Logic in Computer Science

DAT060/DIT202/DIT201 (7.5 hec)

Responsible: Thierry Coquand – Telefon: 1030

Monday 4th of January 2021, 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. (2.5pts) Give a proof in natural deduction of the following sequent:

$$(q \to r) \land (q \lor p) \vdash (p \to q) \to (r \land q)$$

Solution:

1.	$(q \to r) \land (q \lor p)$	premise
2.	$p \to q$	assumption
3.	$q \to r$	$\land e_1$ 1
4.	$q \lor p$	$\land e_2$ 1
5.	q	assumption
6.	r	$\to$e (3,5)
7.	$r \land q$	$\land$i (6,5)
8.	p	assumption
9.	q	$\to$e (2,8)
10.	r	$\to$e (3,9)
11.	$r \land q$	$\land$i (10,9)
12.	$r \land q$	$\lor$e (4,5–7,8–11)
13.	$(p \to q) \to (r \land q)$	$\to$i (2–12)

2. (a) (1.5pt) Without using truth tables, give all valuations for which the formula

$$(s \to \neg p \to \neg r) \land ((r \lor q) \land s \land \neg p)$$

is true.

(b) (2.5pts) Explain how you arrived to your solution.

Solution:

(a) There is only one possible valuation which is when s and q are true, and p and r are false.

(b) For the formula to be true it should be that both $(s \to \neg p \to \neg r)$ and $((r \lor q) \land s \land \neg p)$ are true.

For $(s \to \neg p \to \neg r)$ to be true then either

i. s is false,

ii. or both s and $\neg p \to \neg r$ are true. This will happen when (iia) s is true and $\neg p$ is false, or when (iib) $s, \neg p$ and $\neg r$ are true. Hence, when (iia) s and p are true, or when (iib) s is true and p and r are false.

For $((r \lor q) \land s \land \neg p)$ to be true then both $r \lor q$, s and $\neg p$ need to be true. This will happen if at least r or q is true, s is true and p is false.

Observe that option i. is no longer possible (since s need to be false there), and neither is sub-option (iia) (since p need to be true there). So we only have the sub-option (iib) where s is true and p and r are false. Since r must be false then q must be true for the whole formula to be true and actually, this is the only possible valuation.

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) (2pts) $\forall x.R(x, x) \vdash \forall x.\forall y.(R(x, y) \to x = y)$

Solution:

We will give a counter-model and hence by soundness the sequent is not valid. Let the domain $\mathcal{A}$ be a set with at least 2 elements (which we will call a and b) and the interpretation of R be the Cartesian product of the domain of the model with itself, that is $R^{\mathcal{M}} = \mathcal{A} \times \mathcal{A}$. For all $e \in \mathcal{A}$ we have that $(e, e) \in \mathcal{A} \times \mathcal{A}$ so this model satisfies the premise.

Observe that $(a, b) \in \mathcal{A} \times \mathcal{A}$ but $a \neq b$ so $\forall x.\forall y.(R(x, y) \to x = y)$ doesn't hold in the model.

(b) (2.5pts) $Q(a) \wedge \neg Q(b) \vdash \neg(a = b)$

Solution:

1.	$Q(a) \wedge \neg Q(b)$	premise
2.	$Q(a)$	$\wedge e_1$ 1
3.	$\neg Q(b)$	$\wedge e_2$ 1
4.	$a = b$	assumption
5.	$Q(b)$	=e (4,2) with $\phi(u) \equiv Q(u)$
6.	$\bot$	$\neg$e (3,5)
7.	$\neg(a = b)$	$\neg$i 4–6

(c) (2pts) $\forall x.\forall y.\forall z.(R(x, y) \wedge R(y, z) \to R(x, z)) \vdash \forall x.\forall y.(x = y \to \neg R(x, y))$

Solution:
This says that if a relation is transitive, then there is no element in the domain that is related to itself. This we know doesn't have to be so: consider for example the set of Natural numbers with the $\leqslant$ relation which transitive and reflexive.

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

Solution:

1.	$\forall x.\forall y.\forall z.(R(x, y) \wedge R(x, z) \to R(y, z))$	premise
2.	$\forall x.R(x, x)$	premisse
3.	x_0	fresh
4.	y_0	fresh
5.	$\forall y.\forall z.(R(x_0, y) \wedge R(x_0, z) \to R(y, z))$	$\forall$e 1 with x_0
6.	$\forall z.(R(x_0, y_0) \wedge R(x_0, z) \to R(y_0, z))$	$\forall$e 5 with y_0
7.	$R(x_0, y_0) \wedge R(x_0, x_0) \to R(y_0, x_0)$	$\forall$e 6 with x_0
8.	$R(x_0, x_0)$	$\forall$e 2 with x_0
9.	$R(x_0, y_0)$	assumption
10.	$R(x_0, y_0) \wedge R(x_0, x_0)$	$\wedge$i (9,8)
11.	$R(y_0, x_0)$	$\to$e (7,10)
12.	$R(x_0, y_0) \to R(y_0, x_0)$	$\to$i 9–11
13.	$\forall y.(R(x_0, y) \to R(y, x_0))$	$\forall$i 4–12
14.	$\forall x.\forall y.(R(x, y) \to R(y, x))$	$\forall$i 3–13

