Logic

Final Exam 2020

Results from the course can be used directly, but other results e.g. from the TD sessions need to be proved. Your answers need to be typeset using LaTeX and returned as a PDF file by email to `baelde@lsv.fr` before Tuesday, June 16$^{\text{th}}$ at 5pm. Questions about the exercises should be addressed to both `baelde@lsv.fr` and `dowek@lsv.fr`.

Proof transformations

Establish the following results about NK_1 derivations, for all Γ, ϕ, ϕ' and ψ. For the first two questions, you are not allowed to use the completeness of NK_1, so you will most likely have to reason over the structure of proofs. You cannot describe how each of the many rules is handled, but your proof should detail the important cases and explain why the others are unimportant or similar.

1. If $\phi \wedge \phi', \Gamma \vdash \psi$ is derivable then $\phi, \phi', \Gamma \vdash \psi$ is derivable.
   For any Δ and any derivation Π of $\phi \wedge \phi', \Delta \vdash \psi$ we show that there exists a derivation Π' of $\phi, \phi', \Delta \vdash \psi$. We proceed by induction over the structure of Π'.
   - If Π is an axiom on Δ, then $\psi \in \Delta$ and Π' can be an axiom too.
   - If Π is an axiom on $\phi \wedge \phi'$, then Π' is obtained using the introduction rule for conjunction followed by two axioms, respectively on ϕ and ϕ'.

   $$\dfrac{}{\phi \wedge \phi', \Delta \vdash \phi \wedge \phi'} \quad \rightsquigarrow \quad \dfrac{\dfrac{}{\phi, \phi', \Delta \vdash \phi} \quad \dfrac{}{\phi, \phi', \Delta \vdash \phi'}}{\phi, \phi', \Delta \vdash \phi \wedge \phi'}$$

   - All other rules are insensitive to the left hand-side of the sequent, and can thus easily be handled by induction hypothesis. We show only one case, where the left hand-side is enriched, which goes through thanks to the generalization over Δ. Assume Π is as follows :

   $$\dfrac{\dfrac{\Pi_1}{\phi \wedge \phi', \Delta, \psi \vdash \psi'}}{\phi \wedge \phi', \Delta \vdash \psi \Rightarrow \psi'}$$

   By induction hypothesis on Δ, ψ and Π_1 there is a derivation Π'_1 of $\phi, \phi', \Delta, \psi \vdash \psi'$. We obtain Π' from it using the implication introduction rule.
2. If $\phi \vee \phi', \Gamma \vdash \psi$ is derivable then $\phi, \Gamma \vdash \psi$ and $\phi', \Gamma \vdash \psi$ are derivable.
   The two required derivations are obtained in the same way, by symmetry. For each one we proceed using the same kind of argument as before, only the axiom case is interesting and it as adapted easily : an axiom on $\phi \vee \phi'$ is transformed into an axiom on ϕ (resp. ϕ') followed by an application of $(\vee_I)$ to obtain $\phi \vee \phi'$.

Consider the following claims, give a counter-example when the claim is incorrect, otherwise justify why it is correct (possibly using the completeness of NK_1).

3. If $\phi \Rightarrow \phi', \Gamma \vdash \psi$ is derivable then $\phi', \Gamma \vdash \psi$ and $\Gamma \vdash \phi$ are derivable.
   This is incorrect. Take $\phi := A$, $\phi' := B$, and $\psi := C$ and $\Gamma := (C)$. We obviously have a derivation of $\phi \Rightarrow \phi', \Gamma \vdash \psi$. By soundness, we cannot have a proof of $\Gamma \vdash \phi$, i.e. $C \vdash A$.

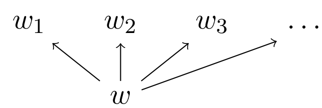
4. If $\exists x.\phi, \Gamma \vdash \psi$ is derivable then $\phi, \Gamma \vdash \psi$ is derivable.
   If a sequent $\exists x.\phi, \Gamma \vdash \psi$ is derivable then it is valid by soundness of LK_1. Its validity implies the validity of $\phi, \Gamma \vdash \psi$, which is thus derivable by completeness of LK_1. (The implication of validities is obvious if we just unfold definitions : if $\mathcal{S}, \sigma \models \phi \wedge \bigwedge \Gamma$ then $\mathcal{S}, \sigma \models (\exists x.\phi) \wedge \bigwedge \Gamma$ and, by validity of the first sequent, we have $\mathcal{S}, \sigma \models \psi$ as required.)

