Final Exam

15-317/657 Constructive Logic
André Platzer

May 8, 2020

Name: André Platzer

Andrew ID: aplatzer

Instructions

- **For fairness reasons all answers must be typed on a computer in text editors/text-processing (e.g. LaTeX) and submitted as PDF. Besides PDF viewers, no other software is allowed and no handwritten answers/scans are accepted. You can use scratch paper but not hand it in.**
- **Only** the following resources can be used during this exam:
  1. 15317 lecture and recitation notes
  2. editors or text-processing software
  3. **private** Piazza posts or email with course staff

  All other communications with anyone about the exam or this course during the exam period constitute an academic integrity violation.
- You have 24 hours from when the exam was available to complete it.
- There are 4 problems on 6 pages.
- **Submit** on GradeScope → Final → Submit assignment

	Max	Score
Proof Terms	90	
Propositional Theorem Proving	80	
Prolog Principles	50	
Linear Logic Cuts	80	
Total:	300	

This is a sample solution, *not a model solution. Problems admit multiple correct answers, and the answer the instructor thought of may not necessarily be the best or most elegant.*

1 Proof Terms (90 points)

This question studies proof terms of natural deduction. Recall that a proof term is called *abnormal* if it can be reduced by some local reduction of proof terms. Otherwise *normal*/irreducible.

10 **Task 1** Give a **normal** proof term for $\big((A \supset C) \wedge (B \supset C)\big) \supset \big((A \vee B) \supset (C \vee C)\big)$ or explain why that is impossible.

> **Solution:** $\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, v \Rightarrow \mathbf{inl}_C(\mathbf{case}\, v\ \ \mathbf{of\ inl}\ w \Rightarrow (\mathbf{fst}\, u)w \mid \mathbf{inr}\ w \Rightarrow (\mathbf{snd}\, u)w)$

10 **Task 2** Give an **abnormal** proof term for $(A \supset (B \wedge C)) \supset (A \supset C)$ or explain why that is impossible.

> **Solution:** $(\mathsf{fn}\, x \Rightarrow x)(\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, v \Rightarrow \mathbf{snd}(uv))$

10 **Task 3** Give a **normal** proof term justifying $A \supset ((A \vee B) \supset A)$ or explain why that is impossible.

> **Solution:** $\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, v \Rightarrow u$

10 **Task 4** Give an **abnormal** proof term justifying $A \supset ((A \vee B) \supset A)$ or explain why that is impossible.

> **Solution:** $\mathsf{fn}\, u \Rightarrow \mathsf{fn}\, v \Rightarrow \mathbf{fst}\langle u, u\rangle$

10 **Task 5** Give an **abnormal** proof term justifying $(A \vee B) \supset A$ or explain why that is impossible.

> **Solution:** By soundness, neither normal nor abnormal proof terms can exist for formulas that are not true as, e.g., witnessed by its instance $(\bot \vee \top) \supset \bot$ which is even classically false.

20 **Task 6** Briefly **explain** whether there is a true proposition A of intuitionistic propositional logic for which there is no proof term M such that $M : A$ proves.

> **Solution:** Every true intuitionistic proposition A has a proof in natural deduction whose corresponding proof term M proves $M : A$. By completeness of the certified proof checker it proves $M : A\!\uparrow$. Alternatively, use completeness of the proof-term-generating sequent calculus.

20 **Task 7** Briefly **explain** whether there is a true proposition A of intuitionistic propositional logic for which there is no **abnormal** proof term M such that $M : A$ proves.

> **Solution:** By the previous task, a proof term always exists for true A. Such a proof term can be made abnormal with any local expansion anywhere, e.g., on the outside by wrapping proof term M as follows $\mathbf{fst}\,\langle M, M\rangle$ to make it reducible/abnormal. The proof of $M : A\!\uparrow$ can be duplicated and prolonged by $\wedge I$ to prove $\langle M, M\rangle : A \wedge A\!\uparrow$, which can be prolonged by $\wedge E_1$ to prove $\mathbf{fst}\,\langle M, M\rangle : A\!\uparrow$.

2 Propositional Theorem Proving (80 points)

The contraction-free sequent calculus $\longrightarrow$ is *sound* and *complete* w.r.t. $\Longrightarrow$ and *terminates*: all its premises are strictly smaller in a well-founded ordering. Each of the following tasks drops one rule from our original contraction-free sequent calculus and replaces it with another. **Explain** whether these properties still hold when replacing *only* the indicated rule and **mark (s)** for **s**ound wrt. $\Longrightarrow$, **(u)** for **u**nsound, **(c)** for **c**omplete wrt. $\Longrightarrow$, **(i)** for **i**ncomplete, **(t)** for **t**erminating, **(n)** for **n**onterminating. If they fail, show an example demonstrating the failure.
To get you started here's a simple example: Replacing rule $\wedge R$ by rule $P0$ would make it

$$\frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge R \qquad \frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \wedge B}\ P0$$

(u) because $\longrightarrow \top \wedge \bot$ proves by $P0 + \top R$ but is (constructively) false as it implies $\bot$ by $\wedge L$.
(c) every sequent provable by $\wedge R$ is provable by $P0$, which has a subset of the premises of $\wedge R$.
(t) the same ordering shows termination because $P0$ produces a subset of the premises of $\wedge R$.