(e) (3.5pts) $\forall x.\exists y.R(x,y) \vdash \forall x.\exists y.\exists z.(R(x,y) \land R(y,z))$

Solution:

1.	$\forall x.\exists y.R(x,y)$	premise
2.	x_0	fresh
3.	$\exists y.R(x_0,y)$	$\forall$e 1 with x_0
4.	y_0	fresh
5.	$R(x_0,y_0)$	assumption
6.	$\exists y.R(y_0,y)$	$\forall$e 1 with y_0
7.	z_0	fresh
8.	$R(y_0,z_0)$	assumption
9.	$R(x_0,y_0) \land R(y_0,z_0)$	$\land$i (5,8)
10.	$\exists z.(R(x_0,y_0) \land R(y_0,z))$	$\exists$i 9
11.	$\exists y.\exists z.(R(x_0,y) \land R(y,z))$	$\exists$i 10
12.	$\exists y.\exists z.(R(x_0,y) \land R(y,z))$	$\exists$e (6, 7–11)
13.	$\exists y.\exists z.(R(x_0,y) \land R(y,z))$	$\exists$e (3, 4–12)
14.	$\forall x.\exists y.\exists z.(R(x,y) \land R(y,z))$	$\forall$i 2–13

4. Consider the following semantic entailments:

   i) $P(a), Q(b) \models \exists x.(P(x) \land Q(x)) \lor \exists x.\exists y.\neg(x = y)$

   ii) $\forall x.\forall y.(R(x,y) \leftrightarrow R(y,x)) \models \forall x.R(x,x)$

   iii) $\forall x.R(x,x) \models \forall x.\forall y.(R(x,y) \to \neg\forall z.\neg(R(x,z) \land R(z,y))$

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

   (b) (2.5+2.5+3.5 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 $=_\mathcal{A} \subseteq \mathcal{A} \times \mathcal{A}$, two constants $a^\mathcal{M}, b^\mathcal{M} \in \mathcal{A}$, two unary relations $P^\mathcal{M}, Q^\mathcal{M} \subseteq \mathcal{A}$, and a binary relation $R^\mathcal{M} \subseteq \mathcal{A} \times \mathcal{A}$.

(b) i) The semantic entailment is valid.
Let $\mathcal{M}$ be a model in which the premises hold. Hence there are constants $a^{\mathcal{M}}, b^{\mathcal{M}} \in \mathcal{A}$ such that $a^{\mathcal{M}} \in P^{\mathcal{M}}$ and $b^{\mathcal{M}} \in Q^{\mathcal{M}}$.
We know that either $a^{\mathcal{M}} = b^{\mathcal{M}}$ or $a^{\mathcal{M}} \neq b^{\mathcal{M}}$.
If $a^{\mathcal{M}} = b^{\mathcal{M}}$ then we also have that $a^{\mathcal{M}} \in Q^{\mathcal{M}}$ and, hence $\mathcal{M} \models \exists x.(P(x) \wedge Q(x))$ holds.
If $a^{\mathcal{M}} \neq b^{\mathcal{M}}$ then we know there are two elements in the model which are not equal so $\mathcal{M} \models \exists x.\exists y.\neg(x = y)$ holds.

ii) The semantic entailment is not valid.
Consider the set of Natural numbers with the empty relation as $R^{\mathcal{M}}$.
Recall that $R(x, y) \leftrightarrow R(y, x)$ is defined as $(R(x, y) \rightarrow R(y, x)) \wedge (R(y, x) \rightarrow R(x, y))$.
In this model the premise is valid simply because no elements in the domain satisfy the relation $R^{\mathcal{M}}$, hence the two implications above will always hold and therefore also the conjunction.
However, there is no $n \in \mathcal{A}$ such that $(n, n) \in R^{\mathcal{M}}$, hence $\mathcal{M} \not\models \forall x.R(x, x)$.

iii) The semantic entailment is valid.
Let us assume a model $\mathcal{M}$ in which the interpretation $R^{\mathcal{M}}$ of R is reflexive, that is, for all $a \in \mathcal{A}$, $(a, a) \in R^{\mathcal{M}}$. We need to show that $\mathcal{M} \models \forall x.\forall y.(R(x, y) \rightarrow \neg\forall z.\neg(R(x, z) \wedge R(z, y))$.
Let $a, b \in \mathcal{A}$ such that $(a, b) \in R^{\mathcal{M}}$. We need to show that $\mathcal{M} \models_{[x \mapsto a, y \mapsto b]} \neg\forall z.\neg(R(x, z) \wedge R(z, y))$.
Observe that whenever z takes the same value as y, in this case b, then we have that $\mathcal{M} \models_{[x \mapsto a, y \mapsto b, z \mapsto b]} R(x, z) \wedge R(z, y)$ since we have that both $(a, b) \in R^{\mathcal{M}}$ by assumption and that $(a, a) \in R^{\mathcal{M}}$ since the model satisfies the premise. Hence $\mathcal{M} \models_{[x \mapsto a, y \mapsto b]} \exists z.(R(x, z) \wedge R(z, y))$.
Note that semantically this is exactly what we want to show since there exists a value that satisfies a property if and only if it is not the case that for all values the property doesn't hold.

