Suggested Exercises

This is a list of practice problems that will periodically updated. Please note that you *do not need to submit the solutions to these problems.*

Discrete Probability

1. **An improved Schwartz-Zippel lemma.** Prove the following version of the Schwartz-Zippel lemma. Let $f(x_1, \ldots, x_n)$ be a non-zero polynomial over a field $\mathbb{F}$ with *degree-sequence* $(d_1, \ldots, d_n)$, defined as follows: let d_1 be the maximum exponent of x_1 in f and let $f_1(x_2, \ldots, x_n)$ be the coefficient of $x_1^{d_1}$ in f; then, let d_2 be the maximum exponent of x_2 in f_1 and let $f_2(x_2, \ldots, x_n)$ be the coefficient of $x_2^{d_2}$ in f_1 and so on. Suppose each variable x_i is assignen a value v_i chosen randomly and independently from a set $S_i \subseteq \mathbb{F}$. Then prove that
$$\mathbb{P}\left[f(v_1, \ldots, v_n) = 0\right] \ \leq \ \frac{d_1}{|S_1|} + \cdots + \frac{d_n}{|S_n|}\,.$$
Can you construct the example of a polynomial where the above bound is strictly better than the bound we derived in the class?

2. **Patterns in coin tosses.** Consider an infinite sequence of independent tosses of a fair coin. Define the following random variables:
$$Y_1 \ = \ \text{Number of occurences of the pattern HTT in the first } n \text{ tosses}$$
$$Y_2 \ = \ \text{Number of occurences of the pattern HTH in the first } n \text{ tosses}$$
As discussed in class, it is easy to compute $\mathbb{E}\left[Y_1\right]$ and $\mathbb{E}\left[Y_2\right]$ and verify that they are equal. Now consider the following two random variables:
$$Z_1 \ = \ \text{Number of tosses after which the pattern HTT first appears}$$
$$Z_2 \ = \ \text{Number of tosses after which the pattern HTH first appears}$$
Compute $\mathbb{E}\left[Z_1\right]$ and $\mathbb{E}\left[Z_2\right]$ and verify that they are *not* equal. Why is one patten more likey to occur first even though they are both occur an equal number of times (in expectation) in a given number of tosses?

3. **Random Polynomials.** For a prime number p, the field $\mathbb{F}_p$ has the elements $\{0, 1, \ldots, p-1\}$, with addition and multiplication done modulo p. A degree-d polynomial in the variable x over the field $\mathbb{F}_p$ (for pime p) is defined as:
$$P(x) \ = \ c_0 + c_1 \cdot x + \ldots + c_d \cdot x^d\,,$$
where the coefficients $c_0, \ldots, c_d$, and the variable x all take values in $\mathbb{F}_p$. , and all addition and multiplication is done modulo p. A value $x \in \mathbb{F}_p$ is called a root of P if $P(x) = 0$. Consider

picking a random polynomial P by selecting $c_0, \ldots, c_d$ randomly from $\mathbb{F}_p$, and define the random variable

$$Z \;=\; \text{Number of roots of } P\,.$$

Calculate $\mathbb{E}[Z]$ and $\mathsf{Var}[Z]$.

4. **Random Permutations.** Consider picking a permutation $\pi : [n] \to [n]$ uniformly at random (here $[n]$ denotes the set $\{1, \ldots, n\}$). A number $i \in [n]$ is said to be a *fixed point* of π if $\pi(i) = i$. Define the random variable

$$Z_1 \;=\; \text{Number of fixed points of } \pi\,.$$

Compute $\mathbb{E}[Z_1]$ and $\mathsf{Var}[Z_1]$. Also, recall that each permutation can be decomposed into cycles, obtained by looking at the orbits of the elements in $[n]$. For example, if $\pi(1) = 3$, $\pi(3) = 6$ and $\pi(6) = 1$, this gives a cycle of size 3. Define the random variable

$$Z_2 \;=\; \text{Number of cycles in } \pi\,.$$

Compute $\mathbb{E}[Z]$.

5. **Coupon Collection Revisited.** Recall that in class we showed that in the coupon collection problem, if T is defined to be the time to collect coupons of all n times, then $\mathbb{E}[T] = n \ln n + \Theta(n)$. Can you compute $\mathsf{Var}[T]$? Use this to derive a bound on the probability that T is significantly larger than $\mathbb{E}[T]$?