

Assignment 3

COMP 531: Theory of Computation (Winter 06)

Due March 9 (Thu), before class

Instructions. Follow the instructions from the first assignment. If you think there's an error in some problem, please let me know asap (navin@cs.mcgill.ca). If you need hints for some problem please feel free to ask me. All problems are worth 10 points.

Problem 1. Show that $P/poly \notin EXPSPACE$ and $EXPSPACE \notin P/poly$.

Problem 2. Prove that if $NP \subseteq BPP$ then $RP = NP$.

Problem 3. Prove that $SPACE(n^{\log n}) \notin BPP$.

Problem 4. Problem 7, Chapter 7 in Arora's book.

Problem 5. A two-way probabilistic finite automata (2pfa) A is a two-tape Turing machine with one input tape and another tape which holds a random bit string. A has a read-only two-way access to the input tape and read-only one-way access to the random tape. So A cannot write and hence the name 2pfa. We say that A recognizes a language L if A halts with probability 1 on all the inputs, and

$$\begin{aligned} \text{if } x \in L \text{ then } \Pr[A \text{ accepts } x] &\geq 2/3, \\ \text{if } x \notin L \text{ then } \Pr[A \text{ accepts } x] &\leq 1/3. \end{aligned}$$

Show that the language $\{0^n 1^n : n \geq 0\}$ is recognizable by a 2pfa.

Problem 6. In this problem you will prove a refined version of the Schwartz–Zippel Lemma:

Let $Q(x_1, \dots, x_n)$ be a multivariate polynomial over some field \mathbb{F} with the *degree sequence* (d_1, \dots, d_n) . A degree sequence is defined as follows: let d_1 be the maximum exponent of x_1 in Q , and $Q_1(x_2, \dots, x_n)$ be the coefficient of $x_1^{d_1}$ in Q ; then, let d_2 be the maximum exponent of x_2 in Q_1 , and $Q_2(x_3, \dots, x_n)$ be the coefficient of $x_2^{d_2}$ in Q_1 ; and so on.

Let $S_1, \dots, S_n \subseteq \mathbb{F}$ be arbitrary subsets. For $r_i \in S_i$ chosen uniformly at random, show that

$$\Pr[Q(r_1, \dots, r_n) = 0 | Q \not\equiv 0] \leq \left(\frac{d_1}{|S_1|} + \dots + \frac{d_n}{|S_n|} \right).$$

Problem 7 (k -wise independence). In many situations instead of having access to independent coin tosses it is enough to guarantee that the coin tosses are pairwise independent (or, more generally, k -wise independent). Formally, we say that random variables X_1, \dots, X_n are k -wise independent if for all distinct $i_1, i_2, \dots, i_k \in \{1, \dots, n\}$ and x_1, \dots, x_k any elements in the ranges of X_1, \dots, X_n respectively, we have

$$\Pr[X_{i_1} = x_1, \dots, X_{i_k} = x_k] = \Pr[X_{i_1} = x_1] \dots \Pr[X_{i_k} = x_k].$$

The advantage we get by working with k -wise independent variables is that the size of the probability space can be much smaller than that for independent random variables when k is a constant or a small function of n . This may lead to deterministic algorithms or randomness efficient randomized algorithms.

In this problem we give a construction of k -wise independent random variables with a small size probability space. k -wise independent random variables X_i where $i \in \mathbb{F}_n$, the finite field with n elements where n is a prime power, and each individual X_i is uniformly distributed in \mathbb{F}_n .

Consider the polynomial $p_{a_0, \dots, a_{k-1}}(x) := a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$. Now choose the a 's uniformly at random from \mathbb{F}_n , and set for $i \in \mathbb{F}_n$:

$$X_i := p_{a_0, \dots, a_{k-1}}(i).$$

Show that the random variables X_i , for $i \in \mathbb{F}_n$ are k -wise independent.

Problem 8. Let G be a strongly-connected directed graph. Consider a random walk in G starting at some vertex and each time choosing an out-neighbor uniformly at random and moving to that vertex. Show that the cover time for such a walk (that is, the expected time before all the vertices of G are visited, for the worst case choice of the starting vertex) can be exponential in the number of vertices.