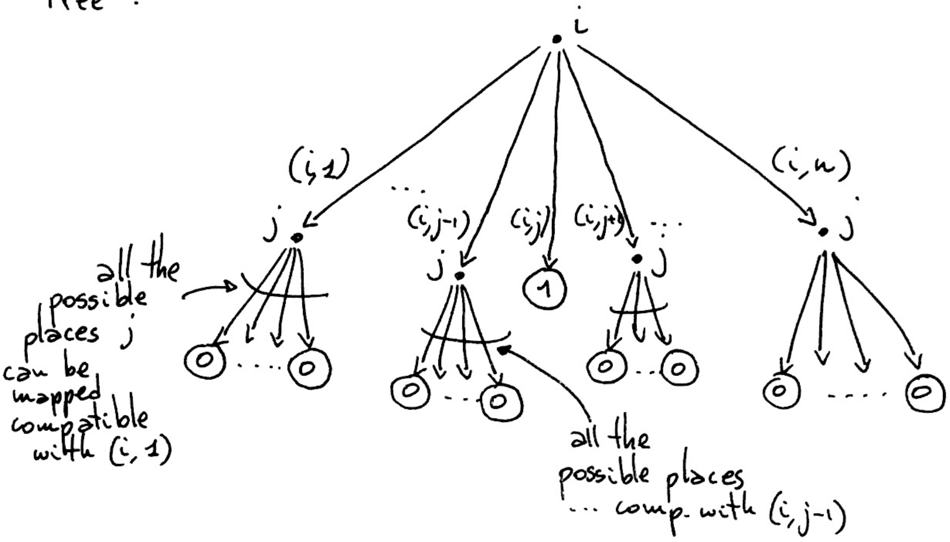
DNFs of this form where each term has variables whose edges give a matching, are called <u>matching DNFs</u>.

We now have all the ingredients needed to define the notion of $\kappa$-evaluations.

<u>Def</u>: ($\kappa$-evaluations) Let $\Gamma$ be a set of formulas over $\mathcal{L}_n$. A <u>$\kappa$-evaluation of $\Gamma$</u> is a function $\nu : \Gamma \longrightarrow CMDT_n$ s.t.

(i) for each $F \in \Gamma$ $\nu(F)$ has depth $\leq \kappa$;

(ii) $\nu(0)$ is the tree having a single node with label $0$ (similarly for $\nu(1)$). For each variable $x_{ij}$, $\nu(x_{ij})$ is the following CMDT tree:




(notice that the only label 1 is the one shown, all the other labels of leaves are 0)

(iii) $\nu(\neg F)$ is $\nu(F)$ with all the labels of the leaves flipped from 0 to 1 and viceversa;

(iv) if $F$ is a disjunction with merged form $\bigvee_{i \in I} F_i$ then $\nu(F)$ represents $\bigvee_{i \in I} Disj(\nu(F_i))$.

---

Given a $\kappa$-evaluation $\nu : \Gamma \to CMDT_n$ and a formula $F \in \Gamma$, our informal notion of being "Kind of a tautology" corresponds on $\nu(F)$ having all leaves with label 1.

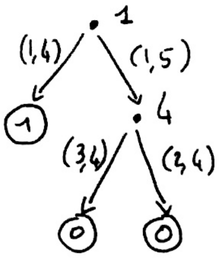
The next example will hopefully clarify this notion and show that the notion of being "Kind of a tautology" is not preserved under under sound inferences.

example: Let $P = \{1,2,3\}$ and $H = \{4,5\}$, let

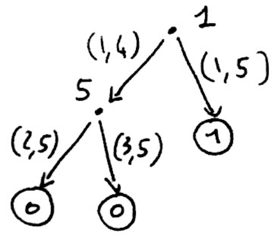
$$\Gamma = \{ x_{14} \vee x_{15},\ \neg x_{15} \vee \neg x_{25},\ x_{14} \vee \neg x_{25} \}$$

let's construct a possible 2-evaluation of $\Gamma$:

$\nu(x_{14}) =$




$\nu(x_{15}) =$

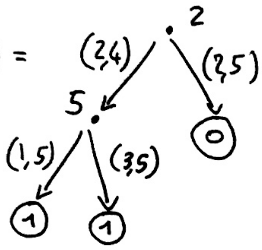



$Disj(\nu(x_{14})) = x_{14}$

$Disj(\nu(x_{15})) = x_{15}$

$Disj(\nu(\neg x_{15})) = (x_{14} \wedge x_{25}) \vee (x_{14} \wedge x_{35})$

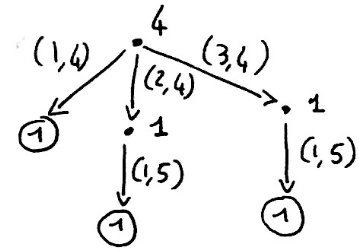
$\nu(\neg x_{25}) =$



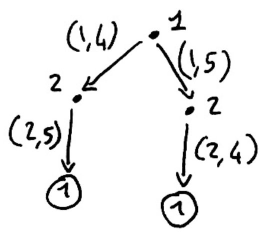

$Disj(\nu(\neg x_{25})) = (x_{24} \wedge x_{15}) \vee (x_{24} \wedge x_{35})$

why can't we just append to every leaf of $\nu(x_{14})$ the tree $\nu(x_{15})$ and choose the leaves s.t. the resulting tree represents $x_{14} \vee x_{15}$?

