University of Ottawa
CSI 2101 – Midterm Test
Instructor: Lucia Moura

February 9, 2010
11:30 pm
Duration: 1:50 hs

Closed book, no calculators

Last name: ____________________

First name: ____________________

Student number: ____________________

There are 5 questions and 100 marks total.

This exam paper should have 12 pages,
including this cover page.

1 – Propositional logic	/ 10
2 – Predicate logic	/ 24
3 – Inference rules	/ 20
4 – Proof Methods	/ 20
5 – Number Theory	/ 26
Total	/ 100

1 Propositional logic — 10 points

Part A — 5 points

Show that the compound proposition below is a **contradiction**:

$$(p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)$$

Via truth tables:

p	q	$p \vee q$	$\neg p \vee q$	$p \vee \neg q$	$\neg p \vee \neg q$	result
T	T	T	T	T	**F**	F
T	F	T	**F**	T	T	F
F	T	T	T	**F**	T	F
F	F	**F**	T	T	T	F

Via equivalences:

$$\begin{aligned}
& (p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q) \\
\equiv\ & ((p \wedge \neg p) \vee q) \wedge ((p \wedge \neg p) \vee \neg q) \\
\equiv\ & (F \vee q) \wedge (F \vee \neg q) \\
\equiv\ & q \wedge \neg q \\
\equiv\ & F
\end{aligned}$$

Part B — 5 points

You go to your digital circuit lab to implement a boolean function represented by the following compound proposition: $(p \wedge q) \vee (\neg q \wedge p) \vee (r \wedge p) \vee (q \wedge r)$.

However, you realise that you only have 2 AND-gates (binary) and 2 OR-gates (binary) in your knapsack.

Give a circuit that implements the boolean function and uses only the gates available in your knapsack. Indeed, you will get a bonus 2 points if you use only 2 gates in total.

$$\begin{aligned}
& (p \wedge q) \vee (\neg q \wedge p) \vee (r \wedge p) \vee (q \wedge r) \\
\equiv\ & (p \wedge (q \vee \neg q)) \vee (r \wedge p) \vee (q \wedge r) \\
\equiv\ & (p \wedge T) \vee (r \wedge p) \vee (q \wedge r) \\
\equiv\ & p \vee (r \wedge p) \vee (q \wedge r)
\end{aligned}$$

The above solution is acceptable, but for bonus marks, can be simplified further to:

$$\begin{aligned}
& p \vee (r \wedge p) \vee (q \wedge r) \\
\equiv\ & (p \wedge T) \vee (p \wedge r) \vee (q \wedge r) \\
\equiv\ & (p \wedge (r \vee T)) \vee (q \wedge r) \\
\equiv\ & (p \wedge T) \vee (q \wedge r) \\
\equiv\ & p \vee (q \wedge r)
\end{aligned}$$

Note that the drawing of the circuit is not included here but was expected in your solution.

2 Predicate logic — 24 points

Part A — 12 points

Circle true or false

1. $\forall x \exists y (x^2 = y)$, where the domain is the set of real numbers.	**[true]** [false]
2. $\exists x \forall y ((y \neq 0) \rightarrow (xy = 1)$, where the domain is the set of real numbers.	[true] **[false]**
3. The following are logically equivalent: $\neg(p \wedge \neg q)$ and $(p \rightarrow q)$	**[true]** [false]
4. The following are logically equivalent: $\forall x \neg Q(x)$ and $\neg \exists x \neg Q(x)$	[true] **[false]**
5. $\exists x P(x) \wedge \forall x \neg Q(x)$ logically implies $\exists x (P(x) \vee Q(x))$	**[true]** [false]
6. Consider the domain of discourse to be the set $\{1, 2, 3\}$, and $Q(x, y) =$"$y \geq x$", and $R(y) =$"y is odd". Then $\forall y ((\forall x Q(x, y)) \rightarrow R(y))$ is true.	**[true]** [false]

Justification not required, but given here for your understanding:

1. $\forall x$, take $y = x^2$.
2. Obviously wrong. For example, if $y = 2$, then the only x satisfying $xy = 1$ is $x = \frac{1}{2}$. If $y = 3$, however, the only x satisfying $xy = 1$ is $x = \frac{1}{3}$. Thus, there is no one x for all y.
3. $\neg(p \wedge \neg q) \equiv (\neg p \vee q) \equiv (p \rightarrow q)$.
4. $\forall x \neg Q(x) \equiv \neg\neg\forall \neg Q(x) \equiv \neg \exists x Q(x) \not\equiv \neg \exists x \neg Q(x)$.
5. $\exists x P(x) \wedge \forall x \neg Q(x)$ implies $\exists x P(x)$, which implies $\exists x (P(x) \vee Q(x))$.
6. $\forall x Q(x, y)$ is only satisfied for $y = 3$, and $R(3)$ is true, so the predicate holds.

