Inst.: Data- och informationsteknik
Kursnamn: Logic in Computer Science
Examinator: Thierry Coquand
Kurs: DIT201/DAT060
Datum: 2018-10-30 No help documents
Telefonvakt: akn. 1030
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. Give proofs in natural deduction of the following sequents:

   (a) (3p) $p \to q, r \to s, p \to r \vdash p \to r \wedge s$

Solution:

1.	$p \to q$	premise
2.	$r \to s$	premise
3.	$p \to r$	premise
4.	p	assumption
5.	r	$\to$e(3,4)
6.	s	$\to$e(2,5)
7.	$r \wedge s$	$\wedge$i(5,6)
8.	$p \to r \wedge s$	$\to$i(4–7)

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

Solution:

1.	$p \vee q$	premise
2.	$p \to \neg s$	premise
3.	s	assumption
4.	p	assumption
5.	$\neg s$	$\to$e(2,4)
6.	$\bot$	$\to$e(5,3)
7.	q	$\bot$e(6,q)
8.	q	assumption
9.	q	$\vee$e(1,4–7,8–8)
10.	$s \to q$	$\to$i(3–9)

(c) (3p) $p \to q \lor r, p \land q \to r \vdash p \to r$

Solution:

1.	$p \to q \lor r$	premise
2.	$p \land q \to r$	premise
3.	p	assumption
4.	$q \lor r$	$\to$e(1,3)
5.	q	assumption
6.	$p \land q$	$\land$i(3,5)
7.	r	$\to$e(2,6)
8.	r	assumption
9.	r	$\lor$e(4,5–7,8–8)
10.	$p \to r$	$\to$i(3–9)

2. 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) (3p) $q \lor p, q \to \neg r \vdash q \lor (p \land \neg r)$

Solution: We give a model for

$$q \lor p, \neg q \lor \neg r, \neg q, \neg p \lor r$$

Define $\mathcal{M}$ as follows

$$A^{\mathcal{M}} = \{0\}$$
$$q^{\mathcal{M}} = \texttt{F}$$
$$p^{\mathcal{M}} = \texttt{T}$$
$$r^{\mathcal{M}} = \texttt{T}$$

(b) (3p) $\forall x \forall y \forall z\, (E(x,z) \land E(y,z) \to E(x,y)) \vdash \forall x \forall y\, (E(x,y) \to E(y,x))$

Solution: Consider the model $\mathcal{M}$ given by

$$A^{\mathcal{M}} = \{0,1\}$$
$$E^{\mathcal{M}} = \{(0,0),(0,1)\}$$

Then $(a,b) \in E^{\mathcal{M}}$ iff $a = 0$. Moreover, if $a = 0$ and $b = 0$, then $a = b$. Hence:

$$\mathcal{M} \models \forall x \forall y \forall z\, (E(x,z) \land E(y,z) \to E(x,y))$$

We have $(0,1) \in E^{\mathcal{M}}$ but $(1,0) \notin E^{\mathcal{M}}$, hence $E^{\mathcal{M}}$ is not symmetric, that is,

$$\mathcal{M} \not\models \forall x \forall y\, (E(x,y) \to E(y,x)).$$

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

Solution:

1.	$\forall x \forall y\, (R(x, y) \to \neg R(y, x))$	premise
2.	z_0	
3.	$R(z_0, z_0)$	assume
4.	$\forall y\, (R(z_0, y) \to \neg R(y, z_0))$	$\forall$e(1,z_0)
5.	$R(z_0, z_0) \to \neg R(z_0, z_0)$	$\forall$e(4,z_0)
6.	$\neg R(z_0, z_0)$	$\to$e(5,3)
7.	$\bot$	$\to$e(6,3)
8.	$\neg R(z_0, z_0)$	$\to$i(3–7)
9.	$\forall z\, \neg R(z, z)$	$\forall$i(2–8,z_0)

(d) (3p) $\forall x \forall y\, (x = y \lor x = f(x)) \vdash \forall x\, x = f(x)$

Solution: We give a natural deduction proof of the sequent.