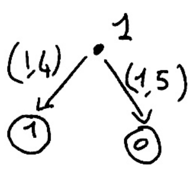
$\nu(x_{14} \vee x_{15})$ represents $x_{14} \vee x_{15}$, take for example




$\nu(\neg x_{15} \vee \neg x_{25})$ must represent $(x_{14} \wedge x_{25}) \vee (x_{14} \wedge x_{35}) \vee (x_{24} \wedge x_{15}) \vee (x_{24} \wedge x_{35})$, take for example:




$\nu(x_{14} \vee \neg x_{25})$ must represent $x_{14} \vee (x_{14} \wedge x_{25}) \vee (x_{14} \wedge x_{35})$, take for example



**Lemma 1**: Let $\Gamma$ be a set of formulas containing $\neg OFPHP_n^{n+1}$ and let $\nu$ be a $k$-evaluation of $\Gamma$ with $k \leq n-1$ then $\nu(\neg OFPHP_n^{n+1})$ has all leaves 0.

**Lemma 2**: Let $\mathcal{S}$ the Shoenfield's system and $\Pi$ any proof in $\mathcal{S}$. Let $\nu$ be a $k$-evaluation of $\Pi$ s.t. $k \leq \frac{n}{7}$ then for every line $F$ in $\Pi$, $\nu(F)$ has all leaves labeled 1.

We will see the proofs of the above two lemmas in the next lecture but already now it should be clear that something is going wrong badly: $\mathcal{S}$ is implicationally complete so there exists a proof of $\neg OFPHP_n^{n+1}$ but now *if* there exists a $k$-evaluation $\nu$ then $\nu(\neg OFPHP_n^{n+1})$ must have both all leaves 0 and all leaves 1 which is obviously impossible. So are $k$-evaluations objects that do not exists after all? No, they exists under certain conditions.

**Lemma 3**: Let $d$ be an integer, $0 < \varepsilon < \frac{1}{5}$, $0 < \delta < \varepsilon^d$ and $\Gamma$ a set of formulas of $\mathcal{L}_n$ of depth $\leq d$ closed under subformulas. If $|\Gamma| \leq 2^{n^\delta}$, $q = \lceil n^{\varepsilon^d} \rceil$ and $n$ sufficiently large, then there exist a matching $\alpha \in \mathcal{M}_n$ of size $n-q$ so that there exists a $2n^\delta$-evaluation of $\Gamma\lceil_\alpha$.

proof in two lectures

Given the lemmas above now the proof of Thm 1 is almost immediate.

Proof (of Thm 1): Let $0 < \delta < (\frac{1}{5})^d$ and, by contradiction, suppose there exists a proof $\Pi = (F_1 \dots F_t)$ of $\neg OFPHP_n^{n+1}$ of size $\leq 2^{n^\delta}$. Take $\varepsilon$ s.t. $\varepsilon < \frac{1}{5}$ and $\delta < \varepsilon^d$, then Lemma 3 applies: there exists a matching $\alpha \in \mathcal{M}_n$ of size $n - \lceil n^{\varepsilon^d} \rceil$ s.t. there exists a $2n^\delta$-evaluation $\nu$ of $(F_1\lceil_\alpha, \dots, F_t\lceil_\alpha) = \Pi\lceil_\alpha$ which is a valid proof of $\neg OFPHP_n^{n+1}\lceil_\alpha$ which is (up to renaming of variables) the same of $\neg OFPHP_{n^{\varepsilon^d}}^{n^{\varepsilon^d}+1}$. Since $\delta < \varepsilon^d$, for $n$ sufficiently large $2n^\delta \leq \frac{n^{\varepsilon^d}}{7}$, so Lemma 1 applies. Since $\Pi\lceil_\alpha$ is a proof in $\mathcal{S}$ of $\neg OFPHP_n^{n+1}\lceil_\alpha$, the last line of $\Pi\lceil_\alpha$ is exactly this formula but then $\nu$ will map it both to a tree with all leaves 0 and all leaves 1. Contradiction. So it must be that $|\Gamma| \geq 2^{n^\delta}$ for $\delta < (\frac{1}{5})^d$ and $n$ suff. large.

$\blacksquare$