Lecturer: Thomas Rothvoss   Due date: Friday, Oct 11, 2024, 11pm, on GradeScope

Problem Set 2

CSE 521 - Design and Analysis of Algorithms

Fall 2024

Exercise 1 (10pts)
We will learn in class that for a prime p one can generate a pairwise independent hash function by choosing a,b independently from the interval $\{0,\dots,p-1\}$ and using $ax+b \pmod p$ as a random number. Now suppose we generate t pseudo random numbers this way, $r_1,\dots,r_t$ where $r_i = ai+b \pmod p$. We want to prove that 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 $1/2^t$.

Exercise 2 (3+3+4=10pts)
Let n be an even integer (you can assume n is large enough). Let $G_k = (V,E)$ 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?).

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

ii) Prove that if $\emptyset \subset S \subset V$ is a set of even cardinality $\ell := |S|$ and M is a uniform random perfect matching, then
$$\Pr[|M \cap \delta(S)| = 0] = \frac{(\ell-1)!! \cdot (n-\ell-1)!!}{(n-1)!!}$$
(where we write $\delta(S) := \{\{i,j\} \in V : |\{i,j\} \cap S| = 1\}$ as the cut w.r.t. the complete graph).

iii) 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.). You will get full points if you prove this when k is some universal constant, say 10 or 100.

Remark. The *double factorial* of an odd integer is $n!! = n \cdot (n-2) \cdot (n-4) \cdot \ldots \cdot 1$ (for an even integer the product ends with 2). You may use without a proof the approximation of
$$(n!!)^2 = \Theta\Big(\frac{n!}{\sqrt{n}}\Big)$$