Andy Liang
CSE 150 - Foundations of Computer Science: Honors
Professor Bender

Homework 1B

Problem 4

Boolean algebra operations can be expressed as arithmetic operations mod 2. Let 1 be true, and 0 false.

(a) **Show that A $\wedge$ B = (A $\cdot$ B mod 2).**

(b) **What is $\neg A$?**

(c) **What is A $\vee$ B?**

Response

(a)

A	B	$A \vee B$
T	T	T
T	F	F
F	T	F
F	F	F

A	B	A $\cdot$ B	A $\cdot$ B mod 2
1	1	1	1
1	0	0	0
0	1	0	0
0	0	0	0

(b) $\neg A = (A + 1) \bmod 2$

A	$\neg A$
T	F
F	T

A	$A + 1$	$(A + 1) \bmod 2$
1	2	0
0	1	1

(c) $A \vee B = (((A + 1) \cdot (B + 1) + 1) \bmod 2)$

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

A	B	A + 1	B + 1	(A + 1) $\cdot$ (B+1)	(A + 1) $\cdot$ (B+1) + 1	((A+1) $\cdot$ (B+1) + 1) mod 2
1	1	2	2	4	5	1
1	0	2	1	2	3	1
0	1	1	2	2	3	1
0	0	1	1	1	2	0

Problem 5

Over lunch at the faculty club, n professors are expressing their concerns over their salaries. Each professor wants to know how his/her salary compares to the average salary of the group, but no professor wants to divulge any information about his/her salary to the other n - 1.

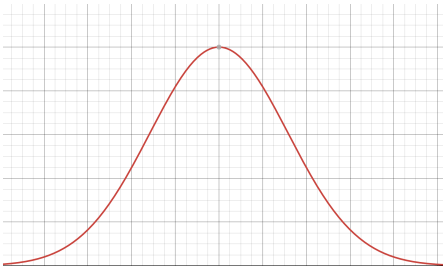
(a) **Devise a scheme that allows the professors to compute the average of their salaries, while preserving their privacy.**
You may assume that all the professors will adhere to the rules of the protocol, although they will try to extract as much information from the protocol as possible. You may also assume that it is public knowledge that the professors' salaries together don't exceed $1 trillion.

(b) **Now extend the protocol to be robust even when groups of professors collude. Specifically, if *i* professors collude, naturally they can learn the average salary of the remaining n - *i*. Your protocol should reveal no additional information.**

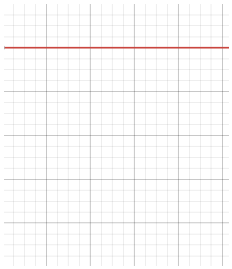
Response

(a) The professors agree on a number L that has a value much larger than one trillion. The first professor picks a random number between 0 and L-1 inclusive. The first professor adds his number to the agreed upon random number and then mods the sum by L. This ensures that the number that the second professor receives is also random, resulting in no information leakage. If the number were not to be modded after the first professor added his salary, the second professor would be able to gain information from his number. The expected value would be the first professor's salary. Modding causes the numbers to be uniformly distributed.

Before Modding:



After Modding:



The second professor adds his salary to the number, mods it by L, then gives it to then next professor until all n professors have added their salary and modded the result. After the first professor receives the number from the nth professor, he subtracts his random number then mods the result by L to get the total salary of all the professors. Dividing by the amount of professors in the room n results in the average salary of all the professors in the room without any information leakage.

$$\text{Total Salary} < 1 \text{ Trillion} \qquad 1 \text{ Trillion} < L \qquad 0 < \text{Random Number, R0} < L$$

Professor One Adds Salary to R then Mods by L:

$$(S_1 + R_0) \bmod L$$

Modding Ensures Uniform Distribution Resulting in Another Random Number:

$$[(S_1+R_0) \bmod L] = R_1$$

All n Professors Do the Same:
$[(S_2+R_1) \bmod L] = R_2$
$[(S_3+R_2) \bmod L] = R_3$
. . .
After All n Professors Added their Salary and Modded the Result:
R_n = (Total Salary of Professors + R_0) mod L
Total Salary of Professors = (R_n - R_0) mod L

