Final Exam

15-317/657 Constructive Logic
André Platzer

December 16, 2016

Name: ____________________

Andrew ID: ____________________

Instructions

- This exam is open-book, closed internet.
- Remember to label all inference rules in your deductions.
- Throughout this exam, explain whenever there are notable steps or choices or subtleties and justify the rationale for your particular choice!
- You have 3 hours to complete the exam.
- There are 6 problems on 14 pages, including blank pages for extra space *at the end*.
- Consider writing out deductions on scratch paper first.

	Max	Score
New Connections	80	
Colorful Cuts in Cutalog	30	
Proof Checking	30	
Miraculously Linear Sequent Rules	50	
Unification	80	
Completely Classical	30	
Total:	300	

1 New Connections (80 points)

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

$$\dfrac{A\ \mathit{true} \quad \begin{array}{c}\overline{B\ \mathit{true}}\ u \\ \vdots \\ D\ \mathit{true}\end{array}}{\odot(A,B,D)\ \mathit{true}}\ \odot I^u$$

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

[10] **Task 2** Prove local soundness for the $\odot$ connective.

[10] **Task 3** Prove local completeness for the $\odot$ connective.

10 **Task 4** 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 natural deduction rules for $\odot(A,B,D)$ in this notation $\Gamma \vdash A$.

10 **Task 5** Give rules for verifications and uses of the $\odot$ connective.

10 **Task 6** Present corresponding sequent calculus rules for $\odot(A,B,D)$

20 **Task 7** Prove the case of the cut theorem for sequent calculus where $\odot(A,B,D)$ is the principal formula in both deductions for $\Gamma \Longrightarrow \odot(A,B,D)$ and $\Gamma, \odot(A,B,D) \Longrightarrow C$ implies $\Gamma \Longrightarrow C$. Explicitly indicate why the induction hypothesis is applicable.

2 Colorful Cuts in Cutalog (30 points)

Recall that *red cuts* change the meaning of a Prolog program, while *green cuts* are merely for efficiency. For *each* cut in the following Prolog programs explain whether it is red or green and give a concrete justification why (e.g. using an explained example).

10 **Task 1**

```
p(X,[Y|Ys]) :- member(X,[Y|Ys]), !, member(X,Ys).
```

10 **Task 2**

```
q(X, [Y|Ys]) :- X=Y.
q(X, [Y|Ys]) :- q(X,Ys), !.
```

10 **Task 3**

```
q(X, [Y|Ys]) :- X=Y, !.
q(X, [Y|Ys]) :- q(X,Ys).
```

3 Proof Checking (30 points)

Consider the following sequent calculus proof in the untyped restricted sequent calculus:

$$
\dfrac{
 \dfrac{
  \dfrac{
   \dfrac{
    \dfrac{
     \dfrac{
      \dfrac{}{p(x) \longrightarrow p(x)}\;\mathit{init}\ \textcircled{7}
      \qquad
      \dfrac{}{q(x,x), p(x) \longrightarrow q(x,x)}\;\mathit{id}\ \textcircled{8}
     }{p(x), p(x) \supset q(x,x) \longrightarrow q(x,x)}\;{\supset}R\ \textcircled{6}
    }{p(x), p(x) \supset q(x,x) \longrightarrow \forall y\, q(y,x)}\;\exists R\ \textcircled{5}
   }{p(x), \forall x\, (p(x) \supset q(x,x)) \longrightarrow \forall y\, q(y,x)}\;\forall L\ \textcircled{4}
  }{\forall x\, (p(x) \supset q(x,x)) \longrightarrow p(x) \supset \forall y\, q(y,x)}\;\textcircled{3}
 }{\forall x\, (p(x) \supset q(x,x)) \longrightarrow \forall y\, (p(y) \supset \forall x\, q(x,y))}\;\forall R\ \textcircled{2}
}{\longrightarrow \forall x\, (p(x) \supset q(x,x)) \supset \forall y\, (p(y) \supset \forall x\, q(x,y))}\;{\supset}L\ \textcircled{1}
$$

At the following rule numbers, indicate **all** errors in the above proof. If a proof step is unsound and there is no way to fix and justify it, explain why.

①

②

③

④

⑤

⑥

⑦

⑧

4 Miraculously Linear Sequent Rules (50 points)

We consider suggestions for new and improved proof rules that fierce Captain Toughch came up with for linear logic. For each rule, **mark** whether it is ⓢ **sound** or ⓤ **unsound**. Then **explain** why the rule is sound (e.g., by deriving it or proving it to be admissible) or unsound (e.g., by showing how it can be used to prove a formula that it should not prove).

