Computing and Software 701

Logic and Discrete Mathematics In Software Engineering

Fall 2005

Midterm Test Answer Key

Instructor: William M. Farmer

You have 110 minutes to complete this test consisting of 2 pages and 7 questions. Write your answers in the examination booklet provided to you. Give reasons for your answers. Good luck!

(1) [10 pts.] Consider the formula

$$(\neg A \Rightarrow (B \vee C)) \Rightarrow ((B \wedge C) \Rightarrow A)$$

of propositional logic. Compute the truth table for this formula. Is this formula valid, satisfiable but not valid, or not satisfiable?

Answer:

A	B	C	$(\neg A \Rightarrow (B \vee C)) \Rightarrow ((B \wedge C) \Rightarrow A)$						
T	T	T	F	T	T	T	T	T	T
T	T	F	F	T	T	T	F	T	T
T	F	T	F	T	T	T	F	T	T
T	F	F	F	T	F	T	F	T	T
F	T	T	T	T	T	F	T	F	F
F	T	F	T	T	T	T	F	T	T
F	F	T	T	T	T	T	F	T	T
F	F	F	T	F	F	T	F	T	T

The formula is satisfiable but not valid.

(2) [10 pts.] Let **H** be the Hilbert-style proof system for the language L_0 of propositional logic given in class. Prove that, if $\Sigma \cup \{A\}$ is inconsistent in **H**, then $\Sigma \vdash_{\mathbf{H}} \neg A$. (Hint: Use the Deduction Theorem for **H**.)

Answer: Assume $\Sigma \cup \{A\}$ is inconsistent in **H**. Then $\Sigma \cup \{A\} \vdash_{\mathbf{H}} \mathsf{F}$, and so by the Deduction Theorem for **H**, $\Sigma \vdash_{\mathbf{H}} A \Rightarrow \mathsf{F}$. It is easy to check that $A \Rightarrow \mathsf{F}$ is logically equivalent to $\neg A$, i.e., $\models (A \Rightarrow \mathsf{F}) \Leftrightarrow \neg A$. Hence, $\Sigma \models A \Rightarrow \mathsf{F}$ iff $\Sigma \models \neg A$. This implies $\Sigma \vdash_{\mathbf{H}} A \Rightarrow \mathsf{F}$ iff $\Sigma \vdash_{\mathbf{H}} \neg A$ since **H** is sound and complete. Therefore, $\Sigma \vdash_{\mathbf{H}} \neg A$. Q.E.D.

(3) [10 pts.] Let $f : A \to B$ be a total function, $g : B \to C$ be a nonempty, partial function, and let $h = g \circ f : A \to C$ be the composition of g and f. Prove that h must be partial, or give a counterexample that shows h could be total. (Recall that a partial function is a function $f : A \to B$ that is undefined on some members of A.)

Answer: Let $A = B = C = \{a, b\}$, $f(x) = a$ for $x \in \{a, b\}$, $g(a) = a$, and $g(b)$ is undefined. Clearly, f is total and g is partial. $h = g \circ f = f$, so h is also total. Therefore, this is a counterexample to the claim that h must be partial.

(4) [10 pts.] Let S be the set of all finite subsets of the natural numbers. Prove that S is equipollent to the natural numbers $\mathbf{N}$, or prove that S is equipollent to the real numbers $\mathbf{R}$.

Answer: There is clearly a one-to-one correspondence between the set of finite strings of 0s and 1s and $\mathbf{N}$: each finite string of 0s and 1s represents a natural number in base 2. There is also clearly a one-to-one correspondence between the set of finite strings of 0s and 1s and the set S of finite subsets of $\mathbf{N}$: each finite string of 0s and 1s represents the characteristic function of a finite set of natural numbers. Putting these two observations together shows that S is equipollent to $\mathbf{N}$. Q.E.D.

(5) Let P be Peano's five-axiom specification of natural number arithmetic.

(a) [10 pts.] Explain why P cannot be directly formalized in FOL.

Answer: The fifth axiom of P is the induction principle for the natural numbers. It involves a quantification over all unary predicates. A "higher-order quantification" like this cannot be directly expressed in a first-order logic such as FOL.

(b) [10 pts.] Explain why the usual formalization of P in first-order logic is a weak approximation to the direct formalization of P in second-order logic or simple type theory.

Answer: The usual formalization of P in first-order logic replaces the induction principle with an induction schema. The induction schema has only a countable numbers of instances, one for each formula. Hence it represents no more than a countable number of instance of the induction principle. However, the induction principle has an uncountable number of instances, one for each unary predicate over the natural numbers. Therefore, the induction schema is a weak approximation of the induction principle, and the usual formalization of P in first-order logic is a weak approximation of a direct formalization of P in second-order logic or simple type theory.

