Inst.: Data- och informationsteknik
Kursnamn: Logic in Computer Science
Examinator: Thierry Coquand
Kurs: DIT201/DAT060
Datum: 2013-10-22 No help documents
Telefonvakt: akn. 5410
All answers and solutions must be carefully motivated!
total 60; $\geq$28: 3, $\geq$38: 4, $\geq$50: 5
total 60; $\geq$28: G, $\geq$42: VG

All answers **must** be carefully motivated.

1. We consider the following language: we have one binary predicate symbol P, a binary function symbol g, and a constant c.

   (a) Define what a model of this language is. (3p)

   Solution: A model $\mathcal{M}$ for this language is:

   i. A nonempty set A,
   ii. a set $P^{\mathcal{M}} \subseteq A^2$,
   iii. a function $g^{\mathcal{M}} : A^2 \to A$,
   iv. and a constant element $c^{\mathcal{M}} \in A$.

   (b) Give an example of a formula using P, g, and c which does not hold in all models. (2p)

   Solution: The formula $\varphi = P(g(c, c), c)$ does not hold in the model $\mathcal{M}$ given by:

   i. $A = \{0, 1\}$,
   ii. $P^{\mathcal{M}} = \{(0, 0)\}$,
   iii. $g^{\mathcal{M}}(x, y) = x$,
   iv. $c^{\mathcal{M}} = 1$.

   With this model and an arbitrary look-up table l we get $\mathcal{M} \not\models_l \varphi$ as $(1, 1) \notin P^{\mathcal{M}}$.

2. Give proofs in natural deduction of the following sequents:

(a) $(p \to s) \lor (q \to t) \vdash (p \land q) \to (t \lor s)$ (3p)

Solution:

1	$(p \to s) \lor (q \to t)$	Premise
2	$p \land q$	Assumption
3	p	$\land_{e_1}$ 2
4	q	$\land_{e_2}$ 2
5	$p \to s$	Assumption
6	s	$\to_e$ 3, 5
7	$t \lor s$	$\lor_{i_2}$ 6
8	$q \to t$	Assumption
9	t	$\to_e$ 4, 8
10	$t \lor s$	$\lor_{i_1}$ 9
11	$t \lor s$	$\lor_e$ $1, 5-7, 8-10$
12	$(p \land q) \to (t \lor s)$	$\to_i$ $1-11$

(b) $p \to \neg q, q \vdash p \to r$ (3p)

Solution:

1	$p \to \neg q$	Premise
2	q	Premise
3	p	Assumption
4	$\neg q$	$\to_e$ 1, 3
5	$\bot$	$\neg_e$ 2, 4
6	r	$\bot_e$ 5
7	$p \to r$	$\to_i$ $3-6$

(c) $\vdash (p \vee \neg q) \to (q \to p)$ (3p)

Solution:

1	$p \vee \neg q$	Assumption
2	q	Assumption
3	p	Assumption
4	$\neg q$	Assumption
5	$\bot$	$\neg_e$ 2, 4
6	p	$\bot_e$ 5
7	p	$\vee_e$ 1, 3 − 3, 4 − 6
8	$q \to p$	$\to_i$ 2 − 7
9	$(p \vee \neg q) \to (q \to p)$	$\to_i$ 1 − 8

3. Consider the transition system $\mathcal{M} = (S, \to, L)$ where the states are $S = \{s_0, s_1, s_2, s_3\}$, the transitions are $s_0 \to s_1, s_0 \to s_3, s_1 \to s_2, s_2 \to s_1, s_2 \to s_3, s_3 \to s_3, s_3 \to s_0$, and $s_3 \to s_1$, and the labeling function is given by $L(s_0) = \{c\}, L(s_1) = \{b\}, L(s_2) = \{t, b\}$, and $L(s_3) = \emptyset$.

   (a) Is the LTL-formula $\mathrm{G}(b \to \mathrm{F}\, t)$ satisfied on all paths of the transition system? (2p)

   Solution: Yes! Let π be a path and $i \geq 1$ with $\pi^i \models b$. We show $\pi^i \models \mathrm{F}\, t$. Since $\pi^i \models b$ we get $\pi(i) = s_1$ or $\pi(i) = s_2$. In the first case we must have $\pi(i+1) = s_2$ as s_2 is the only successor of s_1; hence $\pi^{i+1} \models t$ and thus $\pi^i \models \mathrm{F}\, t$. In the second case, we already have $\pi^i \models t$ and hence $\pi^i \models \mathrm{F}\, t$.

