Cpt S 515 Homework #3

No late homework!

1. Let D be a device that keeps sending out messages. Each message contains two parts A and B where the intruder can not observe A but he can observe B. Suppose that each of A and B takes 10 bits so, each message is exactly 20 bits. Before the developers sell the device to the public (including the intruder), they run some experiments trying to make sure that there isn't any information leakage that is more than 1 bit from A to B in a message. The experiments are done by run the device for a long time and obtain a large and finite set C of messages. Please design a program that can estimate the average number of bits actually leaked from A to B in a message drawn from C.

2. Consider a C-function that has integer variables as arguments and integer as return type:

```
int myFunction(int x1, int x2, ..., int x7)
```

In the function with arguments `x1,x2,...,x7` which are integer variables, there are only 10 lines of code, where each line is in the form of an assignment `variable := Exp` to an integer variable where `Exp` is a linear combination of integer variables (e.g., `y:=2x1+3x2-5`) or an if-then-else statement where the condition is a comparison between two linear constraints on integer variables and the assignments in the if-then-else statement are in the form of `variable := Exp` shown above (e.g., `if (y>12x1-z) then x2:=3x7-15 else x5:=18x4-6x7+6`. The first line of the function declares three integer variable `x,y,z`, while the last line is to return the value `x` back. Please design a program that can verify whether there are values for `x1,x2,...,x7` passed to the function that can make the function return a negative integer.

3. Symbolic representation is way to code a finite object. BDD is a way to code a finite set. However, when a power set (a set of finite sets) is given, BDD is not usually efficient. Sometimes, it is a good idea to code an object as a number since a number itself is a string (e.g., 123 is the string "123"). We now consider a special case. Let $K = \{1, ..., k\}$ for some k, and consider P be a set of disjoint subsets of K. That is, $P = \{K_1, \cdots, K_m\}$ for some m and each $K_i \subseteq K$ and $K_i \cap K_j = \emptyset$ whenever $i \neq j$. I want to design an

algorithm, for a given K, to code (or transform or represent) each such P into a number C_P such that the code C is optimal; i.e.,

(1). C is 1-1,

(2). $C_P \in \{1, ..., B_K\}$,

where B_K is the number of all such P's for the given K.

4. (easy) Let G be a directed graph of 2048 nodes. When we use a Boolean formula to represent the G, how many Boolean variables are needed in the formula?

5. (easy) Data types are an abstraction of data and data structures are a way to store the types into memory. In particular, we never store physical objects in memory; in case when we really want to do it, we first represent the physical objects in an abstract representation and store the representation in memory. Here is a problem. There are 40 students in a classroom. I want to design a closet so that any one of the students can be hidden inside. Imagine that the closet is a chunk of computer memory. Then, how big (in bits) closet do you need?

Assignment 3

Sheryl Mathew

October 21, 2018

1. **Question 1**

Let A be the secret variable, B be the public variable.

Step 1: Sample the values of A and B as binary strings, whenever B changes.

Step 2: The sampled trace of (A,B) pairs called the (A,B) sequence is stored in AB-sequence

Step 3: Remove A from AB-sequence to get A-sequence and B from AB sequence to get B-sequence

Step 4: Using Lempel-Ziv we compress AB-sequence, A-sequence and B-sequence and get the compression rates C_{AB}, C_A, C_B respectively.

Step 5: The information rate for AB-sequence, A-sequence and B-sequence is $\frac{1}{C_{AB}} = I_{AB}, \frac{1}{C_A} = I_A, \frac{1}{C_B} = I_B$ respectively.

Step 6: We can calculate the information flow from A to B as $F(A, B) = I_A + I_B - I_{AB}$. This will determine the number of bits that have been transmitted from A to B. Ideally the value of F(A,B) should be 1 bit.

Source: Sampling Automata and Programs [QinLi, ZheDang]

2. **Question 2**

There are 10 lines of code. 2 lines of code is for initializing the variables x,y,z and returning the value x. The remaining 8 lines are linear equations where all the equations can be written in terms of x assuming a linear relationship. We add 2 variables α to all the equations.

$$x = x_1 + x_2 + \cdots + x_7 + \alpha$$

Using Linear programming with constraint x > 0 we try to find α for all the equations i.e. for the 8 lines of remaining code. If the minimum of the sum of all the $\alpha's$ = 0 then myFunction returns negative integer.

3. **Question 3**

Step 1: Let K = {1, 2, 3 ...k) for some arbitrary k and c is a counter variable i.e. c = 0

Step 2: Find the power set of K as PS which is the set of all subsets of *K*, including the empty set and *K* itself. Remove the last element out of PS and find its corresponding power set PSL. Find the union of PSL and PSL with each element union with the removed element. This will return a set A. Repeat till PS is empty

Step 3: Find all the disjoint power set of A. Remove the last element out of A and find its corresponding power set AL. Find the union of AL and AL with each element union with the removed element. But the union happens only if the intersection of the removed element and element in AL is a null set. Increment c by 1 for each set.

Step 4: For each unique set of disjoint subsets of K from step 4 (i.e., each P) is assigned a binary value starting from 1 to c.

4. **Question 4**

Number of variables needed to represent 2048 nodes

$2^x = 2048$

$2^x = 2^{11}$

$x = 11$

Number of boolean variables needed = $2 * x = 22$

5. **Question 5**

The memory required to store any one of the 40 students is at least 6 bits.

$$2^n = 40$$

If n = 5, $2^5 = 32$ i.e. with 5 bits we can represent only up to 32 unique binary numbers(students) but we need to represent 40 binary numbers(students).

But if n = 6, $2^6 = 64$ i.e. with 6 bits we can represent up to 64 unique binary numbers(students).