CPSC 121: Models of Computation
Assignment #4

Due: Friday, November 14, 2014 at 17:00 **Total Marks: 36**

Submission Instructions-- read carefully

All assignments should be done in groups of 2. It is very important to work with another student and exchange ideas. **Each group should submit ONE assignment**. Type or write your assignment on clean sheets of paper with question numbers prominently labelled. Answers that are difficult to read or locate may lose marks. We recommend working problems on a draft copy then writing a separate final copy to submit.

Your submission must be **STAPLED** and include the **CPSC 121 assignment cover page** – located at the Assignments section of the course web page. Additionally, include your names at the top of each page. We are not responsible for lost pages from unstapled submissions.

Submit your assignment to the appropriately marked box in room **ICCS X235** by the due date and time listed above. **Late submissions are not accepted**.

Note: the number of marks allocated to a question appears in square brackets after the question number.

A Note on the Marking Scheme

Most items (i.e., question or, for questions divided into parts, part of a question) will be worth 3 marks with the following general marking scheme:

- **3 marks:** correct, complete, legible solution.
- **2 marks**: legible solution contains some errors or is not quite complete but shows a clear grasp of how the concepts and techniques required apply to this problem.
- **1 mark**: legible solution contains errors or is not complete but shows a clear grasp of the concepts and techniques required, although not their application to this problem or the solution is somewhat difficult to read but otherwise correct.
- **0 marks**: the solution contains substantial errors, is far from complete, does not show a clear grasp of the concepts and techniques required, or is illegible.

This marking scheme reflects our intent for you to learn the key concepts and techniques underlying computation, determine where they apply, and apply them correctly to interesting problems. It also reflects a practical fact: we have insufficient time to decipher illegible answers. At the instructor's discretion, some items may be marked on a different scale. TAs may very occasionally award a bonus mark for exceptional answers.

Question 1 [6]

Consider the following theorem:

Every odd positive integer can be written as the difference of two perfect squares.

[A number m is a perfect square, if m = k^2, for some number k.]

a. Translate this theorem into predicate logic. You may use predicates *Odd(x)* and *Even(x)* to indicate odd and even numbers,
b. Prove the theorem using a direct proof (that is, you must not use proof by contradiction, or any logical equivalences on the original theorem statement)

Question 2 [6]

Consider the following theorem:

For all integers a, b and c, if a does not divide (b – c) then a does not divide b or a does not divide c.

a. Translate this theorem into predicate logic. You may use the following predicate *Divides(x, y)* : x divides y
b. Prove the theorem using an ***indirect*** proof (that is, you must use either proof by contradiction, or prove a statement that is logically equivalences to the original theorem statement).

Question 3 [6]

Provide a proof by contrapositive that is as complete as possible for the following statement.

$$\forall x \in S, (P(x) \vee Q(x, x)) \rightarrow \exists y \in S, \exists z \in S, y \neq z \wedge Q(x, y) \wedge Q(z, z)$$

As you can see, the predicates in this statement are not defined. Therefore you cannot complete the proof, but you should provide clear steps to show the structure of your proof and complete as much of the proof as it is possible. Check the example at the end of this document.

Question 4 [6]

In an effort to resolve a labour dispute like the recent teachers strike in BC, negotiators from different groups got together to talk to each other with the hope that they will find a solution. Use a **proof by contradiction** to show that

If every participant has talked to at least one other participant, then two of the participants talked to exactly the same number of people.

You don't need to write the statement in logic, but make it clear which are your premises and which is the conclusion in your proof. For convenience, you can use

- **P** to denote the group of people participating in the talks, and
- **t(p)** = the number of people to whom person p has talked (this is a function not a predicate)

Question 5 [6]

Prove that

if $f(n) = 3^n$ then f is not in $O(2^n)$, i,e, f is not in *big-O of* 2^n .

Recall that a function g is in O(h) if

$$\exists c \in \mathbf{R}^+, \exists m \in \mathbf{N}, \forall n \in \mathbf{N},\ n \geq m \rightarrow g(n) \leq c\, h(n)$$

First express the statement in Predicate Logic. Then Prove the statement. A direct proof would work well here. *Hint:* the inside back cover of your textbook contains a list of properties of exponents and logarithms. A web search for "logarithm reference" will also turn up many alternative resources.

Question 6 [6]

Let Σ = {A, C, G, T}. You may think of these as DNA tags (but it is irrelevant to the solution). Design a DFA that accepts exactly the strings that start with either A or T, and end with a character different from the one they started from. For instance, your DFA should accept the strings "ACCGGTAC" and "TCGCCAATA" but not the strings "CGAAGTCA" or "AGGCCAAACGCA".

Example of Abstract Proof (DO NOT HAND IN)

Provide a "direct" proof—no proof by contradiction, no use of logical equivalences—that is as complete as possible for the following statement.

$$\exists p \in A,\ \forall x \in S,\ B(x) \rightarrow \exists q \in A,\ p \neq q \wedge R(p, x) \wedge (\sim R(q, x) \vee G(p, q))$$

As you can see, the predicates in this statement are not defined. Therefore you cannot complete the proof, but you should provide clear steps to show the structure of your proof and complete as much of the proof as it is possible. Check the example at the end of this document.

SOLUTION:

There are other approaches that make sense. This is one option.

- Let p be …… (some element in domain A).
- WLOG, let x be any arbitrary element of S.
- Assume B(x) is true.
- Choose a q from the domain A that is not equal to p. Note that we can base the choice of q on x.
- Show that R(p, x) is true and that either R(q, x) is false or G(p, q) is true.