Inst.: Data- och informationsteknik
Kursnamn: Logic in Computer Science
Examinator: Thierry Coquand
Kurs: DIT201/DAT060
Datum: 2017-10-24 No help documents
Telefonvakt: akn. 1030
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) $p \to (q \land r) \vdash (p \to q) \land (p \to r)$

Solution:

1.	$p \to (q \land r)$	premise
2.	p	assumption
3.	$q \land r$	$\to$e(1,2)
4.	q	$\land$e$_1$(3)
5.	$p \to q$	$\to$i(2–4)
6.	p	assumption
7.	$q \land r$	$\to$e(1,6)
8.	r	$\land$e$_2$(7)
9.	$p \to r$	$\to$i(6–8)
10.	$(p \to q) \land (p \to r)$	$\land$i(5,9)

   (b) (3p) $\neg(p \lor q) \vdash \neg p \land \neg q$

Solution:

1.	$\neg(p \lor q)$	premise
2.	p	assumption
3.	$p \lor q$	$\lor$i$_1$(2)
4.	$\perp$	$\to$e(1,3)
5.	$\neg p$	$\to$i(2–4)
6.	q	assumption
7.	$p \lor q$	$\lor$i$_2$(6)
8.	$\perp$	$\to$e(1,7)
9.	$\neg p$	$\to$i(6–8)
10.	$\neg p \land \neg q$	$\land$i(5,9)

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

Solution:

1.	$p \vee (q \to r)$	premise
2.	$p \vee q$	assumption
3.	p	assumption
4.	$p \vee r$	$\vee i_1(3)$
5.	q	assumption
6.	p	assumption
7.	$p \vee r$	$\vee i_1(6)$
8.	$q \to r$	assumption
9.	r	$\to$e(8,5)
10.	$p \vee r$	$\vee i_2(9)$
11.	$p \vee r$	$\vee$e(1,6–7,8–10)
12.	$p \vee r$	$\vee$e(2,3–4,5–11)
13.	$(p \vee q) \to (p \vee r)$	$\to$i(2–12)

2. Let P, S and M 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) (3p) $\exists x\,(P(x) \wedge \neg M(x)), \exists y\,(M(y) \wedge \neg S(y)) \vdash \exists z\,(P(z) \wedge \neg S(z))$

   Solution: Consider the model $\mathcal{M}$ with universe $A = \{0,1\}$ and $P^{\mathcal{M}} = S^{\mathcal{M}} = \{0\}$ and $M^{\mathcal{M}} = \{1\}$, and l mapping all variables to 0. $\mathcal{M}, l$ satisfies the first premise since $P^{\mathcal{M}} \cap (A - M^{\mathcal{M}}) = \{0\} \neq \emptyset$. Likewise, $\mathcal{M}, l$ satisfies the second premise since $M^{\mathcal{M}} \cap (A - S^{\mathcal{M}}) = \{1\} \neq \emptyset$. But $\mathcal{M}, l$ does *not* satisfy $\exists z\,(P(z) \wedge \neg S(z))$ since $P^{\mathcal{M}} \cap (A - S^{\mathcal{M}}) = P^{\mathcal{M}} \cap (A - P^{\mathcal{M}}) = \emptyset$. By soundness the sequent is thus not valid.

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

   Solution: Consider the model $\mathcal{M}$ with universe $A = \{0,1\}$ and $R^{\mathcal{M}} = \{(0,1),(1,0)\}$. Clearly, $\mathcal{M} \models_l \forall x \neg R(x,x)$ for any look-up function l as $(0,0) \notin R^{\mathcal{M}}$ and $(1,1) \notin R^{\mathcal{M}}$. But $(0,1) \in R^{\mathcal{M}}$ and $(1,0) \in R^{\mathcal{M}}$ so $\mathcal{M} \not\models_l \forall x \forall y\,(R(x,y) \to \neg R(y,x))$. Thus, by the Soundness Theorem, $\forall x \neg R(x,x) \nvdash \forall x\ \forall y\,(R(x,y) \to \neg R(y,x))$.

