CPSC 121 Midterm 1
Tuesday, October 11th, 2011

Name: ______________________ Student ID: ______________________
Signature: ______________________
Your signature acknowledges your understanding of and agreement to the rules below.

Question	Marks
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
Total	

- You have 110 minutes to write the 14 questions on this examination. A total of 100 marks are available.
- You may have as an aide up to 3 textbooks and a 3 inch stack of paper notes and nothing else. **No electronic devices allowed**; so, no cell phones and no calculators.
- Keep your answers short. If you run out of space for a question, you have likely written too much.
- The number in square brackets to the left of the question number indicates the number of marks allocated for that question. Use these to help you plan your use of time on the exam.
- Clearly indicate your answer to each problem. If your answer is not in the provided blank, then indicate where the answer is, and at the answer's location indicate the question it addresses.
- **Good luck!**

UNIVERSITY REGULATIONS:

- Each candidate should be prepared to produce, upon request, his/her UBC card.
- No candidate shall be permitted to enter the examination room after the expiration of one half hour, or to leave during the first half hour of the examination.
- CAUTION: candidates guilty of any of the following, or similar, dishonest practices shall be immediately dismissed from the examination and shall be liable to disciplinary action.
  1. Having at the place of writing, or making use of, any books, papers or memoranda, electronic equipment, or other memory aid or communication devices, other than those authorised by the examiners.
  2. Speaking or communicating with other candidates.
  3. Purposely exposing written papers to the view of other candidates. The plea of accident or forgetfulness shall not be received.
- Candidates must not destroy or mutilate any examination material; must hand in all examination papers; and must not take any examination material from the examination room without permission of the invigilator.

This page left intentionally (almost) blank.

If you write answers here (or anywhere other than their intended location), mark them clearly, indicate which question they respond to, and indicate at the provided solution blank for that question where you wrote your solution.

[1] 1. Do you want tutorial attendance to be mandatory for you? If you answer "yes", then 1% of your course grade will be calculated with $min(100\%, \frac{\text{tuts attended}}{\text{tut weeks}-2})$. If you answer "no", then online quizzes will be worth 5% of your course grade rather than 4%. Either way, you get credit for this problem.

Circle one: YES NO

[4] 2. Building combinational circuitry, without a story:

[2] a. Write a propositional logic expression that corresponds to the following truth table.

x	y	z	p
F	F	F	F
F	F	T	T
F	T	F	F
F	T	T	F
T	F	F	F
T	F	T	F
T	T	F	F
T	T	T	T

Expression:

[2] b. Given the following propositional logic expression, write the directly corresponding circuit: $(\sim a \wedge z) \vee \sim(b \vee c \vee z)$. Label the output *out*. Do not simplify.

[3] 3. **Complete the following truth table** for the logical expression $p \wedge (h \rightarrow \sim s)$, and **then answer the question below**.

p	s	h	$p \wedge (h \rightarrow \sim s)$
F	F	F	
F	F	T	
F	T	F	
F	T	T	
T	F	F	
T	F	T	
T	T	F	
T	T	T	

Is $p \wedge (h \rightarrow \sim s)$ a tautology, contradiction, or contingency?

Circle one: TAUTOLOGY CONTRADICTION CONTINGENCY

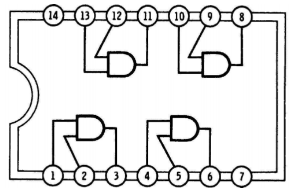
[4] 4. Let s mean "your data is secure", p mean "your password is strong", and h mean "you hid your password under your keyboard".

[2] a. Translate the following from propositional logic into English: $(p \wedge s) \vee h$

[2] b. Translate the following English statement into propositional logic. You need not translate the sentence in parentheses; it's only there to clarify the meaning of the English statement.

> If your password is weak or hidden under your keyboard, then your data is not secure. (But a strong password and not hiding your password under your keyboard don't guarantee that your data is secure.)

[3] 5. Every practical technology for implementing digital logic has its own limitations and peculiarities that propositional logic fails to model. Consider the following chip diagram from the Magic Box Manual:



Give a shortcoming of propositional logic as a model of how difficult it is to wire a circuit using this type of chip for $(p \wedge q \wedge r \wedge s \wedge t)$ as compared to using it for $(p \wedge q \wedge r \wedge s \wedge t \wedge u)$.

