CS 174 Homework Assignment 9 (due Monday, May 6)

1. Let $X_i \in \{0,1\}$ be independent binary random variables. Define $S_n = \sum_{i=1}^{n} X_i$. Note that $\mathrm{E}[S_n] = n/2$ and $\mathrm{E}[S_n/n] = 1/2$.

    (a) Use the additive Chernoff bound that we discussed in class to get an upper bound on the probability $P\left(\frac{S_n}{n} - \frac{1}{2} > \lambda\right)$.

    (b) Show that $S_n - n/2$ is a martingale sequence and show that the conditions needed for Azuma's inequality apply.

    (c) Use Azuma's inequality to obtain an upper bound on the probability $P\left(\frac{S_n}{n} - \frac{1}{2} > \lambda\right)$. Compare to the bound you obtained from Chernoff.

2. (*Polya's urn*). Consider an urn which contains b black balls and w white balls. At each step, we select a ball at random from the urn, and replace that ball with k balls of the same color. Show that the fraction of black balls in the urn at each step forms a martingale.

3. Consider a collection of n random variables X_i drawn independently from the *geometric distribution* with mean 2. That is, X_i is the number of flips of an unbiased coin up to and including the first heads. Let $X = \sum X_i$ and let δ be a positive real constant. Use the Chernoff technique to to derive bounds on the probability that $X > (1+\delta)(2n)$.

4. The class **BPP** (Bounded-error Probabilistic Polynomial time) consists of all languages L that have a randomized algorithm A running in worst-case polynomial time such that for any input x:

    - $x \in L \rightarrow P[A(x) \text{ accepts}] \geq 1/2 + 1/p(n)$,
    - $x \notin L \rightarrow P[A(x) \text{ accepts}] \leq 1/2 - 1/p(n)$,

    where $p(n)$ is a polynomially bounded function of the input size n. Using the Chernoff bound, show that a polynomial number of independent repetitions of a **BPP** algorithm suffice to reduce the error probability to $1/2^n$.

5. Compute 2^{68} mod (19).