# Midterm II Exam

15-317/657 Constructive Logic
André Platzer

November 10, 2015

Name: André Platzer

Andrew ID: aplatzer

## Instructions

- **Throughout this exam, explain whenever there are notable steps or choices or subtleties and justify the rationale for your particular choice!**
- This exam is closed-book with one sheet of notes permitted.
- You have 80 minutes to complete the exam.
- There are 4 problems on 9 pages.
- Read each problem carefully before attempting to solve it.
- Do not spend too much time on any one problem.
- Consider if you might want to skip a problem on a first pass and return to it later.

| | Max | Score |
|---|---|---|
| Sequent Calculus | 70 | |
| Prolog | 25 | |
| More Miraculous Sequent Rules | 30 | |
| Substitutions | 25 | |
| Total: | 150 | |

*Please keep in mind that 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 Sequent Calculus (70 points)

This question considers the sequent calculus with cut, weakening, and identity.

10 **Task 1** Prove the following theorem:

**Theorem (Connection Property):** *If* $\Longrightarrow A \wedge (B \vee C)$ *then* $\Longrightarrow A$ *and either* $\Longrightarrow B$ *or* $\Longrightarrow C$.

**Solution:** By applying sequent calculus rules, no other rules are applicable, and the proof starts as either of the two:

$$\dfrac{\Longrightarrow A \qquad \dfrac{\Longrightarrow B}{\Longrightarrow B \vee C}\,\vee R_1}{\Longrightarrow A \wedge (B \vee C)}\,\wedge R \qquad\qquad \dfrac{\Longrightarrow A \qquad \dfrac{\Longrightarrow C}{\Longrightarrow B \vee C}\,\vee R_2}{\Longrightarrow A \wedge (B \vee C)}\,\wedge R$$

10 **Task 2** If $A \wedge (B \vee C)$ has a verification in the natural deduction calculus, then is $A$ provable? And is it also the case that either $B$ or $C$ are provable, too? Briefly justify your answer.

**Solution:** Yes on both accounts since the sequent calculus is sound and complete with respect to the natural deduction calculus so that a proof exists in one if and only if it exists in the other.

10 **Task 3** Prove that the contraction rule is admissible

$$\dfrac{\Gamma, A, A \Longrightarrow C}{\Gamma, A \Longrightarrow C}$$

**Solution:** Assume the premise $\Gamma, A, A \Longrightarrow C$. Also $\Gamma, A \Longrightarrow A$ by weakening. By cut with formula $A$, the two imply $\Gamma, A \Longrightarrow C$.

20 **Task 4** To justify cuts, prove the principal cut case when the cut $A$ is of the form $A_1 \wedge A_2$. Assume

$$\mathcal{D} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2 \\ \Gamma \Longrightarrow A_1 & \Gamma \Longrightarrow A_2\end{array}}{\Gamma \Longrightarrow A_1 \wedge A_2} \wedge R \qquad \text{and} \qquad \mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1 \\ \Gamma, A_1 \wedge A_2, A_1 \Longrightarrow C\end{array}}{\Gamma, A_1 \wedge A_2 \Longrightarrow C} \wedge L_1$$

and show

$$\Gamma \Longrightarrow C$$

Explicitly justify all invocations of the induction hypothesis and explain what is smaller.

**Solution:**

$\Gamma, A_1 \Longrightarrow C$ — By i.h. on $A_1 \wedge A_2$, $\mathcal{D}$ and $\mathcal{E}_1$

$\Gamma \Longrightarrow C$ — By i.h. on $A_1$, $\mathcal{D}_1$, and previous line

In the first line, the use of the induction hypothesis is possible, since the last proof is one step smaller while the cut formula and first proof remain unchanged. In the second line, the use of the induction hypothesis is possible, even if the proofs got larger but the cut formula has become a smaller subformula.

10 **Task 5** How can you change the rules of the sequent calculus to make it *unsound*? Specify the full change of the calculus and justify why it renders the calculus unsound.

**Solution:** Add the wrong rule which allows it to prove the wrong fact. For example

$$\frac{\Gamma \Longrightarrow A}{\Gamma \Longrightarrow A \wedge B}\ unsound1$$

This rule would make the calculus unsound, because it could prove its instance

$$\frac{\dfrac{}{\Longrightarrow \top}\ \top R}{\Longrightarrow \top \wedge \bot}\ unsound1$$

The formula $\top \wedge \bot$ should not be provable, because it entails falsehood.

