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 \( \text{min}(C) \) 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 \( \rho \), we will let \( F|_\rho \) denote the restriction of \( F \) to those variables that are assigned the value 1 by \( \rho \).

**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 \( G_i \)'s are circuits with OR gates on top and of fan-in \( t \) to these OR gates. Let \( F(x_1, \ldots, x_n) \) be a Boolean function on the same \( n \) variables, and let \( \rho \) be a random distribution in \( \mathcal{R}_p, p > 0 \). Then for every \( s \geq 0 \), we have \( \Pr[\text{min}(G|_\rho) \geq s \mid F|_\rho \equiv 1] \leq \alpha^s \), where \( \alpha = \gamma t \) 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 \( \Pr[\text{min}(G|_\rho) \geq s \mid F|_\rho \equiv 1] \leq \max\{I, II\} \), where \( I = \Pr[\text{min}(G|_\rho) \geq s \mid F|_\rho \equiv 1 \land G_1|_\rho \equiv 1] \) and \( II = \Pr[\text{min}(G|_\rho) \geq s \mid F|_\rho \equiv 1 \land G_1|_\rho \not\equiv 1] \).

![Figure 1: The Circuit G](image)

We shall now examine \( I \). Let \( F' = F \land G_1 \). 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 \( I = \Pr[\text{min}(G|_\rho) \geq s \mid F|_\rho \equiv 1] \).
1 \land G_1|_\rho \equiv 1 \right] = \text{Prob}[ \min(G|_\rho) \geq s \mid (F \land G_1)|_\rho \equiv 1 ]. \text{ Thus I is the probability that } \bigwedge_{i=2}^{w} G_i|_\rho \text{ has a minterm of size at least } s \text{ given } F|_\rho \equiv 1. \text{ By the induction hypothesis, we have } I \leq \alpha^s.

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