6.856 — Randomized Algorithms

David Karger

Handout #10, 2002 — Homework 4 Solutions

M. R. refers to this text:
Motwani, Rajeez, and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge: Cambridge University Press, 1995.

Problem 1

(a) MR Exercise 4.2. Each node $a_i b_i$ sends a packet to node $b_i a_i$ through node $b_i b_i$. There are $2^{n/2} = 2^{\frac{\log N}{2}}$ packets that have to be routed through a given node xx. Half of these packets have to flip the $(\frac{n}{2}+1)$-st bit. All these messages have to cross the one edge that connects xx to the node with a different $(\frac{n}{2}+1)$-st bit. Therefore, at least $\frac{\sqrt{N}}{2} = \Omega\left(\sqrt{N}\right) = \Omega\left(\sqrt{\frac{N}{n}}\right)$ steps are needed.

(b) MR 4.9. Consider the transpose permutation again, and again restrict attention to packets with $b_i = 0^{n/2}$. We show that with high probability, $2^{\Omega(n)}$ packets go through vertex 0^n, which means we take time at least $2^{\Omega(n)}/n = 2^{\Omega(n)}$. For the proof, fix attention on $\binom{n/2}{k}$ packets whose a_i have exactly k ones (we'll fix k later). Note that the bit fixing algorithm must change these k ones to zeroes, and must change a corresponding k zeroes to ones. We go through vertex 0^n if all k ones in a_i are corrected to zeroes before any of the zeroes in b_i are corrected to ones. Since the corrections are in random order, meaning that the first k bits to be fixed are a random subset of the $2k$ that must be fixed, the probability that this happens is

$$\binom{2k}{k}^{-1}.$$

It follows that the expected number of packets hitting 0^n is

$$\begin{aligned} \frac{\binom{n/2}{k}}{\binom{2k}{k}} &\geq \frac{\left(\frac{n}{2k}\right)^k}{\left(\frac{2ek}{k}\right)^k} \\ &= \left(\frac{n}{4ek}\right)^k \end{aligned}$$

Now suppose we take $k = n/8e$. Then we get an expected packet number of $2^{n/8e} = 2^{\Omega(n)}$.

Since each packet is deciding independently whether to go through 0^n, we can apply the Chernoff bound to deduce that at least $\frac{1}{2} \cdot 2^{n/8e}$ packets go through 0^n with high probability.

Problem 2

1. As mentioned in the problem statement, every X_i has a distribution equal to the length of a sequence of coin flips until we see the first heads. Therefore $\sum X_i$ has the same distribution as the length of a sequence of coin flips until we see the n-th head.

   Imagine having an infinite sequence of coin flips, then $\sum X_i$ gives the position of the n-th head. The event $X > (1+\delta)2n$ is therefore the same as saying that the n-th head does not occur among the first $(1+\delta)2n$ coin flips. Let Y be the random variable giving the number of heads among the first $(1+\delta)2n$ coin flips. Then we have

   $$\Pr[X > (1+\delta)2n] = \Pr[Y < n]$$

   Since Y is the sum of independent Poisson trials, we can apply a Chernoff bound on Y to bound the above probability. Noting that $\mu_Y = (1+\delta)n$, we have

   $$\begin{aligned}\Pr[X > (1+\delta)2n] &= \Pr[Y < n] = \Pr\left[Y < (1 - \frac{\delta}{1+\delta})(1+\delta)n\right] \\ &\leq \exp\left(-(1+\delta)n \cdot \frac{\delta^2}{2(1+\delta)^2}\right) \\ &= \exp\left(-\frac{n\delta^2}{2(1+\delta)}\right).\end{aligned}$$