10 **Task 6** How can you change the rules of the sequent calculus to make it *incomplete*? Specify the full change of the calculus and justify why it renders the calculus incomplete.

**Solution:** deleting the $\vee R$ rule will render it incapable of ever verifying a formula with a disjunction (of positive polarity) since there is no rule for it except cut, which is merely admissible. So whenever there is a proof of said formula, there also is a proof without a cut, and in that cut-free proof no rule would ever be applicable to a disjunction (of positive polarity). Example: The following formula is true (provable in the original sequent calculus):

$$\frac{\dfrac{}{\Longrightarrow \top}\ \top R}{\Longrightarrow \top \vee \bot}\ \vee R_1$$

# 2 Prolog (25 points)

You can use these list predicates from lecture: `member/2`, `append/3`, `length/2`. And you can also define auxiliary predicates if you need them. A pair in Prolog is represented by constructor `pair(X,Y)`.

Hint: Use the predicates from the other tasks.

10 **Task 1** Define a predicate `unzip(list,list,list)` which holds if the first list is a list of pairs, the second list is a list of the first elements, while the third list is a list of the second elements.

**Solution:**

```
unzip([],[],[]).
unzip([pair(X,Y) | Ps], [X|Xs], [Y|Ys]) :- unzip(Ps,Xs,Ys).
```

5 **Task 2** Define a predicate `zip(list,list,list)` which holds if the last list is the list of pairs of the corresponding elements from the first and the second list. You can assume the first and second list to be of the same length.

**Solution:**

```
zip(X,Y,P) :- unzip(P,X,Y).
```

10 **Task 3** Define a predicate `rotate(list,list)` which holds if the second list is the first list rotated by one as, e.g., in `rotate([a, b, c, d], [b, c, d, a])`.

**Solution:**

```
rotate([], []).
rotate([X|Xs], L) :- append(Xs, [X], L).
```

# 3 More Miraculous Sequent Rules (30 points)

In this question, we consider suggestions for new and improved proof rules that fierce Captain Toughch came up with. *Either* show the proof rules to be sound by deriving them or proving them to be admissible. *Or* show that they can be used to prove a formula that we cannot prove soundly and *explain briefly* why that formula should not be proved.

10 **Task 1**

$$\frac{\Gamma, B \Longrightarrow A \lor C}{\Gamma, A \supset B \Longrightarrow C}\ R1$$

**Solution:** unsound, e.g., by the instance

$$\cfrac{\cfrac{\cfrac{}{\bot \Longrightarrow \bot \lor \bot}\ \bot L}{\bot \supset \bot \Longrightarrow \bot}\ R1}{\Longrightarrow (\bot \supset \bot) \supset \bot}\ \supset R$$

whose conclusion should not be provable because its assumption is true but its conclusion is not.

10 **Task 2**

$$\frac{\Gamma, A \Longrightarrow D \supset E \quad A, \Gamma \Longrightarrow B}{\Gamma, A \land ((B \lor C) \supset D) \Longrightarrow E \land (A \lor C)}\ R2$$

**Solution:** sound with the most systematic argument being a proof that the rule is derived.

$$\cfrac{\cfrac{\cfrac{\Gamma, A, \Longrightarrow B \qquad \cfrac{\Gamma, A, \Longrightarrow D \supset E \qquad \cfrac{\cfrac{\cfrac{}{B \Longrightarrow B}\ id}{, B, \Longrightarrow B \lor C}\ \lor R_1 \qquad \cfrac{\cfrac{}{D \Longrightarrow D}\ id \quad \cfrac{}{E \Longrightarrow E}\ id}{, , D, D \supset E \Longrightarrow E}\ \supset L}{, B, (B \lor C) \supset D, D \supset E \Longrightarrow E}\ \supset L}{\Gamma, A, B, (B \lor C) \supset D \Longrightarrow E}\ cut}{\Gamma, A, (B \lor C) \supset D \Longrightarrow E}\ cut \qquad \cfrac{\cfrac{}{\Gamma, A, \Longrightarrow A}\ id}{\Gamma, A, \Longrightarrow A \lor C}\ \lor R_1}{\Gamma, A, (B \lor C) \supset D \Longrightarrow E \land (A \lor C)}\ \land R}{\Gamma, A \land ((B \lor C) \supset D) \Longrightarrow E \land (A \lor C)}\ \land L$$

10 **Task 3** Consider untyped first-order logic with only one type "object", where quantifiers are written $\forall x \,.\, A(x)$ without types.

$$\frac{\Gamma \Longrightarrow A(x)}{\Gamma \Longrightarrow \forall x \,.\, A(x)}\ R3$$

**Solution:** unsound

$$\dfrac{\dfrac{\dfrac{}{p(x) \Longrightarrow p(x)}\ \mathit{init}}{p(x) \Longrightarrow \forall x \,.\, p(x)}\ R3}{\Longrightarrow p(x) \supset \forall x \,.\, p(x)}\ {\supset}R$$

because the assumption of the conclusion could be true without its right-hand side being true: for a predicate $p$ that happens to only hold of the particular argument $x$.

