Basic Algorithms — Fall 2014 — Problem Set 3
Due: Sept. 25

1. Three fair coins are tossed. Let \( \mathcal{A} \) be the event that at least two coins are heads. Let \( \mathcal{B} \) be the event that the number of heads is odd. Let \( \mathcal{C} \) be the event that the third coin is heads. Are \( \mathcal{A} \) and \( \mathcal{B} \) independent? \( \mathcal{A} \) and \( \mathcal{C} \)? \( \mathcal{B} \) and \( \mathcal{C} \)?

2. Two dice are tossed. Let \( X \) be a random variable denoting the value of the first die, and \( Y \) be a random variable denoting the value of the second. Let \( \mathcal{A} \) be the event \( X + Y = 7 \), \( \mathcal{B} \) be the event \( X = 1 \), and \( \mathcal{C} \) be the event that either \( X = 1 \) or \( Y = 1 \). Are the events \( \mathcal{A} \) and \( \mathcal{B} \) independent? \( \mathcal{A} \) and \( \mathcal{C} \)?

3. Consider again the dice game played by Alice and Bob in Example 12 in the Primer. The game is changed so that if Bob wins, Alice pays Bob a number of dollars equal to the sum of the values of any dice matching Bob’s guess. So, for example, suppose Bob guesses 3. If Alice rolls (3, 4), she pays Bob 3 dollars; if Alice rolls (5, 3), she also pays Bob 3 dollars; if Alice rolls (3, 3), she pays Bob 6 dollars; if Alice rolls (2, 5), she pays Bob nothing.

Devise an optimal strategy for Bob (remember, Alice tells Bob the sum of the two dice before Bob makes his guess). Also, let \( W \) be a random variable representing his winnings (in dollars). Compute \( E[W] \). Hint: use the law of total expectation, just above Example 23 in the Primer.

4. In class, we discussed the encryption scheme known as the one-time pad. We can prove an important security property using notions from probability. Recall that messages, keys, and ciphertexts are \( \ell \)-bit strings, i.e., elements of the set \( \{0, 1\}^\ell \). We model the key as a random variable \( K \) uniformly distributed over the set \( \{0, 1\}^\ell \). We model the message as a random variable \( M \) taking values in \( \{0, 1\}^\ell \).

The distribution of \( M \) need not be uniform; in fact, we make no assumption about the distribution of \( M \), except that we insist that \( M \) and \( K \) are independent. Now define the random variable \( C := K \oplus M \), which represents the ciphertext (recall that “\( \oplus \)” is the bit-wise exclusive-OR operator).

Prove that \( C \) and \( M \) are independent random variables. Hint: mimic the proof in Example 19 of the Primer that \( Z' \) and \( X \) are independent.

Note: intuitively, independence here means that after an eavesdropper has no more information about the message after seeing the ciphertext than she did before.

5. Suppose \( X_1 \) and \( X_2 \) are independent random variables, each uniformly distributed over the set \( \{\pm 1\} \); that is, each \( X_i \) takes the value \( -1 \) with probability \( 1/2 \) and the value \( 1 \) with probability \( 1/2 \).

(a) Compute \( E[X_1 + X_2] \).
(b) Compute \( E[(X_1 + X_2)^2] \).
(c) Generalize part (b) to \( n \) random variables: compute \( E[(X_1 + \cdots + X_n)^2] \), where each of the \( X_i \)'s are uniformly distributed over \( \{\pm 1\} \); here, you may assume that the \( X_i \)'s are pairwise relatively prime, which means that for every pair of distinct indices \( i \) and \( j \), the variables \( X_i \) and \( X_j \) are independent.

Hint: make use of Theorems 12 and 13 in the Primer.

6. A die is rolled repeatedly until it comes up “1,” or until it is rolled \( n \) times (whichever comes first). What is the expected number of rolls of the die? Hint: use Theorem 15 in the Primer.

The following is for honors students only.

H1. This exercise asks you to generalize Boole’s inequality, proving Bonferroni’s inequalities. Let \( \{\mathcal{A}_i\}_{i \in I} \) be a finite family of events, where \( n := |I| \). For \( m = 0, \ldots, n \), define

\[
\alpha_m := \sum_{k=1}^{m} (-1)^{k-1} \sum_{|J| = k} \Pr\left[ \bigcap_{j \in J} \mathcal{A}_j \right].
\]
Also, define

$$\alpha := \mathcal{P} \left( \bigcup_{i \in I} A_i \right).$$

Show that \(\alpha \leq \alpha_m\) if \(m\) is odd, and \(\alpha \geq \alpha_m\) if \(m\) is even. Hint: use induction on \(n\); also, this problem is really not that hard; the hardest part is just the excessive notation; because of this, you might start with the case \(m = 3\) (but arbitrary \(n\)); after that, it should be clear how to generalize.