   (b) Is the LTL-formula $\mathrm{G}\,\mathrm{F}(\neg b)$ satisfied on all paths of the transition system? (2p)

   Solution: No! Consider the path alternating between s_1 and s_2, $\pi = s_1 \to s_2 \to s_1 \to s_2 \to \ldots$. Here, at any given stage $i \geq 1$, $b \in L(\pi(i))$.

   (c) Which are the states s that satisfy the CTL-formula $\mathrm{E}[\neg c\, \mathrm{U} (b \wedge \neg t)]$ (i.e., where $\mathcal{M}, s \models \mathrm{E}[\neg c\, \mathrm{U} (b \wedge \neg t)]$)? (2p)

   Solution: Let $\varphi = \mathrm{E}[\neg c\, \mathrm{U} (b \wedge \neg t)]$. The state s_0 doesn't satisfy φ since it does neither satisfy $\neg c$ nor $b \wedge \neg t$. Considering s_1, we know $s_1 \models b \wedge \neg t$ and thus we have $s_1 \models \varphi$. For the state s_2 there is the path $\pi = s_2 \to s_1 \to s_2 \to s_1 \to \ldots$ which has $\pi(1) \models \neg c$ and $\pi(2) \models b \wedge \neg t$; hence $s_2 \models \varphi$. Likewise, for the state s_3 there is the path $\pi' = s_3 \to s_1 \to s_2 \to s_1 \to \dots$ which has $\pi'(1) \models \neg c$ and $\pi'(2) \models b \wedge \neg t$; hence $s_3 \models \varphi$.

Hence the states s_1, s_2, and s_3 satisfy φ.

(d) Do we have $\mathcal{M}, s_0 \models \mathrm{AG}(\neg c \to \mathrm{AX}\, b)$? (2p)

Solution: No! Consider the path $\pi = s_0 \to s_3 \to s_3 \to \dots$. We have that $\pi(2) = s_3 \models \neg c$ but s_3 has successors not labeled with b, e.g., s_3 itself.

4. Compute a conjunctive normal form (CNF) of the formula: (3p)

$$\neg r \to (\neg p \wedge (p \to q))$$

Solution: A CNF of the formula is:

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

5. Let P and Q be unary, R a binary, and S a nullary predicate symbols; f is a unary function symbol. Give proofs in natural deduction of the following sequents:

(a) $\vdash \forall x\, ((P(x) \wedge \neg P(f(x))) \to x \neq f(x))$ (3p)

Solution:

1	x_0	
2	$P(x_0) \wedge \neg P(f(x_0))$	Assumption
3	$x_0 = f(x_0)$	Assumption
4	$P(x_0)$	$\wedge_{e_1}$ 2
5	$\neg P(f(x_0))$	$\wedge_{e_2}$ 2
6	$P(f(x_0))$	$=_e$ 3, 4
7	$\bot$	$\neg_e$ 5, 6
8	$x_0 \neq f(x_0)$	$\neg_i$ 3 − 7
9	$(P(x_0) \wedge \neg P(f(x_0))) \to x_0 \neq f(x_0)$	$\to_i$ 2 − 8
10	$\forall x\, ((P(x) \wedge \neg P(f(x))) \to x \neq f(x))$	$\forall_i$ 1 − 9

(b) $\forall x \forall y\,(R(x,y) \to P(x) \lor Q(y)), \exists z\, \neg Q(z) \vdash \exists x\,(R(x,x) \to P(x))$ (3p)

Solution:

1	$\forall x \forall y\,(R(x,y) \to P(x) \lor Q(y))$	Premise
2	$\exists z\, \neg Q(z)$	Premise
3	$z_0 \quad \neg Q(z_0)$	Assumption
4	$\forall y\,(R(z_0,y) \to P(z_0) \lor Q(y))$	$\forall_e$ 1
5	$R(z_0,z_0) \to P(z_0) \lor Q(z_0)$	$\forall_e$ 4
6	$R(z_0,z_0)$	Assumption
7	$P(z_0) \lor Q(z_0)$	$\to_e \; 5, 6$
8	$P(z_0)$	Assumption
9	$Q(z_0)$	Assumption
10	$\bot$	$\neg_e \; 3, 9$
11	$P(z_0)$	$\bot_e$ 10
12	$P(z_0)$	$\lor_e$ $7, 8-8, 9-11$
13	$R(z_0,z_0) \to P(z_0)$	$\to_i \; 5-12$
14	$\exists x\,(R(x,x) \to P(x))$	$\exists_i$ 13
15	$\exists x\,(R(x,x) \to P(x))$	$\exists_e$ $2, 3-14$

