Student Number: ____________________

NATIONAL UNIVERSITY OF SINGAPORE

MA4207 - MATHEMATICAL LOGIC

(Semester 2 : AY2014/2015)

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 $0, 1$ which does the following:

- If $N(x_1, x_2, x_3, x_4, x_5)$ is a prime number then $F(x_1, x_2, x_3, x_4, x_5) = 1$;
- If $N(x_1, x_2, x_3, x_4, x_5)$ is a square number then $F(x_1, x_2, x_3, x_4, x_5) = 0$.

There is no requirement of what value the formula takes on other inputs and one can choose these values such that the formula becomes easier to write down. For example, $F(0, 1, 0, 1, 1)$ should be 1 and $F(0, 0, 0, 0, 1)$ should be 0; $F(0, 0, 1, 1, 0)$ is not specified and can be chosen freely.

Solution. The formula needs to evaluate with 1 the following numbers: 00010 (2), 00011 (3), 00101 (5), 00111 (7), 01011 (11), 01101 (13), 10001 (17), 10011 (19), 10111 (23), 11101 (29), 11111 (31). The formula needs to evaluate with 0 at the following numbers: 00000 (0), 00001 (1), 00100 (4), 01001 (9), 10000 (16), 11001 (25). One sees that most prime numbers satisfy that $x_4 = 1$ or both $x_3 = 1$ and $x_5 = 1$ while no square number has this feature. The only prime number not ending on 1x or 1y1 is 10001 (17). As no square number is of the form 10xy1, one can test this pattern for 17. Hence a valid formula is $x_4 \vee (x_3 \wedge x_5) \vee (x_1 \wedge \neg x_2 \wedge x_5)$.

Assume that $f(a,b,c) = 1$ iff the values of all three inputs a, b, c are equal, that is, $f(a,b,c)$ could be written as $(a \leftrightarrow b) \wedge (a \leftrightarrow c)$. Which of the sets $\{f, 0\}$ and $\{f, 1\}$ are complete? Here a set F of Boolean functions is complete iff all Boolean functions can be expressed using F; the constants $0, 1$ are the logical constants. For example, one can express $a \leftrightarrow b$ as $f(a,a,b)$ and one can also consider nested expressions like $f(a,b,f(a,a,b))$. However, all the connectives and constants used should be members of F. Explain your answer.

Solution. The set $\{f, 1\}$ is not a complete set of Boolean functions. The reason is that whenever all inputs are 1, every application of f or of the constant 1 to some of the inputs gives the output 1 and so also nested expressions of f and 1 give only functions which map the an input of only 1s to 1. Thus, the constant 0 and the negation $\neg$ cannot be expressed.

The set $\{f, 0\}$ is logically complete. The function $a \mapsto f(a, 0, 0)$ maps 0 to 1 and 1 to 0, thus the negation $\neg$ can be expressed using f and 0. The constant 1 is given as $f(0, 0, 0)$. The function $a, b \mapsto f(a, b, 1)$ is 1 iff both inputs are 1, thus the and function $\wedge$ can be expressed by $a \wedge b = f(a, b, 1)$. Furthermore, the or $\vee$ can be expressed using $\neg$ and $\wedge$, thus can be expressed using f, 0 and 1. It follows that the set $\{f, 0\}$ is a complete set of Boolean functions.

Let the logical language contain besides the equality $=$ also an equivalence relation $\equiv$. Let the spectrum of a formula α be the set of all $n \in \{1, 2, \ldots\}$ for which there is a model $(A, \equiv, =)$ of n elements such that

$$(A, \equiv, =) \models \{\alpha, \forall x\, [x \equiv x], \forall x\, \forall y\, [x \equiv y \to y \equiv x], \forall x\, \forall y\, \forall z\, [x \equiv y \to y \equiv z \to x \equiv z]\},$$

that is, a model $(A, \equiv, =)$ of n elements which satisfies α and satisfies the axioms of an equivalence relation. Construct a formula α such that its spectrum are the numbers of the form $3n + 1$ and $3n + 2$, that is, the spectrum of α should be $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, \ldots\}$.