[7] 6. This problem focuses on the equivalence:

$$({\sim}p \vee s) \wedge (p \rightarrow (s \rightarrow {\sim}p)) \equiv {\sim}p$$

[6] a. Prove this equivalence. Use a formal logical equivalence proof, and start your proof from the left-hand side of the equivalence.

[1] b. Is it possible to prove the equivalence starting from the right-hand side?

(a) Yes, and it would likely have been easier.

(b) Yes, but it's often harder to work from the simple side to the complex side.

(c) No, because a proof in that direction would not prove the logical equivalence.

(d) No, because there's no sequence of steps we can follow in that direction.

[6] 7. Answer the following questions related to representing numbers.

[1] a. Convert the 5-bit unsigned binary number 01010 to a decimal number.

[1] b. Convert 01001011 to hexadecimal.

[1] c. Convert the 5-bit signed binary number 11010 to a decimal number.

[1] d. Convert -9 to a 5-bit signed binary number.

[1] e. Convert 4 to a 5-bit signed binary number.

[1] f. Add the 5-bit binary numbers 00101 and 10100 **or** explain why it is not possible to add them without knowing whether to interpret them as signed numbers or unsigned numbers.

[14] 8. Recall "Binary coded decimal" (BCD) from the assignment:

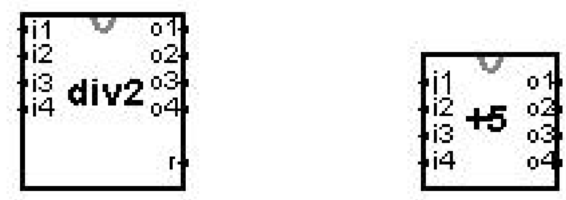
> BCD represents k decimal digits using $4k$ bits in groups of 4. Each group of 4 represents a single digit (0–9). So, for example, 59 would be 01011001 in BCD, a 5 (0101) followed by a 9 (1001).

[7] a. Design the logic statements for a circuit that adds 5 to a 1-digit (4-bit) BCD number $i_1 i_2 i_3 i_4$. **Assume the input value is** 4 **or less**; so, the output is 9 or less.
The rightmost bit of the output $o_4 = {\sim} i_4$. The second bit from the left
$o_2 = ({\sim} i_2 \wedge {\sim} i_3 \wedge {\sim} i_4) \vee ({\sim} i_2 \wedge {\sim} i_3 \ \wedge \ i_4) \vee ({\sim} i_2 \ \wedge \ i_3 \wedge {\sim} i_4)$.
Give one statement for each of the other two bits of output o_1 **and** o_3**.**

[7] b. Design a circuit that takes a 2-digit (8-bit) BCD number $c_{11}c_{12}c_{13}c_{14}\ c_{21}c_{22}c_{23}c_{24}$ as input and produces a 2-digit (8-bit) BCD number $d_{11}d_{12}d_{13}d_{14}\ d_{21}d_{22}d_{23}d_{24}$ as output, which is the input divided by 2. Drop the remainder; for example, the input 25 produces the output 12.

In your solution you can (and should) use your circuit from the previous part plus a new one that inputs a 1-digit BCD number and outputs: (1) the result of dividing it by 2 and (2) a remainder r that is 1 when the input is odd and 0 otherwise. Assume both circuits work correctly, and represent them with the following two chip symbols:

The circuits from part a (left) and b (right) as chips:



Hint: solve $\frac{28}{2}$ by hand—the easier version—and compare to solving $\frac{38}{2}$ by hand—the harder version. When did you divide digit(s) by 2 or add 5 (or maybe add 10 and then divide by 5)? If you have to choose between two operations depending on which version of the input you have, what circuit element can help?

Notes: for any multiplexer you use, indicate which of its inputs is the "0" input; use but **do not** implement (draw the "gates inside") either the `div2` or `+5` circuits here.

[6] 9. For each of the following, apply the indicated rule to create an equivalent statement. (In some cases, you may also need to apply commutativity, associativity, or double negation. You need not write out these steps but should apply them if necessary to make the named rule apply.)

[2] a. Apply distributivity to $(p \wedge q) \vee (\sim r \wedge q)$.

[2] b. Apply De Morgan's to $\sim p \wedge r$.

[2] c. Apply absorption to $(p \vee q \vee r) \wedge (p \vee r) \wedge (r \vee \sim s)$.

[12] 10. For each of the following, apply the indicated rule to create a statement that follows from the given statements **or** indicate that the rule does not apply. (In some cases, you may also need to apply commutativity, associativity, or double negation. You need not write out these steps.)

