Ivan Lin
Dr. Michael Bender
CSE150 - Honors Foundations of Computer Science Fall 2016

Homework 1a

Problem 1 Write $P \implies Q$ using $\vee$ and $\sim$. Show that your two representations are equivalent.

$$(P \implies Q) \iff (\sim P \vee Q)$$

P	Q	$\sim P$	$P \implies Q$	$\sim P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Problem 2 Prove that the propositional formulas

$$P \vee Q \vee R$$

and

$$(P \wedge \sim Q) \vee (Q \wedge \sim R) \vee (R \wedge \sim P) \vee (P \wedge Q \wedge R)$$

are equivalent.

P	Q	R	$\sim P$	$\sim Q$	$\sim R$	$P \wedge \sim Q$	$Q \wedge \sim R$	$R \wedge \sim P$	$P \vee Q \vee R$
T	T	T	F	F	F	F	F	F	T
T	T	F	F	F	T	F	T	F	F
T	F	T	F	T	F	T	F	F	F
F	T	T	T	F	F	F	F	T	F
T	F	F	F	T	T	T	F	F	F
F	F	T	T	T	F	F	F	T	F
F	T	F	T	F	T	F	T	F	F
F	F	F	T	T	T	F	F	F	F

$(P \wedge \sim Q) \vee (Q \wedge \sim R) \vee (R \wedge \sim P) \vee (P \wedge Q \wedge R)$	$P \vee Q \vee R$
T	T
T	T
T	T
T	T
T	T
T	T
T	T
F	F

Problem 3 (a) Write the biconditional ($\Leftrightarrow$) using online implies ($\implies$) and and ($\wedge$). Prove that the new version is equivalent.

$$(P \Leftrightarrow Q) \iff (P \implies Q) \wedge (Q \implies P)$$

P	Q	$P \implies Q$	$Q \implies P$	$P(\implies Q) \wedge (Q \implies P)$	$P \Leftrightarrow Q$
T	T	T	T	T	T
T	F	F	F	F	F
F	T	T	T	F	F
F	F	T	T	T	T

(b) Write it using only $\vee$ and $\sim$. Show your derivation.

$$(P \Leftrightarrow Q) \iff (P \implies Q) \wedge (Q \implies P)$$
$$\text{given } A \iff \sim (P \implies Q), B \iff \sim (Q \implies P)$$
$$(P \implies Q) \wedge (Q \implies P) \iff (\sim A \wedge \sim B)$$
$$(\sim A \wedge \sim B) \iff \sim (A \vee B) \text{ by De Morgan's Laws}$$
$$\sim (A \vee B) \iff \sim (\sim (P \implies Q) \vee \sim (Q \implies P))$$
$$\text{since } (P \implies Q) \iff (\sim P \vee Q)$$
$$\sim (\sim (P \implies Q) \vee \sim (Q \implies P)) \iff \sim (\sim (\sim P \vee Q) \vee \sim (\sim Q \vee P))$$

Homework 1b

Problem 4 Boolean algebra operations can be expressed as arithmetic operations mod 2. Let 1 represent be true and 0 false.

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

A	B	$A \wedge B$	$(A \cdot B)\%2$
T=1	T=1	T	1=T
T=1	F=0	F	0=F
F=0	T=1	F	0=F
F=0	F=0	F	0=F

(b) What is $\sim A$?

$\sim A = (A + 1)\%2$

(c) What is $A \vee B\%$ (Use De Morgan's Laws.)

$$\text{let } P \iff \sim A, Q \iff \sim B$$
$$(A \vee B) \iff (\sim P \vee \sim Q)$$
$$(\sim P \vee \sim Q) \iff \sim (P \wedge Q) \text{ by De Morgan's Laws}$$
$$\text{replace } P, Q$$
$$\sim (P \wedge Q) \iff \sim (\sim A \wedge \sim B)$$

Problem 5 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.

The professors form a closed chain of professors. The first professor chooses a random number, R from a uniform distribution between 0 and L, where L is a huge number that is greater than the sum of the all their salaries could reasonably be.

The first professor then adds their salary, S_1 to the random number. They then take the total modulo L and pass the result to the next professor. As a result, the theoretical expected value the next professor receives is no longer $S_1 + L/2$, since the modulus changes the expected value. Each professor in the chain then adds their salary to the number, modulo by L and pass it on. When the last professor finishes, they pass the result $((R + \sum_{i=1}^{n} S_i) \mod L)$ back to the first professor.

The first professor simply has to subtract R from the sum total and modulo the result by L to obtain the sum total of all salaries. This works because L is so large, the sum of the salaries and the random number will never be more than $2L$.The professor divides the total by n to determine the average salary of the n professors.

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

See next page for answer

Solution developed in collaboration with Andy Liang
Here is an explanation written up by me

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.

Here is an explanation written up by Andy (for documentation purposes)

Collaborated with Ivan Lin

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) and mods it by L to maintain a uniform distribution.

$$\text{Current Total} = (S_1 + R_1) \bmod L$$

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) modded by L to the current total.

$$\text{Current Total} = (S_1 + R_1 + S_2 + R_2) \bmod L$$

The remaining professors do the same resulting in:

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

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

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

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

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

$$\text{Average Professor Salary} = \text{Total Professor Salaries} \ / \ n$$