Solution. The idea is to construct a formula which says the following:

1. There is an equivalence class with one or two members where x_1 is one member and x_2 the other member (they can be equal);
2. For every y_1 there are y_2 and y_3 such that y_1, y_2, y_3 are equivalent and every further y_4 equivalent to y_1 is equal to one of y_1, y_2, y_3;
3. If y_1 represents an equivalence class different from x_1 then y_1, y_2, y_3 are distinct.

These conditions say the following: 1. There is one equivalence class of one or two members represented by x_1; 2. Every equivalence class has at most three members; 3. Every equivalence class different from the one of x_1 has at least three members. So, in the case that the model is finite, its number of elements is a multiple of three plus 1 or 2, depending on whether $x_1 = x_2$ or $x_1 \neq x_2$. The formula is silent about this question. Here the formula α:

- α is $\exists x_1, x_2\, \forall x_3, y_1\, \exists y_2, y_3\, \forall y_4\, [\beta_1 \wedge \beta_2 \wedge \beta_3]$;
- β_1 is $(x_1 \equiv x_2) \wedge (x_3 \equiv x_1 \to x_1 = x_3 \vee x_2 = x_3)$;
- β_2 is $(y_2 \equiv y_1 \wedge y_3 \equiv y_1) \wedge (y_4 \equiv y_1 \to y_4 = y_1 \vee y_4 = y_2 \vee y_4 = y_3)$;
- β_3 is $(y_1 \not\equiv x_1 \to y_1 \neq y_2 \wedge y_1 \neq y_3 \wedge y_2 \neq y_3)$.

Question 4 [6 marks]

Consider the following finite graph:

```
1 - 2 - 3 - 4
    |       |
    5 - 6 - 7   8
```

Which of the nodes in the finite graph are definable and which are not? Explain your answers.

Solution. One can express in a formula that a node has exactly k or at least k neighbours. For example the node 2 is the unique node with three or more neighbours:

$$\phi_2(x) \Leftrightarrow \exists y_1, y_2, y_3\, [y_1 \neq y_2 \wedge y_1 \neq y_3 \wedge y_2 \neq y_3 \wedge E(x, y_1) \wedge E(x, y_2) \wedge E(x, y_3)].$$

Similarly the nodes 1 and 8 are definable since they are the unique nodes with 1 and 0 neighbours, respectively. The node 7 is definable as the node which has two different ways to connect to node 2 by a three-node path:

$$\phi_7(x) \;\Leftrightarrow\; \exists z_1, z_2, z_3, z_4, z_5\, [\phi_2(z_1) \wedge E(z_1, z_2) \wedge E(z_2, z_3) \wedge E(z_3, x) \wedge E(z_1, z_4) \wedge E(z_4, z_5) \wedge E(z_5, x) \wedge (z_2 \neq z_4) \wedge (z_1 \neq z_3) \wedge (z_1 \neq z_5)].$$

The nodes 3, 4, 5, 6 are not definable since one can construct a graph isomorphism f from the graph to itself via the table

x	1	2	3	4	5	6	7	8
$f(x)$	1	2	5	6	3	4	7	8

witnessing that the nodes 3 and 5 and the nodes 4 and 6 can be exchanged with each other.