[3] a. Apply modus ponens to $a \rightarrow (b \wedge c)$ and a.
Write your answer or circle "does not apply": DOES NOT APPLY

[3] b. Apply specialization to $(p \wedge q) \rightarrow r$.
Write your answer or circle "does not apply": DOES NOT APPLY

[3] c. Apply proof by cases to $(a \vee b) \rightarrow \sim c$ and $d \rightarrow \sim c$.
Write your answer or circle "does not apply": DOES NOT APPLY

[3] d. Apply generalization to $p \rightarrow q$.
Write your answer or circle "does not apply": DOES NOT APPLY

[4] 11. Base64 is a scheme for encoding binary data using normal text, such as storing data in XML files (a text file format often used for web applications). In Base64, 64 characters—like the letters a–z, A–Z, 0–9, +, and /—represent the numbers 0–63. For example, the bit pattern 010010010110000101101111 might be represented by the characters "SWFv".

[2] a. Why choose 64 characters rather than using just the "standard" 62 characters a–z, A–Z, and 0–9?

[2] b. Is there any data that can be encoded in normal binary that **cannot** be encoded as Base64 data? Briefly justify your answer.

[6] 12. Consider the predicates $\text{Odd}(x)$ meaning "x is an odd integer" and $\text{Prime}(x)$ meaning "x is a prime integer" and the set of positive integers $\mathbf{Z}^+$. For each statement below, indicate whether the answer is true or false.

[2] a. $\forall x \in \mathbf{Z}^+, \text{Prime}(x) \vee \text{Odd}(x)$
Circle one: TRUE FALSE

[2] b. $\exists x \in \mathbf{Z}^+, \sim\text{Odd}(x) \wedge \text{Prime}(x/2)$
Circle one: TRUE FALSE

[2] c. $\exists x \in \mathbf{Z}^+, (\sim\text{Odd}(x) \wedge x > 2) \rightarrow \text{Prime}(x)$
Circle one: TRUE FALSE

[15] 13. [5] a. Prove using logical equivalences that $p \to (q \to p)$ is a tautology.

[8] b. Prove b using a formal propositional logic proof given the five numbered premises below:

1. $(\sim p \vee q) \to p$	premise
2. $\sim r \to \sim p$	premise
3. $\sim(r \wedge \sim a)$	premise
4. $(\sim a \vee b)$	premise
5. $(q \vee s) \to t$	premise

[2] c. Assuming your proofs are correct, what do they establish? **Circle all that apply.**

(a) That $p \to (q \to p)$ is true.
(b) That $p \to (q \to p)$ is false.
(c) That b is true.
(d) That b is false.
(e) None of these.

[15] 14. A "secure hash algorithm" takes a number as input and produces another number as output. Among other things, secure hash algorithms are used for storing passwords.

In this problem, all numbers are non-negative integers (from $\mathbf{Z}^0$), and all people are from the set P. The predicate SHA(x, y) means "the output of the secure hash algorithm run on x is y", and Knows(p, y) means "person p knows an input to the secure hash algorithm that produces y as an output".

[5] a. Using the predicates above, write the statement "for each input to the secure hash algorithm, there is exactly one unique output" in predicate logic. As always, feel free to define and use helper predicates.

[5] b. The SHA algorithm outputs a 256-bit number. Using the predicates above, write the statement "no output of the secure hash algorithm is too large to fit in an unsigned 256-bit number" in predicate logic. Use exponentiation (write a^b to mean "a raised to the power of b") and relational operators ($<$, $\leq$, $=$, $\geq$, and $>$) if you need them.

[5] c. Define a new predicate Secure(p, x) in terms of the predicates above that means "no one other than p knows any input that produces the result of running the secure hash algorithm on x".

Secure$(p, x) \equiv$

This page left intentionally (almost) blank.

If you write answers here (or anywhere other than their intended location), mark them clearly, indicate which question they respond to, and indicate at the provided solution blank for that question where you wrote your solution.

This page left intentionally (almost) blank.

If you write answers here (or anywhere other than their intended location), mark them clearly, indicate which question they respond to, and indicate at the provided solution blank for that question where you wrote your solution.

This page left intentionally (almost) blank.

If you write answers here (or anywhere other than their intended location), mark them clearly, indicate which question they respond to, and indicate at the provided solution blank for that question where you wrote your solution.