1ST TUTORIAL ON RANDOMIZED ALGORITHMS

Intro and Markov chains

1. *Envelopes.* You are presented with two sealed envelopes. There are k\$ in one of those and ℓ\$ in the other ($k, \ell \in \mathbb{N}$ but you do not know k, ℓ in advance). You may open an envelope and (based on what you see) decide to take this one or the other (without looking into both).

a) Is there a way how to walk away with the larger amoung of money with probability strictly larger than 0.5?
b) What is the expected value you walk away with (in terms of k, ℓ)?

2. *Graph isomorphism.* You have seen an interactive proof of graph non-isomorphism during the lecture. Can you come up with an "zero knowledge" interactive proof of graph isomorphism?

Note: Observe that when the prover provides the isomorphism, this yields a valid interactive proof for graph isomorphism. However, we require that (informally) the verifier "learns nothing" about the isomorphism in case the two graphs are isomorphic. That is, assuming that the verifier cannot solve the graph isomorphism problem and does not know the isomorphism beforehand, the verifier knows nothing more than that the two graphs are isomorphic at the end of the protocol. Such interactive proofs are called *zero knowledge*.

3. *Examples of Markov chains.* Come up with MCs with the following properties:

a) Create a MC that is irreducible.
b) Create a MC that is not irreducible.
c) Create a MC that is periodic.
d) Create a MC that is not periodic.
e) Compute a stationary distribution of the following MC:

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

f) Create a MC that has more stationary distributions.
g) A stochastic process that is *not* a Markov chain.