20 **Task 1** Explain what happens when we only replace rule $\vee{\supset}L$ by rule $P1$:

$$\frac{\Gamma, A_1 \supset B, A_2 \supset B \longrightarrow C}{\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C}\ \vee{\supset}L \qquad \frac{\Gamma, A_1 \supset B \longrightarrow C}{\Gamma, (A_1 \vee A_2) \supset B \longrightarrow C}\ P1$$

Solution:
(s) $P1$ derives from $\vee{\supset}L$ by weakening.
(i) $(\bot \vee \top) \supset B \longrightarrow B$ proves by $\vee{\supset}L + \top{\supset}L + \top R + id$ but is no longer provable as $P1$ is the only applicable rule and leads to classically false $\bot \supset B \longrightarrow B$.
(t) the same ordering shows termination because $P1$ produces the same sequents as $\vee{\supset}L$ with less antecedents.

20 **Task 2** Explain what happens when we only replace rule $\vee R_2$ by rule $P2$:

$$\frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\ \vee R_2 \qquad \frac{\Gamma \longrightarrow B \vee A}{\Gamma \longrightarrow A \vee B}\ P2$$

Solution:
(s) succedent $B \vee A$ is equivalent to $A \vee B$.
(c) $\vee R_2$ derives from $P2 + \vee R_1$.
(n) $P2$ can be used infinitely often on $\longrightarrow \top \vee \bot$ without progress.

20 **Task 3** Explain what happens when we only replace rule $\bot{\supset}L$ by rule $P3$:

$$\frac{\Gamma \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C}\ \bot{\supset}L \qquad \frac{\Gamma, \top \supset B \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C}\ P3$$

Solution:
(u) $\bot \supset \bot \longrightarrow \bot$ proves by $P3 + \top{\supset}L + \bot L$ but is classically false.
(c) $\bot{\supset}L$ derives from $P3$ by weakening
(t) an ordering that considers $\top$ smaller than $\bot$ works for $P3$ and other rules

20 **Task 4** Explain what happens when we only replace rule $P{\supset}L$ by rule $P4$:

$$\frac{P \in \Gamma \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P{\supset}L \qquad \frac{\Gamma \longrightarrow P \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P4$$

Solution:
(s) $P4$ derives from $\supset L$ by weakening:

$$\frac{\Gamma, P \supset P \longrightarrow P \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ \supset L$$

(c) the complete $P{\supset}L$ derives from $P4$ by id or initial rule when $P \in \Gamma$.
(t) the same ordering shows termination, because the modified premise $\Gamma \longrightarrow P$ has a smaller formula and no larger ones.

3 Prolog Principles (50 points)

This question studies symbolic computation in Prolog with polynomials in one variable (written `x`). Polynomials are represented as a list of integer coefficients, e.g.:

```
[5,6,7,8]   represents the polynomial   5 + 6*x + 7*x^2 + 8*x^3
```

In this question you will define predicates `padd/3`, `pscale/3`, `pmul/3` to compute the representation of polynomials representing polynomial addition, scaling, and multiplication, respectively. For example, the following queries are expected to succeed:

```
padd([1,2,3],[5,6],[6,8,3]),pscale(3,[1,2],[3,6]),pmul([1,2,3],[5,7],[5,17,29,21]).
```

Modes describe the intended ways of using a predicate. Mode `+pol` indicates an input argument that needs to be provided satisfying `pol/1`. Mode `-pol` indicates an output argument satisfying `pol/1` that will be computed by the predicate when all inputs are provided, where:

```
pol([A|As]) :- integer(A), pol(As).
pol([]).
```

10 **Task 1** Write a Prolog program `padd(+pol,+pol,-pol)` that takes two `pol` representations as inputs in the first and second arguments and produces a `pol` representation of their sum as the output in the third argument.

Solution:

```
%% (A+X*As) + (B+X*Bs) = (A+B) + X*(As+Bs)
padd(A, [], A).
padd([], B, B).
padd([A|As], [B|Bs], [R|Rs]) :- R is A+B, padd(As,Bs,Rs).
```

10 **Task 2** Write a Prolog program `pscale(+integer,+pol,-pol)` that takes an integer as input in the first argument, a `pol` representation as input in the second argument and produces a `pol` representation of the second argument multiplied/scaled by the first argument as the output in the third argument.

Solution:

```
%% L*(A+X*As) = L*A + X*(L*As)
pscale(L, [], []).
pscale(L, [A|As], [R|Rs]) :- R is L*A, pscale(L,As,Rs).
```

30 **Task 3** Write a Prolog program `pmul(+pol,+pol,-pol)` that takes two `pol` representations as inputs in the first and second arguments and produces a `pol` representation of the product of the input polynomials as the output in the third argument.

