Logic in Computer Science

DAT060/DIT201 (7.5 hec)

Responsible: Thierry Coquand – Telefon: 1030

Tuesday 29th of October 2019

Total: 60 points	
CTH: $\geqslant 30$: 3, $\geqslant 41$: 4, $\geqslant 51$: 5	GU: $\geqslant$30: G, $\geqslant$46: VG

No help material but dictionaries to/from English.

Write in English and as readable as possible (think that what we cannot read we cannot correct).

OBS: All answers should be *carefully* motivated. Points will be deduced when you give an unnecessarily complicated solution or when you do not properly justify your answer.

Good luck!

---

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

   (a) (2pts) $(p \to r) \wedge (q \to s) \vdash p \wedge q \to r \wedge s$

   Solution:

1.	$(p \to r) \wedge (q \to s)$	premise
2.	$p \to r$	$\wedge e_1$ 1
3.	$q \to s$	$\wedge e_2$ 1
4.	$p \wedge q$	assumption
5.	p	$\wedge e_1$ 4
6.	q	$\wedge e_2$ 4
7.	r	$\to e$ (2,5)
8.	s	$\to e$ (3,6)
9.	$r \wedge s$	$\wedge i$ (7,8)
10.	$p \wedge q \to r \wedge s$	$\to i$ 4–9

   (b) (2.5pts) $\neg r \to (s \wedge p), s \to q, \neg q \vdash r$

   Solution:

1.	$\neg r \to (s \wedge p)$	premise
2.	$s \to q$	premise
3.	$\neg q$	premise
4.	$\neg s$	MT (2,3)
5.	$s \wedge p$	assumption
6.	s	$\wedge e_1$ 5
7.	$\perp$	$\to$e (4,6)
8.	$\neg(s \wedge p)$	$\to$i 5–7
9.	$\neg\neg r$	MT (1,8)
10.	r	$\neg\neg$e 9

(c) (2.5pts) $\neg p \to r, r \to s \vdash s \vee p$

Solution:

1.	$\neg p \to r$	premise
2.	$r \to s$	premise
3.	$p \vee \neg p$	LEM
4.	p	assumption
5.	$s \vee p$	$\vee i_2$ 4
6.	$\neg p$	assumption
7.	r	$\to$e (1,6)
8.	s	$\to$e (2,7)
9.	$s \vee p$	$\vee i_1$ 8
10.	$s \vee p$	$\vee$e (3,4–5,6–9)

2. (a) (1pt) Without using truth tables, give a valuation for which the formula

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

is not true.

(b) (2pts) Explain how you arrived to this valuation.

Solution:

(a) p should be true, and q and r should be false.

(b) For the formula to be false it should be that $((p \to q) \to q) \to ((r \to q) \to p)$ is true and $((p \to r) \to q) \to q$ is false.

For $((p \to r) \to q) \to q$ to be false then $(p \to r) \to q$ should be true and q should be false.

For $(p \to r) \to q$ to be true when q is false then $p \to r$ should be false which give us p true and r false.

With this valuation we need to check that $((p \to q) \to q) \to ((r \to q) \to p)$ is true, which is indeed the case since $(p \to q) \to q$ is true (false implies false is true) and $(r \to q) \to p$ is also true (true implies true is true).

3. For each of the sequents below, prove using natural deduction that they are valid, or give a counter-model that they are not.

   (a) (3pts) $\vdash \forall x \forall y \forall z (f(x, z) = f(x, y) \to y = z)$

   Solution: We will give a counter-model $\mathcal{M}$.
   In $\mathcal{M}$, let $A = \mathbb{N}$ and $f^{\mathcal{M}} : A \times A \to A$ be such that $f^{\mathcal{M}}(u, v) = u$.
   Here, we have that $f^{\mathcal{M}}(0, 1) = f^{\mathcal{M}}(0, 2) = 0$ but $2 \neq 1$.
   Hence $\mathcal{M} \not\models \forall x \forall y \forall z (f(x, z) = f(x, y) \to y = z)$ and by soundness $\not\vdash \forall x \forall y \forall z (f(x, z) = f(x, y) \to y = z)$.