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

   Solution:

1.	$\forall x\,(M(x) \to \neg P(x))$	premise
2.	$\exists y\,(P(y) \wedge S(y))$	premise
3.	$y_0 \quad P(y_0) \wedge S(y_0)$	assumption
4.	$M(y_0)$	assumption
5.	$M(y_0) \to \neg P(y_0)$	$\forall$e(1,y_0)
6.	$\neg P(y_0)$	$\to$e(5,4)
7.	$P(y_0)$	$\wedge$e$_1$(3)
8.	$\bot$	$\to$e(6,7)
9.	$\neg M(y_0)$	$\to$i(4–8)
10.	$S(y_0)$	$\wedge$e$_2$(3)
11.	$S(y_0) \wedge \neg M(y_0)$	$\wedge$i(10,9)
12.	$\exists z\,(S(z) \wedge \neg M(z))$	$\exists$i(11,y_0)
13.	$\exists z\,(S(z) \wedge \neg M(z))$	$\exists$e(2,3–12)

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

Solution: Consider the model $\mathcal{M}$ with universe $A = \{0\}$ and $R^{\mathcal{M}} = \emptyset$, and look-up function $l(x) = 0$. Since $R^{\mathcal{M}} = \emptyset$, $\mathcal{M} \models_l \forall x\,\forall y\,\forall z\,((R(x,z) \wedge R(y,z)) \to R(x,y))$. Moreover, $(0,0) \notin R^{\mathcal{M}}$, so $\mathcal{M} \not\models_l \forall x\,R(x,x)$. Thus, by soundness, the sequent is not valid.

3. (3p) We fix a language with a relation symbol R. Describe one model which validates simultaneously all the following formulae

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

$$\forall x\,\exists y\,R(x,y) \qquad \exists x\,\forall y\,(R(x,y) \vee x = y)$$

$$\forall x\,\forall y\,(R(x,y) \to \exists z\,(R(x,z) \wedge R(z,y)))$$

Solution: Consider the relation $<$ on the set of non-negative rational numbers $\mathbb{Q} \cap [0,+\infty)$: it is strict, transitive, it is dense (since $a < \frac{a+b}{2} < b$ for $a < b$ in $\mathbb{Q}$) and satisfies $a < a+1$ for $a \in \mathbb{Q}$. Moreover it has a least element 0.

4. (a) (3p) Explain what is a model of CTL.

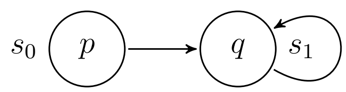
Solution: A CTL model $\mathcal{M}$ consists of a *set of states* S, a binary *transition relation* $\to\, \subseteq S \times S$ without sinks (for all states $s \in S$ there exists a state $t \in S$ such that $s \to t$, that is s can transition to t) and a *labelling function* $L\colon S \to \mathcal{P}(\mathsf{Atom})$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

(b) (3p) Explain why the following CTL formula is valid $(AG\,((q \to p) \wedge (q \to EX\,q))) \to (q \to EG\,p)$.

Solution: Let $\mathcal{M} = (S, \to, L)$ be a CTL model and $s \in S$ a state satisfying both $\mathrm{AG}\,((q \to p) \wedge (q \to \mathrm{EX}\;q))$ and q. We show that s satisfies $\mathrm{EG}\;p$ by recursively constructing a path π which starts in s and satisfies q globally because then, by assumption, π also satisfies $q \to p$ and in particular p globally. Let $i \in \mathbb{N}$ be an index. If $i = 0$, then we define $\pi(i)$ to be s and, by assumption, $\pi(i)$ satisfies q. If $i = j + 1$ for some index $j \in \mathbb{N}$, then, by induction hypothesis, $\pi(j)$ is a state which satisfies q and, by assumption, there exists a state t with a transition from $\pi(j)$ which satisfies q. We define $\pi(i)$ to be t.

5. (a) (2p) Explain why the following LTL formula is *not* valid $G(p \to q) \vee G(q \to p)$

Solution: We give a counterexample. In the following model



the state s_0 does not satisfy $p \to q$ and the state s_1 does not satisfy $q \to p$. Therefore, the path $\pi = (s_0, s_1, s_1, s_1, \ldots)$ does neither satisfy $p \to q$ nor $q \to p$ globally, which means that there exists a path which does not satisfy $\mathrm{G}\,(p \to q) \vee \mathrm{G}\,(q \to p)$.

(b) (2p) Does the same hold for the formula $G((p \to q) \vee (q \to p))$?

Solution: No. The formula $(p \to q) \vee (q \to p)$ is propositionally valid and thus $\mathrm{G}\,((p \to q) \vee (q \to p))$ is a law of LTL.

