Jinyang Ruan

011696096

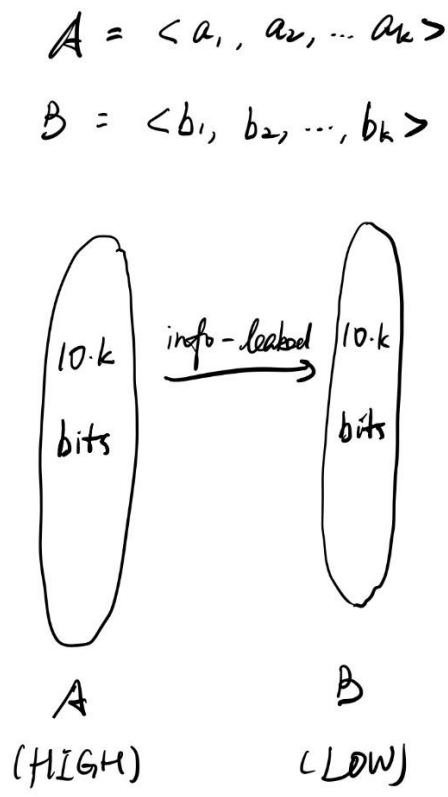
CPT_S 515 Advanced Algorithms HW#3

1. Step 1: Since the intruder cannot observe A but he can observe B, I define A is private variable and B is public variable. Information leaked from A to B. A and B are from one message, so A and B are dependent. Define in a message string C, there are two variables

$$A =< a_1, a_2, \dots a_k >$$

$$B =< b_1, b_2, \dots b_k >$$

Step 2: Draw a bipartite graph G for C with joint distribution $p(A, B)$.



Step 3: The k is a function of time t. In this case, the graph G can be expanding over the time. We can approximate the rate of info-leak .

$$\lambda_G = \limsup_{t\to\infty}(\frac{1}{t}\log_2\frac{N_{Left}\cdot N_{Right}}{E})$$

Step 4: A and B takes 10 bits, for each A, there is one and only one B corresponding to it. Then we get:

$$\lambda_G = \limsup_{t\to\infty}(\frac{1}{t}\log_2(100k))$$

Step 5: For the average of bits actually leaked from A to B, we calculate:

$$I(A;B) = 10 * \lambda_G$$

Ideally, the value of $I(A;B)$ should be less than 1 bit.

2. Step 1: Translate each statement into an integer linear constraint. If it is a linear combination of integer variables. For example,

$$x_1 := x_1 + x_2$$

$$=> x_1' := x_1 + x_2 \; and \; all \; other \; x_n's \; no \; change$$

If it is an if-then-else statement where the condition is a comparison between two linear constraints. I split it into two integer constraints. Then we repeat assigning new value to x_n.

Step 3: Change RHS to nonnegative. Move all elements in the right-hand side to left or multiply negative 1 to both sides.

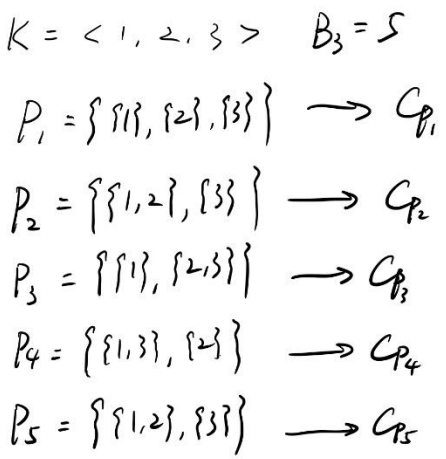
Step 4: Combine all statements in program into a big ILP instance. For each constraint, we add "artificial variables", $\alpha_1, \alpha_2, \ldots, \alpha_n$ and then we get that ILP instance. We want the value of $min\ x$.

Step 5: Observe that:

If the minimum of the $x < 0$, then the program returns negative integer.

Otherwise, the program dose not return negative integer.

3. Step 1: Since the Bell Number can count the possible partitions of a set, the number of set P's can be calculated by B_k. For example, if $K = \{1,2,3\}$, $k = 3$, $B_3 = 5$.



Step 2: We use a binary number n to represent a C_p. Since C is 1-1, we need at least $\lceil \log_2 B_k \rceil$ bits memory to store the total number of C_p.

For instance, if $k = 5$, $B_k = 15$, we need at least $\lceil \log_2 15 \rceil = 4$ bits.

Step 3: All C_p can be represented by a binary number which size is n bits.

4. Number of variables needed to represent 2048 nodes:

$$2^x = 2048 = 2^{11}$$

$$x = 11$$

Number of Boolean variables needed is:

$$N = 2 * x = 22$$

5. Consider one binary number can and only can represent one student, we need n bits to store all 40 students, and n should satisfy:

$$2^n \geq 40$$

$$n \geq 6 \ (n \ is \ a \ positive \ integer)$$

So, we need at least 6 bits to store all 40 students.