Let a logical language with addition $+$ and constants $0, 1, c$ be given and assume that

$$S_n = \{\forall x_0\,[0 + x_0 = x_0],\ \forall x_0\,\forall x_1\,[x_0 + x_1 = 1 \rightarrow x_0 = 1 \vee x_1 = 1],\ 0 \neq 1,\ \alpha_n\}$$

where

- α_0 is $\forall x_0\,[(x_0 = 0) \rightarrow (x_0 \neq c)]$,
- α_1 is $\forall x_0\,\forall x_1\,[(x_0 = 0) \rightarrow (x_1 = x_0 \vee x_1 = x_0 + 1) \rightarrow (x_1 \neq c)]$,
- α_n, for any $n \in \mathbb{N}$, is $\forall x_0\,\forall x_1\,\ldots\,\forall x_n\ [(x_0 = 0) \rightarrow (x_1 = x_0 \vee x_1 = x_0 + 1) \rightarrow (x_2 = x_1 \vee x_2 = x_1 + 1) \rightarrow \ldots \rightarrow (x_n = x_{n-1} \vee x_n = x_{n-1} + 1) \rightarrow (x_n \neq c)]$.

(a) Is every model of S_{n+1} a model of S_n?
(b) Is there for every set S_n a model with domain $\mathbb{N}$ and $+$ being the usual addition in $\mathbb{N}$?
(c) Is there a model with domain $\mathbb{N}$ and $+$ being the usual addition in $\mathbb{N}$ satisfying $\bigcup_n S_n$ (the union of all S_n)?
Explain your answers.

Solution. The answer to (a) is "yes", as α_{n+1} excludes more possible values of c then α_n. Indeed, when m denotes the sum of m 1s for $m \geq 2$, so $2 = 1 + 1$ and $3 = (1 + 1) + 1$ and $4 = ((1 + 1) + 1) + 1$, then the formula α_n says that c is different from $0, 1, \ldots, n$.

The answer to (b) is "yes" by taking the model $(\mathbb{N}, +, 0, 1, c)$ with $c = n+1$. The reason is that the first axioms in S_n just enforce that 0 and 1 are the usual values of these constants and, the last formula says that for all choices of the variables where $x_0 = 0$ and $x_{m+1} \in \{x_m, x_m + 1\}$, it follows that $c \neq x_n$; as for this condition it can be that $x_m \in \{0, 1, \ldots, m\}$, it then says that c is none of the values $0, 1, \ldots, n$ and so $c = n + 1$ is a legitimate choice.

The answer to (c) is "no" as the axioms enforce that 0 and 1 take the usual values in $\mathbb{N}$ and each α_n enforces that $c \neq n$; as the union of all S_n contains all α_n, c cannot be any $n \in \mathbb{N}$. Hence a model as required does not exist.

This answer is consistent with the compactness theorem, as that only states that there is some model for every consistent set of formulas; it does, however, not say that this model is of a specific form (like having the domain $\mathbb{N}$ and the operation $+$ inherited from the natural numbers).

Construct a formula $\phi(x)$ using only bounded quantifiers, constants from $\mathbb{N}$, $+$, $*$ and $<$ such that $\phi(x)$ is true iff x is a prime number or the power of a prime number; x is the only free variable in ϕ. For example, $\phi(2), \phi(3), \phi(4), \phi(5), \phi(7), \phi(8), \phi(9)$ should be true and $\phi(0), \phi(1), \phi(6)$ should be false. Explain how your formula works and why it is correct.

Solution. The formula $\phi(x)$ is

$$\exists p \leq x \, \forall y < x \, \forall z < x \, \exists v < x \, \exists w < x \, [p > 1 \wedge x = y * z \rightarrow y = p * v \wedge z = p * w].$$

The formula says the following: There is a number $p > 1$ such that whenever x has a non-trivial factorisation (both proper factors of x) then p divides both factors. Indeed, if x is a prime number then x is such a p itself, as x has no non-trivial factorisation. If x is a proper power of a prime p, then p is a factor of every non-trivial factor of x and that is expressed by this formula: $p > 1$ so that p is not 1 and p divides both factors v, w for any non-trivial factorisation of x which exists. If x has two different prime factors p, q then p fails to divide both y, z in the case that one of the factors y, z is q. Note that the existence of p implies that x is at least 2, independently of whether any further property on p is postulated (by x having non-trivial factors) or not.