6. Given $W = (\forall x\, R(x,x)) \to \forall x \forall y \forall z\, (R(x,y) \vee R(y,z) \vee R(z,x))$, explain why

(a) (3p) the formula W is valid in any model with a domain/universe having at most 2 elements

Solution: Let $\mathcal{M}$ be a model with universe A with $\#A \leq 2$ and $R^{\mathcal{M}} \supseteq \{(x,x) | x \in A\}$, l a lookup table and $x_0, y_0, z_0 \in A$ arbitrary elements of the domain. Then, by the first assumption and the pigeonhole principle, at least two of the three elements must be identical and, by the second assumption, these two elements are related by $R^{\mathcal{M}}$ so that $\mathcal{M} \models_{l[x \mapsto x_0, y \mapsto y_0, z \mapsto z_0]} R(x,y) \vee R(y,z) \vee R(z,x)$. Since the elements x_0, y_0, and z_0 were arbitrary, $\mathcal{M}$ and l satisfy W.

(b) (3p) the formula W is *not* valid in general

Solution: We give a counterexample $\mathcal{M}$, l. Let a, b, and c be three pairwise distinct elements, and take l to be the constant function mapping all variables to a, the universe to be the set $\{a, b, c\}$ and $R^{\mathcal{M}}$ to be the identity relation, that is $\{(a, a), (b, b), (c, c)\}$. Then, the elements a, b, c are also pairwise unrelated so that $\mathcal{M} \models_{l[x \mapsto a, y \mapsto b, z \mapsto c]} \neg R(x, y) \wedge \neg R(y, z) \wedge \neg R(z, x)$ and because $\mathcal{M} \models_l \forall x\, R(x, x)$ the formula W is not satisfied by $\mathcal{M}$ and l.

7. (4p) We suppose given 8 atomic propositions A, B, C, D, E, F, G, H. We know that exactly one of A, B, C, D and exactly one of E, F, G, H is true. We also know the following

   1. $A \vee E \vee G$
   2. $A \vee B \vee F$
   3. $B \vee C \vee G$
   4. $C \vee E \vee F$

   Which of A, B, C, D and of E, F, G, H is true (and why)?

Solution: If A is true, then B,C, and D are false, so G and $E \vee F$ need to be true, which contradicts the assumption that exactly one of E, F, G, H is true. So A must be false and we know

$$E \vee G, B \vee F, B \vee C \vee G, C \vee E \vee F \qquad \neg A$$

If G is true, then E and F are false, so B and C need to be true, which contradicts the assumption that exactly one of A, B, C, D is true. So G must be false and we know

$$E, B \vee F, B \vee C, C \vee E \vee F \qquad \neg A, \neg G$$

So E must be true and, by the second assumption, also F and H must be false and we know

$$B, B \vee C \qquad \neg A, E, \neg F, \neg G, \neg H$$

So B must be true and, by the first assumption, also C and D must be false and we know

$$\neg A, B, \neg C, \neg D, E, \neg F, \neg G, \neg H$$

So assigning true to exactly B and E is the only possible satisfying valuation, and it is indeed a satisfying valuation.

8. (5p) Let ψ be a predicate logic formula. We assume that for any natural number n, the formula ψ has a model with a domain/universe with more than n elements. Explain why the formula ψ should have a model with an *infinite* domain/universe.

> **Solution:** By assumption, there is a family of models $\mathcal{M}_n$ indexed by $n \geq 1$ such that the universe of $\mathcal{M}_n$ has at least n elements and $\mathcal{M}_n \models \psi$. For each $n \geq 1$, we define φ_n to be the formula $\exists x_1 \ldots \exists x_n \left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j\right)$. The models of φ_n are exactly those with at least n elements, so that the models of $\Phi = \{\varphi_n | n \geq 1\}$ are exactly those with an infinite domain/universe.
>
> We show that ψ has a model with an infinite domain/universe by showing that $\Gamma = \{\psi\} \cup \Phi$ has a model. We apply the Compactness Theorem to show that Γ has a model. Let Γ_0 be a finite subset of Γ, then $\Phi_0 = \Gamma_0 \cap \Phi$ is a finite subset of Φ and Γ_0 is contained in $\{\psi\} \cup \Phi_0$. Γ_0 is satisfied by $\mathcal{M}_m$ where $m \geq 1$ is the maximum of all n with $\varphi_n \in \Phi_0$ (or 1 if Φ_0 is empty), because $\mathcal{M}_m$ is a model of ψ by assumption and of Φ_0 by our earlier remark.