2. *(optional)* Instead of considering $E[X]$ directly, we consider $E[\exp(tX)] = E[\exp(t\sum X_i)] = E[\Pi \exp(tX_i)] = \Pi E[\exp(tX_i)]$, where we fix t later. By applying a Markov bound, we obtain

   $$\begin{aligned}\Pr[X > (1+\delta)2n] &= \Pr[\exp(tX) > \exp(t(1+\delta)2n)] \\ &\leq \frac{E[\exp(tX)]}{\exp(t(1+\delta)2n)} \\ &= \frac{\Pi E[\exp(tX_i)]}{\exp(t(1+\delta)2n)} \qquad (*)\end{aligned}$$

   Now we have (assuming $e^t < 2$):

   $$E[\exp(tX_i)] = \frac{1}{2}e^t + \frac{1}{4}e^{2t} + \frac{1}{8}e^{3t} + \cdots = \sum_{k=1}^{\infty}\left(\frac{e^t}{2}\right)^k = \frac{e^t/2}{1-e^t/2} = \frac{e^t}{2-e^t}$$

   Substitution in $(*)$ yields:

   $$\Pr[X > (1+\delta)2n] \leq \frac{e^{tn}}{(2-e^t)^n e^{t(1+\delta)2n}} = \left(\frac{1}{(2-e^t)e^{t(1+2\delta)}}\right)^n$$

   Taking the derivative by t, and setting it equal to zero shows that this term takes its minimum for $t = \ln(1+\delta/(1+\delta))$, which implies $e^t < 2$ as desired. We therefore have the bound

   $$\Pr[X > (1+\delta)2n] \leq \left(\left(1 - \frac{\delta}{1+\delta}\right)\left(1 + \frac{\delta}{1+\delta}\right)^{(1+2\delta)}\right)^{-n} \qquad (**)$$

This becomes a bit tighter than the result from (a) if δ becomes small. Let $\varepsilon > 0$ be some small constant. Then there is some δ_0 such that for all $\delta < \delta_0$, we have:

$$\begin{aligned} 1 - \delta/(1+\delta) &> \exp(-\varepsilon) \\ (1 + \delta/(1+\delta))^{(1+\delta)/\delta} &> \exp(1-\varepsilon) \\ \delta^2/(1+\delta) + \delta &> \delta^2 \end{aligned}$$

We can use these to bound $(**)$:

$$(**) \leq \left(\exp(-\varepsilon + (1-\varepsilon)(\delta^2/(1+\delta) + \delta))\right)^{-n} \leq \exp(-n((1-\varepsilon)\delta^2 - \varepsilon))$$

Thus, we come arbitrarily close to $\exp(-n\delta^2)$ as ε tends to 0.

Problem 3

(a) The probability of a sample yielding the mean of $n/2$ can be approximated by Stirling's formula as follows:

$$\frac{\binom{n}{n/2}}{2^n} = \frac{n!}{(n/2)!^2 2^n} \approx \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\pi n \left(\frac{n}{2e}\right)^n 2^n} = \sqrt{\frac{2}{\pi n}} = \Theta(1/\sqrt{n}).$$

It is also not hard to see that all other outcomes have lower probability. It follows that the range of values in $n/2 \pm c\sqrt{n}$ has total probability $O(c)$, so by appropriate choice of the constant, one can achieve the desired probability of being outside the range.

(b) We use the set notation, where we have a universe $U = \{1, \ldots, n\}$, subsets S_1, S_2, ..., $S_n \subseteq U$, and a partition $P \subset U$. We call a partition good for S_i if the discrepancy of S_i is at most $2/3c\sqrt{n}$, where c is chosen according to part (a). A partition is good for a choice of sets $\bar{S} = (S_i)_{i=1,\ldots,n}$ if it is good for all sets.