Recall that in the deductive calculus, Λ contains the following formulas:

1. 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);
2. $\forall x\,(\alpha) \to (\alpha)^x_t$ for all well-formed formulas α, variables x and terms t where the substitution $(\alpha)^x_t$ is permitted;
3. $\forall x(\alpha \to \beta) \to \forall x(\alpha) \to \forall x(\beta)$;
4. $\alpha \to \forall x(\alpha)$ for all well-formed formulas α and variables x where x does not occur free in α;
5. $x = x$ for every variable x;
6. $x = y \to \alpha \to \beta$ for all variables x, y and all atomic formulas α and all β derived from α;
7. $\forall x(\alpha)$ whenever α is in Λ by any of the steps 1-7.

Answer the following questions:

(a) What does it mean that a substitution is permitted? Give an example for a permitted and also for a non-permitted substitution.

(b) What is an atomic formula and what is precisely meant with "β is derived from α" in the calculus? Note that the statement in the textbook uses some other word than "derived", it is your task to give a formal answer of what wording should be used in place of "derived" and provide an example of an axiom of type 6.

Solution. For (a), permitted is defined inductively: if α is atomic then every substitution is permitted; if $(\alpha)^x_t$ and $(\beta)^x_t$ are permitted so are $(\neg\alpha)^x_t$ and $(\alpha \to \beta)^x_t$; if α^t_x is permitted and y does not occur in t and y is different from x then $(\forall y\,(\alpha))^x_t$ is permitted; if α^t_x is permitted so is $(\forall x\,(\alpha))^x_t$ and this substitution does not change the formula at all. An example for a permitted substitution is $(\forall y\,(y \cdot y \neq x))^x_z$ and a non-permitted one is $(\forall y\,(y \cdot y \neq x))^x_y$.

For (b), an atomic formula consists of the equality of two terms or a predicate over some terms. The formula β is derived from α by replacing some occurrences of variables x by occurrences of the variable y. An example for this axiom is $x = y \to (x + x = 0) \to (x + y = 0)$.

Explain what the Generalisation Theorem and the Deduction Theorem say. Give a formal proof for the statement

$$\emptyset \vdash \forall x\,[f(x) = 0] \to \forall y\,[f(y) = 0].$$

The logical language used contains one function symbol f and one constant 0 and the equality (=). In the proof, you can besides the formulas from Λ and the Modus Ponens also use the Generalisation Theorem and the two directions of the Deduction Theorem.

Solution. The Generalisation Theorem says the following: If Γ is a set of formulas not containing the free variable y and if one can show that $\Gamma \vdash \alpha$ then one can also show that $\Gamma \vdash \forall y\,[\alpha]$.

The Deduction Theorem says the following: If Γ is a set of formulas then $\Gamma \vdash \alpha \to \beta$ iff $\Gamma \cup \{\alpha\} \vdash \beta$. One can use the Deduction Theorem in both directions of this equivalence.

The proof is the following.

1. $\{\forall x\,[f(x) = 0]\} \vdash \forall x\,[f(x) = 0]$ (Copying formula)
2. $\{\forall x\,[f(x) = 0]\} \vdash \forall x\,[f(x) = 0] \to f(y) = 0$ (Axiom)
3. $\{\forall x\,[f(x) = 0]\} \vdash f(y) = 0$ (Modus Ponens)
4. $\{\forall x\,[f(x) = 0]\} \vdash \forall y\,[f(y) = 0]$ (Generalisation Theorem)
5. $\emptyset \vdash \forall x\,[f(x) = 0] \to \forall y\,[f(y) = 0]$ (Deduction Theorem)

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

$$\Gamma = \{\forall x\,[x = f(f(x))], \forall x\,\forall y\,[x = y \to f(x) = f(y)]\}.$$

Give a formal proof for the following statement:

$$\Gamma \vdash \forall x\,[f(x) = f(f(f(x)))].$$

You can use the axioms from Λ, the formulas in Γ, the Modus Ponens and the Generalisation Theorem for making the proof.

