Logic in Computer Science

DAT060/DIT202/DIT201 (7.5 hec)

Responsible: Thierry Coquand – Telefon: 1030

Tuesday 27th of October 2020, 14:00–18:00

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

Write in English and as readable as possible; make sure the uploaded file is visible/readable (think that what we cannot read we cannot correct).

OBS: All answers should be *carefully* motivated.
Points will be deduced when you do not properly justify your answer.

Good luck!

---

1. (2pts) Give proofs in natural deduction of the following sequent:

$$r \to (p \vee q), \neg(r \wedge q) \vdash r \to p$$

Solution:

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

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

$$(s \vee q \to p \wedge r) \vee (p \to q \wedge r)$$

is not true.

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

Solution:

(a) At least one of s and q should be true, p should be true and r should be false.

(b) For the formula to be false it should be that both $(s \vee q \to p \wedge r)$ and $(p \to q \wedge r)$ are false.

For $(s \vee q \to p \wedge r)$ to be false then $s \vee q$ should be true and $p \wedge r$ should be false. This gives us that at least one of s and q should be true (*), and at least one of p and r should be false (**).

For $(p \to q \wedge r)$ to be false then p should be true and $q \wedge r$ should be false, which give us that at least one of q and r should be false.

Since p is true then r should be false because of (**).

There are no more constrains so it is enough that at least one of s and q should be true because of (*) for the formula to be false.

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

(a) (2.5pts) $P(b) \wedge Q(b), \forall x.(P(x) \to x = a) \vdash Q(a)$

Solution:

1.	$P(b) \wedge Q(b)$	premise
2.	$\forall x.(P(x) \to x = a)$	premise
3.	$P(b) \to b = a$	$\forall$e b
4.	$P(b)$	$\wedge e_1$ 1
5.	$b = a$	$\to$e (3,4)
6.	$Q(b)$	$\wedge e_1$ 1
7.	$Q(a)$	=e with 5, $\phi(u) \equiv Q(u)$

(b) (2.5pts) $\forall x.\forall y.(P(x, y) \to Q(x, y)), \forall x.Q(x, x) \vdash \forall x.P(x, x)$

Solution:
We will give a counter-model $\mathcal{M}$.
In $\mathcal{M}$, let $A = \mathbb{N}$, $P^{\mathcal{M}} \subset \mathbb{N} \times \mathbb{N}$ be such that $x^2 = y$ in $\mathbb{N}$ and $Q^{\mathcal{M}} \subset \mathbb{N} \times \mathbb{N}$ be such that $x \leqslant y$.
Here, for any $a, b \in \mathbb{N}$ we have that whenever $a^2 = b$ then $a \leqslant b$.
Also, we know that $a \leqslant a$ for all $a \in \mathbb{N}$.

Hence both premises are valid in this model.
On the other hand it is not the case that $a^2 = a$ for all $a \in \mathbb{N}$.

(c) (3pts) $\forall x.(\forall y.P(x,y) \lor \forall y.Q(x,y)) \vdash \forall x.\exists y.(P(x,y) \lor Q(x,y))$

Solution:

1.	$\forall x.(\forall y.P(x,y) \lor \forall y.Q(x,y))$	premise
2.	x_0	fresh
3.	$\forall y.P(x_0,y) \lor \forall y.Q(x_0,y)$	$\forall$e 1 with x_0
4.	$\forall y.P(x_0,y)$	assumption
5.	y_0	fresh
6.	$P(x_0,y_0)$	$\forall$e 3 with y_0
7.	$P(x_0,y_0) \lor Q(x_0,y_0)$	$\lor$i$_1$ 6
8.	$\exists y.(P(x_0,y) \lor Q(x_0,y))$	$\exists$i 7
9.	$\forall y.Q(x_0,y)$	assumption
10.	y_0	fresh
11.	$Q(x_0,y_0)$	$\forall$e 3 with y_0
12.	$P(x_0,y_0) \lor Q(x_0,y_0)$	$\lor$i$_2$ 11
13.	$\exists y.(P(x_0,y) \lor Q(x_0,y))$	$\exists$i 12
14.	$\exists y.(P(x_0,y) \lor Q(x_0,y))$	$\lor$e (3,4–8,9–13)
15.	$\forall x.\exists y.(P(x,y) \lor Q(x,y))$	$\forall$i 2–14