... continued

Part B — 12 points

Consider the following statements:
$B(x)$: "x is a baby"
$L(x)$: "x is logical"
$M(x)$ "x is able to manage a crocodile"
$D(x)$: "x is despised"

Suppose the domain consists of all people.

B1 Express each of the following statements using quantifiers, logical connectives and the propositional functions given above.

	phrase in English	logical statement
1.	Babies are illogical.	$\forall x(B(x) \to \neg L(x))$
2.	Nobody despised who can manage a crocodile.	$\neg\exists x(D(x) \wedge M(x)) \equiv \forall x(D(x) \to \neg M(x))$
3.	Illogical persons are despised.	$\forall x(\neg L(x) \to D(x))$
4.	Babies cannot manage crocodiles.	$\forall x(B(x) \to \neg M(x))$

B2 Does 4. follows from 1., 2., 3. ?

If yes, justify your argument.

If no, explain why it doesn't.

Using 1, 2, 3 by universal instantiation, for an arbitrary a:

1. $B(a) \to \neg L(a)$
2. $D(a) \to \neg M(a)$
3. $\neg L(a) \to D(a)$

Applying the transitivity of $\to$ on 1 and 3, we get $B(a) \to D(a)$. Applying transitivity again on this and 2, we get $B(a) \to \neg M(a)$. Since the choice of a was arbitrary, we have that:

$$\forall x(B(x) \to \neg M(x)).$$

... continued

3 Inference rules — 20 points

Part A — 10 points Using inference rules, show that the hypotheses:

- If a student likes chocolate then he/she answers the questions.
- If a student doesn't like chocolate then he/she is not motivated to go to class.
- If a student is not motivated to go to class then he/she fails the course.

lead to the conclusion:

- If a student doesn't like chocolate then he/she fails the course.

Define the following:

l :	student likes chocolate
a :	student answers the question
m :	student is motivated to go to class
f :	student fails the course

We translate the hypotheses and conclusion into propositions as follows:

1. $l \rightarrow a$
2. $\neg l \rightarrow \neg m$
3. $\neg m \rightarrow f$
4. $\neg l \rightarrow f$

Formal argument:

1.	$\neg l \rightarrow \neg m$	hypothesis
2.	$\neg m \rightarrow f$	hypothesis
3.	$\neg l \rightarrow f$	hypothetical syllogism of 1, 2

... continued

Part B — 10 points Justify the rule of **universal transitivity**, which states that if $\forall x(P(x) \to Q(x))$ and $\forall x(Q(x) \to R(x))$ are true then $\forall x(P(x) \to R(x))$ is true, where the domain of all quantifiers is the same.

	Step	Justification
1.	$\forall x(P(x) \to Q(x))$	hypothesis
2.	$P(a) \to Q(a)$	universal instantiation for arbitrary a
3.	$\forall x(Q(x) \to R(x))$	hypothesis
4.	$Q(a) \to R(a)$	universal instantiation for arbitrary a
5.	$P(a) \to R(a)$	hypothetical syllogism for 2, 4
6.	$\forall x(P(x) \to R(x))$	universal generalization

... continued

4 Proof Methods — 20 points

For this question you will need the definitions of odd and even, seen in class.

DEFINITION: An integer n is **even** if there exists an integer k such that $n = 2k$.
An integer n is **odd** if there exists an integer k such that $n = 2k + 1$.

Part A — 10 points Prove that if $m+n$ and $n+p$ are even numbers, then $m+p$ is even.

Let m, n, p be integers such that $m+n$ is even and $n+p$ is even. By definition of odd, there exist k and k' such that $m + n = 2k$ and $n + p = 2k'$. Thus, $m = 2k - n$ and $p = 2k' - n$. This gives:

$$\begin{aligned} m + p &= (2k - n) + (2k' - n) \\ &= 2k - n + 2k' - n \\ &= 2(k + k' - n) \end{aligned}$$

Therefore $m + p$ is even.

Part B — 10 points Prove the following:

For any integer number n, if $n^2 + 5$ is odd then n is even.

using

B1 (5 points) a proof by contraposition.

