

Randomized Algorithms – Problem Set 2

Robert Krauthgamer and Moni Naor

Date Due: December 30th, 2018

Homework. Please keep the answers to the following questions short and easy to read.

1. Prove that in any graph $G = (V, E)$ there is an independent set of size at least $\sum_{v \in V} \frac{1}{\text{degree}(v)+1}$
2. Consider a distributed algorithm for 2Δ coloring a graph where Δ is a bound on the largest degree (and is known to all processors): Each node selects a random “palette” (i.e. subset) of $O(\log n)$ colors. Afterwards we proceed in rounds where in each round a node selects a color from his palette and sees whether no neighbor chose the same color and fixes the color in this case. What is the probability of success of the algorithm?

Show how to use this idea in order to obtain a sublinear sequential algorithm for 2Δ coloring in the model where the graph is given as an $n \times n$ adjacency matrix. The algorithm should be sublinear, i.e. $o(n^2)$ when $\Delta \gg 1$. The algorithm should be always correct, but the expectation is sublinear.

Bonus: is it true that the palettes of the neighbors are not going to cover the palette of a node, that is the union of the palettes of the neighbor does not include the palette of a node?

3. Consider the simultaneous message model for evaluating a function $f(x, y)$: Alice and Bob share a random string. They receive inputs x and y respectively and each should send a message to a referee, Charlie, who should evaluate the function $f(x, y)$. They may also have their own private source of randomness. The goal is for Alice and Bob to send short messages to Charlie.

We will consider the equality function, i.e. $x, y \in \{0, 1\}^n$ and $f(x, y) = 1$ if $x = y$ and 0 otherwise.

- (a) Suppose that Alice and Bob send to Charlie an inner product of their input with a common random string r . What happens to this protocol if Eve, who selects the inputs and whose goal is to make Charlie compute the wrong value, knows the common string r when she selects x and y ?
- (b) Suggest a non-trivial protocol for this case, where Eve knows the common random string but not the private source of randomness that Alice and Bob each have. By non-trivial we mean one with message length which is sublinear in the input length and probability of Charlie being correct at least $2/3$ for any pair of inputs chosen by Eve.

Hint: you may use the fact that there are good error correcting codes $C : \{0, 1\}^n \mapsto \{0, 1\}^m$ where m is $O(n)$ and for any two different strings $x_1, x_2 \in \{0, 1\}^n$ the distance between $C(x_1)$ and $C(x_2)$ is $\Omega(n)$.

4. Consider the following family of functions H where each member $h \in H$ is such that $h : \{0, 1\}^\ell \mapsto \{0, 1\}$. The members of H are indexed with a vector $r \in \{0, 1\}^{\ell+1}$. The value $h_r(x)$

for $x \in \{0, 1\}^\ell$ is defined by considering the vector $x' \in \{0, 1\}^{\ell+1}$ obtained by appending 1 to x and the value is $\langle r, x' \rangle$ - the inner product of r and x' over $GF[2]$.

Prove that the family H is three-wise independent.

5. Prove that for *any* hash function $h : \{0, 1\}^* \mapsto \{0, 1\}^\ell$, the expected time (i.e. evaluations of h) to find a collision is $O(2^{\ell/2})$.
6. Extra Credit: A hundred people are in line to enter a movie theater with a hundred seats. Each person holds a ticket with an assigned seat. The first in line drops his ticket and, instead of looking for it, sits in a random place. The others enter the theater one by one and each one, if their seat is taken, instead of arguing, sits in a random vacant seat. What is the probability that the last person in line will sit in her assigned seat?