Randomized Algorithms
Homework Set 2

Due Date: Dec. 9th 2024

Moni Naor

A. Recall the *simultaneous message model*, where Alice with input x and Bob with input y each send a message to a referee Charlie who computes $f(x, y)$. For the randomized case there are two models, (i) With shared random bits and (ii) With private random bits only. Consider the k-disjoint problem where the two parties each receive a subset $S_A \subseteq U$ and $S_B \subseteq U$ respectively and the goal is to determine whether the two subsets intersect (whether $S_A \cap S_B = \phi$) and where $|S_A| = |S_B| = k$. Show that there is a shared randomness protocol for this problem where the message lengths are $O(k \log k)$ and the probability of error is $O(1/poly(k))$.

Hint: consider a mapping to an intermediate range of size $poly(k)$.

Open (AFAIK): is there an $O(k)$ protocol with constant error?

B. Suppose that there is graph $G = (V, E)$ that is streamed to a low memory processor M and the goal is for M to check whether G is Hamiltonian or not (output 'accept' or 'reject'). By streaming we mean that the processor sees the input just once, in a single pass and can store only a small part of it. Obviously, this is hard to perform even without the streaming requirement (at least if $P \neq NP$), so we want to add a proof that G contains a Hamiltonian cycle, also in a streaming fashion. That is, following the graph G there will be a polynomial-sized witness W added that will help M check this fact. That is the new stream will be (G, W). The properties we want are:

1. Completeness: If G is Hamiltonian there is a witness W that will make the processor M 'accept' after seeing G and W.
2. Soundness: If G is not Hamiltonian, then for any W', after streaming (G, W') the processor M outputs 'reject' with probability at least $1 - \varepsilon$. The probability is over M's random string.

Suggest such a scheme where the memory M requires is polynomial in $\log n$ and $\log(1/\varepsilon)$.

Hint: You may use the memory-checking process we saw.

C. Is it true that every graph G with m edges and no self-loops has a cut with at least $m/2$ edges? Think of a random partition.