4^{TH} TUTORIAL ON RANDOMIZED ALGORITHMS

Exponentially decreasing bounds on the tails with Chernoff

1. *Simulating a biased coin using a fair coin.* We are given a fair coin with $\Pr[\text{tails}] = 0.5$. Show how to generate a random bit with $\Pr[1] = p$ for a given $p \in (0, 1)$ (both $p = 0$ and $p = 1$ are a bit boring). How many fair coin flips do we need in expectation? (This could be useful for some homework...)

i) First, assume that $p = k/2^\ell$ for some integers k and ℓ.

ii) What about any rational p, say, $p = 1/3$? What about irrational p?

2. *Anti-Chernoff.* Give an example of n *dependent* random variables $X_i \in \{0, 1\}, i = 1, \ldots, n$ such that each X_i is a (fair or biased) coin flip but Chernoff bounds do not hold for $\sum_i X_i$. Are X_i's positively or negatively correlated or uncorrelated?

3. *Distinguishing coins.* You are given two coins. One is fair and the other one has $\Pr[\text{tails}] = 1/4$. We use the following algorithm to distinguish those:

- Pick a coin and toss it n times.
- Let $\hat{p}$ be the probability of getting a tails (number of tails over n).
- If $\hat{p} \geq 3/8$ we say this coin is fair.

Show that if $n \geq 32 \ln(2/\delta)$ then our algorithm answers correctly with probability at least $1 - \delta$.

4. *Estimator Theorem.* Let U be a finite set and $G \subseteq U$ its subset. We know $|U|$ and wish to estimate $|G|$. If we take n uniformly random and independent samples from U (with replacement), calculate $X =$ number of samples inside of G, and output $A = X\frac{|U|}{n}$. How large n do we need to choose so that A is a $(1 \pm \varepsilon)$-approximation of $|G|$ with probability at least $1 - \delta$, i.e.,

$$\Pr\left[(1-\varepsilon)|G| \leq A \leq (1+\varepsilon)|G|\right] \geq 1 - \delta\,?$$

5. *QuickSort analysis.* Consider the QuickSort algorithm with uniformly random pivot choice. Show that the expected number of comparisons is $c \cdot n \ln(n)$ for some constant c. Prove that the probability of it making at least $32n \ln(n)$ comparisons is at most $1/n^3$.