(d) (3pts)
$\forall x.\exists y.(P(x,y) \to R(x,y)), \exists x.\forall y.(P(x,y) \to R(x,y)) \vdash \forall x.\forall y.(P(x,y) \land R(x,y))$

Solution:
We will give a counter-model $\mathcal{M}$.
In $\mathcal{M}$, let $A = \{1,2\}$, $P^{\mathcal{M}} = R^{\mathcal{M}} = \{(1,1),(1,2),(2,2)\}$.
We have that $\mathcal{M} \models \forall x.\exists y.(P(x,y) \to R(x,y))$ and
$\mathcal{M} \models \exists x.\forall y.(P(x,y) \to R(x,y))$ hold.
However, $\mathcal{M} \not\models \forall x.\forall y.(P(x,y) \land R(x,y))$ since $(2,1) \notin P^{\mathcal{M}} = R^{\mathcal{M}}$.

(e) (3pts) $\exists x.(P(x) \land Q(x)), \neg\exists x.(Q(x) \land R(x)) \vdash \exists x.(P(x) \land \neg R(x))$

Solution:

1.	$\exists x.(P(x) \wedge Q(x))$	premise
2.	$\neg\exists x.(Q(x) \wedge R(x))$	premise
3.	x_0	fresh
4.	$P(x_0) \wedge Q(x_0)$	assumption
5.	$P(x_0)$	$\wedge e_1$ 4
6.	$Q(x_0)$	$\wedge e_2$ 4
7.	$R(x_0)$	assumption
8.	$Q(x_0) \wedge R(x_0)$	$\wedge$i (6,7)
9.	$\exists x.(Q(x) \wedge R(x))$	$\exists$i 8
10.	$\bot$	$\neg$e (2,9)
11.	$\neg R(x_0)$	$\neg$i 7–10
12.	$P(x_0) \wedge \neg R(x_0)$	$\wedge$i (5,11)
13.	$\exists x.(P(x) \wedge \neg R(x))$	$\exists$i 12
14.	$\exists x.(P(x) \wedge \neg R(x))$	$\exists$e (1, 3–13)

4. Consider the following semantic entailments:

   i) $\exists x.\forall y.x = y \models \forall x.\forall y.x = y$

   ii) $\forall x.(P(x) \to \exists x.R(x)) \models \exists x.(P(x) \to R(x))$

   iii) $\exists x.(P(x) \to R(x)), \exists x.(R(x) \to P(x)) \models \exists x.(P(x) \wedge R(x))$

   (a) (1.5 pts) What is a model for the language of these entailments?

   (b) (2.5+3.5 + 2.5 pts) Explain semantically (that is, reasoning with models) whether these entailments are valid or not.

Solution:

(a) A model $\mathcal{M}$ for the language consists of a domain $\mathcal{A} \neq \emptyset$ with an equality relation $=_{\mathcal{A}} \subseteq \mathcal{A} \times \mathcal{A}$, and two unary relations $R^{\mathcal{M}}, P^{\mathcal{M}} \subseteq \mathcal{A}$.

(b) **i)** The semantic entailment is valid.

Consider a model $\mathcal{M}$ with domain $\mathcal{A}$ such that $\mathcal{M} \models \exists x.\forall y.x = y$.
We need to show that $\mathcal{M} \models \forall x.\forall y.x = y$.
In this model, there is $a \in \mathcal{A}$ such that for all $b \in \mathcal{A}$, $a =_{\mathcal{A}} b$. That is, all elements in the set are equal to the element a.
So any two elements in the set $\mathcal{A}$ are equal, hence $\mathcal{M} \models \forall x.\forall y.x = y$.

ii) The semantic entailment is valid.

