

1. Say we are given three  $n \times n$  matrices,  $X$ ,  $Y$ , and  $Z$ , and we wish to determine whether or not  $XY = Z$ . We could of course multiply  $XY$  directly, but in this problem we develop a randomized algorithm for testing  $XY \stackrel{?}{=} Z$  more quickly.
  - (a) Consider the case where  $XY \neq Z$ , and let  $W = XY - Z$ . Let  $i$  be any row of  $W$  that is not  $\bar{0}$  (the vector consisting of  $n$  zeros). Let  $R$  be any binary vector of length  $n$ , and let  $R'$  be a binary vector that is the same as  $R$ , except that the  $i$ th entry of  $R'$  is a 1 if and only if the  $i$ th entry of  $R$  is a 0. Show that either  $RW \neq \bar{0}$  or  $R'W \neq \bar{0}$ .
  - (b) Given any  $n \times n$  matrices  $X$ ,  $Y$  and  $Z$ , and binary vector  $R$ , show how to compute  $R(XY - Z)$  in time  $O(n^2)$ .
  - (c) Using parts (a) and (b), describe a randomized algorithm for testing  $XY \stackrel{?}{=} Z$  in  $O(n^2)$  time. Prove that your algorithm returns the correct answer with probability at least  $1/2$  for any matrices  $X$ ,  $Y$  and  $Z$ .
  - (d) Describe how to improve the probability that your algorithm returns the correct answer to any value  $p$ ,  $0 < p < 1/2$ , and the running time of the resulting algorithm.
2. [CLRS] Problem 5-1 (page 118).
3. One of the earliest uses of randomized algorithms was to estimate the value of  $\pi$  (the ratio of the area of a circle to the square of its radius). In particular, consider the following experiment: drop a needle in a random position and at a random angle on a floor made of boards of a constant width, where the length of the needle is exactly half of the width of the boards. The probability that the needle falls across a crack is exactly  $1/\pi$ .
  - (a) Describe a randomized algorithm for estimating  $\pi$  using an appropriate needle and floor.
  - (b) Let  $\bar{\pi}$  be the estimate of  $\pi$  obtained by your procedure in part (a). Say we are given two values  $a$  and  $b$  and wish to estimate  $\pi$  with the guarantee that  $\Pr[|\bar{\pi} - \pi| > a] < b$ . How many times do you have to drop the needle for your procedure to make such a guarantee?

You should not assume that you know  $\pi$  in advance. However, you can assume that we know that  $3 \leq \pi \leq 4$ . Also, you should use the following two Chernoff bounds, seen in lecture:

$$\Pr[B(n, p) \leq (1 - \delta)np] \leq e^{-\delta^2 np/2}, \text{ and}$$

$$\Pr[B(n, p) \geq (1 + \delta)np] \leq e^{-\delta^2 np/3},$$

where  $B(n, p)$  is a random variable representing the number of heads seen in  $n$  tosses of a coin that is heads with probability  $p$ .

4. Say we have a decision problem  $R$ , and a randomized algorithm  $A$  for  $R$ , such that on any given input,  $A$  may return the wrong answer, but  $\Pr[A \text{ is wrong}] \leq 1/2 - 1/p(n)$ , for some polynomially bounded function  $p(n)$  of the input size  $n$ . Use a Chernoff bound to show that a polynomial number of repetitions of  $A$  can be used to reduce the error probability to  $1/2^n$ .