Logic in Computer Science

DAT060/DIT202 (7.5 hec)

Responsible: Ana Bove – Telefon: 1020

Tuesday 3rd of January 2023, 14:00–18:00

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) (3pts) $p \land \neg q \to r \vdash \neg r \land p \to q$

   Solution:

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

   (b) (3pts) $p \lor q, p \to r, \neg s \to \neg q \vdash r \lor s$

Solution:

1.	$p \vee q$	premise
2.	$p \rightarrow r$	premise
3.	$\neg s \rightarrow \neg q$	premise
4.	p	assumption
5.	r	$\rightarrow$e (2,4)
6.	$r \vee s$	$\vee$i$_1$ 5
7.	q	assumption
8.	$\neg\neg q$	$\neg\neg$i 7
9.	$\neg\neg s$	MT (3,8)
10.	s	$\neg\neg$e 9
11.	$r \vee s$	$\vee$i$_2$ 10
12.	$r \vee s$	$\vee$e (1,4–6,7–11)

2. (a) (1pt) Without using truth tables, find a valuation that makes the following formula false:

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

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

Solution:

(a) When p, q and s are true and r is false then the formula becomes false.

(b) For the formula to be false, all three parts of the disjunction need to be false.
All three subformulas are implications and for an implication to be false then the condition needs to be true while the conclusion has to be false.
So, for the leftmost subformula to be false then p needs to be true and $q \wedge r$ needs to be false.
For the middle subformula to be false then $q \wedge p$ needs to be true and $r \wedge s$ needs to be false.
Putting things together we get that q should also be true (hence $p \wedge q$ is true) and r should be false (making both $q \wedge r$ and $r \wedge s$ false).
Finally, for the rightmost subformula to be false then s should be true and $p \wedge q \rightarrow r$ should be false, which is indeed the case with the values we have already assigned to p, q and r.

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) $\neg(\forall x.P(x) \vee \forall x.Q(x)) \vdash \exists x.\neg(P(x) \wedge Q(x))$

   Solution:
   The sequent is not valid. We will give a counter-model.
   Consider $\mathcal{A} = \mathbb{N}$, $P^{\mathcal{M}}$ the set of even numbes, and $Q^{\mathcal{M}}$ the set of odd numbers.
   In this model the premise holds since it is indeed the case that not all numbers are even or all number are odd.
   On the other hand, there is no number which is neither even nor odd.

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

   Solution:

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

   (c) (3.5pts) $\exists x.\forall y.R(y,x), \forall x.\exists y.R(x,y) \to \neg\exists x.R(x,x) \vdash \forall x.\neg R(x,x)$

   Solution:

1.	$\exists x.\forall y.R(y,x)$	premise
2.	$\forall x.\exists y.R(x,y) \to \neg\exists x.R(x,x)$	premise
3.	z_0	fresh
4.	$\forall y.R(y,z_0)$	assumption
5.	x_0	fresh
6.	$R(x_0,z_0)$	$\forall$e 4 with x_0
7.	$\exists y.R(x_0,y)$	$\exists$i 6
8.	$\forall x.\exists y.R(x,y)$	$\forall$i (5–7)
9.	$\neg\exists x.R(x,x)$	$\to$e (2,8)
10.	x_0	fresh
11.	$R(x_0,x_0)$	assumption
12.	$\exists x.R(x,x)$	$\exists$i 11
13.	$\perp$	$\neg$e (9,12)
14.	$\neg R(x_0,x_0)$	$\neg$i (11–13)
15.	$\forall x.\neg R(x,x)$	$\forall$i (10–14)
16.	$\forall x.\neg R(x,x)$	$\exists$e (1,3–15)

(d) (3.5pts) $\exists x.\forall y.x = y \vdash \forall x.\forall y.x = y$

Solution:

1.	$\exists x.\forall y.x = y$	premise
2.	z_0	fresh
3.	$\forall y.z_0 = y$	assumption
4.	x_0	fresh
5.	y_0	fresh
6.	$z_0 = x_0$	$\forall$e 3 with x_0
7.	$z_0 = y_0$	$\forall$e 3 with y_0
8.	$x_0 = y_0$	$=$e (6,7) with $\phi(u) \equiv u = y_0$
9.	$\forall y.x_0 = y$	$\forall$i (5–8)
10.	$\forall x.\forall y.x = y$	$\forall$i (4–9)
11.	$\forall x.\forall y.x = y$	$\exists$e (1,2–10)

4. Consider the following semantic entailments

   (i) $\forall x.(R(x) \to \exists y.P(y,x)) \models \exists z.P(z,p) \vee \forall x.\neg R(x)$

   (ii) $\forall x.(P(x,x) \vee \forall y.Q(x,y)) \models \forall x.(\exists y.P(x,y) \vee Q(x,x))$

   (iii) $\exists x.(P(x,x) \wedge \forall y.Q(x,y)) \models \exists x.(\exists y.P(x,y) \wedge Q(x,x))$

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

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

   (b) (3x3pts) Explain semantically (that is, reasoning with models) whether the above entailments hold or not.

