Lecture 15: “PHP is hard for $\beta d$Frege” - part III -

We conclude the proof of the following theorem.

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

**Lemma 3:** Let $d$ be an integer, $0 < \varepsilon < \frac{1}{5}$, $0 < \delta < \varepsilon^d$ and $\Gamma$ a set of formulas of depth $\leq d$ closed under subformulas.

If $|\Gamma| < 2^n$ then there exist $\rho \in M_n^q$ with $q = \varepsilon^d$ and there exist $\sigma \in 2n^\delta$-evaluation of $\Gamma^\rho$.

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

The proof of Lemma 3 will construct (by ind on the depth) a $K$-evaluation using some very specific kind of CHDT, 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 $F = t_1 \vee \ldots \vee t_m$, and a matching $\rho \in M_n$, the **canonical matching decision tree** $T(F, \rho)$ is the following tree in $CMDT(VF_{\rho})$ representing $F|_{\rho}$: fix an ordering on the terms of $F$ and fix an ordering on the variables of $F$,

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

(ii) if $F|_{\rho} \neq 0$ and $F|_{\rho} \neq 1$ let $t$ be first term in $F|_{\rho}$ then $T(F, \rho)$ is constructed as follows:

There is only one leaf with label 1, full matching tree for the variables in $t$; query in order the variables in $t$, i.e., for $x_{ij}$ query first $i$, then $j$, both have outgoing edges: all the possible edges $(i, x)$ (resp. $(j, x)$) with $x \in V_{\rho}$ consistent with the path leading to $i$.

Example: the trees we used in the definition of $\kappa$-evaluations for $x_{ij}$ are canonical.

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

$F = (x_{17} \land x_{38}) \lor (x_{16} \land x_{27}) \lor (x_{6} \land x_{49}) \lor (x_{16} \land x_{59})$

$\rho = \{(1, 6)\}$

Suppose that the terms and vars are ordered according the way they are written in $F$ above.

Write $T(F, \rho)$.

$F|_{\rho} = x_{27} \lor x_{49} \lor x_{59}$

$V|_{\rho} = \{2, 3, 4, 5, 7, 8, 9\}$

- Level when 2 is queried
- Level when 7 is queried
Lemma 4 (switching lemma): Let $F = t_v \ldots t_m$ be an $r$-matching DNF over $P$, resp. of size $m, n$. Let $s$ be an integer, $l \leq n$ and let

$$\text{Bad}_n^2(F, 2s) = \{ p \in M_n^2 : T(F, p) \text{ has depth } \geq 2s \}$$

Then

$$\frac{|\text{Bad}_n^2(F, 2s)|}{|M_n^2|} \leq \left( \frac{2r}{n-l} \right)^s$$  \((\star)\)

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

Proof: (using the encoding idea by Razborov)

We build an injective mapping $\gamma: \text{Bad}_n^2(F, 2s) \rightarrow M_n^{l-s} \times \text{code}(r, s) \times [2^{l+1}]^{2s}$, where $\text{code}(r, s)$ is the set of all strings $\beta = (\beta_1, \ldots, \beta_d)$ s.t. $\beta \in \{0, 1\}^r \setminus \{0\}^r$ and the number of occurrences of 1s in $\beta$ is exactly $s$.

From the existence of such $\gamma$, the fact that $|\text{code}(r, s)| \leq \left( \frac{r}{k_2} \right)^s$ (\(\star\)) and the fact that $\frac{|M_n^{l-s}|}{|M_n^2|} \leq \left( \frac{d(k+1)}{n-l} \right)^s$ (also \(\star\)) we immediately get the bound in \((\star)\). So let's focus on building such $\gamma$.

If $p \in \text{Bad}_n^2(F, 2s)$ then $T(F, p)$ looks like the following picture:

- Full tree for $t_{i_1}$, first term in $F$ s.t. $t_{i_1} \uparrow p \neq 0$
- Full tree for $t_{i_2}$, first term in $F$ s.t. $t_{i_2} \uparrow p \neq 0$
- Full tree for $t_{i_3}$, s.t. etc.
Let's say that $\pi = \pi_i u \cdots u \pi_j$ is the leftmost path in $T(F, \rho)$ of length $2s$. (It exists by our assumption on the depth of $T(F, \rho)$.)

The paths $\sigma_i, \ldots, \sigma_D$ are the paths setting to true the terms $t_{i_1}, \ldots, t_{i_D}$, more precisely, for each $k \leq D$ $t_{i_k} \mid \rho \cup \sigma_i u \cdots u \sigma_D u \sigma_k = 1$.

Let $\sigma = \sigma_i u \cdots u \sigma_D$, then we define $\eta(\rho)$ as:

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

By construction, along $\pi$ and $\sigma$ the same variables are queried, since the length of $\pi$ is $2s$, then the variables queried are exactly $s$ and $|\sigma| = s$ too.

So $\rho \cup \sigma \in \mathcal{M}_{s} - s$.

Let $\beta$, the second entry of $\eta(\rho)$, be the following string $\beta = (\beta_1, \ldots, \beta_D)$ where

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

Clearly $\beta \in \text{code}(r, s)$, since there are exactly $s$ variables queried in the whole $\pi$.

The last entry $m$ of $\eta(\rho)$ says how the variables whose position is encoded by $\beta$ are set by $\pi$. More precisely, if $\beta$ says that the variable $X_i^j$ is queried then $m$ says where $X_i$ is mapped by $\pi$ among the $s$ holes not covered by $\rho$, and where $b$ is mapped by $\pi$ among the $m_i$ pigeons not covered by $\rho$.

To encode this we just need the set $[2l + 1]_2$.

This concludes the construction of $\eta$, so why is it injective?

This follows from the fact that from $(\rho \cup \sigma, \beta, m)$ in the image of $\eta$ we can reconstruct $\rho$.

Let $t_{i_1}$ be the first term in $F$ s.t. $t_{i_1} \mid \rho \cup \sigma = 1$, let $\rho'$ be in the counter-image of $(\rho \cup \sigma, \beta, m)$. It must be that $\rho' \leq \rho \cup \sigma$. Let $t_{i_1}$ be the first term of $F$ s.t. $t_{i_1} \mid \rho' \neq 0$. We have that $t_{i_1} \mid \rho', \neq 0$ and so $i_1 \leq i_1'$. By construction $t_{i_1} \mid \rho \cup \sigma = 1$ 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 $\beta$ now we know all the positions of the variables in $t_{i_1}$ set by $\sigma_i$, and hence we know $\sigma_i$. From $m$ now we know how the underlying set of vertices of such variables are set in $t_{i_1}$.

Now we can repeat the previous argument using $(\rho \cup \sigma \setminus \sigma_i) u t_{i_1}$ instead of $\rho \cup \sigma$. As before we find $t_{i_2}, \sigma_2$ and $t_{i_2}$ etc. In the end we found all $\sigma_1, \ldots, \sigma_D$ so from $\rho \cup \sigma$ we can reconstruct $\rho$. 