(6) Let R be a pre-order on a set S and E to be the relation $\{(s,t) \mid s\ R\ t \wedge t\ R\ s\}$.

(a) [10 pts.] Show that E is an equivalence relation of S.

Answer: Note that since R is a pre-order, R is reflexive and transitive. We will show that E is reflexive, symmetric, and transitive, and therefore, an equivalence relation.

i. $x\ E\ x$ iff $x\ R\ x \wedge x\ R\ x$ iff $x\ R\ x$. Therefore, E is reflexive since R is reflexive.

ii. $x\ E\ y$ iff $x\ R\ y \wedge y\ R\ x$ iff $y\ R\ x \wedge x\ R\ y$ iff $y\ E\ x$. Therefore, E is symmetric.

iii. $x\ E\ y \wedge y\ E\ z$ iff $x\ R\ y \wedge y\ R\ x \wedge y\ R\ z \wedge z\ R\ y$. The last statement implies $x\ R\ z \wedge z\ R\ x$ by the transitivity of R, and thus $x\ E\ z$ holds by the definition of E. Therefore, E is transitive.

Q.E.D.

(b) [10 pts.] Let X be the set of equivalence classes of E. For $A, B \in X$, let $A \leq B$ mean that, for all $a \in A$ and $b \in B$, $a\ R\ b$. Show that $\leq$ is a weak partial order on X.

Answer: We will show that $\leq$ is reflexive, antisymmetric, and transitive, and therefore, a weak partial order.

i. $A \leq A$ iff, for all $a, a' \in A$, $a\ R\ a'$. The last statement is true since A is an equivalence class of E and thus, for all $a, a' \in A$, $a\ E\ a'$. Therefore, $\leq$ is reflexive.

ii. $A \leq B \wedge B \leq A$ iff, for all $a \in A$ and $b \in B$, $a\ R\ b \wedge b\ R\ a$ iff, for all $a \in A$ and $b \in B$, $a\ E\ b$ iff $A = B$. Therefore, $\leq$ is antisymmetric.

iii. $A \leq B \wedge B \leq C$ iff, for all $a \in A$, $b \in B$, and $c \in C$, $a\ R\ b \wedge b\ R\ c$. The last statement implies, for all $a \in A$ and $c \in C$, $a\ R\ c$, and thus, $A \leq C$ by the definition of $\leq$.

Q.E.D.

(7) Let $L = (\{\mathsf{min}, \mathsf{max}\}, \emptyset, \{=, <\})$ be a language of FOL where $\mathsf{min}, \mathsf{max}$ are individual constants and $<$ is a binary predicate symbol.

(a) [10 pts.] Find a set Γ of sentences of FOL such that, for each model $M = (D, I)$ of $T = (L, \Gamma)$, $I(<)$ is a strict total order on D; $I(\mathsf{min}) \neq I(\mathsf{max})$; and $I(\mathsf{min})$ and $I(\mathsf{max})$ are minimum and maximum elements, respectively, of the strict total order.

Answer: Let Γ be the following set of sentences of L:

i. $\forall x \,.\, \neg(x < x)$.
ii. $\forall x, y \,.\, x < y \Rightarrow \neg(y < x)$.
iii. $\forall x, y, z \,.\, (x < y \wedge y < z) \Rightarrow x < z$.
iv. $\forall x, y, z \,.\, x < y \vee y < x \vee x = y$.
v. $\mathsf{min} < \mathsf{max}$.
vi. $\forall x \,.\, x \neq \mathsf{min} \Rightarrow \mathsf{min} < x$.
vii. $\forall x \,.\, x \neq \mathsf{max} \Rightarrow x < \mathsf{max}$.

(b) [10 pts.] Find an extension $T' = (L, \Gamma')$ of the theory T above such that T' is satisfiable and, for each model $M = (D, I)$ of T', D is infinite. (Notice that T and T' share the same language.)

Answer: Let Γ' be Γ plus the following sentence of L:

viii. $\forall x, y \,.\, x < y \Rightarrow (\exists z \,.\, x < z \wedge z < y)$.

$(\mathbf{Q}^*, =, <)$, where $\mathbf{Q}^*$ is the set of rational numbers with endpoints $-\infty$ and $+\infty$, is the smallest model for T'. Therefore, T' is satisfiable and every model of T' is infinite.

Other solutions are also possible.