Solution.

1. $\Gamma \vdash \forall x\,[x = f(f(x))]$ (from Γ)
2. $\Gamma \vdash \forall x\,[x = f(f(x))] \to f(x) = f(f(f(x)))$ (Axiom, this substitution is permitted as the formula $x = f(f(x))$ does not contain any quantifier)
3. $\Gamma \vdash f(x) = f(f(f(x)))$ (Modus Ponens)
4. $\Gamma \vdash \forall x\,[f(x) = f(f(f(x)))]$ (Generalisation Theorem, x is not free in Γ)

Assume that the logical language contains one operator $\circ$ and a constant e and the axioms

$$\Gamma = \{\forall x\,[x \circ (x \circ x) = e],\ \forall v\,\forall w\,[v = w \to w = v]\}.$$

Give a formal proof for the following statement:

$$\Gamma \vdash \forall x\,\forall y\,[y = x \circ x \to x \circ y = e].$$

You can use the axioms from Λ, the formulas in Γ, the Modus Ponens, the Deduction Theorem (both directions) and the Generalisation Theorem for making the proof.

Solution.

1. $\Gamma \vdash z = y \to x \circ z = e \to x \circ y = e$ (Axiom)
2. $\Gamma \vdash \forall z\,[z = y \to x \circ z = e \to x \circ y = e]$ (Generalisation Theorem)
3. $\Gamma \vdash \forall z\,[z = y \to x \circ z = e \to x \circ y = e] \to (x \circ x = y \to x \circ (x \circ x) = e \to x \circ y = e)$ (Axiom)
4. $\Gamma \vdash x \circ x = y \to x \circ (x \circ x) = e \to x \circ y = e$ (Modus Ponens)
5. $\Gamma \cup \{x \circ x = y\} \vdash x \circ (x \circ x) = e \to x \circ y = e$ (Deduction Theorem)
6. $\Gamma \cup \{x \circ x = y\} \vdash \forall x\,[x \circ (x \circ x) = e]$ (from Γ)
7. $\Gamma \cup \{x \circ x = y\} \vdash \forall x\,[x \circ (x \circ x) = e] \to x \circ (x \circ x) = e$ (Axiom)
8. $\Gamma \cup \{x \circ x = y\} \vdash x \circ (x \circ x) = e$ (Modus Ponens)
9. $\Gamma \cup \{x \circ x = y\} \vdash x \circ y = e$ (Modus Ponens)
10. $\Gamma \vdash x \circ x = y \to x \circ y = e$ (Deduction Theorem)
11. $\Gamma \vdash \forall v\,\forall w\,[v = w \to w = v]$ (from Γ)
12. $\Gamma \vdash \forall v\,\forall w\,[v = w \to w = v] \to \forall w\,[y = w \to w = y]$ (Axiom)
13. $\Gamma \vdash \forall w\,[y = w \to w = y]$ (Modus Ponens)
14. $\Gamma \vdash \forall w\,[y = w \to w = y] \to y = x \circ x \to x \circ x = y$ (Axiom)
15. $\Gamma \vdash y = x \circ x \to x \circ x = y$ (Modus Ponens)
16. $\Gamma \vdash (y = x \circ x \to x \circ x = y) \to (x \circ x = y \to x \circ y = e) \to (y = x \circ x \to x \circ y = e)$ (Axiom stating $(\alpha \to \beta) \to (\beta \to \gamma) \to (\alpha \to \gamma)$)
17. $\Gamma \vdash (y = x \circ x \to x \circ y = e)$ (Modus Ponens twice)
18. $\Gamma \vdash \forall x\,\forall y\,[y = x \circ x \to x \circ y = e]$ (Generalisation Theorem twice)