Divide the Total Salary by n to get the Average Value:
Total Salary / n = Average Salary

(b) **Collaborated with Ivan Lin**

My Explanation

Similar to part a, the professors start by agreeing on a number L that has a value much larger than one trillion. The first professor picks a random number R_1 between 0 and L-1 inclusive. However, instead of the first professor adding his salary to the random number, he splits it into n smaller random numbers that add up to the initial random number r_1 to r_n. He then randomly picks a number between r_1 to r_n inclusive before distributing the rest to the other professors. After the other n-1 professors repeat the same process, each professor should have two random numbers: the random number they chose between 0 and L -1 (R_n) and the sum of all the random pieces they were given ($\sum_{i=1}^{n} r_i$). The first professor then adds either R_1 or $\sum_{i=1}^{n} r_i$ to his salary (for the sake of this explanation, I'll say he uses R_1)

Current Total = $S_1 + R_1$

Rather than telling the professor next to him, the first professor says his number aloud for all professors to hear. The next professor volunteers and then adds his salary (S_2) plus his random number (R_2) to the current total.

Current Total = $S_1 + R_1 + S_2 + R_2$

The remaining professors do the same resulting in:

Total = Total Professor Salaries ($\sum_{i=1}^{n} S_i$) + Total Random Numbers ($\sum_{i=1}^{n} R_i$)

To figure out the total professor salaries, the professors all subtract the sum of their random pieces ($\sum_{i=1}^{n} r_i$)

$$\sum_{i=1}^{n} R_i = \sum_{i=1}^{n} \sum_{i=1}^{n} r_i$$

Total Professor Salaries ($\sum_{i=1}^{n} S_i$) = Total - Total Random Pieces ($\sum_{i=1}^{n} \sum_{i=1}^{n} r_i$)

To find the average of their salaries, the professors divide their total by n.

Average Professor Salary = Total Professor Salaries / n

Ivan's Explanation Given n professors and a huge number L.

Each professor randomly chooses a random number R uniformly distributed from 0 to L.

Each professor then randomly distributes R into n components (divided randomly, not evenly) that add up to N, where each component is represented by r.

Every professor receives one of these components, and this is true for each professor, so each professor eventually has their salary, S, and the sum of the salary components from other professors, $\sum_{i=1}^{n} r_i$.

The professors each take $S + \sum_{i=1}^{n} r_i$ (the sum of their salary and the sum of the components they received) together.

Each takes that total modulo L (which obfuscates the expected value), and add them all together with that of other professors.

$\sum_{i=1}^{n}[(S_i + \sum_{j=1}^{n} r_{i,j})\%L] = \sum_{i=1}^{n}[(S_i + R_i)\%L]$.

The total is equal to the sum of all salaries and all individual components, which is also equal to the sum of all salaries and all the originally chosen random numbers.

Each professor than subtracts their original random number, R_i, from the total.

Note Alternatively, each professor add $(S + R)\%L$ (their salary and their original random number) to the total. Each professor then subtracts $\sum_{i=1}^{n} r_i$ (the sum of the components they receive) from the sum total.

Regardless of the method, $\sum_{i=1}^{n} R_i = \sum_{i=1}^{n} \sum_{j=1}^{n} r_{i,j}$. The total sum of the random numbers are equal to that of the random components. However, each individual professor's random number R and component sum $\sum_{i=1}^{n} r_i$ are different, so it is impossible to discern each professor's individual salary.

Once the random numbers have been subtracted and the difference has been found, the answer should first be taken modulo L. The output is then $\sum_{i=1}^{n} S_i$, which can be divided by n to find the average salary of the professors.