Solution:

```
%% (A+X*As) * B = (A*B) + X*(As * B)
pmul([], B, []).
pmul([A|As], B, R) :- pscale(A,B,AB), pmul(As,B,AsB), padd(AB,[0|AsB],R).
```

4 Linear Logic Cuts (80 points)

This question studies cuts in linear logic. We simply write $\Delta, A \Vdash C$ for $\Delta, A\ \mathit{res} \Vdash C\ \mathit{true}$. Recall that the *linear* cut theorem for linear logic constructs a deduction $\mathcal{F}$ from deductions $\mathcal{D}$ and $\mathcal{E}$ and (just like the ordinary cut theorem for intuitionistic logic) is also proved by induction on the structure of the formula A as well as the deductions $\mathcal{D}$ and $\mathcal{E}$.

Theorem (Linear cut) If $\overset{\mathcal{D}}{\Delta \Vdash A}$ and $\overset{\mathcal{E}}{\Delta', A \Vdash C}$ then $\overset{\mathcal{F}}{\Delta, \Delta' \Vdash C}$.

20 **Task 1** Provide and briefly explain a counterexample justifying from its resource semantics why the *ordinary* structural cut theorem of intuitionistic logic does *not* hold for linear logic:

If $\Delta \Vdash A$ and $\Delta, A \Vdash C$ then $\Delta \Vdash C$

Solution: $A \Vdash A$ and $A, A \Vdash A \otimes A$ but not $A \Vdash A \otimes A$, because one A cannot be duplicated into two A.

20 **Task 2** Commodore Horgiatiki performed one case of linear cut elimination. But he is missing some parts and is unsure whether he got a correct proof. Fill in **all** missing arguments and justifications and steps so that you obtain a complete proof. If there are any errors or missing justifications in Horgiatiki's proof, clearly mark and explain in one line. Unnecessary steps are not necessarily incorrect but still need a justification of their (in)correctness.

$$\mathcal{D} = \dfrac{\overset{\mathcal{D}_1}{\Delta \Vdash A_1} \quad \overset{\mathcal{D}_2}{\Delta \Vdash A_2}}{\Delta \Vdash A_1 \,\&\, A_2} \,\&R \quad \text{and} \quad \mathcal{E} = \dfrac{\overset{\mathcal{E}_1}{\Delta', A_1 \Vdash C}}{\Delta', A_1 \,\&\, A_2 \Vdash C} \,\&L_1$$

$\Delta \Vdash A_1$	1 By $\mathcal{D}_1 \prec \mathcal{D}$
$\Delta \Vdash A_2$	2 By $\mathcal{D}_2 \prec \mathcal{D}$
$\Delta', A_1 \Vdash C$	3 By $\mathcal{E}_1 \prec \mathcal{E}$
$\Delta', A_2 \Vdash C$	4 By not provable: $A \,\&\, B \Vdash A \,\&\, B$ and $A \,\&\, B \Vdash A$ but not $A \,\&\, B \Vdash B$
$\Delta, \Delta' \Vdash C$	5 By IH on $A_1 \prec A_1 \,\&\, A_2$ from line 1 as $\mathcal{D}_1 \prec \mathcal{D}$ and line 3 as $\mathcal{E}_1 \prec \mathcal{E}$

20 **Task 3** Prove the case of the *linear* cut theorem where $\mathcal{D}$ ends with $\multimap R$ and $\mathcal{E}$ ends with $\multimap L$:

$$\mathcal{D} = \dfrac{\overset{\mathcal{D}_1}{\Delta, A_1 \Vdash A_2}}{\Delta, \Vdash A_1 \multimap A_2} \multimap R \quad \text{and} \quad \mathcal{E} = \dfrac{\overset{\mathcal{E}_1}{\Delta_1' \Vdash A_1} \quad \overset{\mathcal{E}_2}{\Delta_2', A_2 \Vdash C}}{\Delta_1', \Delta_2', A_1 \multimap A_2 \Vdash C} \multimap L$$

Solution:

$\Delta, \Delta_1' \Vdash A_2$	1 By IH on $A_1 \prec A_1 \multimap A_2$ from $\mathcal{D}_1 \prec \mathcal{D}$ and $\mathcal{E}_1 \prec \mathcal{E}$
$\Delta, \Delta_1', \Delta_2' \Vdash C$	2 By IH on $A_2 \prec A_1 \multimap A_2$ from line 1 and $\mathcal{E}_2 \prec \mathcal{E}$

20 **Task 4** When replacing $\multimap$ by $\supset$ and $\Vdash$ by $\Longrightarrow$ does a proof of Task 3 justify the case of cut formula $A_1 \supset A_2$ as principal formula of the ordinary cut theorem for intuitionistic logic? Explain.

Solution: No, it does not, because the $\supset L$ rule of intuitionistic propositional logic has a crucial extra antecedent $A_1 \supset A_2$ in its left premise (and could optionally have a redundant extra antecedent $A_1 \supset A_2$ in the second premise). This first needs an extra cut by IH on the same cut formula $A_1 \supset A_2$ but smaller proofs $\mathcal{D}$ and $\mathcal{E}_1 \prec \mathcal{E}$.