Consider a model $\mathcal{M}$ with domain $\mathcal{A}$ such that $\mathcal{M} \models \forall x.(P(x) \to \exists x.R(x))$.
We need to show that $\mathcal{M} \models \exists x.(P(x) \to R(x))$.
If there is an $a \in \mathcal{A}$ such that $a \notin P^{\mathcal{M}}$ then $\mathcal{M} \models_{[x \mapsto a]} P(x) \to R(x)$ (since $\mathcal{M} \not\models_{[x \mapsto a]} P(x)$) and hence $\mathcal{M} \models \exists x.(P(x) \to R(x))$.
Otherwise, $P^{\mathcal{M}} = \mathcal{A} \neq \emptyset$ and $R^{\mathcal{M}} \subseteq P^{\mathcal{M}}$. Observe that in this case $R^{\mathcal{M}} \neq \emptyset$: since we have that $\mathcal{M} \models_{[x \mapsto a]} P(x) \to \exists x.R(x)$ for all $a \in \mathcal{A}$ and $\mathcal{M} \models_{[x \mapsto a]} P(x)$ for all $a \in \mathcal{A}$, so it should be that $\mathcal{M} \models \exists x.R(x)$. This means there is $b \in \mathcal{A}$ such that $\mathcal{M} \models_{[x \mapsto b]} R(x)$. Since $P^{\mathcal{M}} = \mathcal{A}$ then $\mathcal{M} \models_{[x \mapsto b]} P(x)$ and hence $\mathcal{M} \models \exists x.(P(x) \to R(x))$.

iii) The semantic entailment is not valid.

Consider a model $\mathcal{M}$ with domain $\mathcal{A}$ such $P^{\mathcal{M}} = R^{\mathcal{M}} = \emptyset$.
Here both premises are valid simply because there is no element satisfying the condition of the implication.
That is, there no $a \in \mathcal{A}$ such that $a \in P^{\mathcal{M}}$ and $a \in R^{\mathcal{M}}$. Hence the conclusion is not valid.

5. Consider a language with relation symbols $A(x, y, z)$, $M(x, y, z)$, a constant zero and a function symbol $s(x)$.

   Let T be the following theory

   - $\forall x\ A(x, \mathsf{zero}, x)$
   - $\forall x \forall y \forall z\ A(x, y, z) \to A(x, s(y), s(z))$

   Let $s^2(x)$ denote $s(s(x))$, $s^3(x)$ denote $s(s(s(x)))$ and so on.

   (a) (3 pts) Show that for all Natural numbers p, q, r, we have $A(s^p(\mathsf{zero}), s^q(\mathsf{zero}), s^r(\mathsf{zero}))$ provable in T if, and only if, r is equal to the addition of p and q.

   (b) (3 pts) Is the theory T, $A(s(\mathsf{zero}), s(\mathsf{zero}), \mathsf{zero})$ inconsistent?

Solution:

(a) If $r = p + q$ then we can use the axioms of T to prove $A(s^p(\mathsf{zero}), s^q(\mathsf{zero}), s^r(\mathsf{zero}))$ by *induction on* q.

Conversely, we have a model of T by taking for domain the set of natural numbers and s^M the successor function and zero^M to be 0 and $A(x, y, z)$ to mean $z = x + y$. It follows by *soundness* that if $A(s^p(\mathsf{zero}), s^q(\mathsf{zero}), s^r(\mathsf{zero}))$ is provable in T then r is equal to the addition of p and q.

(b) Another model is obtained by taking for domain the set $\{0\}$ and $\mathsf{zero}^M = 0$ and $s^M(x) = 0$ and $A(x, y, z)$ always true. This is a model of the theory

T, $A(s(\mathsf{zero}), s(\mathsf{zero}), \mathsf{zero})$ and hence, using *soundness* again, this theory is not inconsistent.

6. Are the following LTL formulae valid?

   (a) (2 pts) $G(p \to Xp) \to (Gp \vee G(\neg p))$

   (b) (3 pts) $(G(Fp) \wedge G(p \to Fq)) \to GFq$

   (c) (3 pts) $G(Fp \to p) \to (Gp \vee F(G\neg p))$

   (d) (2 pts) $G(b \to (b\ U\ (a \wedge \neg b))) \to (G(\neg b) \vee F(a \wedge \neg b))$

Solution:

(a) The first formula is not valid. We take a path π with $L(\pi(0), p) = 0$ and $L(\pi(n), p) = 1$ for $n > 0$. We then have $\pi \models G(p \to Xp)$ and π does not validate Gp and π does not validate $G(\neg p)$.

