Final Exam

15-317/657 Constructive Logic
André Platzer

December 16, 2016

Name: André Platzer

Andrew ID: aplatzer

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	

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 (80 points)

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

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

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

Solution:

$$\dfrac{\odot(A,B,D)\ \mathit{true}}{A\ \mathit{true}}\ \odot E_1 \qquad \dfrac{\odot(A,B,D)\ \mathit{true} \quad B\ \mathit{true}}{D\ \mathit{true}}\ \odot E_2$$

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

Solution:

$$\dfrac{\dfrac{\mathcal{A}\ A\ \mathit{true} \quad \dfrac{\mathcal{D}\ D\ \mathit{true} \quad [B\ \mathit{true}]^{\,u}}{\odot(A,B,D)\ \mathit{true}}\ \odot I^{u}}{A\ \mathit{true}}\ \odot E_1}{} \quad \Longrightarrow_R \quad \mathcal{A}\ A\ \mathit{true}$$

$$\dfrac{\mathcal{A}\ A\ \mathit{true} \quad \dfrac{\mathcal{D}\ D\ \mathit{true} \quad [B\ \mathit{true}]^{\,u}}{\odot(A,B,D)\ \mathit{true}}\ \odot I^{u} \quad \mathcal{B}\ B\ \mathit{true}}{D\ \mathit{true}}\ \odot E_2 \quad \Longrightarrow_R \quad \dfrac{\mathcal{B}}{B\ \mathit{true}}\ u \quad \begin{array}{c}\mathcal{D}\\ D\ \mathit{true}\end{array}$$

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

Solution:

$$\begin{array}{c}\mathcal{D}\\ \odot(A,B,D)\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\mathcal{D}\ \odot(A,B,D)\ \mathit{true}}{A\ \mathit{true}}\ \odot E_1 \quad \dfrac{\mathcal{D}\ \odot(A,B,D)\ \mathit{true} \quad [B\ \mathit{true}]^{\,u}}{D\ \mathit{true}}\ \odot E_2}{\odot(A,B,D)\ \mathit{true}}\ \odot I^{u}$$

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 $\Gamma \vdash A$.

Solution:

$$\frac{\Gamma \vdash A \quad \Gamma, B \vdash D}{\Gamma \vdash \odot(A,B,D)}\ \odot I \qquad \frac{\Gamma \vdash \odot(A,B,D)}{\Gamma \vdash A}\ \odot E_1 \qquad \frac{\Gamma \vdash \odot(A,B,D) \quad \Gamma \vdash B}{\Gamma \vdash D}\ \odot E_2$$

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

Solution:

$$\frac{\begin{array}{c}\overline{B{\downarrow}}^{\,u}\\ \vdots \\ A{\uparrow} \quad D{\uparrow}\end{array}}{\odot(A,B,D){\uparrow}}\ \odot I^u \qquad \frac{\odot(A,B,D){\downarrow}}{A{\downarrow}}\ \odot E_1 \qquad \frac{\odot(A,B,D){\downarrow} \quad B{\uparrow}}{D{\downarrow}}\ \odot E_2$$

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

Solution:

$$\frac{\Gamma \Longrightarrow A \quad \Gamma, B \Longrightarrow D}{\Gamma \Longrightarrow \odot(A,B,D)}\ \odot R$$

$$\frac{\Gamma, \odot(A,B,D), A \Longrightarrow C}{\Gamma, \odot(A,B,D) \Longrightarrow C}\ \odot L_1 \qquad \frac{\Gamma, \odot(A,B,D) \Longrightarrow B \quad \Gamma, \odot(A,B,D), D \Longrightarrow C}{\Gamma, \odot(A,B,D) \Longrightarrow C}\ \odot L_2$$

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.