We choose the sets as follows: we set $S_1 = U$, and let the other S_i be independent random sets that include each element with probability 1/2. We want to show that there exists a choice of sets $\bar{S}$, so that no partition is good for it. Using the probabilistic method, this amounts to showing:

$$\Pr_{\bar{S}}[\exists \text{ good partition } P \text{ for } \bar{S}] < 1$$

We have

$$\begin{aligned} \Pr_{\bar{S}}[\exists \text{ good partition } P \text{ for } \bar{S}] &\leq \sum_P \Pr_{\bar{S}}[P \text{ is good for } \bar{S}] \\ &= \sum_P \prod_{i=1}^n \Pr_{S_i}[P \text{ is good for } S_i], \end{aligned}$$

by a union bound and the independence of the S_i. Let P be fixed in the following, and we will estimate $\Pi_{i=1}^n \Pr_{S_i}[P \text{ is good for } S_i]$. Since $S_1 = U$, this quantity is non-zero only if

$$|P| \in [n/2 - c\sqrt{n}/3, n/2 + c\sqrt{n}/3], \quad (*)$$

since P would otherwise split S_1 too unevenly. So we can assume that P is in this range for the following.

Consider some set S_i for $i \geq 2$. Let X, Y, Z be the following random variables:

$$X = |S_i \cap P|, \quad Y = |S_i \cap \bar{P}|, \quad Z = |\bar{S}_i \cap \bar{P}|.$$

Note that all three are Poisson variables, and that $Y + Z = n - |P|$. So we have:

$$\begin{aligned}
1 - \Pr[P \text{ is good for } S_i] &= \Pr[|X - Y| \geq \frac{2}{3}c\sqrt{n}] \\
&= \Pr[|X + Z - n + |P|| \geq \frac{2}{3}c\sqrt{n}] \\
&= \Pr[X + Z - n + |P| \geq \frac{2}{3}c\sqrt{n}] + \Pr[X + Z - n + |P| \leq -\frac{2}{3}c\sqrt{n}] \\
&\overset{(*)}{\geq} \Pr[X + Z \geq n/2 + c\sqrt{n}] + \Pr[X + Z \leq n/2 - c\sqrt{n}] \\
&= \Pr[|X + Z - n/2| \geq c\sqrt{n}] \geq \frac{3}{4}
\end{aligned}$$

It follows that the probability that P is good for S_i is at most $1/4$. So we have

$$\begin{aligned}
\Pr_{\bar{S}}[\exists \text{ good partition } P \text{ for } \bar{S}] &\leq \sum_P \prod_{i=1}^{n} \Pr_{S_i}[P \text{ is good for } S_i] \\
&\leq 2^n \cdot \frac{1}{4^{n-1}} < 1,
\end{aligned}$$

which proves the existence of the desired sets for large enough n.

Problem 4 In the analysis of the min-cut algorithm (cf. section 1.1 in the text), it was shown that the algorithm chooses a particular min-cut with probability $1/\binom{n}{2}$ (see page 8 of the text). If there were k different minimum cuts, then the probability that any one of them would be output is at least $k/\binom{n}{2}$. This follows from the fact that these resultant events are all disjoint; if one min-cut is chosen then no other min-cut is chosen on that run of the algorithm. If there were $\binom{n}{2}$ min-cuts, then the probability that any one at all would be chosen would be exactly 1. If there were more, the probability of a min-cut being found would be greater than one, which is a contradiction. Thus the number of min-cuts in a graph cannot exceed $\binom{n}{2}$.

Note that it is incorrect to argue that since the algorithm collapses edges until two vertices remain, and there are at most $\binom{n}{2}$ pairs of vertices that could be left at the end, the number of min-cuts is bounded by the same number. This reasoning is unsound, as multiple reductions can lead to the same pair of nodes. Consider a ring graph with four nodes, numbered clockwise 1,2,3,4. One could reduce the graph to 1,2 by contracting 3 and 4 into 1, or contracting 3 and 4 into 2. The pair 1,2 represents at least two different cuts, one separating the graph into 1 and 2,3,4 and one into 1,3,4 and 2. Thus a pair can represent more than one minimum cut, and the argument that there are $\binom{n}{2}$ pairs of vertices is insufficient to prove the bound.