1.	$\forall x \forall y\, (x = y \lor x = f(x))$	premise
2.	a	
3.	$\forall y\, (a = y \lor a = f(a))$	$\forall$e(1,a)
4.	$a = f(a) \lor a = f(a)$	$\forall$e(3,$f(a)$)
5.	$a = f(a)$	assume
6.	$a = f(a)$	assume
7.	$a = f(a)$	$\lor$e(4,5–5,6–6)
8.	$\forall x\, x = f(x)$	$\forall$i(2–7,a)

3. Give a proof in natural deduction of the following sequents:

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

Solution:

1.		$\forall x\,(P(x) \to \exists y\, R(x,y))$	premise
2.		$\forall x \forall y\,(R(x,y) \to Q(x))$	premise
3.	a		
4.		$P(a) \to \exists y\, R(a,y)$	$\forall$e(1,a)
5.		$\forall y\,(R(a,y) \to Q(a))$	$\forall$e(2,a)
6.		$P(a)$	assume
7.		$\exists y\, R(a,y)$	$\to$e(4,6)
8.	w	$R(a,w)$	assume
9.		$R(a,w) \to Q(a)$	$\forall$e(5,w)
10.		$Q(a)$	$\to$e(9,8)
11.		$Q(a)$	$\exists$e(7,8–10,w)
12.		$P(a) \to Q(a)$	$\to$i(6–11)
13.		$\forall x\,(P(x) \to Q(x))$	$\forall$i(3–12,a)

   (b) (3p) $\forall x\,(P(x) \to \neg M(x)), \exists y\,(M(y) \wedge S(y)) \vdash \exists z\,(S(z) \wedge \neg P(z))$

Solution:

1.		$\forall x\,(P(x) \to \neg M(x))$	premise
2.		$\exists y\,(M(y) \wedge S(y))$	premise
3.	w	$M(w) \wedge S(w)$	assume
4.		$M(w)$	$\wedge$e$_1$(3)
5.		$S(w)$	$\wedge$e$_2$(3)
6.		$P(w) \to \neg M(w)$	$\forall$e(1,w)
7.		$P(w)$	assume
8.		$\neg M(w)$	$\to$e(6,7)
9.		$\bot$	$\to$e(8,4)
10.		$\neg P(w)$	$\to$i(7–9)
11.		$S(w) \wedge \neg P(w)$	$\wedge$i(5,10)
12.		$\exists z\,(S(z) \wedge \neg P(z))$	$\exists$i(11,w)
13.		$\exists z\,(S(z) \wedge \neg P(z))$	$\exists$e(2,3–12,w)

4. Consider the language with one unary predicate symbol P and one unary function symbol f.

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

Solution: A model $\mathcal{M}$ of this language is given by a nonempty set $A^{\mathcal{M}}$, a subset $P^{\mathcal{M}} \subseteq A^{\mathcal{M}}$ and a function $f^{\mathcal{M}} : A^{\mathcal{M}} \to A^{\mathcal{M}}$.

(b) (3p) Explain why the following entailment is valid:

$$\forall x\, (\neg P(x) \to P(f(x))) \models \exists x\, P(x)$$

Solution: Let $\mathcal{M}$ be an arbitrary model with domain A that satisfies

$$\forall x\, (\neg P(x) \to P(f(x))),$$

that is, for all $a \in A$ we have

$$a \notin P^{\mathcal{M}} \text{ implies } f^{\mathcal{M}}(a) \in P^{\mathcal{M}}. \tag{1}$$

Since A is non-empty, there exists $a_0 \in A$. In case $a_0 \in P^{\mathcal{M}}$ we immediately get $\mathcal{M} \models \exists x\, P(x)$. Otherwise, we have $a_0 \notin P^{\mathcal{M}}$, hence by (1) we get $f^{\mathcal{M}}(a_0) \in P^{\mathcal{M}}$, proving $\mathcal{M} \models \exists x\, P(x)$. So in either case $\mathcal{M} \models \exists x\, P(x)$.

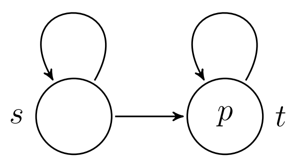
5. (a) (3p) Explain what is a model of LTL/CTL.

Solution: An LTL/CTL model $\mathcal{M}$ consists of a *set of states* S, a binary *transition relation* $\to \subseteq S \times S$ without sinks (for all states $s \in S$ there exists a state $t \in S$ such that $s \to t$, that is s can transition to t) and a *labelling function* $L \colon S \to \mathcal{P}(\mathsf{Atom})$ mapping states $s \in S$ to sets of atoms $L(s)$.

(b) (3p) Give an example of a LTL/CTL model $\mathcal{M}$ where we have $\mathcal{M} \models \mathrm{AG}\,\mathrm{EF}\, p$ in CTL but not $\mathcal{M} \models \mathrm{G}\,\mathrm{F}\, p$ in LTL.

