CS 5150/6150: Graduate Algorithms **Nov 19, 2007**

Lecture 23: Chernoff Bounds for Amplification

Lecturer: Suresh Venkatasubramanian *Scribe:*

We start with a simpler version of the standard Chernoff bounds that will be suitable for our purpose.

Theorem 1 *Let $X_1, ..., X_n$ be independent Poisson trials such that $Pr(X_i) = p_i$. Let $X = \sum_{i=1}^{n} X_i$ and $\mu = E[X]$. Then the following Chernoff bounds hold:*

1. *for any $\delta > 0$,*
$$Pr(X \geq (1+\delta)\mu) \leq \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}; \tag{23.1}$$

2. *for $0 < \delta \leq 1$,*
$$Pr(X \geq (1+\delta)\mu) \leq e^{-\mu\delta^2/3}; \tag{23.2}$$

3. *for $R \geq 6\mu$,*
$$Pr(X \geq R) \leq 2^{-R}. \tag{23.3}$$

The first bound of the theorem is the strongest, and it is from this bound that we derive the other two bounds, which have the advantage of being easier to state and compute with in many situations.

Proof: Applying Markov's inequality, for any $t > 0$ we have

$$\begin{aligned} Pr(X \geq (1+\delta)\mu) &= Pr(e^{tX} \geq e^{t(1+\delta)\mu}) \\ &\leq \frac{E[e^{tX}]}{e^{t(1+\delta)\mu}} \\ &\leq \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}}. \end{aligned}$$

For any $\delta > 0$, we can set $t = \ln(1+\delta) > 0$ to get (23.1):

$$Pr(X \geq (1+\delta)\mu) < \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}.$$

To obtain (23.2) we need to show that, for $0 < \delta \leq 1$,

$$\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}} \leq e^{-\delta^2/3}.$$

Taking the logarithm of both sides, we obtain the equivalent condition

$$f(\delta) = \delta - (1+\delta)\ln(1+\delta) + \frac{\delta^2}{3} \leq 0.$$

Computing the derivatives of $f(\delta)$, we have

$$\begin{aligned} f'(\delta) &= 1 - \frac{1+\delta}{1+\delta} - \ln(1+\delta) + \frac{2}{3}\delta \\ &= -\ln(1+\delta) + \frac{2}{3}\delta; \\ f''(\delta) &= -\frac{1}{1+\delta} + \frac{2}{3}. \end{aligned}$$

We see that $f''(\delta) < 0$ for $0 \leq \delta < 1/2$ and that $f''(\delta) > 0$ for $\delta > 1/2$. Hence $f'(\delta)$ first decreases and then increases over the interval [0, 1]. Since $f'(0) = 0$ and $f'(1) < 0$, we can conclude that $f'(\delta) \leq 0$ in the interval [0, 1]. Since $f(0) = 0$, it follows that $f(\delta) \leq 0$ in that interval, proving the second bound.

To prove (23.3), let $R = (1+\delta)\mu$. Then, for $R \geq 6\mu$, $\delta = R/\mu - 1 \geq 5$. Hence, using (23.1),

$$\begin{aligned} Pr(X \geq (1+\delta)\mu) &\leq \left(\frac{e^\delta}{(1+\delta)^{(1+\delta)}}\right)^\mu \\ &\leq \left(\frac{e}{1+\delta}\right)^{(1+\delta)\mu} \\ &\leq \left(\frac{e}{6}\right)^R \\ &\leq 2^{-R}. \end{aligned}$$

■

We obtain similar results bounding the deviation below the mean.

Theorem 2 *Let* $X_1, ..., X_n$ *be independent Poisson trials such that* $Pr(X_i) = p_i$. *Let* $X = \sum_{i=1}^n X_i$ *and* $\mu = E[X]$. *Then, for* $0 < \delta < 1$:

1.
$$Pr(X \leq (1-\delta)\mu) \leq \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^\mu; \tag{23.4}$$

2.
$$Pr(X \leq (1-\delta)\mu) \leq e^{-\mu\delta^2/2}; \tag{23.5}$$

3.
$$Pr(|X-\mu| \geq \delta\mu) \leq 2e^{-\mu\delta^2/3}. \tag{23.6}$$

Now suppose we have a randomized algorithm A that outputs a 1 or 0 given an input x, and gives the correct answer with probability $p = \frac{1}{2} + \epsilon$, where $0 < \epsilon < \frac{1}{2}$ is a constant. We'd like to *amplify* this probability of success to some function of $1 - 1/n$, so that as n gets larger, the probability of success gets larger and larger.

Suppose we now run A k times, recording the answer each time. We then output the majority answer (we can assume that k is odd). Let X_i be a random variable that is 1 if the algorithm generates the correct answer (w.l.o.g 1) in the i^{th} iteration. The event that the algorithm returns the correct answer is thus the event "$\sum X_i > k/2$", and the corresponding failure event is "$\sum X_i < k/2$".

Let $X = \sum X_i$. Since $EX_i = p$, by linearity of expectation $EX = kp$. We can rewrite the event $X < k/2$ as the event $X < \frac{1}{2p} \cdot EX$. Since $p = \frac{1}{2} + \epsilon$, $\frac{1}{2p} = \frac{1}{1+2\epsilon}$. We can now rewrite the desired event as $X < (1 - (1 - \frac{1}{2p})) \cdot EX$, which is equivalent to $X < (1 - \frac{2\epsilon}{1+2\epsilon}) \cdot EX$.

Setting $\delta = \frac{2\epsilon}{1+2\epsilon}$, we can apply the inequality (23.5), yielding

$$\begin{aligned} Pr(X < k/2) &\leq e^{-k\frac{1+2\epsilon}{4}(\frac{2\epsilon}{1+2\epsilon})^2} \\ &= e^{-k\frac{\epsilon^2}{1+2\epsilon}} \end{aligned}$$

To reduce this probability to $1/n$, we need to set $k = \frac{1+2\epsilon}{\epsilon^2} \log n$.

Notice that merely increasing k by a constant factor will decrease by the failure probability by a *polynomial factor*. This is the power of Chernoff bounds.