   (b) (3pts) $\vdash \forall x \forall y \forall z (y = z \to f(x, z) = f(x, y))$

   Solution:

1.	x_0	fresh
2.	y_0	fresh
3.	z_0	fresh
4.	$y_0 = z_0$	assumption
5.	$f(x_0, z_0) = f(x_0, y_0)$	=e with 5, $\phi(u) \equiv f(x_0, u) = f(x_0, y_0)$
6.	$y_0 = z_0 \to f(x_0, z_0) = f(x_0, y_0)$	$\to$i 4–5
7.	$\forall z (y_0 = z \to f(x_0, z) = f(x_0, y_0))$	$\forall$i 3–6
8.	$\forall y \forall z (y = z \to f(x_0, z) = f(x_0, y))$	$\forall$i 2–7
9.	$\forall x \forall y \forall z (y = z \to f(x, z) = f(x, y))$	$\forall$i 1–8

   (c) (3pts) $\vdash \neg \forall x \neg A(x) \to \neg\neg \exists x A(x)$

   Solution:

1.	$\neg\forall x \neg A(x)$	premise
2.	$\neg\exists x A(x)$	assumption
3.	x_0	fresh
4.	$A(x_0)$	assumption
5.	$\exists x A(x)$	$\exists$i 4
6.	$\bot$	$\to$e (2,5)
7.	$\neg A(x_0)$	$\to$i 4–6
8.	$\forall x \neg A(x)$	$\forall$i 3–7
9.	$\bot$	$\to$e (1,8)
10.	$\neg\neg\exists x A(x)$	$\to$i (2,9)

(d) (3pts) $\vdash \exists x P(x) \wedge \exists x(P(x) \to Q(x)) \to \exists x Q(x)$

Solution: We will give a counter-model $\mathcal{M}$.
In $\mathcal{M}$, let $A = \{0, 1\}, P^{\mathcal{M}} = \{0\}$ and $Q^{\mathcal{M}} = \emptyset$.
We have that $\mathcal{M} \models \exists x P(x)$ and $\mathcal{M} \models \exists x(P(x) \to Q(x))$ hold because $0 \in P^{\mathcal{M}}$ and $1 \notin P^{\mathcal{M}}$. However, $\mathcal{M} \not\models \exists x Q(x)$ since $Q^{\mathcal{M}} = \emptyset$.
Hence $\mathcal{M} \not\models \exists x P(x) \wedge \exists x(P(x) \to Q(x)) \to \exists x Q(x)$ and by soundness $\not\vdash \exists x P(x) \wedge \exists x(P(x) \to Q(x)) \to \exists x Q(x)$.

(e) (4pts) $\forall x \neg\forall y(P(x, y) \to Q(x, y)) \vdash \forall x \neg\forall y \neg P(x, y)$

Solution:

1.	$\forall x \neg\forall y(P(x, y) \to Q(x, y))$	premise
2.	x_0	fresh
3.	$\neg\forall y(P(x_0, y) \to Q(x_0, y))$	$\forall$e 1
4.	$\forall y \neg P(x_0, y)$	assumption
5.	y_0	fresh
6.	$\neg P(x_0, y_0)$	$\forall$e 4
7.	$P(x_0, y_0)$	assumption
8.	$\bot$	$\to$e (6,7)
9.	$Q(x_0, y_0)$	$\bot$e
10.	$P(x_0, y_0) \to Q(x_0, y_0)$	$\to$i 7–9
11.	$\forall y(P(x_0, y) \to Q(x_0, y))$	$\forall$i 5–10
12.	$\bot$	$\to$e (3,11)
13.	$\neg\forall y \neg P(x_0, y)$	$\to$i 4–12
14.	$\forall x \neg\forall y \neg P(x, y)$	$\forall$i 2–13

4. Consider the following semantic entailment
$\forall x(Q(x) \to \exists y R(x,y)) \land \forall x \forall y(R(x,y) \to P(x)) \models \forall x(Q(x) \to P(x))$

   (a) (2pts) What is a model for the language?

