Math261AB - Randomized Algorithms

Spring 2014

Instructor: Sam Buss

Homework problems.

Instructions Please do a selection of the problems listed below as discussed with the instructor.

1. Prove the inequality

$$\sum_{i=0}^{n-2}\sum_{j=1}^{n-1}\frac{2}{\max\{j-i,j-k,k-i\}} \;=\; 2(1+\ln 2)+o(n) \;\approx\; 3.386n.$$

Hint: This is done by a case analysis. Second hint: See the web page by Dave Eppstein, "Blum-style analysis of QuickSort", 1996.

2. Explain a proof of the following sharpened Chernoff bound of the tail of the hypergeometric distribution: If pN of N balls are red, and M balls are chosen without replacement, then the probability that $\geq (p+t)M$ red balls are drawn is $\leq e^{-2t^2M}$.

3. Analyze the worst-case number of comparison needed by the deterministic k-th element selection algorithm (D-SELECT) described in class. (The "median-of-median" algorithm using blocks of size 5.) You should obtain a bound $< 24n$.

4. Prove a $n + \min\{n, n-k\} - 1$ lower bound on the number of comparisons needed for any deterministic algorithm for the k-element selection problem.

5. In the first part of [Schönhage-Paterson-Pippener, 1976] it is shown that under a conjecture of F. Yao, there is a deterministic algorithm for the k-element selection problem which uses $2.5n + o(n)$ comparisons. Understand and explain this result. In your opinion, does the conjecture seem plausible?

6. Prove the following strengthened corollary of the Lovász Local Lemma. Suppose that the probability of event E_i is $\leq p$, for $i = 1, \ldots, n$. Also suppose the dependency graph for the events E_i has degree d and that $e \cdot p \cdot d \leq 1$. Prove that $\text{Prob}[\bigcap_{i=1}^{n} \overline{E_i}] > 0$.

7. [Open problem.] Extend the Moser-Tardős-style analysis to establish the traditional statement of the Lovász Local Lemma, namely to get the conclusion that $\text{Prob}[\bigcap_{i=1}^{n} \overline{E_i}] \geq \prod_{i=1}^{n}(1 - x_i)$.

8*. From the proof of the FKG inequality: Prove that $M(i')$ is log supermodular, assuming that $\mu(\vec{i})$ is log supermodular.

9. a. Suppose $\mu(i_0, \ldots, i_{k-1})$, for $\vec{i} \in \{0,1\}^k$ is equal to the probability that, for each ℓ, event E_ℓ holds iff $i_\ell = 1$. In class, we showed that log supermodularity

$$\mu(\vec{i})\mu(\vec{j}) \leq \mu(\vec{i} \wedge \vec{j})\mu(\vec{i} \vee \vec{j})$$

holds with equality if the events E_ℓ are independent. Given an intuitive explanation of what the log supermodularity inequality condition means in general (without independence).

b. Give an example of how the FKG inequality can fail if the log supermodularity property does not hold.

10. We described the algorithm QuadRes in class for finding square roots of quadratic residues mod p for p a prime. Generalize this to work mod p^k for $k > 1$ with p a prime:

a. Prove that $x \in \mathbb{Z}^*_{p^k}$ is a quadratic residue iff

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

b. Give a expected polynomial-time randomized algorithm that, given an input x a quadratic residue mod p^k, outputs a square root of x in $\mathbb{Z}^*_{p^k}$. (You should use QuadRes as a subroutine!)

11. Give a randomized, expected polynomial time, algorithm which, given a Carmichael number n as input, outputs a non-trivial factor of n. Explain why your algorithm works. Hint: Use ideas from the Miller-Rabin primality algorithm, and the algorithm for computing factors of n from n and $\varphi(n)$.

12. Extend the algorithm from problem 11 to give the complete factorization of the Carmichael number n.

13. Finish the proof for the Jacobi symbol that $\left[\frac{2}{n}\right] = (-1)^{(n^2-1)/8}$. For this, see the material and hint from the lecture on Cinco de Mayo, 2014.

14. Prove that an $(\epsilon, \frac{1}{3})$-FPRAS can be converted into an (ϵ, δ)-FPRAS. [Hint: Iterate and take the median estimate.]