(b) The second formula is valid: if for a path π we have $L(\pi(k), p) = 1$ infinitely often and whenever p holds q holds later eventually, then q also holds infinitely often.

(c) The third formula is valid. If we have for a path π that p holds whenever p holds later eventually and we have $\pi \models F(\neg p)$ then $\neg p$ holds eventually, and from this point on, we have $\neg p$ always, so $\pi \models FG(\neg p)$.

(d) The last formula $G(b \to (b\ U\ (a \wedge \neg b))) \to (G(\neg b) \vee F(b \wedge a))$ also holds. If for a path π we have $\pi \models Fb$ and $\pi \models G(b \to (b\ U\ a \wedge \neg b))$ then we have $L(\pi(k), b) = 1$ for some k and $\pi^k \models b \to (b\,U\,a \wedge \neg b)$ and hence $\pi^k \models b\,U\,(a \wedge \neg b)$ and so we have eventually $a \wedge \neg b$ as desired.

7. Are the following CTL formulae valid?

   (a) (3 pts) $AF(EGp) \to EGp$

   (b) (3 pts) $(AG(AXp \to p) \wedge \neg p) \to EG(\neg p)$

   (c) (2 pts) $EF(AGp) \to EGp$

   (d) (2 pts) $AG(p \to E(p\ U\ q)) \to (AG(\neg p) \vee EFq)$

Solution:

(a) The first formula is not valid: a counter model is given by $S_0 \to S_1$ and $S_1 \to S_1$ and p holds for S_1. We then have $S_0 \models AF(EGp)$ by not $S_0 \models EGp$.

(b) The second formula is valid. For any model, is we have $s \models \neg p$ and $s \models AXp \to p$ then we have $s \to s_1$ such that $s_1 \models \neg p$. We also have $s_1 \models AXp \to p$ since $s \models AG(AXp \to p)$ and so we can find $s_1 \to s_2$ such that $s_2 \models \neg p$ and so on. We build in this way a path $s \to s_1 \to s_2 \to \dots$ where we have $s_n \models \neg p$ for all n and so $s \models EG(\neg p)$.

(c) The third formula $EF(AGp) \to EGp$ is not valid. A counter model is given by $S_0 \to S_1$ and $S_1 \to S_1$ and p only valid at S_1.

(d) The last formula $AG(p \to E(p\ U\ q)) \to (AG(\neg p) \vee EFq)$ is valid. If we have $s \models AG(p \to E(p\ U\ q))$ and $s \models \neg AG(\neg p) = EFp$ then we have a finite path from s to a state s' satisfying p. We then have $s' \models p \to E(p\ U\ q)$ and so $s' \models E(p\ U\ q)$ and we have a finite path from s' to a state satisfying q. So we have $s \models EFq$ as desired.

8. Consider a language with constant zero and function symbol $s(x)$ and the following theory

$$\forall x\ (\mathsf{zero} \neq s(x)) \qquad \forall x \forall y\ (s(x) = s(y) \to x = y)$$

Let $s^2(x)$ denote $s(s(x))$, $s^3(x)$ denote $s(s(s(x)))$ and so on.

(a) (3 pts) Show that for any Natural numbers p and q we have that if $p \neq q$ then $T \vdash s^p(\mathsf{zero}) \neq s^q(\mathsf{zero})$

(b) (2 pts) Can T have a finite model?

Solution:

(a) Clearly we have by the first axiom $T \vdash \mathsf{zero} \neq s^q(\mathsf{zero})$ if $q \neq 0$. Also, $T \vdash s^p(\mathsf{zero}) \neq \mathsf{zero}$ if $p \neq 0$ by the first axiom and symmetry of equality. Finally by the second axiom we have

$$T \vdash s^{p+1}(\mathsf{zero}) = s^{q+1}(\mathsf{zero}) \to s^p(\mathsf{zero}) = s^q(\mathsf{zero})$$

and so we have by induction $T \vdash s^{p+1}(\mathsf{zero}) \neq s^{q+1}(\mathsf{zero})$ if $p \neq q$.

(b) It follows that, in any model of T, the interpretations of zero, $s(\mathsf{zero})$, $s^2(\mathsf{zero}), \dots$ are all distinct and so T does not have any finite model.