   Solution: A model $\mathcal{M}$ for the language consists in a domain $\mathcal{A} \neq \emptyset$, two unary relations $Q^{\mathcal{M}}, P^{\mathcal{M}} \subseteq \mathcal{A}$ and a binary relation $R^{\mathcal{M}} \subseteq \mathcal{A} \times \mathcal{A}$.

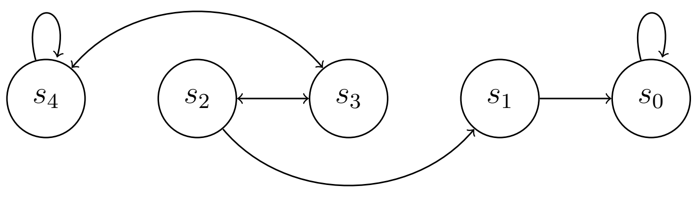
   (b) (3.5pts) Explain if the semantic entailment is valid.

   Solution: The semantic entailment is valid.
   Consider a model $\mathcal{M}$ with domain $\mathcal{A}$ such that $\mathcal{M} \models \forall x(Q(x) \to \exists y R(x,y))$ and $\mathcal{M} \models \forall x \forall y(R(x,y) \to P(x))$. We need to show that $\mathcal{M} \models \forall x(Q(x) \to P(x))$.
   Let $a \in \mathcal{A}$ such that $a \in Q^{\mathcal{M}}$. We need to show that $a \in P^{\mathcal{M}}$.
   Now, since $a \in Q^{\mathcal{M}}$ and $M \models \forall x(Q(x) \to \exists y R(x,y))$ then there is $b \in \mathcal{A}$ such that $(a,b) \in R^{\mathcal{M}}$.
   Now, since $M \models \forall x \forall y(R(x,y) \to P(x))$ and $(a,b) \in R^{\mathcal{M}}$ then we must have $a \in P^{\mathcal{M}}$, which ends our poof.

5. (3.5pts) Explain if the following semantic entailment is valid
$\models \forall x \forall y(R(x,y) \land \neg(x=y) \to \exists z(R(x,z) \land R(z,y) \land \neg(x=z) \land \neg(y=z)))$

   Solution: This semantic entailment is not valid.
   Consider a model $\mathcal{M}$ with domain $\mathcal{A} = \{2,3\}$ and the binary relation
   $R^{\mathcal{M}} = \{(2,3),(3,2)\} \subseteq \mathcal{A} \times \mathcal{A}$.
   Here, for any a and b in $\mathcal{A}$ such that $\neg(a=b)$, we have that $(a,b) \in R^{\mathcal{M}}$.
   On other hand, there is no element c such that $\neg(a=c)$ and $\neg(b=c)$.
   Hence for any $a,b \in \mathcal{A}$, $\mathcal{M} \models_{[x \mapsto a, y \mapsto b]} R(x,y) \land \neg(x=y)$ but
   $\mathcal{M} \not\models_{[x \mapsto a, y \mapsto b]} \exists z(R(x,z) \land R(z,y) \land \neg(x=z) \land \neg(y=z))$.
   This concludes that
   $\mathcal{M} \not\models \forall x \forall y(R(x,y) \land \neg(x=y) \to \exists z(R(x,z) \land R(z,y) \land \neg(x=z) \land \neg(y=z)))$

6. Consider the transition system $\mathcal{M} = (S, \to, L)$ where the states are $S = \{s_0, s_1, s_2, s_3, s_4\}$, the transitions are $s_0 \to s_0$, $s_1 \to s_0$, $s_2 \to s_1$, $s_2 \to s_3$, $s_3 \to s_2$, $s_3 \to s_4$, $s_4 \to s_3$, $s_4 \to s_4$, and the labeling function is given by $L(s_0) = L(s_4) = \{p\}$, $L(s_1) = L(s_3) = \{q\}$, and $L(s_2) = \emptyset$.



   (a) (3pts) Do we have $\mathcal{M} \models G(Fp)$?

(b) (3pts) Which are the states s that satisfy the CTL formula $AG(q \to AFp)$ (i.e., where $\mathcal{M}, s \models AG(q \to AFp)$)?

