Michael A. Bender

CSE 150 – Honors Foundations of Computer Science – Fall 2016

Homework 1

You should hand in your problem set *online* using blackboard. Write your solutions using latex. *No late problem sets accepted.*

Part A

Problem 1

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

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.

Problem 3

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

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

Part B

Problem 4

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

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

(b) What is $\sim A$?

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

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, naturally they can learn the average salary of the remaining $n - i$. Your protocol should reveal no additional information.