Student Number: ______________________________

NATIONAL UNIVERSITY OF SINGAPORE

MA4207 - MATHEMATICAL LOGIC

(Semester 2 : AY2015/2016)

Time allowed : 2 hours 30 minutes

INSTRUCTIONS TO CANDIDATES

1. **Write down your matriculation/student number clearly in the space provided at the top of this page.** This booklet (and only this booklet) will be collected at the end of the examination.
2. Please write your matriculation/student number only. Do not write your name.
3. This examination paper contains **10** questions (each carrying **6** marks) and comprises **13** printed pages.
4. Answer **ALL** questions.
5. This is a **CLOSED BOOK** examination.
6. Students can use calculators which do not have any information in the memory when brought to the examination hall. When using a calculator, students should still lay out systematically the various steps in the calculations.

For official use only. Do not write below this line.

Question	1	2	3	4	5	6	7	8	9	10	Total
Marks											

For five Boolean input-variables x_1, x_2, x_3, x_4, x_5, let $N(x_1, x_2, x_3, x_4, x_5)$ be the numerical value of $x_1x_2x_3x_4x_5$ viewed as a binary number, for example, $N(0, 1, 0, 1, 1)$ is eleven. Construct a formula $F(x_1, x_2, x_3, x_4, x_5)$ using and ($\wedge$), or ($\vee$), implication ($\rightarrow$), equivalence ($\leftrightarrow$), not ($\neg$), logical constants $0, 1$ with $F(x_1, x_2, x_3, x_4, x_5) = 1$ iff $N(x_1, x_2, x_3, x_4, x_5)$ is an odd prime number or a power of an odd prime number. Here the zeroth power is not included and $F(0, 0, 0, 0, 1) = 0$.

Solution. The formula needs to evaluate with 1 the following numbers: 00011 (3), 00101 (5), 00111 (7), 01001 (9), 01011 (11), 01101 (13), 10001 (17), 10011 (19), 10111 (23), 11001 (25), 11011 (27), 11101 (29), 11111 (31); it has to be 0 on all others. The odd numbers on which it has to be 0 are 00001 (1), 01111 (15) and 10101 (21). A formula for doing this is

$$x_5 \wedge (x_1 \vee x_2 \vee x_3 \vee x_4) \wedge (x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg x_4) \wedge (\neg x_1 \vee x_2 \vee \neg x_3 \vee x_4),$$

which says that the number is odd and different from $1, 15, 21$.

Let S, T be two sets of formulas. Now let $S \models T$ denote the following relation between S and T: for every truth-assignment v, if v makes all formulas in S true then v makes also all formulas in T true. Is the following statement always true?

> If $S \models T$ then there is a finite subset U of S with $U \models T$.

If the statement is true then give a short proof of the statement else provide as a counterexample some sets S, T of formulas satisfying $S \models T$ while no finite subset U of S satisfies $U \models T$.

Solution. The statement looks like a form of the compactness theorem; however, the compactness theorem holds only if T is a finite set of formulas. To see that the statement is false in its full generality, let $S = \{A_1, A_2, \ldots\}$ be the set which asserts that all atoms are true and let $T = S$. The atoms in S are independent of each other; thus if U is a subset of S which does not contain A_k then $U \not\models A_k$. The reason is that there is a truth-assignment v_k with $v_k(A_k) = 0$ and $v_k(A_h) = 1$ for all $h \neq k$. Note that $v_k \models U$ but $v_k \not\models T$. It follows that there is no proper subset U of S with $U \models T$, in particular no finite such U.

Consider the following axioms Γ for structures of the form $(G, \circ, e)$; all these structures are groups but not all groups satisfy all axioms in Γ:

1. (Associativity) $\forall x\, \forall y\, \forall z\, [x \circ (y \circ z) = (x \circ y) \circ z]$;
2. (Commutativity) $\forall x\, \forall y\, [x \circ y = y \circ x]$;
3. (Neutral Element) $\forall x\, [x \circ e = x]$;
4. (Inverse Element) $\forall x\, \exists y\, [x \circ y = e]$;
5. (Bounded Cardinality) $\exists x\, \exists y\, \forall z\, [z = x \vee z = y]$.

Is the statement $\Gamma \models \forall x\, [x \circ x = e]$ true? Explain your answer.

