Recent advances in Complexity CIS 6930/CIS 4930	September 12, 2002

Lecture 6

Lecturer: Dr. Meera Sitharam | Scribe: Zia Uddin

In today's lecture, we will start the proof of the stronger version of Hastad's Lemma stated in Lecture 4. We first explain some notation.

We will let $min(C)$ denote the maximum possible length of a minterm of the function computed by the circuit C. And given a Boolean function F and a random distribution ρ, we will let $F|_\rho$ denote the restriction of F to those variables that are assigned the value 1 by ρ.

Lemma 1 (Stronger Hastad Lemma) *Let $G = \bigwedge_{i=1}^{w} G_i$ be a Boolean circuit of n variables with an AND gate at the top, where the G_is are circuits with OR gates on top and of fan-in $\leq t$ to these OR gates. Let $F(x_1, \ldots, x_n)$ be a Boolean function on the same n variables, and let ρ be a random distribution in $\mathcal{R}_p$, $p > 0$. Then for every $s \geq 0$, we have Prob[$min(G|_\rho) \geq s \mid F|_\rho \equiv 1] \leq \alpha^s$, where $\alpha = \gamma pt$ and $\gamma = 2/\ln\phi \approx 4.16$, $\phi = (1+\sqrt{5})/2$ being the golden ratio.*

Proof: We proceed by induction on w. If $w = 0$, then $G \equiv 1$ and the lemma is clearly true.

Now assume the lemma is true when the number of $G_i s$ is $w-1$ or less. Let G_1 be the rightmost "OR gate." (See Figure 1.) Then we have Prob[$min(G|_\rho) \geq s \mid F|_\rho \equiv 1] \leq \max\{I, II\}$, where I = Prob[$min(G|_\rho) \geq s \;\mid\; F|_\rho \equiv 1 \;\wedge\; G_1|_\rho \equiv 1$] and II = Prob[$min(G|_\rho) \geq s \;\mid\; F|_\rho \equiv 1 \;\wedge\; G_1|_\rho \not\equiv 1$].

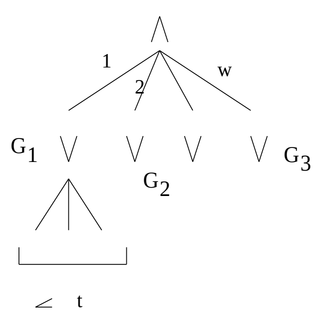

Figure 1: The Circuit G

We shall now examine I. Let $F' = F \wedge G_1$. We observe that if $G_1 \equiv 1$, then $G|_\rho = \bigwedge_{i=1}^{w} G_i|_\rho = \bigwedge_{i=2}^{w} G_i|_\rho$. We have I = Prob[$min(G|_\rho) \geq s \;\mid\; F|_\rho \equiv$

$1 \ \wedge \ G_1|_\rho \equiv 1 \ ] = \text{Prob}[\ min(G|_\rho) \geq s \ \ | \ \ (F \wedge G_1)|_\rho \equiv 1 \ ]$. Thus I is the probability that $\bigwedge_{i=2}^{w} G_i|_\rho$ has a minterm of size at least s given $F'|_\rho \equiv 1$. By the indction hypothesis, we have $\text{I} \leq \alpha^s$.

Now we examine $\text{II} = \text{Prob}[\ min(G|_\rho) \geq s \ | \ F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1\ ]$. Suppose that the variables "going into" G_1 have indices in a set $T \subset \{1, \ldots, n\}$, where $|T| \leq t$. Write $\rho = \rho_1 \circ \ \rho_2$, where $\rho_1 : \{x_i\}_{i \in T} \to \{0, 1, *\}$ is the restriction of ρ to the variables indexed by T, and $\rho_2 : \{x_i\}_{i \in \{1,\ldots,n\} \setminus T} \to \{0, 1, *\}$, $* \in T$, is the restriction of ρ to the variables not indexed by T. We now have $G_1|_\rho \not\equiv 1$ if and only if $G_1|_{\rho_1} \not\equiv 1$. Since G_1 is an OR circuit, $G_1|_\rho \not\equiv 1$ if and only if ρ_1 assigns all the variables indexed by T to the values 0 and $*$ only. Thus we in fact have $\rho_1 : \{x_i\}_{i \in T} \to \{0, *\}$. Since G is an AND of ORs circuit, every minterm of $G|_\rho$ makes G_1 true. Hence for every minterm σ of $G|_\rho$, there exists a variable x_i, $i \in T$, such that if $\sigma = 1$, then $x_i = 1$.