B2 (5 points) a proof by contradiction.

B1. Assume n is odd, and show $n^2 + 5$ is even.

Let n be an even number. Thus, $n = 2k + 1$ for some integer k. Then:

$$\begin{aligned} n^2 + 5 &= (2k+1)^2 + 5 \\ &= 4k^2 + 4k + 1 + 5 \\ &= 4k^2 + 4k + 6 \\ &= 2(2k^2 + 2k + 3) \end{aligned}$$

Thus, $n^2 + 5$ is even.

B2. Assume $n^2 + 5$ is odd and n is odd and reach a contradiction.

Let n be an odd number such that $n^2 + 5$ is odd. Thus, there exist k, k' such that $n = 2k + 1$ and $n^2 + 5 = 2k' + 1$. Thus, $n^2 + 5 = (2k + 1)^2 + 5 = 2k' + 1$, so $4k^2 + 4k + 6 = 2k' + 1$, i.e. $5 = 2k' - 4k^2 - 4k = 2(k' - 4k^2 - 4k)$. This implies that 5 is an even number, which is a contradiction.

... continued

5 Number Theory — 26 points

Part A — 6 points Find **counterexamples** to each of these statements about congruences:

A1 Let a, b, c, and m be integers with $m \geq 2$.
If $ac \equiv bc$ (mod m), then $a \equiv b$ (mod m).

Counterexample:

Take $a = 1$, $b = 2$, $c = 0$, $m = 3$. Then:

$$\begin{array}{ll} ac \equiv bc \ (\text{mod m}): & 1 \cdot 0 \equiv 2 \cdot 0 \ (\text{mod } 3) \\ a \not\equiv b \ (\text{mod m}): & 1 \not\equiv 2 \ (\text{mod } 3) \end{array}$$

A2 Let a, b, c, d and m be integers with c and d positive and $m \geq 2$.
If $a \equiv b$ (mod m) and $c \equiv d$ (mod m), then $a^c \equiv b^d$ (mod m).

Counterexample:

Take $a = 2$, $b = 5$, $c = 4$, $d = 1$, $m = 3$. Then:

$$\begin{array}{ll} a \equiv b \ (\text{mod m}): & 2 \equiv 5 \ (\text{mod } 3) \\ c \equiv d \ (\text{mod m}): & 4 \equiv 1 \ (\text{mod } 3) \\ a^c \not\equiv b^d \ (\text{mod m}): & 2^4 = 16 \not\equiv 5^1 = 5 \ (\text{mod } 3) \end{array}$$

... continued

Part B — 5 points

What is the **greatest common divisor** and the **least common multiple** of:
$3^7 \cdot 5^3 \cdot 7^3$ and $2^{11} \cdot 3^5 \cdot 5^2$.

$$\begin{aligned} \mathrm{gcd}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^2) &= 3^5 \cdot 5^2 \\ \mathrm{lcm}(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^2) &= 2^{11} \cdot 3^7 \cdot 5^3 \cdot 7^3 \end{aligned}$$

Part C — 5 points

Use the Euclidean algorithm to calculate $gcd(100, 270)$. Show each step.

$$\begin{aligned} 100 &= 0 \cdot 270 + 100 \\ 270 &= 2 \cdot 100 + 70 \\ 100 &= 1 \cdot 70 + 30 \\ 70 &= 2 \cdot 30 + 10 \\ 30 &= 3 \cdot 10 + 0 \end{aligned}$$

Thus, $\mathrm{gcd}(135, 50) = 10$.

... continued

Part D — 10 points Prove the following result.

> Let a, b and m be integers with $m \geq 2$.
> If $a \equiv b$ (mod m) then $gcd(a, m) = gcd(b, m)$.

Let a, b, m be integers with $m \geq 2$. Assume $a \equiv b$ (mod m).

So $m|a - b$, or in other words, $a - b = km$ for some integer k.

We will show that the common divisors of a and m are the same as the common divisors of b and m.

($\Rightarrow$) Let d be a common divisor of a and m. Since $d|a$ and $d|m$, we conclude that $d|a-km = b$. Thus, d is a common divisor of b and m.

($\Leftarrow$) Let d be a common divisor of b and m. Since $d|b$ and $d|m$, we conclude that $d|b+km = a$. Thus, d is a common divisor of a and m.

So we have shown that a and m, b and m have the same common divisors, so their greatest common divisor is the same. Thus, $\gcd(a, m) = \gcd(b, m)$.

... End Of Midterm Test