(c) $S \to \exists x\, P(x) \vdash \exists x\, (S \to P(x))$ (4p)

Solution:

1	$S \to \exists x\, P(x)$	Premise
2	$S \vee \neg S$	*LEM*
3	S	Assumption
4	$\exists x\, P(x)$	$\to_e$ 1, 3
5	$x_0 \quad P(x_0)$	Assumption
6	S	Assumption
7	$P(x_0)$	copy 5
8	$S \to P(x_0)$	$\to_i$ $6-7$
9	$\exists x\, (S \to P(x))$	$\exists_i$ 8
10	$\exists x\, (S \to P(x))$	$\exists_e$ $4, 5-9$
11	$\neg S$	Assumption
12	S	Assumption
13	$\perp$	$\neg_e$ 11, 12
14	$P(x_0)$	$\perp_e$ 13
15	$S \to P(x_0)$	$\to_i$ $12-14$
16	$\exists x\, (S \to P(x))$	$\exists_i$ 15
17	$\exists x\, (S \to P(x))$	$\vee_e$ $2, 3-10, 11-16$

where $x \neq y$ is $\neg(x = y)$.

6. Let P and Q be unary predicates and R a binary predicate. Decide for each of the sequents below whether they are valid or not, i.e., give a proof in natural deduction or a counter-model.

(a) $(\exists x\, Q(x)) \to (\exists y\, P(y)) \vdash \forall z\, (Q(z) \to P(z))$ (3p)

Solution: This is not valid, a counter-model $\mathcal{M}$ is given by:

- $A = \mathbb{N}$,
- $P^{\mathcal{M}} = \{x \mid x \text{ is even}\}$,
- $Q^{\mathcal{M}} = \{x \mid x \text{ is odd}\}$.

With an arbitrary look-up table l we have $\mathcal{M} \models_l (\exists x\, Q(x)) \to (\exists y\, P(y))$ as there are even and odd numbers, but $\mathcal{M} \not\models_l \forall z\, (Q(z) \to P(z))$ as $1 \in Q^{\mathcal{M}}$ but $1 \notin P^{\mathcal{M}}$. So by *soundness* we get $(\exists x\, Q(x)) \to (\exists y\, P(y)) \nvdash \forall z\, (Q(z) \to P(z))$.

(b) $\forall x\, (f(f(x)) = x) \vdash \forall x\, (f(x) = f(f(x)))$ (3p)

Solution: This is not valid, a counter-model $\mathcal{M}$ is given by:

- $A = \mathbb{Z}$,
- $f^{\mathcal{M}}(x) = -x$.

With an arbitrary look-up table l we have $\mathcal{M} \models_l \forall x\, (f(f(x)) = x)$ as $-(-x) = x$ for all elements in $\mathbb{Z}$. But $\mathcal{M} \not\models_l \forall x\, (f(x) = f(f(x)))$ as for example $-1 \neq 1$. So by *soundness* we get $\forall x\, (f(f(x)) = x) \nvdash \forall x\, (f(x) = f(f(x)))$.

(c) $\forall x \forall y (R(x, y) \to \neg R(y, x)) \vdash \forall x \neg R(x, x)$ (3p)

Solution: This is valid, proof:

1	$\forall x \forall y (R(x, y) \to \neg R(y, x))$	Premise
2	x_0	
3	$\forall y (R(x_0, y) \to \neg R(y, x_0))$	$\forall_e$ 1
4	$R(x_0, x_0) \to \neg R(x_0, x_0)$	$\forall_e$ 1
5	$R(x_0, x_0)$	Assumption
6	$\neg R(x_0, x_0)$	$\to_e$ 4
7	$\bot$	$\neg_e$ 5, 6
8	$\neg R(x_0, x_0)$	$\neg_i$ 5 − 7
9	$\forall x\, \neg R(x, x)$	$\forall_i$ 2 − 8

(d) $\forall x \forall y \forall z\, (R(x, y) \wedge R(y, z) \to R(x, z)), \forall x\, \exists y\, R(x, y) \vdash \forall x\, R(x, x)$ (3p)

Solution: This is not valid, a counter-model $\mathcal{M}$ is given by:

- $A = \mathbb{N}$,
- $R^{\mathcal{M}} = \{(x, y) \mid x < y\}$.