Solution. Assume that $(G, \circ, e)$ is a structure satisfying Γ. The axiom (Bounded Cardinality) says that there is either only one element e or two elements d, e. Note that $e \circ e = e$ and thus e is inverse to itself. Furthermore, $e \circ d = d$ and therefore the inverse of d must be d in the case that d exists. Thus all elements of the group G are self-inverses, so the statement $(G, \circ, e) \models \forall x\, [x \circ x = e]$ is true. As this is true for every structure satisfying Γ, it holds that $\Gamma \models \forall x\, [x \circ x = e]$.

Construct a structure of four members in which exactly two members are definable. The structure can be anything (group, graph or the like). Provide the formulas defining the two elements and a self-isomorphism which proves that the other two elements are not definable. Here a member c is definable iff there is a formula α with one free variable x such that α is true iff the variable x has the value c.

Solution. There are many ways. Here four examples of possible solutions. First is the graph:

```
0 - 1 - 2    3
```

So let $V = \{0, 1, 2, 3\}$ be the vertices and $E(x, y)$ be true iff there is an edge from x to y; the graph is symmetric, so $E(x, y)$ and $E(y, x)$ are the same. Now one can define the node 3 by $\forall y\, [\neg E(x, y)]$ and node 1 by $\exists y\, \exists z\, [E(x, y) \wedge E(x, z) \wedge y \neq z]$. Furthermore, the isomorphism $0 \mapsto 2, 1 \mapsto 1, 2 \mapsto 0, 3 \mapsto 3$ witnesses that 1,3 are not definable.

Another structure would be $\{00, 01, 10, 11\}$ with bitwise And and bitwise Or. Then 00 is the neutral element for Or and 11 is the neutral element for And, that is, $\forall y\, [(y \text{ And } x) = y]$ is true iff $x = 11$ and $\forall y\, [(y \text{ Or } x) = y]$ is true iff $x = 00$. The other two elements are exchanged by the isomorphism $f(ab) = ba$ which interchanges the two bits.

A third example would be $(\{0, 1, 2, 3\}, +)$ the set of the additive group of numbers modulo 4. Now 0 is the neutral element with $\forall y\, [x+y = y]$. Furthermore, 2 is the only self-inverse element besides 0, so $x = 2$ satisfies $\forall y\, [x+x \neq x \wedge x+x+y = y]$. The mapping $f : y \mapsto y+y+y$ is an isomorphism, as f is one-one and $f(y+z) = f(y)+f(z)$. Note that $f(0) = 0$, $f(2) = 2$, $f(1) = 3$ and $f(3) = 1$; hence the values 1 and 3 are not definable in the structure $(\{0, 1, 2, 3\}, +)$.

A fourth structure would be a four-element set with two constants a, b and equality. The constants a, b are different and define the elements denoted by them, so the formula $x = a$ would define the element denoted by a and $x = b$ the element denoted by b. The other two elements cannot be defined and can be interchanged by an isomorphism which has, of course, to map a to a and b to b.

Consider the structure $(\mathbb{Q}, +, \cdot, <, \ldots, -2, -1, 0, 1, 2, \ldots)$ of the rational numbers with addition, multiplication, order and all integer constants. Which of the following formulas are true or false in the rationals and why?

(a) $\forall x\, \exists y\, \exists z\, [x + y = 0 \wedge (x = z \cdot z \vee y = z \cdot z)]$;

(b) $\forall x\, \exists y\, [x \cdot x \cdot y = x]$;

(c) $\forall x\, \exists y\, \forall v\, \forall w\, [x < y \wedge (v \cdot w = y \rightarrow (v = y \vee v = 1 \vee y + v = 0 \vee 1 + v = 0))]$.

Solution. The answer to (a) is "no". The formula says that for each number x, either x or $y = -x$ is a square. This is true in the real numbers but not in the rational numbers. For example, it is well known that $\sqrt{2}$ is not rational. So taking $x = 2$, it follows that $y = -2$ and both numbers satisfy that they are not the square of any rational number z.

The answer to (b) is "yes". Though the number 0 has no multiplicative inverse, the formula takes this into account by saying for each x there is a number y such that x multiplied with $x \cdot y$ is x. In the case that $x \neq 0$, one takes y to be the multiplicative inverse and $x \cdot x \cdot y = x \cdot 1 = x$. In the case that $x = 0$ one can take for y any value and $x \cdot x \cdot y = 0 \cdot y = 0 = x$.