10 **Task 1**

$$\frac{\Gamma; \Delta \Vdash A \otimes B}{\Gamma; \Delta \Vdash A \,\&\, B}\ R1$$

10 **Task 2**

$$\frac{\Gamma; \Delta \Vdash A \,\&\, B}{\Gamma; \Delta \Vdash A \otimes B}\ R2$$

10 **Task 3**

$$\frac{\Gamma; \Delta \Vdash A \quad \Gamma'; \Delta' \Vdash B \multimap C}{\Gamma, \Gamma'; \Delta, \Delta', A \multimap B \Vdash C}\ R3$$

10 **Task 4**

$$\frac{\Gamma; \Delta \Vdash A \quad \Gamma; \Delta', A \multimap B, B \Vdash C}{\Gamma; \Delta, \Delta', A \multimap B \Vdash C}\ R4$$

10 **Task 5**

$$\frac{}{\Gamma; \Delta, P \Vdash P}\ R5$$

5 Unification (80 points)

Unification specified the judgment $t \doteq s \mid \theta$ where θ is the most-general unifier for terms t and s. Recall that a most-general unifier θ is a unifier, i.e., $t\theta = s\theta$, and most-general among all unifiers, i.e., all other unifiers for s and t are of the form $\tau\sigma$ (that is σ after τ) for some substitution σ.

10 **Task 1** Identify conditions on the input under which the following unification rule is sound:

$$\frac{s_1 \doteq t_1 \mid \theta_1 \quad s_2 \doteq t_2 \mid \theta_2}{f(s_1, s_2) \doteq f(t_1, t_2) \mid \theta_1\theta_2}$$

20 **Task 2** Prove soundness of the above rule under the circumstances that you have identified. That is: if $f(s_1, s_2) \doteq f(t_1, t_2) \mid \theta_1\theta_2$ by the above rule, then $\theta_1\theta_2$ unifies $f(s_1, s_2)$ and $f(t_1, t_2)$.

10 **Task 3** Under which circumstances is the following unification rule sound, in which function symbol g is used on the left instead of f? Justify why.

$$\frac{s_1 \doteq t_1 \mid \theta_1 \quad s_2 \doteq t_2 \mid \theta_2}{\mathbf{g}(s_1, s_2) \doteq f(t_1, t_2) \mid \theta_1\theta_2}$$

Substitutions on propositional logical formulas are defined like for terms. They replace variables by terms and leave the formulas unchanged otherwise. Recall the usual naming conventions that u, v, w, x, y, z are logical variables, a, b, c constant symbols, f, g, h, k function symbols, and p, q, r predicate symbols.

10 **Task 4** Give a most-general unifier of the following formulas or explain why none exists:

$$\begin{array}{ll} & p(\,f(x), x\,) \lor q(\,h(f(x), c)) \\ \text{and} & p(\,f(a), g(b)\,) \lor q(\,h(z, c)) \end{array}$$

10 **Task 5** Give a most-general unifier of the following formulas or explain why none exists:

$$\begin{array}{ll} & p(\,f(x), x, u, f(u)\,) \lor q(\,h(f(x), a)) \\ \text{and} & p(\,z, g(b), k(z), w\,) \lor q(\,h(z, a)) \end{array}$$

10 **Task 6** Does the unification algorithm for terms given in the lecture give unique results? Or are there cases where the same input s, t give different unifiers θ for which $s \doteq t \mid \theta$ holds? Explain briefly.

10 **Task 7** Give a simple expression describing the complexity of checking whether the result θ of a unification algorithm on input s, t is sound, so really a unifier.

6 Completely Classical (30 points)

Recall propositional classical logic, in which a formula is *valid* iff it is true for all ways of assigning true or false to its atomic formulas. Here we only consider classical propositional formulas with implication $\supset$ and negation $\neg$ (because those are enough to express all others).

A set of axioms of classical logic is called *complete* if every (classical) propositional logical formula that is valid can be proved from the axioms (using a proof rule called *modus ponens*, i.e., if A and $A \supset B$ are proved then so is B).

Carew Meredith showed that the following single axiom, called CM, is *complete* for classical propositional logic:

$$\Big(\big(((A \supset B) \supset (\neg C \supset \neg D)) \supset C\big) \supset E\Big) \supset \big((E \supset A) \supset (D \supset A)\big)$$

Prove the Carew Meredith axiom in your favorite calculus for intuitionistic logic or explain why that is not possible.

Blank page for extra answers if needed