Lecture 15: "PHP is hard for bd Frege" - part III -

We conclude the proof of the following theorem.

Thm: Let $\mathcal{F}$ be a Frege system over $\{\vee, \neg\}$ and let $d > 3$. For sufficiently large n, every depth d proof of $\neg \text{OFPHP}_n^{n+1}$ in $\mathcal{F}$ has size $\geq 2^{n^\delta}$ for $0 < \delta < \left(\frac{1}{5}\right)^d$.

Lemma 3: Let d be an integer, $0 < \varepsilon < \frac{1}{5}$, $0 < \delta < \varepsilon^d$ and Γ a set of formulas of depth $\leq d$ closed under subformulas.
If $|\Gamma| < 2^{n^\delta}$ then there exist a $\rho \in M_n^q$ with $q = n^{\varepsilon^d}$ and there exist a $2n^\delta$-evaluation of $\Gamma\restriction_\rho$.

M_n^q = the set of all matchings of size q over P, H of size $n+1$ and n resp.

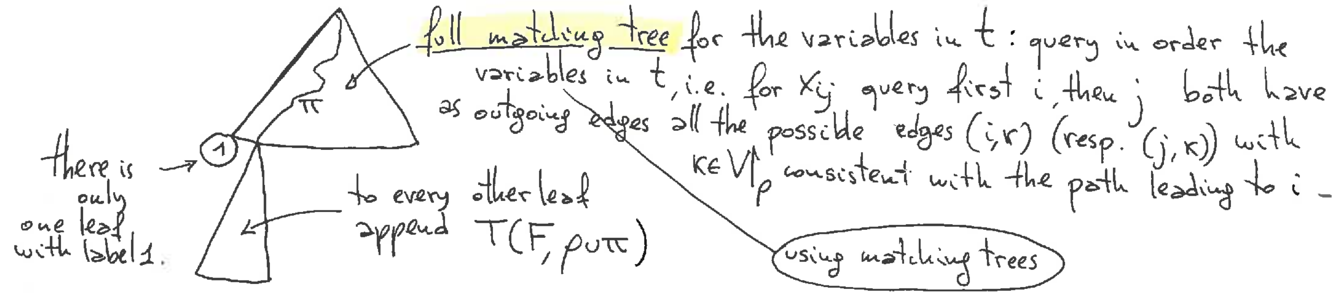
The proof of Lemma 3 will construct (by ind on the depth) a K-evaluation using some very specific Kind of CMDT, i.e. canonical trees. To Keep their depth small we will use restrictions and a Switching Lemma then since K-evaluations are well-behaved under restrictions then we will be able to build a K-evaluation in Lemma 3. This is from a very high level perspective the plan of the lecture.

- Canonical Matching Decision Trees -

Given a matching disjunction $F = t_1 \vee \dots \vee t_m$, and a matching $\rho \in \mathcal{M}_n$, the canonical matching decision tree $T(F,\rho)$ is the following tree in $CMDT(V\restriction_\rho)$ representing $F\restriction_\rho$: fix an ordering on the terms of F and fix an ordering on the variables of F,

(i) if $F\restriction_\rho \equiv 0$ then $T(F,\rho)$ is a single node labeled 0, analogously for $F\restriction_\rho \equiv 1$

(ii) if $F\restriction_\rho \not\equiv 0$ and $F\restriction_\rho \not\equiv 1$ let t be first non-zero term in $F\restriction_\rho$ then $T(F,\rho)$ is constructed as follows:



example 1: the trees we used in the definition of k-evaluations for x_{ij} are canonical.

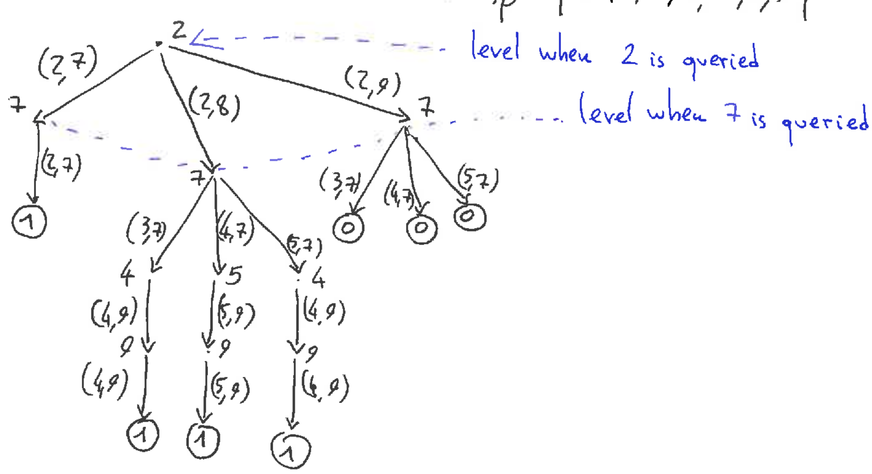
example 2: $P = \{1,2,3,4,5\}$ $H = \{6,7,8,9\}$

$$F = (x_{17} \wedge x_{38}) \vee (x_{16} \wedge x_{27}) \vee (x_{16} \wedge x_{49}) \vee (x_{16} \wedge x_{59})$$

$\rho = \{(1,6)\}$ suppose that the terms and vars are ordered according the way they are written in F above.