5. If $\phi, \Gamma \vdash \psi$ is derivable then $\exists x.\phi, \Gamma \vdash \psi$ is derivable.
   This is incorrect without a condition on the occurrences of x. Take $\phi := A(x)$, $\psi := A(x)$ and an empty Γ. The sequent $\phi \vdash \psi$ is valid and thus derivable, but $\exists x.\phi \vdash \psi$ is invalid and thus cannot be derived.

Flat Kripke structures

In this exercise we consider only propositional logic, i.e. formulas are built from propositional variables using boolean connectives only.

Let $\mathcal{K}$ be a Kripke structure with a set of worlds $\mathcal{W}$. We write $w < w'$ when $w \leq w'$ and $w \neq w'$. We say that $\mathcal{K}$ is *flat* when it does not contain three worlds w, w' and w'' such that $w < w' < w''$. Graphically, such structures look like this :



We say that a sequent $\Gamma \vdash \phi$ is valid wrt. flat Kripke structures when, for any flat Kripke structure $\mathcal{K}$ and $w \in \mathcal{W}(\mathcal{K})$ such that $\mathcal{K}, w \models \wedge\Gamma$, we also have $\mathcal{K}, w \models \phi$.

1. Show that the rules of propositional intuitionistic natural deduction (NJ_0) are sound wrt. flat Kripke structures : NJ_0 derivability implies validity wrt. flat Kripke structures.
   We have seen in the course that the rules are sound wrt. Kripke structures in general. In the proof of this result, we never have to modify Kripke structures : considering a conclusion sequent $\Gamma \vdash \phi$, and a $\mathcal{K}$ and a world $w \in \mathcal{K}$ that satisfies all formulas of Γ, we make use of the validity of the premisses for the same $\mathcal{K}$ (but possibly different worlds) to conclude that $\mathcal{K}, w \models \phi$. These arguments go through unchanged if one considers flat Kripke validity instead of general Kripke validity.
2. Show that validity wrt. flat Kripke structures is not implied by classical validity. In other words, NK_0 is not sound wrt. flat Kripke structures.
   The typical counter-example for the law of excluded middle is actually flat : the formula $P \vee \neg P$ is classically valid but it is not satisfied in world w of the flat Kripke structure with two worlds w and w' with $w \leq w'$, $\alpha(w) = \emptyset$ and $\alpha(w') = \{P\}$.
3. Show that NJ_0 is not complete wrt. flat Kripke structures.
   We exhibit a formula that is valid in all flat Kripke structures but not in the Kripke structure with three worlds $w < w' < w''$ with
   $$\alpha(w) = \emptyset,\ \alpha(w') = \{P\} \text{ and } \alpha(w'') = \{P, Q\}.$$
   The formula is
   $$\phi := (\neg\neg(\neg P \vee Q)) \Rightarrow ((P \Rightarrow Q) \vee P).$$

We can verify that this formula is not satisfied in world w of the above Kripke structure : clearly $\neg\neg(\neg P \vee Q)$ is satisfied (because every world has a successor world where Q holds) but neither $P \Rightarrow Q$ nor P are satisfied in w.
Let us now show that ϕ is satisfied in every world w of a flat Kripke formula. Assume $w \models \neg\neg(\neg P \vee Q)$. This means that for every $w' \geq w$ there exists $w'' \geq w'$ such that $w'' \models \neg P \vee Q$. Assume that $w \not\models P \Rightarrow Q$: this means that there is some $w' \geq w$ such that $w' \models P$ but $w' \not\models Q$. If $w' = w$ then we have $w \models P$ hence $w \models \phi$. Otherwise the w'' obtained above must be equal to w, by flatness of our structure, thus we have $w' \models \neg P \vee Q$: contradiction.

Ehrenfeucht-Fraïssé games for two-variable logic

Consider the modification of Ehrenfeucht-Fraïssé games where Spoiler wins if, after some round $n \geq 2$ when $(a_1, b_1), \ldots, (a_{n-1}, b_{n-1}), (a_n, b_n)$ have been played, the two pairs (a_{n-1}, b_{n-1}) and (a_n, b_n) do not induce a partial isomorphism. (In the standard games seen during the course, the partial isomorphism condition is only on the list of pairs from the last round. Here, we impose the condition for all rounds : it makes a difference because only the last two pairs are considered.)

