Discrete Mathematics

Assignment 7

Date Due: 8:00 PM, Thursday, the 7th of July 2011

Office hours: Tuesdays, 1:00-3:00 PM, and Wednesdays, 12:00-1:00 PM

Exercise 1. Let $n \in \mathbb{Z}_+$ such that $n-1 = 2^s t$ for $s \in \mathbb{N}$ and $t = 2k+1$ for some $k \in \mathbb{N}$. We say that n passes Miller's test for the base b if either $b^t \equiv 1 \mod n$ or $b^{2^j t} \equiv -1 \mod n$ for some j with $o \le j \le s-1$. It can be shown that a composite integer passes Miller's test for fewer than $n/4$ bases b with $1 < b < n$. A composite integer that passes Miller's test to the base b is called a *strong pseudoprime to the base b*

i) Show that if n is prime and $b \in \mathbb{Z}_+$ with $b \nmid n$, then n passes Miller's test for the base b.

ii) Show that 2047 passes Miller's test to the base 2, but that it is composite.

(3 + 2 Marks)

Exercise 2. Show that if $k, n \in \mathbb{N}$ with $1 \le k \le n$, then

$$\binom{n}{k} \le \frac{n^k}{2^{k-1}}$$

(2 Marks)

Exercise 3. The multinomial formula states that for $a_1, \dots a_k \in \mathbb{R}$ and $n \in \mathbb{N}$

$$(a_1 + \ldots + a_k)^n = \sum_{j_1+j_2+\ldots j_k = n} c_{j_1,j_2,\ldots,j_k} a_1^{j_1} a_2^{j_2} \ldots a_k^{j_k}.$$

where $c_{j_1,j_2,\ldots,j_k} \in \mathbb{R}$. Determine the constants $c_{j_1,j_2,\ldots,j_k}$ by considering permutations of indistinguishable objects.
(3 Marks)

Exercise 4. How many solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 29$$

where $x_i \in \mathbb{N}$, $i = 1, \ldots, 6$ are such that

i) $x_i > 1$ for $i = 1, \ldots, 6$?

ii) $x_i \ge i$ for $i = 1, \ldots, 6$?

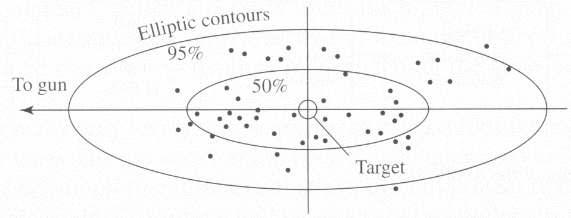
iii) $x_1 > 8$ and $x_2 < 8$?

(3 × 2 Marks)

Exercise 5. Show that if A and B are events and P is a probability function, then $P[A \cap B] \ge P[A] + P[B] - 1$. This is known as *Bonferroni's inequality.*
(2 Marks)

Exercise 6. In ballistics studies conducted during World War II it was found that, in ground-to-ground firing, artillery shells tended to fall in an elliptical pattern such as that shown below.

The probability that a shell would fall in the inner ellipse is 0.50; the probability that it would fall in the outer ellipse is 0.95.



i) A firing is considered a success (s) if the shell falls within the inner ellipse; otherwise it is a failure (f). Construct a tree to represent the firing of three shells in succession.

ii) List the sample points (of the sample space S) generated by the tree.

iii) Let A_1 denote the event that the first firing is successful, A_2 the event that the scond firing is successful and A_3 the event that the third firing is successful. List the sample points that make up these three events. Are the events mutually exclusive? Explain from both a practical and a mathematical point of view.

iv) Describe the event $A_1^c = S \setminus A_1$ verbally, and then list the sample points that make up this event.

v) Describe the event $A_1 \cap A_2^c \cap A_3^c$ verbally, and then list the sample points that make up this event.

vi) Find the probability of the event $A_1 \cap A_2^c \cap A_3^c$.

(1 + 1 + 2 + 2 + 2 + 1 Marks)

Exercise 7. Devise a Monte Carlo algorithm that determines whether a permutation of the integers 1 through n has already been sorted (that is, in increasing order), or, instead, is a random permutation. A step of the algorithm should answer "true" if it determines the list is not sorted and "unknown" otherwise. After k steps the algorithm decides that the numbers are sorted if the answer is "unknown" in each step. Estimate the probability that the algorithm produces an incorrect answer as a function of k and n.

Hint: For each step, whether two randomly selected elements are in the correct order. Make sure these tests are independent!
(4 Marks)

Exercise 8. Show that the Fibonacci numbers satisfy the recurrence relation $f_n = 5f_{n-4} + 3f_{n-5}$ for $n = 5, 6, 7, \ldots$ together with the initial conditions $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$. Use this to recurrence relation to show that $5 \mid f_{5n}$.
(2 + 2 Marks)

Exercise 9. Let T be the set of Dyck words, i.e., the set of words w whose letters are taken from the alphabet $\{\uparrow, \downarrow\}$ and satisfy

A) $\#(\downarrow) = \#(\uparrow) = n \in \mathbb{N}$

B) In any word consisting of the first k letters of w, $\#(\uparrow) \geq \#(\downarrow)$ $(k = 1, \ldots, 2n)$.

Let S be the set of words constructed inductively from the alphabet $\{\uparrow, \downarrow\}$ through the principles

- The empty string $\emptyset$ is an element of S,
- If $w_1, w_2 \in S$, then $\uparrow w_1 \downarrow w_2 \in S$.

The goal of this exercise is to show that $S = T$.

i) Use structural induction on S to show that every element in S satisfies the properties A) and B). Conclude that $S \subset T$.

ii) Show that every Dyck word w can be written in the form $\uparrow w_1 \downarrow w_2$ for some (possibly empty) Dyck words w_1, w_2. Conclude that $T \subset S$.

(2 + 3 Marks)