Write $T(F,\rho)$.

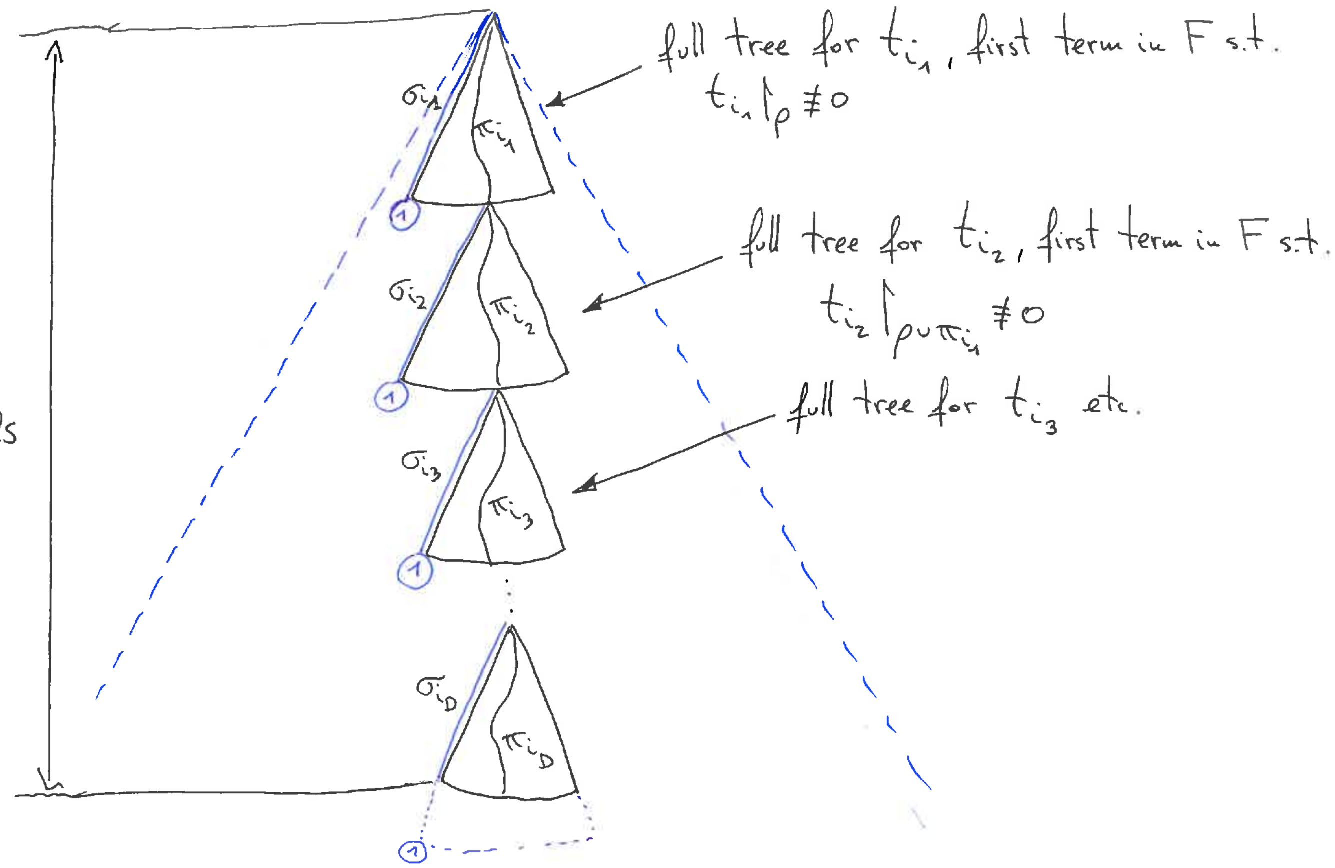
$F\restriction_\rho = x_{27} \vee x_{49} \vee x_{59}$ $V\restriction_\rho = \{2,3,4,5,7,8,9\}$



Lemma 4 (switching lemma): Let $F = t_1 \vee \cdots \vee t_m$ be an r-matching DNF over P,H resp of size $n+1, n$. Let s be an integer, $\ell \leq n$ and let
$$Bad_n^\ell(F,2s) = \{\rho \in M_n^\ell : T(F,\rho) \text{ has depth} \geq 2s\}$$
Then
$$\frac{|Bad_n^\ell(F,2s)|}{|M_n^\ell|} \leq \left(\frac{2r(2\ell+1)^4}{n-\ell}\right)^s \qquad (*)$$

