Computing and Software 701

Logic and Discrete Mathematics In Software Engineering

Fall 2008

Final Exam Answer Key

Instructor: William M. Farmer

You have 110 minutes to complete this exam consisting of 2 pages and 6 questions. Write your answers in the examination booklet provided to you. Give reasons for your answers. The use of any calculators, notes, and books is permitted during this exam, but you may not use any other electronic devices. Good luck!

(1) Let

$$L = (\{p_1, p_2, p_3 \ldots\}, \{\neg, \Rightarrow, \wedge, \vee, \bowtie\})$$

be the propositional language where $\neg, \Rightarrow, \wedge, \vee$ denote the usual function truth functions and $\bowtie$ denotes the truth function given by:

p_1	p_2	$(p_1 \bowtie p_2)$
T	T	F
T	F	T
F	T	F
F	F	F

(a) [10 pts.] Show that the formula

$$(p_1 \bowtie (p_2 \wedge p_3)) \Rightarrow ((p_1 \bowtie p_2) \wedge (p_1 \bowtie p_3))$$

is satisfiable but not valid.

Answer: The truth table for the formula is below. Since the value of the formula is true for at least one row and is false for at least one row, the formula is satisfiable but not valid.

(b) [10 pts.] Find a formula in the propositional language

$$L' = (\{p_1, p_2, p_3 \ldots\}, \{\neg, \Rightarrow, \wedge, \vee\})$$

that is logically equivalent to $p_1 \bowtie p_2$.

Answer: The formula $\neg(p_1 \Rightarrow p_2)$ has the same truth table as $p_1 \bowtie p_2$ and is thus logically equivalent to $p_1 \bowtie p_2$.

p_1	p_2	p_3	$(p_1 \bowtie (p_2 \land p_3)) \Rightarrow ((p_1 \bowtie p_2) \land (p_1 \bowtie p_3))$	
T	T	T	T F T T T T T F T F T F T	T
T	T	F	T T T F F F T F T F T T F	F
T	F	T	T T F F T F T T F F T F T	F
T	F	F	T T F F F T T T F T T T F	T
F	T	T	F F T T T T F F T F F F T	T
F	T	F	F F T F F T F F T F F F F	T
F	F	T	F F F F T T F F F F F F T	T
F	F	F	F F F F F T F F F F F F F	T

(2) Let $T = (L, \Gamma)$ be a theory of groups in FOL where

$$L = (\{\mathsf{e}\}, \{\mathsf{mul}, \mathsf{inv}\}, \{=\})$$

with mul binary and inv unary and Γ is the set of the following formulas of L:

1. $\forall x, y, z \, . \, x \ \mathsf{mul}\ (y \ \mathsf{mul}\ z) = (x \ \mathsf{mul}\ y) \ \mathsf{mul}\ z$.
2. $\forall x \, . \, x \ \mathsf{mul}\ \mathsf{e} = x$.
3. $\forall x \, . \, \mathsf{e}\ \mathsf{mul}\ x = x$.
4. $\forall x \, . \, x \ \mathsf{mul}\ \mathsf{inv}(x) = \mathsf{e}$.
5. $\forall x \, . \, \mathsf{inv}(x) \ \mathsf{mul}\ x = \mathsf{e}$.

Suppose A is a set and BF is the set of functions $f : A \to A$ that are bijective.

(a) [10 pts.] Construct a model $M = (\mathsf{BF}, I)$ for L such that $I(\mathsf{mul})$ is function composition on BF, i.e., $o : \mathsf{BF} \times \mathsf{BF} \to \mathsf{BF}$.

Answer: $I(\mathsf{e})$ is the identity function on BF, and $I(\mathsf{inv})$ is the function $i : \mathsf{BF} \to \mathsf{BF}$ such that, for $f \in \mathsf{BF}$, $i(f)$ is the inverse of f which exists and is unique since f is bijective.

(b) [10 pts.] Show that M is a model of T.

Answer: Axiom 1 holds since function composition is associative. Axioms 2 and 3 hold since the identity function is an identity element respect to function composition. Axioms 4 and 5 hold since $i(f)$ is the inverse of f.

(3) Let $T = (L, \Gamma)$ be the equational theory of FOL where

$$L = (\{\,\}, \{f, g\}, \{=\})$$

with f and g unary and Γ is the singleton set

$$\{\forall\, x \,.\, f(f(x)) = g(x)\}.$$

Let $\mathcal{R} = \{f(f(x)) \rightarrow g(x)\}$ be a set of rewrite rules for T.