Consider the following three structures over $\mathcal{F} = \emptyset$ and $\mathcal{P} = \{R\}$ where the interpretation of the binary symbol R is represented by arrows :

$\mathcal{S}_2$: $a_1 \longrightarrow a_2$

$\mathcal{S}_3$: $b_1 \longrightarrow b_2 \longrightarrow b_3$

$\mathcal{S}_4$: $c_1 \longrightarrow c_2 \longrightarrow c_3 \longrightarrow c_4$

1. Show that Duplicator does not have a winning strategy for two rounds over $\mathcal{S}_2$ and $\mathcal{S}_3$.
Spoiler first plays b_2. If Duplicator chooses a_1, then Spoiler plays b_1 : Duplicator cannot find a_i such that $(a_i, a_1) \in R_{\mathcal{S}_2}$. Symmetrically, if Duplicator chooses a_2, Spoiler wins by playing b_3 next.
2. What is the largest number of rounds for which Duplicator has a winning strategy over $\mathcal{S}_3$ and $\mathcal{S}_4$?
Duplicator can play without loosing for the first round, avoiding the problem from the previous question. For two rounds he looses : Spoiler plays c_2, Duplicator must play b_2, then Spoiler plays c_4 and Duplicator cannot find a b_i that is unrelated to b_2.

$\mathcal{Z}$

$$\cdots \longrightarrow c_{-1} \longrightarrow c_0 \longrightarrow c_1 \longrightarrow \cdots \longrightarrow c_n \longrightarrow c_{n+1} \longrightarrow \cdots$$

$\mathcal{C}_n$

$$\begin{tikzcd} c'_1 \arrow[r] & c'_2 \arrow[r] & \cdots \arrow[r] & c'_{n-1} \arrow[r] & c'_n \arrow[llll, bend right] \end{tikzcd}$$

3. What is the least n such that Duplicator has a winning strategy between $\mathcal{Z}$ and $\mathcal{C}_n$ (for any number of rounds) ? Justify your answer.
Let us show that Duplicator wins as soon as $n \geq 4$. Consider the last two pairs $(a, a'), (b, b')$ at any point in the game, and assume that they induce a partial isomorphism (i.e. $a = a'$ iff $b = b'$, $(a, b) \in R_{\mathcal{Z}}$ iff $(a', b') \in R_{\mathcal{C}_4}$, and conversely). If Spoiler plays some $c_i \in \mathcal{Z}$, then Duplicator answers as follows :

— if $c_i = b$, Duplicator plays b' ;
— if $(c_i, b) \in R_{\mathcal{Z}}$ then Duplicator plays the only c'_j such that $(c'_j, b') \in R_{\mathcal{C}_4}$, and symmetrically when Spoiler plays the successor of b ;
— if c_i is unrelated to b then Duplicator plays the only c'_j that is unrelated to b'.

The strategy is similar when Spoiler plays some $c'_i \in \mathcal{C}_4$: the only difference is that, in the last situation, Duplicator can pick from infinitely many possibilities to find an unrelated c_j.

From this construction it is clear that Spoiler wins if $n < 4$. Indeed he can play c_0 and then c_2 but Duplicator cannot reply with two unrelated elements in $\mathcal{C}_n$.

The two-variable fragment of first-order logic is the set of formulas that use only two variables. For instance $R(x, y)$ and $R(x, y) \wedge \exists x.\ R(y, f(x))$ are two-variable formulas, but not $R(x, y) \wedge R(y, z)$ or even $R(x, y) \wedge \exists z.\ R(y, f(z))$ if x, y and z are distinct variables.

4. Give a two-variable formula ϕ that is closed and flat, and such that $\mathcal{S}_2 \models \phi$ and $\mathcal{S}_3 \not\models \phi$.

   One possible solution :

$$\phi := \neg\exists x.\ (\exists y.\ R(y, x)) \wedge (\exists y.\ R(x, y))$$

   This formula has minimal rank among possible answers, and it corresponds to the game described above where Spoiler wins of $\mathcal{S}_2$ and $\mathcal{S}_3$.

