Midterm II Exam

15-317/657 Constructive Logic
André Platzer

November 10, 2016

Name: André Platzer

Andrew ID: aplatzer

Instructions

- This exam is closed-book with one sheet of notes permitted.
- You have 80 minutes to complete the exam.
- There are 3 problems on 6 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.
- Explicitly label the proof rules you use in a formal proof.
- Explain your decisions in case you run into subtleties.

	Max	Score
New Connections	90	
Quantifiers	40	
Prolog	20	
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 New Connections (90 points)

Consider the new connective $\lozenge(A,B,C)$ that your friendly verificationists gave meaning to by the following introduction rule:

$$\dfrac{\begin{array}{cc}\overline{A\ \mathit{true}}^{\,u} & \overline{B\ \mathit{true}}^{\,w}\\ \multicolumn{2}{c}{\vdots}\\ \multicolumn{2}{c}{D\ \mathit{true}}\end{array}}{\lozenge(A,B,D)\ \mathit{true}}\ \lozenge I^{u,w}$$

Notation: If no confusion arises, you can abbreviate $\lozenge(A,B,D)$ by $\lozenge\lozenge$ in your answers.

10 **Task 1** Give the elimination rule(s) that harmoniously fit to $\lozenge I$:

Solution:

$$\dfrac{\lozenge(A,B,D)\ \mathit{true} \quad A\ \mathit{true} \quad B\ \mathit{true}}{D\ \mathit{true}}\ \lozenge E$$

10 **Task 2** Recall the alternative notation $A_1, A_2, \ldots, A_n \vdash A$ to indicate that A *true* is provable in the natural deduction calculus from the assumptions A_1 *true* and A_2 *true* and $\ldots A_n$ *true*. Rewrite all rules for $\lozenge(A,B,D)$ in this notation $\Gamma \vdash A$.

Solution:

$$\dfrac{\Gamma, A, B \vdash D}{\Gamma \vdash \lozenge(A,B,D)}\ \lozenge I \qquad \dfrac{\Gamma \vdash \lozenge(A,B,D) \quad \Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash D}\ \lozenge E$$

10 **Task 3** Present corresponding sequent calculus rules for $\lozenge(A,B,D)$

Solution:

$$\dfrac{\Gamma, A, B \Longrightarrow D}{\Gamma \Longrightarrow \lozenge(A,B,D)}\ \lozenge R \quad \dfrac{\Gamma, \lozenge(A,B,D) \Longrightarrow A \quad \Gamma, \lozenge(A,B,D) \Longrightarrow B \quad \Gamma, \lozenge(A,B,D), D \Longrightarrow C}{\Gamma, \lozenge(A,B,D) \Longrightarrow C}\ \lozenge L$$

You can assume without proof the usual theorems to hold after adding the $\Diamond$ connective:

Weaken: If $\Gamma \vdash C$ then $\Gamma, A \vdash C$.

Substitution: If $\Gamma \vdash A$ and $\Gamma, A \vdash C$ then $\Gamma \vdash C$.

Weakening: If $\Gamma \Longrightarrow C$ then $\Gamma, A \Longrightarrow C$.

Identity: $\Gamma, A \Longrightarrow A$.

Cut: If $\Gamma \Longrightarrow A$ and $\Gamma, A \Longrightarrow C$ then $\Gamma \Longrightarrow C$.

20 **Task 4** Prove that the sequent calculus is sound w.r.t. natural deduction, i.e., $\Gamma \Longrightarrow A$ implies $\Gamma \vdash A$, for the new cases for $\Diamond(A,B,D)$.

Solution: In the structural induction of the proof of $\Gamma \Longrightarrow A$, the new cases are where $\Diamond L$ or $\Diamond R$ have been the last step of the deduction. The first case is immediate

$$\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma, A, B \Longrightarrow D\end{array}}{\Gamma \Longrightarrow \Diamond(A,B,D)}\ \Diamond R \qquad \text{implies by IH} \qquad \dfrac{\begin{array}{c}\text{IH}(\mathcal{D})\\ \Gamma, A, B \vdash D\end{array}}{\Gamma \vdash \Diamond(A,B,D)}\ \Diamond I$$

