

# 6.856 — Randomized Algorithms

David Karger

Handout #2, September 5, 2002 — Homework 1, Due 9/11

M. R. refers to this text:

Motwani, Rajeez, and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge: Cambridge University Press, 1995.

1. MR 1.1.

- (a) Suppose you are given a coin for which the probability of *HEADS*, say  $p$ , is *unknown*. How can you use this coin to generate unbiased (i.e.,  $\Pr[\text{HEADS}] = .5$ ) coin flips? Give a scheme for which the expected number of flips of the biased coin for extracting one unbiased coin flip is no more than  $1/[p(1-p)]$ . (Hint: Consider two consecutive flips of the biased coin.)
- (b) Strengthen the scheme from part (a) to be as efficient as you can manage. That is, modify the scheme from (a) to extract as many bits as possible (in expectation) per biased coin flip.
- (c) (*optional*) In fact, the maximum number of unbiased coin flips that can be extracted (in expectation) from a sequence of  $n$  biased coin flips is

$$n \left( p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} \right) \quad (*)$$

Show that the quantity (\*) is indeed an upper bound on the maximum number of unbiased bits that can be extracted from  $n$  biased coin flips.

2. MR 1.5. Consider the problem of using a source of unbiased random bits to generate a sample from the set  $S = \{1, \dots, n\}$  such that element  $i$  is chosen with probability  $p_i$ .

- (a) Show how to perform this sampling using  $O(\log n)$  random bits *in expectation* per sample, regardless of the values of the  $p_i$ . (Hint: start with an easy scheme that uses an infinite number of random bits to choose the sample. Then make it lazy, generating/examining only enough bits to uniquely identify the item that would be selected with by the infinite sequence. See MR 1.4.c).
- (b) Prove that for certain  $p_i$  and  $n$  (for example, a uniform sample from  $\{1, 2, 3\}$ ), if you only have unbiased random bits, it is *impossible* to generate an appropriately distributed sample using a finite number of bits *in the worst case*.
- (c) (*optional*) Using a technique similar to that in (a), show how to extract unbiased coin flips from a coin with bias  $p$ , where  $p$  is *known*. Given a stream of biased coin flips, your scheme should output a stream of unbiased coin flips, but be simpler than

the method developed in problem 1(b) (where we did not know  $p$ ). Asymptotically, the expected number of unbiased coin flips that were output should be close to the optimal value given in problem 1(c).

3. You are watching a stream of packets go by one at a time, and want to take a random sample of  $k$  distinct packets from the stream. You face several problems:
- You only have room to save  $k$  packets at any one time.
  - You do not know the total number of packets in the stream.
  - If you choose not to save a packet as it goes by, it is gone forever.

Devise a scheme so that, whenever the packet stream terminates, you are left holding a subset of  $k$  packets chosen uniformly at random from the entire packet stream. If the total number of packets in the stream is less than  $k$ , you should hold all of these packets.