Solution: Define $\mathcal{M}$ as follows:

$$\begin{aligned} S^{\mathcal{M}} &= \{s, t\} \\ \to^{\mathcal{M}} &= \{(s,s), (s,t), (t,t)\} \\ L^{\mathcal{M}}(s) &= \emptyset \\ L^{\mathcal{M}}(t) &= \{p\} \end{aligned}$$



We have that $\mathcal{M}, t \models \mathrm{EF}\, p$ since $\mathcal{M}, t \models p$; moreover $\mathcal{M}, s \models \mathrm{EF}\, p$ since the state t is reachable from s. Thus either state also satisfies $\mathrm{AG}\,\mathrm{EF}\, p$.

But $\pi \not\models \mathrm{G}\,\mathrm{F}\, p$ for $\pi = s \to s \to s \to \dots$ since π never visits the sate t and $p \notin L^{\mathcal{M}}(s)$.

6. (3p) Justify the following implication: if φ and ψ are LTL formulae and $\models \mathrm{G}\,\psi \to \varphi$ then $\models \mathrm{G}\,\psi \to \mathrm{G}\,\varphi$. Recall that $\models \delta$ means that the formula δ is valid on all paths in all LTL models.

> **Solution:** Assume $\pi \models \mathrm{G}\,\psi \to \varphi$ (1) for all paths π in all models $\mathcal{M}$. Let $\sigma \models \mathrm{G}\,\psi$ (2) for some path σ in some model. We show $\sigma \models \mathrm{G}\,\varphi$. So let i be some arbitrary index and we show $\sigma^i \models \varphi$. From (2) we have $\sigma^j \models \psi$ for all indices j, in particular $\sigma^j \models \psi$ for all indices $j \geq i$ and hence $\sigma^i \models \mathrm{G}\,\psi$. From this and (1) we get the claim $\sigma^i \models \varphi$.

7. We consider a language with one function symbol f. We write $f^2(x)$ for $f(f(x))$, $f^3(x)$ for $f(f^2(x))$ and so on. Decide which entailment is valid:

   (a) (3p) $\forall x\, f^2(x) = x \models \forall x\, f(x) = x$

> **Solution:** We give a model $\mathcal{M}$ for
>
> $$\forall x\, f^2(x) = x, \exists x\, f(x) \neq x$$
>
> Define $\mathcal{M}$ as follows:
>
> $$\begin{aligned} A^{\mathcal{M}} &= \{0, 1\} \\ f^{\mathcal{M}}(0) &= 1 \\ f^{\mathcal{M}}(1) &= 0 \end{aligned}$$

   (b) (3p) $\forall x\, f^3(x) = x, \forall x\, f^5(x) = x \models \forall x\, f(x) = x$

> **Solution:** We give a natural deduction proof of the sequent.
>
> | | | |
> |---|---|---|
> | 1. | $\forall x\, f^3(x) = x$ | premise |
> | 2. | $\forall x\, f^5(x) = x$ | premise |
> | 3. | a | |
> | 4. | $f^3(a) = a$ | $\forall$e(1,a) |
> | 5. | $f^5(a) = a$ | $\forall$e(2,a) |
> | 6. | $f^2(a) = a$ | =e(4,5,$f^2(\_) = a$) |
> | 7. | $f(a) = a$ | =e(6,4,$f(\_) = a$) |
> | 8. | $\forall x\, f(x) = x$ | $\forall$i(3–7,a) |
>
> By soundness, the entailment is valid.

8. (4p) Explain why the following entailment is valid:

$$\forall x \exists y\, R(x, y) \models \forall x_1 \forall x_2 \exists y_1 \exists y_2\, (R(x_1, y_1) \wedge R(x_2, y_2) \wedge (x_1 = x_2 \to y_1 = y_2))$$

Solution: We will show that any model $\mathcal{M}$ that satisfies the premise also satisfies the conclusion.

To show that $\mathcal{M}$ satisfies the conclusion we have to show that: $(*)$ for all $a_1, a_2 \in A^{\mathcal{M}}$ there are some $b_1, b_2 \in A^{\mathcal{M}}$ such that $(a_1, b_1) \in R^{\mathcal{M}}$ and $(a_2, b_2) \in R^{\mathcal{M}}$ and if $a_1 = a_2$ then $b_1 = b_2$.

So let $a_1, a_2 \in A^{\mathcal{M}}$ be two arbitrary elements, from $\mathcal{M} \models \forall x \exists y \, R(x, y)$ we know there exists a $b_1 \in A^{\mathcal{M}}$ such that $(a_1, b_1) \in R^{\mathcal{M}}$. Now we have two cases:

- if $a_1 = a_2$ then we also have $(a_2, b_1) \in R^{\mathcal{M}}$, so we can choose $b_2 = b_1$ to satisfy all the conditions in $(*)$;
- if $a_1 \neq a_2$ then we use again that $\mathcal{M} \models \forall x \exists y \, R(x, y)$ to obtain that there is a $b_2 \in A^{\mathcal{M}}$ such that $(a_2, b_2) \in R^{\mathcal{M}}$, and since the implication at the end of the formula has a false premise, this is again sufficient to satisfy the conditions in $(*)$.

