IS 2935/TEL 2810 Introduction to Computer Security

Homework 1

Due Date: By Midnight September 10, 2004

1. **[30 Points]** Do the following problems from Chapter 1, Section 1.12: **1, 4, 7**

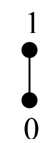
2. **[50 Points]** ***Exercise on Propositional/Predicate logic & Induction***

    1. Show that $\mathbf{p \rightarrow q}$ is equivalent to $\mathbf{(\neg p) \vee q}$ using truth table.
    2. Do the following from Exercise 34.4 (page 956-957): **2(a), 2(b), 3, 4(a), 4(b)**

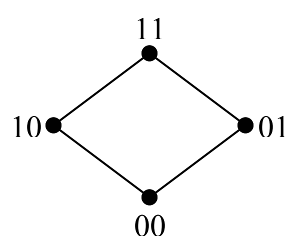
3. **[20 Points]** ***Exercise on Lattice***

    Let S_n denote a set of all binary numbers containing n digits. For $a \in S_n$, we can write $a = a_1 a_2 ..... a_n$ where a_is are binary digits. Let relation $\lesssim$ be the "*dominance*" relation on S_n. For every $a, b \in S_n$ we say a is *dominated* by b (written as $a \lesssim b$) if $a_i \leq b_i$ for all $i = 1$ to n (here $\leq$ is the "*less than or equal to*" relation on binary digits, i.e., $0 \leq 0$, $0 \leq 1$, $1 \leq 1$)

    For example $S_1 = \{0, 1\}$; Here $0 \lesssim 1$. As a lattice diagram, it can be represented as



    Similarly, $S_2 = \{00, 01, 10, 11\}$ (set of all binary numbers containing 2 digits). The lattice formed by $\lesssim$ over S_3 can be represented as



    Does relation $\lesssim$ over S_3 form a *total* ordering or *partial* ordering? Represent the ordering diagrammatically (as above and as was done in class).