

# Randomized Algorithms 2021A – Final (Take-Home Exam)

Robert Krauthgamer and Moni Naor

February 1, 2021  
Due within one week

**General instructions.** The exam has 2 parts.

Policy: You may consult textbooks and the class material (lecture notes and homework), but no other sources (like web search). You should work on these problems and write up the solutions by yourself with no help from others.

You may use without proof theorems stated in class, provided you state the appropriate theorem that you are using. As usual, assume  $n$  (or  $|V|$ ) is large enough.

## Part I (25 points)

Answer 3 of the following 4 questions. Give short answers, that sketch the proof or provide a convincing justification in 2-5 sentences, even for true/false questions.

- A. Prove that in any graph  $G = (V, E)$  there is an independent set of size at least  $\sum_{v \in V} \frac{1}{\text{degree}(v)+1}$ .

This is an ‘easy’ question in that there are a number of ways of showing this. One way is to consider a probabilistic process that assigns random ids to nodes and declares that a node is in the set if it is a local maximum.

- B. Suppose you have a list of  $N$  common passwords, each of average length  $\ell$  and you want to prevent users from picking a password from this set. The act of deciding whether password is forbidden or not should be done at the users’ device. A fraction of  $\delta$  of the good passwords may be rejected (You may assume that there is a bound  $L$  on the length of the longest possible password). How many bits should be downloaded by a user’s device in order to execute this prevention policy?
- C. Explain whether the following claim is true or false: In every undirected graph  $G = (V, E)$ ,

$$\forall x, y, z \in V, \quad H(x, y) + H(y, z) + H(z, x) = H(x, z) + H(z, y) + H(y, x).$$

(Informally, this is about visiting the same ”triangle” in reverse direction.)

- D. Explain whether the following claim is true or false: In every undirected graph  $G$  where vertices  $u, v$  are *not* connected, adding  $(u, v)$  as a new edge will strictly decrease the hitting time  $h_{u,v}$  (for same  $u, v$ ).

## Part II (75 points)

Answer 3 of the following 5 questions.

1. Let  $k, m$  and  $n$  be natural numbers. Let  $H_1$  and  $H_2$  be two families of  $k$ -wise independent hash functions, where every  $h \in H_1 \cup H_2$  is  $h: \{0, 1, \dots, n-1\} \mapsto \{0, 1, \dots, m-1\}$ . Consider the family  $H$  of functions  $h(x) = h_1(x) + h_2(x) \bmod m$  where  $h_1 \in H_1$  and  $h_2 \in H_2$ . To sample from  $H$  one samples independently  $h_1 \in_R H_1$  and  $h_2 \in_R H_2$ .
  - (a) Is it necessarily true that  $H$  is  $k$ -wise independent?
  - (b) Is it necessarily true that  $H$  is  $2k$ -wise independent? (assume  $2k \leq n$ ).

2. Suppose two independent random walks are started at the same  $n$ -vertex graph  $G$ , from two arbitrary vertices  $u$  and  $v$ . Let the random variable  $T$  be the first time that the two walks *meet* (i.e., they are at the same vertex at the same time). Show that  $\mathbb{E}[T] \leq \text{poly}(n)$ .

Remark: You can choose any of the following models: (a) the two walkers move simultaneously at each time step; (b) the two walkers take alternate turns, i.e., one walker moves in odd time steps and the other in even time steps; (c) the two walkers take turns at random, i.e., at each step a random coin decides which walker takes a move. If necessary, you may assume also that each walker performs a lazy random walk, i.e., with probability  $1/2$  it moves and with probability  $1/2$  it stays put.

3. Consider a class with  $n$  students,  $k$  of whom want to talk in a Zoom session (we do not know which ones). The Zoom session is divided into slots. If two students attempt to talk simultaneously, then the students hear only noise and the slot is wasted. If only one student speaks at a given slot then she is happy for the rest of the session. A student who does not want to speak will be quiet throughout the session.

For given  $k$  and  $n$  we want to come up with a schedule that will tell each student when to talk (if they want to talk). The student will follow the schedule and attempt to talk on the slots assigned to her, until there is a slot where she is the **single speaker** and then shut up for the rest of the session.

**The goal is to show that there exists a “universal” schedule of length  $O(k \log n)$  slots that is good for all possible sets of  $k$  speakers.**

As a first step, show that there is a schedule of length  $O(k \log n)$  that for any  $k$ -set allows a constant fraction of the students of the set to be a single speaker in one of the slots of the session.

Hint: what happens if we select at random for each slot  $n/k$  of the  $n$  students and assign them to be potential speakers. For a fixed set  $S$  of size  $k$  and one particular slot, what is the probability that a single speaker from  $S$  is chosen?

From this step conclude that there is a schedule of length  $O(k \log n)$  slots that allows all students to be speakers in a single session.

4. Design a randomized algorithm that, given as input  $w_1, \dots, w_n \geq 0$  and an accuracy parameter  $\varepsilon \in (0, 1)$ , the algorithm stores only  $t = t(\varepsilon)$  memory words, from which one can estimate the

sum of any large-enough interval  $[a, b]$  of the inputs by an estimator  $Z_{ab}$ , that satisfies

$$\forall a, b \in [n] \text{ such that } b - a > \frac{n}{10}, \quad \Pr \left[ Z_{ab} \in (1 \pm \varepsilon) \sum_{i \in [a, b]} w_i \right] \geq \frac{3}{4}.$$

Notice that the algorithm decides what to store *before* knowing  $a, b$ , that the memory size  $t(\varepsilon)$  is independent of  $n$ , and that the accuracy is multiplicative (not additive).

**UPDATE: This question is flawed and was eventually cancelled.** A possible fix is to add that every  $w_j \in \{0, 1, 2, 3\}$  and change the goal to  $t = \text{poly}(1/\varepsilon, \log n)$ .

5. Given a simple graph  $G = (V, E)$  we are interested in **rainbow colorings**: assignments of colors to nodes, so that every node (with some minimum degree) sees many different colors in its immediate neighborhood. For a given coloring, we say that a node of degree  $d$  is  $\alpha$ -happy if the number of colors in its neighborhood is at least  $\lfloor \alpha d \rfloor$ .

Let  $\Delta$  be the maximum degree in the graph. Suppose that the nodes are colored at random from one of  $\Delta$  colors. Consider a node  $v \in V$  of degree  $1 \leq d \leq \Delta$ . What is the probability that  $v$  is  $\alpha$ -happy for some fixed  $0 < \alpha < 1/4$ ? Come up with a "nice" expression involving  $\alpha, d$  and  $\Delta$ .

Let  $A_v$  be the event that node  $v$  is  $\alpha$ -happy. For two nodes  $u$  and  $v$  that are not neighbors, are the events  $A_v$  and  $A_u$  necessarily independent? What about  $u$  and  $v$  of distance at least 3?

Show that there is a constant  $\alpha > 0$  s.t. for any graph there is a coloring with  $\Delta$  colors where all nodes of degree at least  $\log \Delta$  are  $\alpha$ -happy.

**Good Luck.**