   Solution:

   (i) This entailment is not valid.
   Consider a model $\mathcal{M}$ with domain $\mathcal{A} = \mathbb{N}$, $R^{\mathcal{M}}$ the property of being an even natural number, $P^{\mathcal{M}}$ being such that $(x,y) \in P^{\mathcal{M}}$ if $2y = x$, and $p^{\mathcal{M}}$ being any odd natural number, say 5.
   In this model, the premise $\forall x.(R(x) \to \exists y.P(y,x))$ is valid since every even number x is a multiple of 2 (so there is a y such that $2y = x$).
   On there other hand $\exists z.P(z,p) \vee \forall x.\neg R(x)$ is not valid in the model since 5 is not multiple of 2 (there is no y such that $2y = 5$) and also, it is not the case that none natural number is even.

   (ii) This entailment is valid.
   Consider a model $\mathcal{M}$ such that $\mathcal{M} \models \forall x.(P(x,x) \vee \forall y.Q(x,y))$.
   This tells us that for all $a \in \mathcal{A}$, $(a,a) \in P^{\mathcal{M}}$ or for all $b \in \mathcal{A}$, $(a,b) \in Q^{\mathcal{M}}$.
   So for any $a \in \mathcal{A}$, we have that $(a,b) \in Q^{\mathcal{M}}$ for any $b \in \mathcal{A}$. In particular when $b = a$ we then have $(a,a) \in Q^{\mathcal{M}}$. Hence $\forall x.(\exists y.P(x,y) \vee Q(x,x))$ is valid in the model.
   Alternative: If for all $a \in \mathcal{A}$ we have that $(a,a) \in P^{\mathcal{M}}$ then we know that there exists a $b \in \mathcal{A}$ (namely $b = a$) such that $(a,b) \in P^{\mathcal{M}}$. Hence $\forall x.(\exists y.P(x,y) \vee Q(x,x))$ is valid in the model.

   (iii) The entailment is valid.
   Consider a model $\mathcal{M}$ such that $\mathcal{M} \models \exists x.(P(x,x) \wedge \forall y.Q(x,y))$.
   This tells us that there is an $a \in \mathcal{A}$, such that $(a,a) \in P^{\mathcal{M}}$ and for all $b \in \mathcal{A}$, $(a,b) \in Q^{\mathcal{M}}$.
   If $(a,a) \in P^{\mathcal{M}}$ then there exists a $b \in \mathcal{A}$ (namely $b = a$) such that $(a,b) \in P^{\mathcal{M}}$.
   Also, since $(a,b) \in Q^{\mathcal{M}}$ for any $b \in \mathcal{A}$, in particular when $b = a$ we then have $(a,a) \in Q^{\mathcal{M}}$.
   Hence $\exists x.(\exists y.P(x,y) \wedge Q(x,x))$ is valid in the model.

5. Consider a language with one constant symbol leaf, one binary function symbol branch and one unary function symbol rev.

   (a) (1pt) What is a model for this language?

   (b) (2pts) Consider the two formulae

   $$\psi_1 \equiv \mathsf{rev}(\mathsf{leaf}) = \mathsf{leaf} \qquad \psi_2 \equiv \forall x \forall y\ \mathsf{rev}(\mathsf{branch}(x, y)) = \mathsf{branch}(\mathsf{rev}(y), \mathsf{rev}(x))$$

   Show that we do *not* have $\psi_1, \psi_2 \vdash \mathsf{branch}(\mathsf{leaf}, \mathsf{leaf}) \neq \mathsf{leaf}$.

   (c) (2pts) Build a model of ψ_1, ψ_2 and $\exists x\ \mathsf{rev}(\mathsf{rev}(x)) \neq x$.
   Hint: there is such a model with two elements.

Solution:

(a) A model M is a set $A \neq \emptyset$ with an element $\mathsf{leaf}^M \in A$, a function $\mathsf{rev}^M : A \to A$ and a binary function $\mathsf{branch}^M : A \times A \to A$.