5. Let F be a monotone function $Pow(S) \rightarrow Pow(S)$ where S is a set and $Pow(S)$ the set of all subsets of S. Let A and B be two subsets of S.

(a) (3 pts) Is the function $G(X) = A \cup (B \cap F(X))$ monotone? Why?

(b) (2 pts) Can the function $H(X) = A \cap (S - F(X))$ be monotone? Justify.

Solution:

(a) The function G is monotone. If $X \subseteq Y$ then we have $F(X) \subseteq F(Y)$ and so $B \cap F(X) \subseteq B \cap F(Y)$ and $G(X) \subseteq G(Y)$.

(b) The function H can be monotone if A is empty. It is then the constant empty function.

6. We consider the following theory with two axioms $\psi_1 = \forall x P(\mathsf{zero}, S(x))$ and $\psi_2 = \forall x \forall y\ (P(x,y) \to P(S(x), S(y)))$.

   (a) (2 pts) Show that $P(S(\mathsf{zero}), S(S(\mathsf{zero})))$ is provable in this theory.

   (b) (3 pts) Explain why $P(\mathsf{zero}, \mathsf{zero})$ is *not* provable in this theory.

Solution:

(a) We have $P(\mathsf{zero}, S(\mathsf{zero}))$ by ψ_1 and $P(\mathsf{zero}, S(\mathsf{zero})) \to P(S(\mathsf{zero}), S(S(\mathsf{zero})))$ by ψ_2. Hence $P(S(\mathsf{zero}), S(S(\mathsf{zero})))$ by modus ponens ($\to$e).

(b) We have a particular model of universe $\mathbf{N}$ and zero interpreted by 0 and S by $n \mapsto n+1$ and $P(x,y)$ means $x < y$. This is a model of ψ_1 and ψ_2 and in this model $P(\mathsf{zero}, \mathsf{zero})$ is not valid. By soundness, $P(\mathsf{zero}, \mathsf{zero})$ is not provable.

7. Are the following LTL formulae valid?

   (a) (3pts) $(GF(p) \wedge G(p \to q)) \to FG(q)$

   (b) (3pts) $(G(p \vee G(q)) \wedge G(q \vee G(p))) \to G(p) \vee G(q)$

Solution:

(a) The first formula is not valid. We can have p and q valid at time $0, 2, 4, \ldots$ and false at time $1, 3, 5, \ldots$. Then $GF(p)$ and $G(p \to q)$ are both valid, but $FG(q)$ is not.

(b) The second formula is valid. If we have $\neg p$ at time n and $\neg q$ at time m then $p \vee G(q)$ is not valid at time n if $n \leqslant m$ and $q \vee G(p)$ is not valid at time m if $m \leqslant n$.

8. Are the following CTL formulae valid?

   (a) (3 pts) $(AG(p) \wedge AF(q)) \to AF(p \wedge q)$

   (b) (3 pts) $(EG(p \to AG(p)) \wedge AF(p)) \to EF(AG(p))$

   (c) (3 pts) $(EG(p \to AG(p)) \wedge EF(p)) \to EF(AG(p))$

Solution:

(a) The first formula is valid. We follow the path which reach a state where q holds and p holds as well since $AG(p)$ holds.

(b) The second formula is valid. We follow the path where we have globally $p \rightarrow AG(p)$. Since $AF(p)$ holds, we have eventually p. At this point, we have $AG(p)$.

(c) The third formula is not valid. We take a model with 4 states s_0, s_1, s_2, s_3 and $s_0 \rightarrow s_1 \rightarrow s_3 \rightarrow s_3$ and $s_0 \rightarrow s_2 \rightarrow s_2$. We take p valid only for s_1. We then have $EG(p \rightarrow AG(p))$ on the path $s_0 \rightarrow s_2 \rightarrow s_2$ and $EF(p)$ but $EF(AG(p))$ does not hold at s_0.

9. (a) (2 pts) Give a formula which holds in a model if, and only if, the universe/domain of this model has at most 2 elements.

   (b) (3 pts) Explain why there is no formula such that this formula holds in a model if, and only if, the universe/domain of this model is finite.

Solution:

(a) We take $\forall x\ y\ z\ (x = y \vee y = z \vee z = x)$. The negation of this formula expresses that the universe has more than 2 elements.

(b) We can similarly write a formula ψ_n expressing that the universe has more than n elements.

Assume that there is such a formula δ which holds if, and only if, the model is finite. The theory with formulae $\delta, \psi_0, \psi_1, \ldots$ is then consistent since any finite subtheory is consistent. By compactness it has a model. This model should be finite since it is a model of δ but for any n, it has more than n elements since it is a model of ψ_n. This is a contradiction which shows that there cannot be such a formula δ.