Solution:

(a) We do not have $\mathcal{M} \models G(Fp)$ since there is the path $\sigma = s_2 \to s_3 \to s_2 \ldots$ such that $\sigma \models G(\neg p)$

(b) s_4, s_3 and s_2 do not satisfy this property because of the previous path σ. Both s_1 and s_0 this property since we have only one path starting from s_1 (resp. s_0) and we can directly check the property for this path.

7. (a) (4pts) Explain why the following LTL formula is valid $(Fp \wedge Fq \wedge G(q \to G(\neg p))) \to F(p \wedge XFq)$.

(b) (4pts) Explain why the following LTL formula is *not* valid $(G(p \to Fp) \wedge p) \to Gp$.

Solution:

(a) This formula is valid since for any model and any path σ if we have $\sigma \models Fp \wedge Fq \wedge G(q \to G(\neg p))$ then $p \in L(\sigma(n))$ and $q \in L(\sigma(m))$ for some n and m. Since $\sigma \models G(q \to G(\neg p))$ we have $n < m$ and then $\sigma^n \models p \wedge XFq$ and some $\sigma \models F(p \wedge XFq)$.

(b) We define a model with two states s_0 and s_1 and $s_0 \to s_1$ and $s_1 \to s_1$ and $L(s_0) = \{p\}$ and $L(s_1) = \emptyset$. The path $\sigma = a_0 \to s_1 \to s_1 \ldots$ satisfies then $\sigma \models G(p \to Fp) \wedge p$ and $\sigma \models \neg(Gp)$.

8. (3pts) Let S be a set and A, B two subsets of S. Let F be the monotone function $F : Pow(S) \to Pow(S),\ X \mapsto (X \cup A) \cap B$ What are the least fix point and the greatest fix point of F?

Solution: If $F(X) = X$ then we have $X \subseteq B$. We also have $F(B) = B$ so B is the greatest fix point of F. Also $F(\emptyset) = A \cap B$ and $F(A \cap B) = A \cap B$ so $A \cap B$ is the least fix point of F.

9. Make sure to justify your answers below!

(a) (2pts) Give a CTL model where the formula $AG((EF\ p) \wedge EF(\neg p))$ is valid.

(b) (2pts) Give a model where the formula $EF\ p \to AG(EF\ p)$ is *not* valid.

Solution:

(a) We define a model with two states s_0 and s_1 and $s_0 \to s_1$ and $s_1 \to s_0$ and $L(s_0) = \{p\}$ and $L(s_1) = \emptyset$. For this model M we $M, s_0 \models (EF\ p) \wedge EF(\neg p)$ and $M, s_1 \models (EF\ p) \wedge EF(\neg p)$, so M is a model of $AG((EF\ p) \wedge EF(\neg p))$ is

(b) We build a model M and a state s where $EF\ p$ is valid but $AG(EF\ p)$ is not valid. We take a model with two states s_0 and s_1 and $s_0 \to s_1$ and $s_1 \to s_1$ and $L(s_0) = \{p\}$ and $L(s_1) = \emptyset$. We have then $M, s_0 \models EF\ p$ and $s_0 \to s_1$ and $M, s_1 \models \neg(EF\ p)$. So we have $M, s_0 \models \neg(AG(EF\ p))$.

10. (4pts) Suppose that Γ is a set of formulae in a given language with a binary relation R such that for any natural number $n \geq 0$, Γ has a model M whose domains contains elements $a_0, a_1, \ldots, a_n$ such that $(a_i, a_{i+1}) \in R^M$ for $i = 0, \ldots, n-1$. Show that Γ has a model whose domain contains an infinite sequence $a_0, a_1, \ldots$ satisfying $(a_n, a_{n+1}) \in R^M$ for all n.

Solution: We use the Compactness Theorem. We add infinitely many constant $c_0,\ c_1,\ c_2, \ldots$ and consider the theory

$$\Gamma,\ R(c_0, c_1),\ R(c_1, c_2),\ \ldots$$

By hypothesis any finite subset of this theory is satisfiable. By Compactness, this theory is satisfiable and a model M of this theory has a domain which contains an infinite sequence $a_0 = c_0^M, ,\ a_1 = c_1^M, \ldots$ satisfying $(a_n, a_{n+1}) \in R^M$ for all n.