(Notice that the bound in $(*)$ does not depend on the number of terms in F)

proof: (using the encoding idea by Razborov)
We build an injective mapping $\eta : Bad_n^\ell(F,2s) \longrightarrow M_n^{\ell-s} \times code(r,s) \times [2\ell+1]^{2s}$, where $code(r,s)$ is the set of all strings $\vec{\beta} = (\beta_1, \ldots, \beta_D)$ s.t. $\beta_i \in \{0,1\}^r \setminus \{0\}^r$ and the number of occurrences of 1s in $\vec{\beta}$ is exactly s.
From the existence of such η, the fact that $|code(r,s)| \leq \left(\frac{r}{\ln 2}\right)^s$ (ex.) and the fact that $\frac{|M_n^{\ell-s}|}{|M_n^\ell|} \leq \left(\frac{\ell(\ell+1)}{n-\ell}\right)^s$ (also ex.) we immediately get the bound in $(*)$. So let's focus on building such η.
If $\rho \in Bad_n^\ell(F,2s)$ then $T(F,\rho)$ looks like the following picture:



Let's say that $\pi = \pi_{i_1} \cup \dots \cup \pi_{i_D}$ is the leftmost path in $T(F,\rho)$ of lenght $2s$. (It exists by our assumption on the depth of $T(F,\rho)$).

The paths $\sigma_{i_1}, \dots, \sigma_{i_D}$ are the paths setting to true the terms $t_{i_1}, \dots, t_{i_D}$, more precisely for each $k \leq D$ $\quad t_{i_k}\restriction_{\rho \cup \pi_{i_1} \cup \dots \cup \pi_{i_{k-1}} \cup \sigma_{i_k}} \equiv 1$.

Let $\sigma = \sigma_{i_1} \cup \dots \cup \sigma_{i_D}$, then we define $\eta(\rho)$ as:

$$\eta(\rho) = (\rho \cup \sigma, \beta, m).$$

By construction along π and σ the same variables are queried, since the lenght of π is $2s$, then the variables queried are exactly s and $|\sigma| = s$ too. So $\rho \cup \sigma \in M_n^{\ell - s}$.

Let β, the second entry of $\eta(\rho)$, be the following string $\vec{\beta} = (\beta_1, \dots, \beta_D)$ where

$$(\beta_j)_k = \begin{cases} 1 & \text{if the } k\text{-th variable of } t_{i_j} \text{ is queried in } \pi \\ 0 & \text{otw} \end{cases}$$

Clearly $\vec{\beta} \in \mathrm{code}(r,s)$, since there are exactly s variables queried in the whole π.
The last entry m of $\eta(\rho)$ says how the variables whose position is encoded by $\vec{\beta}$ are set by π. More precisely if $\vec{\beta}$ says that the variable x_{ab} is queried then m says where a is mapped by π among the ℓ holes not covered by ρ and where b is mapped by π among the $\ell+1$ pigeons not covered by ρ.

To encode this we just need the set $[2\ell+1]^{2s}$.

This conclude the construction of η, so why is it injective?
This follows from the fact that from $(\rho \cup \sigma, \beta, m)$ in the image of η we can reconstruct ρ.

Let $t_{i_1'}$ be the first term in F s.t. $t_{i_1'}\restriction_{\rho\cup\sigma} \equiv 1$, let ρ' be in the counter-image of $(\rho\cup\sigma, \beta, m)$. It must be that $\rho' \subseteq \rho \cup \sigma$. Let t_{i_1} be the first term of F s.t. $t_{i_1}\restriction_{\rho'} \not\equiv 0$. We have that $t_{i_1'}\restriction_{\rho'} \not\equiv 0$ and so $i_1 \leq i_1'$. By construction $t_{i_1}\restriction_{\rho\cup\sigma} \equiv 1$ but i_1' was the first index with this property so $i_1' \leq i_1$ and hence $i_1 = i_1'$. We found t_{i_1}! From β now we know all the positions of the variables in t_{i_1} set by σ_{i_1} and hence we know σ_{i_1}. From m now we know how the underlying set of vertices of such variables are set in π_{i_1}.
Now we can repeat the previous argument using $((\rho\cup\sigma)\setminus\sigma_{i_1})\cup\pi_{i_1}$ instead of $\rho\cup\sigma$. As before we find t_{i_2}, σ_{i_2} and π_{i_2} etc. In the end we found all $\sigma_{i_1}, \dots, \sigma_{i_D}$ so from $\rho\cup\sigma$ we can reconstruct ρ. $\blacksquare$