(a) [10 pts.] Is $\mathcal{R}$ finitely terminating? Justify your answer.

Answer: Yes, each application of the single rewrite rule $f(f(x)) \rightarrow g(x)$ to a term reduces the number of fs by 2 and so eventually the rewrite rule will not be applicable.

(b) [10 pts.] Is $\mathcal{R}$ confluent? Justify your answer.

Answer: No, because $f(f(f(x)))$ rewrites to $g(f(x))$ and $f(g(x))$, which are both normal forms.

(4) [10 pts.] Let $\mathcal{T}$ be the set of types of STT. For $\alpha \in \mathcal{T}$, let $L(\alpha)$ be the number of left parentheses in α and $R(\alpha)$ be the number of right parentheses in α. Prove by structural induction that, for all $\alpha \in \mathcal{T}$, $L(\alpha) = R(\alpha)$.

Answer: The proof consists of the following two steps:

- *Basis: Show that the statement holds for ι and $*$.* If $\alpha \in \{\iota, *\}$, then $L(\alpha) = R(\alpha) = 0$.
- *Induction step: Assume the statement holds for β and γ and show that the statement holds for $\alpha = \beta \rightarrow \gamma$.* The induction hypothesis implies $L(\beta) = R(\beta)$ and $L(\gamma) = R(\gamma)$. Then $L(\alpha) = L(\beta) + L(\gamma) + 1 = R(\beta) + R(\gamma) + 1 = R(\alpha)$.

(5) [15 pts.] Let α and β be two arbitrary types of STT. Construct a sentence of STT that says the domain denoted by α is equipollent to the domain denoted by β.

Answer:

$$\begin{array}{l} \exists\, f : \alpha \rightarrow \beta \,. \\ \quad (\forall\, x_1, x_2 : \alpha \,.\, f(x_1) = f(x_2) \Rightarrow x_1 = x_2) \wedge \\ \quad (\forall\, y : \beta \,.\, \exists x : \alpha \,.\, f(x) = y) \end{array}$$

(6) [15 pts.] Let **PA** $= (L, \Gamma)$ be the theory of STT such that:

- $L = (\{0, S\}, \tau)$ where $\tau(0) = \iota$ and $\tau(S) = \iota \rightarrow \iota$.
- Γ is the set of the following three formulas:
  1. $\forall\, x : \iota \,.\, 0 \neq S(x)$.
  2. $\forall\, x, y : \iota \,.\, S(x) = S(y) \Rightarrow x = y$.
  3. $\forall\, P : \iota \rightarrow * \,.$
     $P(0) \wedge (\forall\, x : \iota \,.\, P(x) \Rightarrow P(S(x))) \Rightarrow \forall\, x : \iota \,.\, P(x)$.

Let $+$ be a constant of type $\iota \rightarrow (\iota \rightarrow \iota)$.

(a) [10 pts.] Construct a sentence A of STT that defines $+$ to be the usual addition function in **PA**. (You may write $+$ as an infix operator.)

Answer:

$$\forall\, x, y : \iota \,.\, x + y = \mathsf{if}(y = 0, x, S(x + (\mathrm{I}\, z : \iota \,.\, S(z) = y)))$$

(b) [5 pts.] Show that your definition of $+$ makes sense by proving

$$\mathbf{PA} \models \exists\,!\, f : \iota \rightarrow (\iota \rightarrow \iota) \,.\, A'$$

where:

- A' is obtained from A by replacing each occurrence of $+$ in A by the variable $(f : \iota \rightarrow (\iota \rightarrow \iota))$.
- $\exists\,!\, x : \alpha \,.\, B$ means there is a unique x of type α that satisfies B.

Answer: The following is a sketch of the proof in **PA**:

i. Prove the principle of definition via well-found recursion.

ii. Define the strict total order $<$ on ι as the transitive closure of the binary relation (represented by the predicate)
$$\lambda\, x : \iota \,.\, \lambda\, y : \iota \,.\, y = S(x).$$

iii. Show that $<$ is well founded.

iv. Show that 0 is the unique $<$-least element of ι.

v. Show that
$$A' \Rightarrow \forall\, x : \iota \,.\, f(x)(0) = x.$$

vi. Show that
$$\forall\, y : \iota \,.\, y \neq 0 \Rightarrow (\mathrm{I}\, z : \iota \,.\, S(z) = y) < y.$$

vii. Conclude that
$$\exists\,!\, f : \iota \rightarrow (\iota \rightarrow \iota) \,.\, A'$$
holds by applying the principle of definition via well-found recursion.