5. Give a two-variable formula ψ that is closed and flat, and such that $\mathcal{S}_4 \models \psi$ and $\mathcal{S}_3 \not\models \psi$.

$$\phi := \exists x.\ (\exists y.\ R(y, x)) \wedge (\exists y.\ R(x, y)) \wedge (\exists y.\ y \neq x \wedge \neg R(x, y) \wedge \neg R(y, x))$$

Fix some finite $\mathcal{F}$ and $\mathcal{P}$. We write $\mathcal{S} \sim_k \mathcal{S}'$ when $\mathcal{S} \models \phi$ iff $\mathcal{S}' \models \phi$ for all closed flat two-variable formula ϕ of rank $\leq k$. It can be shown that, if Duplicator has a winning strategy on $\mathcal{S}$ and $\mathcal{S}'$ for n rounds, then $\mathcal{S} \sim_n \mathcal{S}'$: the argument is the same as for the analogue result for standard games.

6. The converse can also be proved by adapting the corresponding argument from the course : $\mathcal{S} \sim_n \mathcal{S}'$ implies that Duplicator has a winning strategy for n rounds. Explain how. You must precisely describe how the formulas $\phi_k^{b_1,\ldots,b_{n-k}}$ from the course can be adapted, and informally justify why the argument goes through with your modification. You do not need to *write* further details but be careful to *check* them, otherwise you might miss something in the adaptation of the formula !

   There are two differences between our games and the standard games, that need to be taken into account here : first we only check the partial isomorphism condition for the last two pairs, which can be shown to be equivalent to checking the equisatisfiability of two-variable flat atoms ; second this verification must be performed at each round $k \geq 2$ of the game, and not only for the final round n.

   As in the lecture notes, fix some variables $x_1, \ldots, x_n$. We define $\mathcal{A}^k(b_1, \ldots, b_k)$ as the empty set when $k < 2$. For $k \geq 2$ it is defined as the set of *two-variable* flat literals A over x_{k-1}, x_k such that $\mathcal{S}', \{x_i \mapsto b_i\}_{1 \leq i \leq k} \models A$.

We modify the definition of our formulas as follows :

$$\begin{aligned}
\phi_0^{b_1,\dots,b_n} &\overset{def}{=} \bigwedge_{A\in\mathcal{A}^n(b_1,\dots,b_n)} A \\
\phi_{k+1}^{b_1,\dots,b_{n-k-1}} &\overset{def}{=} (\forall x_{n-k}.\ \bigvee_{b\in\mathcal{S}_2} \phi_k^{b_1,\dots,b_{n-k-1},b}) \\
&\quad \wedge (\bigwedge_{b\in\mathcal{S}_2} \exists x_{n-k}.\ \phi_k^{b_1,\dots,b_{n-k-1},b}) \\
&\quad \wedge \bigwedge_{A\in\mathcal{A}^{n-k-1}(b_1,\dots,b_{n-k-1})} A
\end{aligned}$$

We can verify that $\phi_k^{b_1,\dots,b_{n-k}}$ has rank k, free variables x_{n-k-1} and x_{n-k} when $k < n-1$, and no free variable at all for $k \geq n-1$.
For our formulas to be two-variable formulas, we take two variables $y \neq z$ and fix $x_k = y$ when k is even, and z otherwise. Intuitively, this creates no confusion since we never need to refer to variables other than the last two ones.
With these modifications, the argument from the lecture notes can be replayed. The structure $\mathcal{S}'$ satisfies our formulas, in the sense made precise in equation (1) of the lecture notes, by construction. We show next that, if $\mathcal{S}$ satisfies our formulas, then Duplicator has a winning strategy : we can show this fact because we have imposed the satisfaction of two-variable flat atoms at each step ; we can conclude using $\mathcal{S} \sim_n \mathcal{S}'$ because ϕ_n has rank n and only two variables.