9. We consider a language with one relation symbol R. A model $\mathcal{M}$ is given by a nonempty set $A^{\mathcal{M}}$ and an interpretation $R^{\mathcal{M}} \subseteq A^{\mathcal{M}} \times A^{\mathcal{M}}$. We recall that a strict order relation is a model for the two formulae

$$\psi_1 = \forall x \, \neg R(x, x) \qquad \psi_2 = \forall x \forall y \forall z \, (R(x, y) \wedge R(y, z) \to R(x, z))$$

We want to analyse the following condition on models:

W There is no infinite sequence $a_0, a_1, \ldots$ of elements of $A^{\mathcal{M}}$ such that $(a_{n+1}, a_n) \in R^{\mathcal{M}}$ for all $n \in \mathbb{N}$.

(a) (2p) Give one example of a model satisfying this condition **W** and one example of a model not satisfying this condition.

Solution: A model $\mathcal{M}$ satisfying **W** is given by $A^{\mathcal{M}} = \mathbb{N}$ and $R^{\mathcal{M}} = \{(m, n) \mid m < n\}$, as any sequence will eventually reach 0 and will not be able to continue further.
Instead a model $\mathcal{M}'$ that does not satisfy **W** is given by $A^{\mathcal{M}'} = \mathbb{Z}$ and $R^{\mathcal{M}'} = \{(i, j) \mid i < j\}$ because in the integers we can keep finding smaller and smaller elements.

(b) (3p) Explain why any model of ψ_1, ψ_2 where $A^{\mathcal{M}}$ is finite has to satisfy this condition.

Solution: Given a sequence $a_0, a_1, \ldots$ of elements related by $R^{\mathcal{M}}$ as in **W**, we want to show that there cannot be repetitions, because then by finiteness of $A^{\mathcal{M}}$ this sequence must be finite.
Because of $\mathcal{M} \models \psi_2$ we have $(a_{n+k+1}, a_n) \in R^{\mathcal{M}}$ for all $n, k \in \mathbb{N}$. This means that every element of the sequence is related by $R^{\mathcal{M}}$ to all those that come

before. Because of $\mathcal{M} \models \psi_1$ we have that $R^{\mathcal{M}}$ does not relate equal elements, so in conclusion no element of $A^{\mathcal{M}}$ appears twice in the sequence.

(c) (3p) Explain why there is no predicate logic formula ψ_3 such that $\mathcal{M}$ is a model of ψ_1, ψ_2 satisfying the condition **W** if and only if $\mathcal{M}$ is a model of ψ_1, ψ_2 satisfying ψ_3. (Hint: Use the Compactness Theorem)

Solution: We show that if such a formula ψ_3 exists we can reach a contradiction.

Let us define $\Psi = \{\psi_1, \psi_2, \psi_3\}$. Also consider the set of formulas $\Delta = \{R(c_{n+1}, c_n) \mid n \in \mathbb{N}\}$, where each c_n is a new constant for each $n \in \mathbb{N}$. We have that if $\mathcal{M} \models \Delta$ then $\mathcal{M}$ cannot satisfy **W** and hence Ψ, because $c_0^{\mathcal{M}}, c_1^{\mathcal{M}}, \ldots$ is an infinite sequence of elements related by $R^{\mathcal{M}}$.

We derive a contradiction with the paragraph above by showing that there is a model that satisfies $\Psi \cup \Delta$. We do so by the compactness theorem.

To satisfy the premise of the compactness theorem we have to show that every finite subset Γ_0 of $\Psi \cup \Delta$ has a model. If Γ_0 is finite then the set of all mentioned constants $C = \bigcup\{\{c_{n+1}, c_n\} \mid R(c_{n+1}, c_n) \in \Gamma_0, n \in \mathbb{N}\}$ is finite. We create a model $\mathcal{M}$ such that $A^{\mathcal{M}} = C$, $c_n^{\mathcal{M}} = c_n$ and $R^{\mathcal{M}} = \{(c_{n+k+1}, c_n) \mid c_{n+k+1}, c_n \in C, n, k \in \mathbb{N}\}$. Then $\mathcal{M} \models \Gamma_0$ because it models the constants c_n and the relations on them by construction, it models ψ_1 and ψ_2 because $R^{\mathcal{M}}$ can be verified to be a total order on the constants, and it models ψ_3 because $A^{\mathcal{M}}$ is finite and by (b) any model with a finite universe satisfies **W**.

Good Luck!

Simon and Thierry