With an arbitrary look-up table l we have $\mathcal{M} \models_l \forall x \forall y \forall z\, (R(x, y) \wedge R(y, z) \to R(x, z))$ as $<$ is transitive and $\mathcal{M} \models_l \forall x\, \exists y\, R(x, y)$ as we can always take $y = x + 1$. But $\mathcal{M} \not\models_l \forall x\, R(x, x)$ as $<$ is not reflexive. So by *soundness* we get $\forall x \forall y \forall z\, (R(x, y) \wedge R(y, z) \to R(x, z)), \forall x\, \exists y\, R(x, y) \nvdash \forall x\, R(x, x)$.

7. A set of connectives is called *adequate* if for every formula of propositional logic there is an equivalent formula using only connectives from this set. Show that, if $C \subseteq \{\neg, \wedge, \vee, \rightarrow, \bot\}$ is adequate, then $\neg \in C$ or $\bot \in C$. (4p)

   Solution: Let C be a subset not containing $\neg$ and $\bot$, and φ a formula constructed using the connectives in C. Consider a valuation v assigning the value $\mathtt{T}$ to all propositional variables in φ, then $v(\varphi) = \mathtt{T}$ as all connectives in φ evaluates to $\mathtt{T}$ for input $\mathtt{T}$. Hence can neither $\neg$ nor $\bot$ be expressed using C, which means that C is not adequate.

8. Is the following LTL-formula valid, i.e., satisfied on all paths of all transition systems? (4p)

$$\mathrm{G}(p \rightarrow \mathrm{F}\,\mathrm{G}\,q) \rightarrow (\mathrm{G}\,\neg p) \vee (\mathrm{F}\,\mathrm{G}\,q)$$

   Solution: Yes it is valid. Let π be a path in a model $\mathcal{M}$ such that $\pi \models \mathrm{G}(p \rightarrow \mathrm{F}\,\mathrm{G}\,q)$ and $\pi \not\models \mathrm{G}\,\neg p$. We now have to show that $\pi \models \mathrm{F}\,\mathrm{G}\,q$. The assumption $\pi \not\models \mathrm{G}\,\neg p$ yields $\pi \models \mathrm{F}\,p$, i.e., there is an $i \geq 1$ with $\pi^i \models p$. By the other assumption we get from this $\pi^i \models \mathrm{F}\,\mathrm{G}\,q$, i.e., $\pi^{i+j} \models \mathrm{G}\,q$ for some $j \geq 0$. Hence we have shown $\pi \models \mathrm{F}\,\mathrm{G}\,q$.

9. Consider propositional atoms $p_1, p_2, \ldots, p_n$ for $n \geq 1$. Define the formula $G = p_1 \wedge p_2 \wedge \cdots \wedge p_n$. Prove that if n is odd, then

$$(p_1 \leftrightarrow p_2) \rightarrow G, (p_2 \leftrightarrow p_3) \rightarrow G, \ldots, (p_{n-1} \leftrightarrow p_n) \rightarrow G, (p_n \leftrightarrow p_1) \rightarrow G \vDash G$$

   where $p_1 \leftrightarrow p_2$ is $(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_1)$ etc. (5p)

   Solution:

   Consider a valuation v that makes all the premises

$$(p_1 \leftrightarrow p_2) \rightarrow G, (p_2 \leftrightarrow p_3) \rightarrow G, \ldots, (p_{n-1} \leftrightarrow p_n) \rightarrow G, (p_n \leftrightarrow p_1) \rightarrow G.$$

   true. Assume $v(G) = \mathtt{F}$. Then by assumption we obtain $v(p_i \leftrightarrow p_{i+1}) = \mathtt{F}$, i.e., v must assign different to values to each consecutive pair (p_i, p_{i+1}). Say v assigns $\mathtt{T}$ to p_1 (the other case is similar), we must then have $v(p_2) = \mathtt{F}$ which means that $v(p_3) = \mathtt{T}$, etc. But as n is odd we will have $v(p_n) = \mathtt{T}$ (as we have flipped the value $n-1$ times), hence $v(p_n \leftrightarrow p_1) = \mathtt{T}$ which implies $v(G) = \mathtt{T}$, a contradiction. Hence $v(G) = \mathtt{T}$.

   Thus we have proved

$$(p_1 \leftrightarrow p_2) \rightarrow G, (p_2 \leftrightarrow p_3) \rightarrow G, \ldots, (p_{n-1} \leftrightarrow p_n) \rightarrow G, (p_n \leftrightarrow p_1) \rightarrow G \vDash G$$