The second case

$$\dfrac{\begin{array}{c}\mathcal{A}\\ \Gamma, \Diamond(A,B,D) \Longrightarrow A\end{array} \quad \begin{array}{c}\mathcal{B}\\ \Gamma, \Diamond(A,B,D) \Longrightarrow B\end{array} \quad \begin{array}{c}\mathcal{C}\\ \Gamma, \Diamond(A,B,D), D \Longrightarrow C\end{array}}{\Gamma, \Diamond(A,B,D) \Longrightarrow C}\ \Diamond L$$

follows by induction hypothesis applied to the smaller deductions:

$$\dfrac{\dfrac{}{\Gamma, \Diamond(A,B,D) \vdash \Diamond(A,B,D)}\ \text{hyp} \quad \begin{array}{c}\text{IH}(\mathcal{A})\\ \Gamma, \Diamond(A,B,D) \vdash A\end{array} \quad \begin{array}{c}\text{IH}(\mathcal{B})\\ \Gamma, \Diamond(A,B,D) \vdash B\end{array}}{\Gamma, \Diamond(A,B,D) \vdash D}\ \Diamond E$$

The Substitution principle combines the resulting $\Gamma, \Diamond(A,B,D) \vdash D$ with

$$\begin{array}{c}\text{IH}(\mathcal{C})\\ \Gamma, \Diamond(A,B,D), D \vdash C\end{array} \quad \text{to prove} \quad \Gamma, \Diamond(A,B,D) \vdash C$$

20 **Task 5** Prove that the sequent calculus is complete w.r.t. natural deduction, i.e., $\Gamma \vdash A$ implies $\Gamma \Longrightarrow A$, for the new cases for $\Diamond(A,B,D)$.

Solution: In the structural induction of the proof of $\Gamma \vdash A$, the new cases are where $\Diamond I$ or $\Diamond E$ have been the last step of the deduction. The first case is immediate

$$\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma, A, B \vdash D\end{array}}{\Gamma \vdash \Diamond(A,B,D)}\,\Diamond I \qquad \text{implies by IH} \qquad \dfrac{\begin{array}{c}\text{IH}(\mathcal{D})\\ \Gamma, A, B \Longrightarrow D\end{array}}{\Gamma \Longrightarrow \Diamond(A,B,D)}\,\Diamond R$$

The second case

$$\dfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash \Diamond(A,B,D)\end{array} \quad \begin{array}{c}\mathcal{A}\\ \Gamma \vdash A\end{array} \quad \begin{array}{c}\mathcal{B}\\ \Gamma \vdash B\end{array}}{\Gamma \vdash D}\,\Diamond E$$

follows by induction hypothesis applied to the smaller deductions:

$$\dfrac{\begin{array}{c}\text{IH}(\mathcal{D})\\ \Gamma \Longrightarrow \Diamond(A,B,D)\end{array} \quad \dfrac{\dfrac{\begin{array}{c}\text{IH}(\mathcal{A})\\ \Gamma \Longrightarrow A\end{array}}{\Gamma, \Diamond(A,B,D) \Longrightarrow A}\,W \quad \dfrac{\begin{array}{c}\text{IH}(\mathcal{B})\\ \Gamma \Longrightarrow B\end{array}}{\Gamma, \Diamond(A,B,D) \Longrightarrow B}\,W \quad \dfrac{}{\Gamma, \Diamond(A,B,D), D \Longrightarrow D}\,\text{id}}{\Gamma, \Diamond(A,B,D) \Longrightarrow D}\,\Diamond L}{\Gamma \Longrightarrow D}\,\text{cut}$$

20 **Task 6** Prove the case of the cut theorem for sequent calculus where $\Diamond(A,B,D)$ is the principal formula in both deductions for $\Gamma \Longrightarrow \Diamond(A,B,D)$ and $\Gamma, \Diamond(A,B,D) \Longrightarrow C$ implies $\Gamma \Longrightarrow C$. Explicitly indicate why the induction hypothesis is applicable.

Solution:

$$\dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A, B \Longrightarrow D\end{array}}{\Gamma \Longrightarrow \Diamond(A,B,D)}\,\Diamond R \qquad \dfrac{\begin{array}{c}\mathcal{A}\\ \Gamma, \Diamond(A,B,D) \Longrightarrow A\end{array} \quad \begin{array}{c}\mathcal{B}\\ \Gamma, \Diamond(A,B,D) \Longrightarrow B\end{array} \quad \begin{array}{c}\mathcal{C}\\ \Gamma, \Diamond(A,B,D), D \Longrightarrow C\end{array}}{\Gamma, \Diamond(A,B,D) \Longrightarrow C}\,\Diamond L$$