Russell's paradox in Resolution

1. Let A be the comprehension axiom

$$\forall x\ (x \in R \Leftrightarrow \neg x \in x)$$

   In which language is the proposition A expressed ?
   The language, in which the proposition A is expressed, contains one constant R and one binary predicate symbol $\in$.
2. What is the clausal form of A ?
   The clausal form of this proposition contains two clauses

$$\neg x \in R \vee \neg x \in x$$

$$x \in R \vee x \in x$$

3. Provide a derivation in Resolution of the clause $\perp$, from this clausal form.
   A derivation, among others, is

$$\dfrac{\dfrac{x \in R \vee x \in x}{R \in R}\ \text{Factorization} \qquad \dfrac{\neg x \in R \vee \neg x \in x}{\neg R \in R}\ \text{Factorization}}{\perp}\ \text{Resolution}$$

4. Show that there is no derivation using the Resolution rule only.
   All the derivable clauses have two literals.
5. Let B be the separation axiom

$$\forall x \ (x \in R \Leftrightarrow (x \in E \wedge \neg x \in x))$$

   Express the proposition C : "the set E is not the set of all sets"
   $\neg \forall x \ x \in E$
6. Find a Resolution proof of the sequent $B \vdash C$.
   The clausal form of the sequent is

$$x \in E$$

$$\neg x \in R \vee x \in E$$

$$\neg x \in R \vee \neg x \in x$$

$$x \in R \vee \neg x \in E \vee x \in x$$

   A derivation, among others, is

$$\dfrac{\dfrac{\dfrac{x \in R \vee \neg x \in E \vee x \in x \quad y \in E}{x \in R \vee x \in x}\text{Resolution}}{R \in R}\text{Factorization} \qquad \dfrac{\neg x \in R \vee \neg x \in x}{\neg R \in R}\text{Factorization}}{\bot}\text{Resolution}$$

Consistency

Consider a language $\mathcal{L}$ that contains the symbols 0, S, and $\leq$ and a theory $\mathcal{T}$ in this language that has a model $\mathcal{M}$ such that

— the domain of the model is the set $\mathbb{N}$,
— the interpretation of the symbol 0 is the natural number 0,
— the interpretation of the symbol S is the function $n \mapsto n+1$,
— the interpretation of the symbol $\leq$ is the usual order on natural numbers.

Consider the language $\mathcal{L}' = \mathcal{L} \cup \{c\}$ and the theory $\mathcal{U}$ containing the an infinity of axioms of axioms

$$0 \leq c$$

$$S(0) \leq c$$

$$S(S(0)) \leq c$$

$$S(S(S(0))) \leq c$$

$$\ldots$$

1. Build a model of the theory $\mathcal{T} \cup \{S(0) \leq c, S(S(S(S(0)))) \leq c\}$.
   Extend the model $\mathcal{M}$ with 100 for the interpretation of c.

2. Let $\mathcal{F}$ be any finite subset of $\mathcal{U}$. Build a model of the theory $\mathcal{T} \cup \mathcal{F}$.

   Let E be the finite set of natural numbers n such that the axiom $S^n 0 \leq c$ is in the considered subset of $\mathcal{U}$.

   Let k be the largest number in E.

   Extend the model $\mathcal{M}$ with k for the interpretation of c.

3. Is there a proof of the proposition $\perp$ in the theory $\mathcal{T} \cup \mathcal{F}$?

   No. By the soundness theorem, as $\mathcal{T} \cup \mathcal{F}$ has a model, it is consistent.

4. Is there a proof of the proposition $\perp$ in the theory $\mathcal{T} \cup \mathcal{U}$?

   No. If there were one, it would be a finite tree and use a finite number of axioms of $\mathcal{U}$, thus it would be a proof in $\mathcal{T} \cup \mathcal{F}$ for some finite subset $\mathcal{F}$ of $\mathcal{U}$.

5. Does the theory $\mathcal{T} \cup \mathcal{U}$ have a model ?

   Yes. By the completeness theorem, as $\mathcal{T} \cup \mathcal{F}$ is consistent, it has a model.

6. Does the theory $\mathcal{T} \cup \mathcal{U}$ have a model where the domain is $\mathbb{N}$, the interpretation of the symbol 0 is the natural number 0, the interpretation of the symbol S is the function $n \mapsto n + 1$, and the interpretation of the symbol $\leq$ is the usual order on natural numbers ?

   No. Consider a model where the domain is $\mathbb{N}$, the interpretation of the symbol 0 is the natural number 0, the interpretation of the symbol S is the function $n \mapsto n + 1$, and the interpretation of the symbol $\leq$ is the usual order on natural numbers.

   Let k be the interpretation of c in this model.

   The axiom $S^{k+1} 0 \leq c$ is not valid in the model. Hence this model is not a model of $\mathcal{T} \cup \mathcal{U}$.