CS 70 FALL 2006 — DISCUSSION #9

D. GARMIRE, L. ORECCHIA & B. RUBINSTEIN

1. Administrivia

(1) Course Information
   - The 9^{th} homework is due Friday at 4pm in 283 Soda Hall.

2. Random Variables: Independence & Conditional Probabilities

Recall the definition of random variables and their distributions from class.

Definition 1. A *random variable* X on probability space (Ω, P) is a function from sample points in Ω to integers $\mathbb{Z}$. The notation $\{X = m\}$ for some $m \in \mathbb{Z}$ is shorthand for the event $\{\omega \in \Omega \mid X(\omega) = m\}$, so $P(X = m)$ is just the probability of that event. The *distribution* of X is the set of all possible pairs of X value and its probability, $\{(m, P(X = m)) \mid m \in \mathbb{Z}\}$.

The sets $X^{-1}(m) = \{\omega \in \Omega \mid X(\omega) = m\}$ partition Ω and so $\sum_{m\in\mathbb{Z}} \Pr(X = m) = 1$; also $\Pr(X = m) \geq 0$ for each $m \in \mathbb{Z}$. Two important distribution parameters are the mean and variance.

Definition 2. The *expectation* and *variance* of a r.v. X are defined as $\mathbb{E}[X] = \sum_{m\in\mathbb{Z}} m \cdot \Pr(X = m)$ and $\mathrm{Var}(X) = \mathbb{E}\left[(X - \mathbb{E}[X])^2\right] = \mathbb{E}\left[X^2\right] - (\mathbb{E}[X])^2$, respectively.

The concepts of conditional probability and independence naturally extend to events about r.v.'s.

Definition 3. Let r.v.'s X and Y be defined on a common probability space (Ω, P). Then for any $y \in \mathbb{Z}$ such that $\Pr(Y = y) > 0$, the probability the *conditional distribution* of X given $\{Y = y\}$ is $\Pr(X = x \mid Y = y) = \frac{\Pr(X=x \wedge Y=y)}{\Pr(Y=y)}$ for each $x \in \mathbb{Z}$. X and Y are said to be *independent* if for each $x, y \in \mathbb{Z}$, $\Pr(X = x \mid Y = y) = \Pr(X = x)$ or equivalently if $\Pr(X = x, Y = y) = \Pr(X = x)\Pr(Y = y)$.

To demonstrate some of these ideas consider the following.

Exercise 1. Pairwise but non-mutually independent events. In class we mentioned that there can be 3 events $A, B, C \subseteq \Omega$ which are all pairwise independent, but such that their collection is not mutually independent. Consider two independent random variables X_1, X_2 distributed uniformly over $\mathbb{Z}_m = \{0, 1, \cdots m-1\}$:

$$\forall a \in \mathbb{Z}_m, \forall i \in \{1, 2\}, \ \Pr(X_i = a) = \frac{1}{m} \ .$$

Date: October 25, 2006.

The authors gratefully acknowledge Chris Crutchfield and Amir Kamil for the use of their previous notes, which form part of the basis for this handout.

(a) Check that this defines valid *marginal* distributions for X_1 and X_2. What is $\Pr(X_1 = x, X_2 = x')$? Check that your answer sums to 1 over $\mathbb{Z}_m^2$. Can you compute the marginals from the joint?
(b) Now consider the r.v. $S_1 = X_1 + X_2 \mod m$, which takes values in $\mathbb{Z}_m$ just like X_1, X_2. What is the distribution of S?
(c) Prove that X_1, X_2, S are pairwise independent. [**Hint:** for fixed $a, b, c \in Z_m$ define the events $A = \{X_1 = a\}$, $B = \{X_2 = b\}$, $C = \{S = c\}$, then prove that these events are pairwise independent. **Hint:** you already know that A, B are independent, and you can write S in terms of X_1, X_2].
(d) Finally show that A, B, C are not mutually independent (equivalently that X_1, X_2, S aren't). [**Hint:** what happens if $c \neq a + b \mod m$?]

3. Linearity of Expectation

Definition 4. An *indicator variable* is a r.v. that takes on only the values 0 and 1. Since it is a r.v., it is a function of $\omega \in \Omega$ and so is written is as function of a predicate: $\mathbf{1}[P(\omega)] = \begin{cases} 1 & P(\omega) = T \\ 0 & P(\omega) = F \end{cases}$.

Exercise 2. Indicator Variables. Let I be an indicator r.v. on predicate P.
(a) Show that $\mathbb{E}[I] = \Pr(I = 1) = \Pr(P \text{ is true})$.
(b) Suppose we toss a fair coin n times, landing $Y \in \{0, 1, \ldots, n\}$ heads. If X is the indicator of the first coin toss landing heads, calculate $\mathbb{E}[X]$.
(c) Calculate $\mathbb{E}[Y]$. Your answer should be a simple function of n. [**Hint**: use linearity of expectation.]
(d) Use the previous part to prove the following identity:

$$\sum_{i=1}^{n} i \cdot \binom{n}{i} = n2^{n-1}.$$

Exercise 3. Shakespearean Monkey. A monkey types on a 26-letter keyboard, with all lowercase letters. Assume that the monkey choses each character independently and uniformly at random and that it types 1,000,000 characters total. What is the expected number of times the sequence "hamlet" appears?

Exercise 4. Number of Runs[1]. We toss a fair coin n times. Runs are consecutive tosses with the same result. For instance, the toss sequence HHHTTHTH has 5 runs. What is the expected number of runs?

4. Variance

Exercise 5. What is the variance of an indicator r.v.?

Exercise 6. What is the variance and expectation of the constant r.v. $X = C$?

[1] From 'Invitation to Discrete Mathematics', Matousek and Nesetril