9. Explain why the following LTL formulae are valid, i.e., satisfied on all paths of all transition systems

   (a) (3p) $(\mathrm{F}\, p \wedge \mathrm{F}\, q) \to ((\mathrm{F}(p \wedge \mathrm{F}\, q)) \vee \mathrm{F}(q \wedge \mathrm{F}\, p))$

   > **Solution:** Let π be an arbitrary path satisfying $\mathrm{F}\ p \wedge \mathrm{F}\ q$, that is there exist indices $i, j \in \mathbb{N}$ such that $\pi(i)$ satisfies p and $\pi(j)$ satisfies q. It is either the case that $i \leq j$ or that $i > j$. If $i \leq j$, then π^i also satisfies $\mathrm{F}\ q$ so that π actually satisfies $\mathrm{F}\,(p \wedge \mathrm{F}\ q)$. If $i > j$, then π^j also satisfies $\mathrm{F}\ p$ so that π actually satisfies $\mathrm{F}\,(q \wedge \mathrm{F}\ p)$. In either case, π satisfies $\mathrm{F}\,(p \wedge \mathrm{F}\ q) \vee \mathrm{F}\,(q \wedge \mathrm{F}\ p)$ and since π was arbitrary, the formula is a law.

   (b) (3p) $\mathrm{F}(p \to \mathrm{X}\, p)$

   > **Solution:** Let π be an arbitrary path. It is either the case that $\pi(1)$ satisfies p or not. If $\pi(1)$ satisfies p, then π^0 satisfies $\mathrm{X}\ p$ and in particular $p \to \mathrm{X}\ p$ and $\mathrm{F}\,(p \to \mathrm{X}\ p)$. If $\pi(1)$ does not satisfy p, then π^1 in particular satisfies $p \to \mathrm{X}\ p$ and π^0 in particular satisfies $\mathrm{F}\,(p \to \mathrm{X}\ p)$. Since π was arbitrary, the formula is a law.

10. (5p) Let $R(x, y)$ and $S(x, y)$ be two relation symbols. We define ψ_1 to be

$$\forall x\, \forall y\, \forall z\, ((R(x, y) \wedge R(y, z)) \to R(x, z))$$

and ψ_2 to be

$$\forall x\, \forall y\, \forall z\, ((R(x, y) \wedge R(x, z)) \to S(y, z))$$

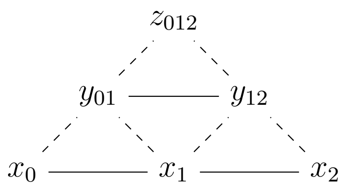
and ψ_3 to be

$$\forall x\, \forall y\, (S(x, y) \leftrightarrow \exists z\, (R(x, z) \wedge R(y, z)))$$

where $p \leftrightarrow q$ means $(p \to q) \wedge (q \to p)$

Show that $\psi_1, \psi_2, \psi_3 \models \forall x\, \forall y\, \forall z\, ((S(x, y) \wedge S(y, z)) \to S(x, z))$

Solution: Let $\mathcal{M}$ be a model satisfying ψ_1, ψ_2, ψ_3 and $x_0, x_1, x_2 \in A$ elements such that $(x_0, x_1), (x_1, x_2) \in S^{\mathcal{M}}$. By the third assumption, there exist elements $y_{01}, y_{12} \in A$ such that $(x_0, y_{01}), (x_1, y_{01}), (x_1, y_{12}), (x_2, y_{12}) \in R^{\mathcal{M}}$. Then, by the second assumption we have that $(y_{01}, y_{12}) \in S^{\mathcal{M}}$. Again, by the third assumption, there exists an element $z_{012} \in A$ such that $(y_{01}, z_{012}), (y_{12}, z_{012}) \in R^{\mathcal{M}}$. Lastly, by the first and third assumption, we have $(x_0, z_{012}), (x_2, z_{012}) \in R^{\mathcal{M}}$ and then $(x_0, x_2) \in S^{\mathcal{M}}$. Graphically,



Since x_0, x_1, and x_2 were arbitrary, $\mathcal{M}$ satisfies $\forall x\, \forall y\, \forall z\, (S(x, y) \wedge S(y, z) \to S(x, z))$.

Good Luck!

Jan and Thierry