# 4 Substitutions (25 points)

Recall that a *substitution* is a function $\sigma$ from terms to terms that satisfies

$$f(t_1, \dots, t_n)\sigma = f(t_1\sigma, \dots, t_n\sigma) \qquad \text{for all function symbols } f \text{ and terms } t_i$$

and has a finite domain $\mathrm{dom}(\sigma) = \{x : x\sigma \neq x\}$ of variables. Recall that a *representation $\ell$ for a substitution* is of the form, e.g.:

$$\ell = (r_1/x_1, r_2/x_2, \dots, r_n/x_n)$$

5 **Task 1** Define *all* the conditions required for a list $\ell$ to qualify as a representation of a substitution.

**Solution:** The minimal requirements are the following:

1. All $x_1, \dots, x_n$ have to be variables
2. All $t_1, \dots, t_n$ have to be terms
3. All variable names $x_1, \dots, x_n$ have to be pairwise different.

10 **Task 2** For any such representation $\ell$ of a substitution, let $\hat{\ell}$ denote the substitution belonging to that representation $\ell$.
Construct a representation of the substitution that is a composition $\hat{k}\hat{\ell}$ of $\hat{\ell}$ after $\hat{k}$ from the representation $k$ of $\hat{k}$ and the representation $\ell$ of $\hat{\ell}$.
You can assume $\ell$ and $k$ to meet your requirements from Task 1 but should clearly mark if you make any additional assumptions on $\ell$ and $k$.

**Solution:** The easiest solution assumes both substitution representations to have disjoint domains: $\mathrm{dom}(\hat{\ell}) \cap \mathrm{dom}(\hat{k}) = \emptyset$. If

$$\ell = (r_1/x_1, r_2/x_2, \dots, r_n/x_n)$$
$$k = (s_1/y_1, s_2/y_2, \dots, s_m/y_m)$$

Then their composition $\hat{k}\hat{\ell}$ alias $\hat{\ell}$ after $\hat{k}$ is represented by

$$(s_1\hat{\ell}/y_1, s_2\hat{\ell}/y_2, \dots, s_m\hat{\ell}/y_m, r_1/x_1, r_2/x_2, \dots, r_n/x_n)$$

So the representation of $\hat{k}\hat{\ell}$ can be computed from the representations $\ell$ and $k$ as the list:

$$(s_i\hat{\ell}/y_i : 1 \leq i \leq m) \cup \ell$$

Without the assumption $\mathrm{dom}(\hat{\ell}) \cap \mathrm{dom}(\hat{k}) = \emptyset$, the representation of $\hat{k}\hat{\ell}$ is

$$(s_i\hat{\ell}/y_i : 1 \leq i \leq m) \cup (r_i/x_i : 1 \leq i \leq n, x_i \notin \{y_1, \dots, y_m\})$$

10 **Task 3** Some substitutions can also be applied to formulas. Define how for the cases of $\neg A$, $A \vee B$, and $\forall x.A$. If your substitution is undefined in some cases, briefly explain why.

**Solution:** The substitution $\sigma$ applies to formulas satisfying the following conditions:

$$
\begin{aligned}
(\neg A)\sigma &= \neg(A\sigma) \\
(A \vee B)\sigma &= (A\sigma) \vee (B\sigma) \\
(\forall x.A)\sigma &= \forall x.(A\sigma) && \text{if } x \notin \mathrm{dom}(\sigma) \cup \mathrm{cod}(\sigma)
\end{aligned}
$$

The condition on $x$ is, in general, needed for correctness to avoid capture:

$(\forall x.p(y))(x/y)$ is not $\forall x.(p(y)(x/y))$ which would be $\forall x.p(x)$ instead of $p(y)$

$(\forall x.p(x))(y/x)$ is not $\forall x.(p(x)(y/x))$ which would be $\forall x.p(y)$ alias $p(y)$

More general capture-avoiding substitutions can be defined as well that rename bound quantifiers as needed on demand to avoid capture. Another elegant answer is to give a judgmental style answer for applying substitutions.