CS 217 – Algorithms Design and Analysis
Homework Assignment 4

Shanghai Jiaotong University, Fall 2015

Handed out on Wednesday 2015-12-05

Due on Thursday 2015-12-11

You can hand in your solution either as a printed file or hand-written on paper (in this case please *write nicely*). You have to justify your solutions (i.e., provide proofs).

You can solve the homework assignment in your group, and every group should hand in *one* solution. Do not copy solutions from other groups! If you are completely stuck, you may ask me for advice!

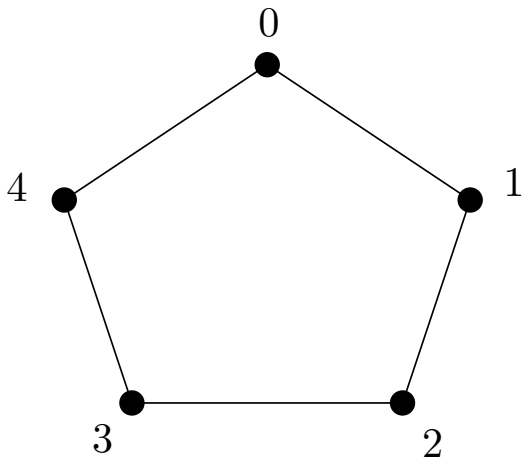
5 Basic Probability Theory

Exercise 5.1. Let X be a random variable taking on values in $\mathbb{N}_0$. Prove that $\mathbb{E}[X] = \sum_{k \geq 1} \Pr[X \geq k]$.

Exercise 5.2. We toss a coin that shows 1 with probability p and 0 with probability $1 - p$. We toss it until it shows 1. Let T be the number of tosses we have done in total.

- What is $\Pr[T = k]$?
- What is $\Pr[T \geq k]$?
- What is $\mathbb{E}[T]$?

Exercise 5.3. Consider the following graph:



A drunk person starts at some vertex u. In every step, the drunkard walks to a random one of the two neighboring vertices. Once he reaches 0, he stays there (and sleeps until he sobers up).

Let t_i be the expected number of steps he takes until he reaches 0 if he starts his random walk at vertex i. Compute t_i for $i \in \{0, 1, 2, 3, 4\}$.

Exercise 5.4. Let p be a prime number and $\mathbb{F}_p$ be the finite field of size p. We sample two elements $a, b \in \mathbb{F}_p$ uniformly at random, independently (formally (a, b) is uniform over $\mathbb{F}_p^2$). For each $u \in \mathbb{F}_p$ define the random variable

$$X_u := a + bu$$

where addition and multiplication is done in $\mathbb{F}_p$.

1. Show that the X_u are pairwise independent. What is $\Pr[X_u = i]$?

Now sample (a, b, c) uniformly at random from $\mathbb{F}_p^3$ and set

$$Y_u := a + bu + cu^2 \ .$$

2. Show that the Y_u are 3-wise independent. That is, for any distinct $u, v, w \in \mathbb{F}_p$ the three random variables Y_u, Y_v, Y_w are independent.

Hint. You have to use the fact that a polynomial $p(x)$ over $\mathbb{F}_p$ of degree d has at most d roots.

3. Construct a 3-wise independent class of hash functions. That is, a set $\mathcal{H}$ of functions $\mathbb{F}_p \to \mathbb{F}_p$ such that for distinct $u, v, w \in \mathbb{F}_p$ and arbitrary $i, j, k \in \mathbb{F}_p$:

$$\Pr_{h \in \mathcal{H}}[h(u) = i, h(v) = j, h(w) = k] = \frac{1}{p^3} \ .$$

The size of your set $\mathcal{H}$ should be polynomial in p. That is, you cannot simply let $\mathcal{H}$ be the set of *all* functions (which would clearly be 3-wise independent).