The answer to (c) is "no". The formula would be true in $\mathbb{Z}$ and says that above every number x there is a prime number y which only has the divisors $y, -y, 1, -1$. However, for the rational numbers, this formula does not work, as the number y can be split into the products $1/2$ times $2y$ and $1/3$ times $3y$. At least one of the numbers $1/2$ and $1/3$ is different from $y, -y, 1, -1$ and thus for all x there is no y above x meeting the specification.

Consider the structure $(\mathbb{Z}, \cdot, +, -, <, \ldots, -2, -1, 0, 1, 2, \ldots)$ of the integers with order, addition and multiplication and all integer constants. Construct in the language of the structure formulas with one free variable x satisfying the following respective specifications:

(a) α is true iff x is a square number and not a cubic number;

(b) β is true iff $x > 0$ and x is the product of exactly three prime numbers.

Solutions. The solutions are not unique. Possible formulas are the following ones:

(a) α is $\exists y \, \forall z \, [x = y \cdot y \wedge x \neq z \cdot z \cdot z]$;

(b) β is $\exists u \, \exists v \, \exists w \, \forall y \, \forall z \, [x = u \cdot v \cdot w \wedge 1 < u \wedge 1 < v \wedge 1 < w \wedge (1 < y \wedge 1 < z \rightarrow (y \cdot z \neq u \wedge y \cdot z \neq v \wedge y \cdot z \neq w))]$.

In the deductive calculus, Λ contains the below axioms. However, this list has three groups of axioms added in which do not belong there. Which are these added axiom groups and which of the added ones are provable from Λ and which are not valid (true in all structures)?

(a) α when α is obtained by taking a tautology in sentential logic and replacing all atoms by well-formed formulas in a consistent way (the same atom needs always be replaced by the same formula);

(b) $\forall x\,(\alpha) \rightarrow (\alpha)^x_t$ for all well-formed formulas α, variables x and terms t where the substitution $(\alpha)^x_t$ is permitted;

(c) For each well-formed formula α there is a constant c for which the axiom $\exists x\,(\alpha) \rightarrow (\alpha)^x_c$ is in Λ, c depends on α;

(d) $\forall x(\beta) \rightarrow \forall x(\neg\beta) \rightarrow \forall x(\alpha)$;

(e) $\forall x(\alpha \rightarrow \beta) \rightarrow \forall x(\alpha) \rightarrow \forall x(\beta)$;

(f) $\alpha \rightarrow \forall x(\alpha)$ for all well-formed formulas α and variables x where x does not occur free in α;

(g) $x \neq y$ for every two distinct variables x, y;

(h) $x = x$ for every variable x;

(i) $x = y \rightarrow \alpha \rightarrow \beta$ for all variables x, y and all atomic formulas α and all β derived from α by replacing some occurrences of x by occurrences of y;

(j) $\forall x(\alpha)$ whenever α is in Λ by any of the previous axioms.

Solution
The following axioms are added in.

Axiom Group (c). Some of these formulas are not valid. For example, they require that for each formula there is a constant witnessing that the formula is true. If one would have the field of real numbers as a structure with the constants being all rational numbers then there is no constant which can be used for x in the true formula $\exists x\,[x \cdot x = 2]$. In other words, although 2 has a square root, there is no constant for this and the formula $\exists x\,[x \cdot x = 2] \rightarrow c \cdot c = 2$ would not be true for any of the constants which exists in the given structure. So this axiom group does not produce valid formulas.

Axiom Group (d). Also these axioms are added in. However, they are valid statements, that is, the statement

$$\forall x\,(\beta) \rightarrow \forall x\,(\neg\beta) \rightarrow \forall x\,(\alpha)$$

is true in all structures and thus a valid formula. However, due to the usage of quantifiers, it is not a tautology from Group 1.

Axiom Group (g). This axiom group is also added in. It is not valid in general. In a structure with only one element, all variables have to take as the default this element and, for any two distinct variables x, y, the formula $x \neq y$ is not true. Thus there are structures for which this proposed axiom group would not be true.

Assume that $\Gamma \cup \{\alpha\} \vdash \neg\alpha$. Is it then true that $\Gamma \vdash \neg\alpha$? Either prove the implication formally using the axioms of Λ and the Deduction Theorem or provide a counter example where $\Gamma \cup \{\alpha\} \vdash \neg\alpha$ while $\Gamma \nvdash \neg\alpha$.

