CSE 521: Design and Analysis of Algorithms **Fall 2023**

Problem Set 1

Deadline: Oct 16 (at 11:59 PM) in gradescope

Instructions

- You should think about each problem by yourself for at least an hour before choosing to collaborate with others.
- You are allowed to collaborate with fellow students taking the class in solving the problems. But you **must** write your solution on your own.
- You are not allowed to search for answers or hints on the web. You are encouraged to contact the instructor or the TAs for a possible hint.
- You cannot collaborate on Extra credit problems
- Solutions typeset in LATEX are preferred.
- Feel free to use the Discussion Board or email the instructor or the TAs if you have any questions or would like any clarifications about the problems.
- Please upload your solutions to Gradescope.

In solving these assignments and any future assignment, feel free to use these approximations:

$$1 - x \approx e^{-x}, \qquad \sqrt{1-x} \approx 1 - x/2, \qquad n! \approx (n/e)^n, \qquad \left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{en}{k}\right)^k$$

1) For a prime p we can generate a pairwise independent hash function by choosing a, b independently from the interval $\{0, \dots, p-1\}$ and using $ax + b$ as a random number (see lecture 4). Suppose we generate t pseudo random numbers this way, $r_1, \dots, r_t$ where $r_i = ai + b \pmod{p}$. We want to say this set is far from being mutually independent. Consider the set $S = \{p/2, \dots, p-1\}$ which has half of all elements. Prove that with probability at least $\Omega(1/t)$ none of the pseudo-random-numbers are in S. Note that if we had mutual independence this probability would have been $1/2^t$.

2) Let n be an even integer (you can assume n is large enough). Let G_k be the (multi)-graph on n vertices formed by taking the union of k perfect matchings which are chosen uniformly at random from the set of all perfect matchings among n vertices (A sanity check: how would you efficiently sample a uniformly random perfect matching?).

   a) Prove that if $k \geq 3$, then G_k is connected with high probability? Any probability of the form $1 - 1/n$ or $1 - 1/\log n$ that that approach 1 as n tends to infinity suffices.)

      A side note: In fact one can show that for $k \geq 3$, G is a very well connected in the sense that it becomes an expander. We will learn more about expanders in future lectures.

   b) Show that if $k = 2$ then the probability that G is connected goes to 0 as $n \to \infty$.