$\Gamma \Longrightarrow A$	By IH on $\Diamond(A,B,D)$, $\mathcal{D}$ and $\mathcal{A} \prec$
$\Gamma \Longrightarrow B$	By IH on $\Diamond(A,B,D)$, $\mathcal{D}$ and $\mathcal{B} \prec$
$\Gamma, D \Longrightarrow C$	By IH on $\Diamond(A,B,D)$, $\mathcal{D}$ and $\mathcal{C} \prec$
$\Gamma, B \Longrightarrow D$	By IH on $A \prec \Diamond(A,B,D)$, $\mathcal{D}_1$ and $\Gamma \Longrightarrow A$
$\Gamma \Longrightarrow D$	By IH on $B \prec \Diamond(A,B,D)$, above and $\Gamma \Longrightarrow B$
$\Gamma \Longrightarrow C$	By IH on $C \prec \Diamond(A,B,D)$, above and $\Gamma, D \Longrightarrow C$

2 Quantifiers (40 points)

Complete the proofs of the following formulas in (either original or restricted) sequent calculus **or** explain why they are not true. Indicate the rules used or weakening, cut, identity. You can leave out typing judgments from the proofs as long as they are unambiguously correct.

20 **Task 1**

Solution: The formula is not even true classically, e.g., when $p(x, y)$ stands for x less than y. Since constructively true facts are classically true, the given formula cannot be proved. Alternatively, exhaustive expansion in restricted sequent calculus, noticing that no more rules apply at some point.

$$\dfrac{\dots}{;\ \longrightarrow (\forall x{:}\tau.\ \exists y{:}\tau.\ p(x,y)) \supset (\exists y{:}\tau.\ \forall x{:}\tau.\ p(x,y))}$$

20 **Task 2**

Solution: Provable

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a{:}\tau, b{:}\tau \vdash b{:}\tau} \quad \dfrac{\dfrac{}{a{:}\tau, b{:}\tau \vdash a{:}\tau} \quad \dfrac{}{a{:}\tau, b{:}\tau;\ \forall y{:}\tau.\ p(b,y), p(b,a) \longrightarrow p(b,a)}\,init}{a{:}\tau, b{:}\tau;\ \forall y{:}\tau.\ p(b,y) \longrightarrow p(b,a)}\,\forall L}{a{:}\tau, b{:}\tau;\ \forall y{:}\tau.\ p(b,y) \longrightarrow \exists x{:}\tau.\ p(x,a)}\,\exists R}{a{:}\tau;\ \exists x{:}\tau.\ \forall y{:}\tau.\ p(x,y) \longrightarrow \exists x{:}\tau.\ p(x,a)}\,\exists L}{;\ \exists x{:}\tau.\ \forall y{:}\tau.\ p(x,y) \longrightarrow \forall y{:}\tau.\ \exists x{:}\tau.\ p(x,y)}\,\forall R}{;\ \longrightarrow (\exists x{:}\tau.\ \forall y{:}\tau.\ p(x,y)) \supset (\forall y{:}\tau.\ \exists x{:}\tau.\ p(x,y))}\,\supset R$$

$$\dfrac{\dots}{;\ \longrightarrow (\exists y{:}\tau.\ \forall x{:}\tau.\ p(x,y)) \supset (\forall x{:}\tau.\ \exists y{:}\tau.\ p(x,y))}$$

3 Prolog (20 points)

Recall that we have studied Prolog predicates defining addition `plus/3` and multiplication `times/3` of natural numbers represented in unary from constructors `0/0` and successor `s/1`:

```
plus(N,M,R)   true iff R = N + M
times(N,M,R)  true iff R = N * M
```

10 **Task 1** Define a predicate `exp/3` for exponentiation of natural numbers in Prolog.

```
exp(B,N,R)   true iff R = (B power N)
```

Solution:

```
exp(B,0,s(0)).
exp(B,S(N),R) :- exp(B,N,Q), times(B,Q,R).
```

10 **Task 2** Recall that modes in Prolog describe the intended ways of using a predicate. Mode `+nat` refers to an input argument of type `nat` that needs to be provided. Mode `-nat` refers to an output argument of type `nat` that will be computed by the predicate when all inputs are provided. For example the most interesting modes for `plus` and `times` were

```
plus(+nat,+nat,-nat)
plus(+nat,-nat,+nat)
times(+nat,+nat,-nat)
times(+nat,-nat,+nat)
```

Give all modes that make sense for your definition of `exp/3` and say what mathematical operation they correspond to.

Solution:

```
exp(+nat,+nat,-nat)   exponentiation alias B power N
exp(+nat,-nat,+nat)   logarithm of R base B
exp(-nat,+nat,+nat)   inverse logarithm: find base B such that B^N is R
exp(+nat,+nat,+nat)   check exponentiation output
Less determined modes correspond to enumerating corresponding powers.
```