IITM-CS6845: Theory Toolkit March 31, 2012

Lecture 48 : Håstad's Switching Lemma

Lecturer: Jayalal Sarma M.N. *Scribe: Prashant Vasudevan*

THEME: Håstad's Switching Lemma
LECTURE PLAN:Prove Håstad's Switching Lemma

Lemma 1 (Håstad's Switching Lemma)**.** *Let F be a DNF formula of term size r on n variables. Then, for $s > 0$, $l = pn$, $p \leq \frac{1}{7}$,*

$$\frac{|\{\rho \in R_n^l : |T(F|_\rho)| \geq s\}|}{|R_n^l|} < (7pr)^s$$

(For definitions, refer previous lecture notes.)

We shall need further the following definitions:

1. $S = \{\rho \in R_n^l : |T(F|_\rho)| \geq s\}$.
2. $stars(r, s) = \{(\beta_1, \beta_2, \cdots, \beta_k) \mid \beta_i \in \{*, -\}^*$ such that total number of $* \leq s$ and each β_i has at least one $*\}$.

We prove the lemma by establishing a one-to-one mapping,

$$\phi : S \to R_n^{l-s} \times stars(r, s) \times \{0, 1\}^s$$

and counting the right hand side, which shall give us an upper bound on $|S|$.

Suppose the formula in canonical DNF is $F = C_1 \vee C_2 \vee \ldots$. Let ρ be any restriction in S, and π be the path consisting of the first s edges of the lexicographically first root-to-leaf path in the canonical decision tree of $F|_\rho$ that is of length at least s. Let C_{ν_1} be the first clause in F that is not falsified by ρ. The variables of this clause are those that appear at the top of the canonical decision tree for $F|_\rho$.

Let π_1 be the part of π that deals with variables that are present in C_{ν_1}. Let σ_1 be the path in the tree corresponding to the unique assignment of variables that satisfy C_{ν_1}. Note that as there is no clause that is made true by the assignment corresponding to π (because it is part of a longer path), π_1 is different from σ_1. Also define $\beta_1 \in \{*, -\}^r$ such that β_{1i} is $*$ if the ith variable of C_{ν_1} is set by σ_1 and $-$ otherwise. Note that β_1 has at least one $*$ because C_{ν_1} is not falsified before σ_1 comes in. Also notice that given C_{ν_1} and β_1, we can reconstruct σ_1.

After the above step, consider the resulting tree for $F|_{\rho\pi_1}$ and do the same to obtain σ_2, π_2, β_2 for the then first unfalsified clause C_{ν_2} and so on till π is exhausted and we have $\pi = \pi_1\pi_2\ldots\pi_k$, $\sigma = \sigma_1\sigma_2\ldots\sigma_k$ and $(\beta_1, \beta_2, \ldots, \beta_k)$. Now define $\delta \in \{0,1\}^s$ such that δ_i is 0 whenever $\pi_i \neq \sigma_i$ and 1 otherwise.

Define the promised mapping to be $\phi(\rho) = (\rho\sigma, (\beta_1, \beta_2, \ldots, \beta_k), \delta)$. That the co-domain is as specified above is straightforward. To see that the mapping is one-one, we see that we can reconstruct ρ uniquely given its image - we can find C_{ν_1} as defined above by finding the first clause in F that is satisfied by the restriction $\rho\sigma$. Using this clause and β_1 we can find σ_1 which along with δ gives π_1. Next, replace σ_1 by π_1 and repeat to get σ_2 and π_2. Proceeding along these lines gives σ, removing which from the restriction $\rho\sigma$ gives ρ uniquely.

In order to count the number of elements in the co-domain of ϕ, we need the following lemma:

Lemma 2. $|stars(r,s)| < (r/ln2)^s$

Proof. By induction, we show $|stars(r,s)| < \gamma^s$ for γ such that $(1+1/\gamma)^r = 2)$. For $s = 0$, the statement is trivially true.

Suppose for some s, the statement is true for all values less than s. Then, let β_1 have i $*$'s. This requires $(\beta_2, \ldots, \beta_k)$ to have $(s-i)$ $*$'s. This procedure gives us the folowing:

$$\begin{aligned} |stars(r,s)| &= \sum_{i=1}^{min(r,s)} \binom{r}{i} |stars(r, s-i)| \\ &\leq \sum_{i=1}^{r} \binom{r}{i} \gamma^{s-i} \\ &= \gamma^s \sum_{i=1}^{r} \binom{r}{i} (1/\gamma)^i \\ &= \gamma^s[(1+1/\gamma)^r - 1] = \gamma^s \end{aligned}$$

As $(1+1/\gamma)^r < e^{r/\gamma}$, $2 < e^{r/\gamma}$ and $\gamma < (r/ln2)$.
Thus, $|stars(r,s)| < (r/ln2)^s$.

□

Using above results, we have:

$$
\begin{aligned}
\frac{|S|}{|R_n^l|} &\leq \frac{|R_n^{l-s}||stars(r,s)|2^s}{|R_n^l|} \\
&\leq \frac{\binom{n}{l-s}2^{n-l+s}}{\binom{n}{l}2^{n-l}}\left(\frac{2r}{ln2}\right)^s \\
&\leq \frac{l^s}{(n-l+s)^s}2^s\left(\frac{2r}{ln2}\right)^s \\
&\leq \left(\frac{4pr}{(1-p)ln2}\right)^s
\end{aligned}
$$

(As $l = pn$.)

For $p < 1/7$, this is at most $(7pr)^s$, proving the Switching Lemma.