Homework #2

Probability and More Functions

Out : September 16, 2:30 pm
Due : September 23, 12:30 pm

Instructions: Please fill in the graphs and diagrams provided and write the rest of your answers on separate paper. Staple them together, put your name and "CS007" at the top, and put it in the CS007 handin bin in CIT room 242.

1. For each of the following figures, decide whether or not the figure shows a valid probability distribution, and if so, identify it as a uniform or non-uniform distribution.

   (a)
   -bb-error = =

   (b)
   -bb-error = =

(c)
-bb-error = =

(d)
-bb-error = =

2. Consider a 5-sided die.
   - (a) The set of possible values for the die roll is the integers from 1-5. Draw the probability distribution graph for the set of these possible values, and label the values on the axes.
     -bb-error = =
   - (b) Is this a uniform distribution over the set of possible values?
3. Now consider two 5-sided dice.
   - (a) If you were to roll the two dice, what would be the possible values for the sum of the two dice?
   - (b) Draw the probability distribution graph for the set of possible values, and label the values on the axes. Don't put any values on the graph that have a probability of zero.
     -bb-error = =
   - (c) Is this a uniform distribution over the set you gave in part (a)?
4. Given a table which represents a function with two inputs, we can transform the function to a function with one input by choosing of the inputs and fixing it to be a specific constant value. We get another one-input function by plugging in a different value for that input. In this way we get one one-input function for each different value of that input. *Example:*
   - *We start with the table describing a two-input function:*

		y	
		1	*0*
x	*1*	*%*	*#*
	0	*&*	*$*

   - *Now we fix the x input to be 1.*
   - *We now look only at the relevant row of our table:*

	y	
	1	*0*
$x = 1$	*%*	*#*

- *This can be interpreted as a function of one input, y, like the ones you saw in the last homework:*

-bb-error = =

- *If we do this for both of the possible x inputs from our table, this gives us a complete description of the function.*

-bb-error = =

-bb-error = =

Below we use a table to describe a function of two inputs, x and y. Your job is to take each value for x in turn, plug that value in and thus obtain a one-input function.

		y	
		1	0
x	1	7	13
	0	17	5

Fill in the arrows in the following diagram to get the appropriate one-input function diagrams.

-bb-error = =

-bb-error = =

5. Now let's look at the way in which some of these concepts can be applied to cryptography. We have talked about how a cryptosystem can be described as a two-input function. That is, $f(plain, key) = cyph$. As we saw in the previous problem, we can hold either the key or the plain input fixed, and make functions with one input for all the possible values of the fixed input.

   (a) Consider the following two-input function table that describes a cypher function for encrypting one character out of an alphabet of only three characters. That is, the plaintext and cyphertext can both be either 0, 1, or 2.

		key	
		0	1
	0	0	1
plain	1	1	2
	2	2	0

   Treat the plaintext input as the fixed variable, and fill in the one-input function diagrams provided so that you have a complete description of the function.

   -bb-error = =

   -bb-error = =

   -bb-error = =

(b) Imagine that you are Eve, and you see a cyphertext that was encrypted and sent by Alice using the encryption function described above. The cyphertext is 2. Given this, one of the plaintexts is not possible. Which one is it?

6. Now we will use a rule to describe a cypher system and do the same kind of analysis as in the last problem. To make things less complicated, we are going to stick with schemes which are designed to encrypt a character from a very small alphabet. Imagine once again that we are going to encrypt one of three possible plaintexts: 0, 1, or 2. As in the Caesar cypher, we are going to pick a key that is also either 0, 1, or 2 and add it to the plaintext. However, in this system, we will do the addition (mod 4). Thus, $f(plain, key) = plain + key \pmod 4$.

   (a) Make a two-input function table for this encryption function.

		key		
		0	1	2
plain	0			
	1			
	2			

   (b) Using the same method as above, describe the function as a collection of one-input functions where the plaintext is fixed for each function.

-bb-error = =

-bb-error = =

-bb-error = =

   (c) Now imagine you are Eve, and you observe a cyphertext of 3. How does this limit the possible plaintexts that could have been encrypted?

7. Now consider the following table for an encryption function designed to be used for encrypting either a 0 or a 1.

		key			
		0	1	2	3
plain	0	1	1	1	0
	1	0	0	0	1

The corresponding one-input function obtained by holding the plaintext fixed as before is as follows:

-bb-error = =
-bb-error = =

(a) Imagine an experiment in which the key is chosen uniformly at random. Let A be the random variable that is the encryption of plaintext 0. Draw the probability distribution of A.

-bb-error = =

(b) Let B be the random variable that is the encryption function of the plaintext 1. Draw the probability distribution of B.

-bb-error = =

(c) Fill in the arrows in the following function diagrams so that you have the decryption function for thia encryption function.

-bb-error = =
-bb-error = =

(d) Imagine that you are Eve. Since you have no idea what plaintext Alice encrypted, your best guess given no other information would be that it is just as likely to have been a 1 as a 0. However, you could perform an experiment similar to the one described in part (a), trying all the possible key on the cyphertext to get the corresponding plaintext and obtaining a probability function for the plaintext.

i. Let the key be selected randomly according to a uniform distribution on {0,1,2,3}. Let A be the decryption of the cyphertext 0 using the random key. Draw the probability distribution of A.
-bb-error = =

ii. Let B be the decryption of the cyphertext 1. Draw the probability distribution of B.
-bb-error = =

(e) Still Eve, you now intercept a cyphertext encrypted with this cypher scheme, and sent by Alice. The cyphertext is 0. Which possible plaintext is your best guess for the true plaintext?

8. Consider the following table for a decryption function:

		key		
		0	1	2
plain	0	2	1	0
	1	0	1	2
	2	1	0	2
	3	2	0	1
	4	1	2	0
	5	0	2	1

   (a) Fill in the arrows in the following function diagrams to represent the above decryption function:

   -bb-error = =

   -bb-error = =

   -bb-error = =

   (b) Let the key be selected randomly according to a uniform distribution on {0,1,2}.

   i. Let A be the decryption of the cyphertext 0 using the random key. Draw the probability distribution of A.

   -bb-error = =

ii. Let B be the decryption of the cyphertext 1. Draw the probability distribution of B.

-bb-error = =

iii. Let C be the decryption of the cyphertext 2. Draw the probability distribution of C.

-bb-error = =