Solution. Assume that $\Gamma \cup \{\alpha\} \vdash \neg\alpha$. Note that also $\Gamma \cup \{\alpha\} \vdash \alpha$. Thus $\Gamma \cup \{\alpha\}$ is inconsistent and by Reductio ad Absurdum, $\Gamma \vdash \neg\alpha$.

A formal proof using the Axioms of Λ and the Deduction Theorem is the following one:

1. $\Gamma \cup \{\alpha\} \vdash \neg\alpha$ (Assumption)
2. $\Gamma \vdash \alpha \to \neg\alpha$ (Deduction Theorem)
3. $\Gamma \vdash (\alpha \to \neg\alpha) \to \neg\alpha$ (Axiom Group 1)
4. $\Gamma \vdash \neg\alpha$ (Modus Ponens)

For the logical language containing one function symbol f, give a formal proof for the statement

$$\emptyset \vdash \forall x\, \forall y\, [f(x) = f(y) \to f(y) = f(x)]$$

using the axioms from Λ and the Deduction Theorem and the Generalisation Theorem.

Solution.

1. $\emptyset \vdash \forall v\, \forall w\, [v = w \to v = v \to w = v]$ (Axiom Group 6 Quantified from Λ)
2. $\emptyset \vdash \forall v\, \forall w\, [v = w \to v = v \to w = v] \to \forall w\, [f(x) = w \to f(x) = f(x) \to w = f(x)]$ (Axiom Group 2)
3. $\emptyset \vdash \forall w\, [f(x) = w \to f(x) = f(x) \to w = f(x)]$ (Modus Ponens)
4. $\emptyset \vdash \forall w\, [f(x) = w \to f(x) = f(x) \to w = f(x)] \to (f(x) = f(y) \to f(x) = f(x) \to f(y) = f(x))$ (Axiom Group 2)
5. $\emptyset \vdash f(x) = f(y) \to f(x) = f(x) \to f(y) = f(x)$ (Modus Ponens)
6. $\{f(x) = f(y)\} \vdash f(x) = f(x) \to f(y) = f(x)$ (Deduction Theorem)
7. $\{f(x) = f(y)\} \vdash \forall u\, [u = u] \to f(x) = f(x)$ (Axiom Group 2)
8. $\{f(x) = f(y)\} \vdash \forall u\, [u = u]$ (Axiom Group 5)
9. $\{f(x) = f(y)\} \vdash f(x) = f(x)$ (Modus Ponens)
10. $\{f(x) = f(y)\} \vdash f(y) = f(x)$ (Modus Ponens)
11. $\emptyset \vdash f(x) = f(y) \to f(y) = f(x)$ (Deduction Theorem)
12. $\emptyset \vdash \forall y\, [f(x) = f(y) \to f(y) = f(x)]$ (Generalisation Theorem)
13. $\emptyset \vdash \forall x\, \forall y\, [f(x) = f(y) \to f(y) = f(x)]$ (Generalisation Theorem)

Assume that the logical language contains one unary function symbol f and consider

$$\Gamma = \{\forall x\,[f(f(x)) = x], \forall x\,[f(x) \neq x]\}$$

and the formula α given as

$$\exists x_1\,\exists x_2\,\exists x_3\,[x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3] \rightarrow$$
$$\exists x_1\,\exists x_2\,\exists x_3\,\exists x_4\,[x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3 \wedge x_1 \neq x_4 \wedge x_2 \neq x_4 \wedge x_3 \neq x_4].$$

Does $\Gamma \vdash \alpha$ hold? Give a proof for your answer, all theorems from the lecture can be used.

Solution. The formula α says "if there are at least three elements then there are at least four elements" and thus it says that a structure is a model of α if the number of its elements is different from three. Assume now by way of contradiction that Γ has a model with three elements and without loss of generality these three elements have the names $1, 2, 3$. Now $f(1)$ must be different from 1, say $f(1) = 2$. By $f(f(1)) = 1$, it follows that $f(2) = 1$. Now, again $f(3) \neq 3$, so $f(3) \in \{1, 2\}$ and $f(f(3)) \in \{f(1), f(2)\} = \{1, 2\}$. However, Γ postulate $f(f(3)) = 3$. So Γ does indeed not have a model of three elements. Thus $\Gamma \models \alpha$. By Gödel's Completeness Theorem, $\Gamma \vdash \alpha$.

Note that many questions have different ways to solve them and that therefore the solutions provided in this examination are not unique.