(b) Consider the model with one element $A = \{a\}$ with $\mathsf{leaf}^M = a$, $\mathsf{branch}^M(x, y) = a$ and $\mathsf{rev}^M(a) = a$. This is a model of ψ_1 and ψ_2 and in this model we have $\mathsf{branch}(\mathsf{leaf}, \mathsf{leaf}) = \mathsf{leaf}$.

(c) Consider the model $A = \{a, b\}$ with $\mathsf{leaf}^M = a$, $\mathsf{branch}^M(x, y) = a$ and $\mathsf{rev}^M(a) = \mathsf{rev}^M(b) = a$. This is model of ψ_1 and ψ_2 by $\mathsf{rev}^M(\mathsf{rev}^M(b)) = a \neq b$ in this model.

6. Let S be a finite set and A, B subsets of S. Consider the function $F(X) = (X - A) \cup B$ on subsets of S.

   (a) (2pts) Explain why this function has a least and greatest fixpoint.

   (b) (3pts) ompute these two fixpoints.

Solution:

(a) This function is monotone, and hence has a least fixpoint and greatest fixpoint.
Let $X \subseteq Y$. We need to show that $F(X) \subseteq F(Y)$. That is, $(X - A) \cup B \subseteq (Y - A) \cup B$ which is indeed the case since set difference and union are also monotone.

(b) For computing the least fixpoint, we consider $F(\emptyset) = B$ and $F(B) = (B - A) \cup B = B$. Hence the least fixpoint is B.

For computing the greatest fixpoint, we consider $F(S) = (S - A) \cup B$ and $F(F(S)) = ((S - A) \cup B) - A) \cup B = (S - A) \cup B$. Hence the greatest fixpoint is $(S - A) \cup B$.

7. (a) (1pt) Explain what is a model of LTL.

(b) (2pts) Explain why the following LTL formula $(Fp \wedge Fq) \rightarrow (F(p \wedge Fq) \vee F(q \wedge Fp))$ is valid?

Solution:

(a) A model of LTL is given by a finite transition system $S, \rightarrow$ such that for any state s there is s' with $s \rightarrow s'$ and with a labelling function L, where $L(s)$ is the set of atomic formulae valid at state s.

(b) If we have π in such a model and $\pi \models Fp \wedge Fq$ we have p valid at time m and q valid at time n. If $m \leqslant n$ we have $\pi \models F(p \wedge Fq)$ and if $n \leqslant m$ we have $\pi \models F(q \wedge Fp)$.

8. Are the following LTL formulae valid? Justify your answer in each case.

(a) (2pts) $Fp \rightarrow (p\ U\ p)$

(b) (2pts) $Fp \rightarrow (\neg p\ U\ p)$

(c) (2pts) $GFp \wedge GFq \rightarrow GF(p \wedge q)$

Solution:

(a) The formula is not valid. Consider a path π where we have p neither in $L(\pi(0))$ nor in $L(\pi(1))$ but we have p in $L(\pi(2))$. We have $\pi \models F\ p$ but not $\pi \models p\ U\ p$.

(b) The formula is valid. If $\pi \models F\ p$ take n the first number such that p is in $L(\pi(n))$. We then have p not in $L(\pi(k))$ for $k < n$ and so $\pi \models \neg p\ U\ p$.

(c) The formula is not valid. Consider a path π where p holds for $\pi(n)$ when n is even, and q holds for $\pi(n)$ when n is odd. We have $\pi \models GFp$ and $\pi \models GFq$ but π is not a model of $GF(p \wedge q)$.

9. Are the following CTL formulae valid? Justify your answer in each case.

   (a) (2 pts) $(AF(p) \wedge AF(q)) \rightarrow AF(p \wedge q)$

   (b) (3 pts) $(EG(p \rightarrow q) \wedge AF(p)) \rightarrow EF(q)$

   (c) (3 pts) $AF(p) \vee AF(\neg p)$

Solution:

(a) The formula is not valid. Consider a model with two states s_0, s_1 with $s_0 \rightarrow s_1$ and $s_1 \rightarrow s_1$, p holds only at s_0 and q holds only at s_1. We have $AF(p)$ and $AF(q)$ at s_0 but not $AF(p \wedge q)$ at s_0.

(b) The formula is valid. We have a path where always on this path $p \rightarrow q$ is valid. Since we have $AF(p)$ we have eventually p on this path, and so q as well.

(c) The formula is valid. For any state s, we have p or $\neg p$ valid at s and then either $AF(p)$ is valid or $AF(\neg p)$ is also valid at s.