

You can find many more wonderful problems from the two textbooks Randomized Algorithms (RA), Probability and Computing (PC). Some of the problems from Randomized Algorithms are more challenging (e.g., results from classical research papers). Each problem below has 10 points. I marked the difficult ones with *.

1. Exercise 1.1(a) from RA: (Due to J. von Neumann.) 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.,

$$\Pr[\text{Heads}] = \Pr[\text{Tails}] = 1/2$$

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.)

2. Exercise 1.6 from PC: Consider the following balls-and-bin game. We start with one black ball and one white ball in a bin. We repeatedly do the following: choose one ball from the bin uniformly at random, and then put the ball back in the bin with another ball of the same color. We repeat until there are n balls in the bin. Show that the number of white balls is equally likely to be any number between 1 and $n - 1$.

3. Exercise 1.9 from PC: Suppose that a fair coin is flipped n times. For $k > 0$, find an upper bound on the probability that there is a sequence of $\log_2 n + k$ consecutive heads.

4. (Universal Hashing) Let the universe U be the set of n -tuples of values drawn from $\mathbb{Z}_p = \{0, 1, \dots, p - 1\}$, where p is a prime. For each n -tuple $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}_p^n$, define the hash function $h_{\mathbf{a}}$ from U to \mathbb{Z}_p by

$$h_{\mathbf{a}}(\mathbf{x}) = \left(\sum_{j=1}^n a_j x_j \right) \bmod p, \quad \text{for any tuple } \mathbf{x} = (x_1, \dots, x_n) \in U.$$

Show that for any two distinct $\mathbf{x}, \mathbf{y} \in U$, if we pick $a_0, \dots, a_n \in \mathbb{Z}_p$ independently and uniformly at random, then

$$\Pr[h_{\mathbf{a}}(\mathbf{x}) = h_{\mathbf{a}}(\mathbf{y})] = 1/p$$

5. Exercise 1.22 from PC: (a) Consider the set $\{1, 2, \dots, n\}$. We generate a subset X of this set as follows: a fair coin is flipped independently for each element of the set; if the coin lands heads then the element is added to X , and otherwise it is not. Argue that the resulting set X is equally likely to be any one of the 2^n possible subsets. (b) Suppose that two sets X and Y are chosen independently and uniformly at random from all the 2^n subsets of $\{1, 2, \dots, n\}$. Determine $\Pr(X \subseteq Y)$ and $\Pr(X \cup Y = \{1, 2, \dots, n\})$. (Hint: Use (a) of this problem.)

6*. Exercise 1.15 from RA (Read the section on complexity classes first): (Due to K-I. Ko.) Show that $\text{NP} \subseteq \text{BPP}$ implies $\text{NP} \subseteq \text{RP}$. (Hint: NP problems have certificates.)