Randomized algorithms - seminar exercises

December 13, 2023

1) Let X be the random variable determining the absolute value of the difference between the number of heads and tails after n flips of an unbiased coin. Show that the expected value of X is Θ(n).

2) Show that there exists $c > 0$ such that the expected length of the longest increasing subsequence in a randomly chosen permutation of order n is at least $c \cdot n^{1/2}$.

3) Give examples of random variables for which Markov's Inequality and Chebyshev's Inequality are tight.

4) Suppose that n balls are placed into n urns uniformly and independently of each other. Show that the expected number of empty urns is $n/e + o(n)$.

5) A family H is strongly 2-universal if for all $x \neq y$ from the universe [m] and all s and t from the range [n], it holds that $Pr_h[h(x) = s \text{ and } h(y) = t] = 1/n^2$. Show that if $n = m = p$ is a prime, then the family from the lecture is strongly 2-universal.

6) Suppose that $m = 2^s$ and $n = 2^t$. Define H as a family of functions h_A associated with binary matrices A with t rows and s+1 columns such that $h_A(x) = A \cdot x'$ where x' is x appended with an extra entry equal to 1. Show that H is a 2-universal hash family. Is it strongly 2-universal?

7) Consider the family H of functions mapping x to (ax mod p) mod n, for $a \neq 0$. Show that for every $x \neq y$, $Pr_h[h(x) = h(y)] <= 2/n$.

8) [use probabilistic method] Fix $m >= n$. Show that there exists a (not necessarily constructible) family H of hash functions, $|H| <= m$, such that for any (n-1)-element subset S, there exists h from H such that each bucket contains at most O(log n) elements.

9) Fix $m >= s$. Show that for $n = \Omega(s^2)$ there exists a family H of hash functions, $|H| <= m$, such that for any s-element subset S, there exists h from H that is injective on S.

10) Show that PP class is closed under the complement.

11) Find deterministic 3/4-approximative algorithm for MAX 2-SAT.

12) Find deterministic 7/8-approximative algorithm for MAX 3-SAT.

13) Prove that for all $k > 0$ and $\epsilon > 0$ there exists an instance of MAX 2-SAT such that the maximum number of satisfiable clauses is at most $3/4 + \epsilon$, but any k clauses are satisfiable.

14) Using Yao's principle show that any Las Vegas algorithm, which decides the existence of perfect matching has the worst-case expected time complexity

$\Omega(n^2)$, where n is the number of vertices.

15) Using "Schwartz-Zippel Polynomial Identity Testing" design a probabilistic algorithm that decides if two rooted trees are isomorphic with linear time complexity.

16) Let $n = p_1^{a_1} \cdot ... \cdot p_m^{a_m}$. Show that $x^{n-1} = 1$ mod n for every x coprime with n if and only if $\phi(p_i^{a_i})|n-1$ for every i=1,...,m.

17) Let $n = p_1 \cdot ... \cdot p_m$. Show that $x^{n-1} = 1$ mod n for every x coprime with n if and only if $p_i - 1|n-1$.

18) Let $n = pq$, where p, q are primes. Show that calculating $\phi(n)$ is equally hard as factorization of n. (from black-box for one problem calculate the other)

19) https://codeforces.com/contest/1823/problem/F

20) https://codeforces.com/problemset/problem/1743/D

21) https://codeforces.com/problemset/problem/1453/D

22) https://codeforces.com/problemset/problem/1770/E

23) https://codeforces.com/problemset/problem/839/C