Solution:

$$\dfrac{\dfrac{\mathcal{D}_1}{\Gamma \Longrightarrow A} \quad \dfrac{\mathcal{D}_2}{\Gamma, B \Longrightarrow D}}{\Gamma \Longrightarrow \odot(A,B,D)}\,\odot R \qquad \dfrac{\dfrac{\mathcal{E}_1}{\Gamma, \odot(A,B,D), A \Longrightarrow C}}{\Gamma, \odot(A,B,D) \Longrightarrow C}\,\odot L_1$$

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

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

$$\dfrac{\dfrac{\mathcal{D}_1}{\Gamma \Longrightarrow A} \quad \dfrac{\mathcal{D}_2}{\Gamma, B \Longrightarrow D}}{\Gamma \Longrightarrow \odot(A,B,D)}\,\odot R \qquad \dfrac{\dfrac{\mathcal{E}_1}{\Gamma, \odot(A,B,D) \Longrightarrow B} \quad \dfrac{\mathcal{E}_2}{\Gamma, \odot(A,B,D), D \Longrightarrow C}}{\Gamma, \odot(A,B,D) \Longrightarrow C}\,\odot L_2$$

$\Gamma, D \Longrightarrow C$ By IH on $\odot(A,B,D)$, $\mathcal{D}$ and $\mathcal{E}_2 \prec \mathcal{E}$

$\Gamma \Longrightarrow B$ By IH on $\odot(A,B,D)$, $\mathcal{D}$ and $\mathcal{E}_1 \prec \mathcal{E}$

$\Gamma \Longrightarrow D$ By IH on $B \prec \odot(A,B,D)$, above and $\mathcal{D}_2$

$\Gamma \Longrightarrow C$ By IH on $D \prec \odot(A,B,D)$, above and first line

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).
```

Solution: Red cut when X is not ground, because it commits to the first element of the list `[Y|Ys]`, so to Y and then checks whether X occurs a second time in the remaining Ys. Without that red cut, p would additionally unify X with every element in Ys, because both member tests then succeed. For example p(X,[1,2,1,2]) will only succeed with X=1 with a cut but also with X=2 without the cut.

10 **Task 2**
```
q(X, [Y|Ys]) :- X=Y.
q(X, [Y|Ys]) :- q(X,Ys), !.
```

Solution: Red cut because q(X, [1,2,3]) will never yield X=3 with the cut because it will only X=1, X=2 since it cuts off backtracking at the first match of the second clause.

10 **Task 3**
```
q(X, [Y|Ys]) :- X=Y, !.
q(X, [Y|Ys]) :- q(X,Ys).
```

Solution: Red cut, because it commits to the first match because unifiability of X and the first list element Y will cause the second clause to never be used again. q(A, [1,2]) will only yield A=1 with the cut but will yield A=1 then A=2 without the cut.

3 Proof Checking (30 points)

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

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

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.

Solution:

① $\supset R$ has been used instead of $\supset L$

② the parameter has been called like an existing variable name x, which is not what the rule says but acceptable here since x does not occur free in the sequent.

③ rule name $\supset R$ missing

④ Optional: weakening has been used implicitly

⑤ rule $\forall R$ has been used here, but the step is unsound, as a fresh name should have been chosen for y not reuse parameter x. This is *unsound* and renders this proof unsound

⑥ $\supset L$ has been used instead of $\supset R$.

⑦ weakening was used implicitly on $p(x) \supset q(x,x)$

⑧ Optional: identity is admissible but init rule would have sufficed

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**

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

Solution: ⓤ unsound since the premise allows resources from Δ to be split to produce A and B separately, while the conclusion provides all of Δ both for A and for B. So only sound in may-use sublinear logic.

$$\dfrac{\dfrac{\dfrac{}{A \Vdash A}\ init \quad \dfrac{}{A \Vdash A}\ init}{A, A \Vdash A \otimes A}\ \otimes R}{A, A \Vdash A \,\&\, A}\ R1$$

should not prove since only one A is needed for $A \,\&\, A$ but two are supplied.

10 **Task 2**

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

Solution: ⓤ unsound since the premise provides all of Δ both for A and for B, while the conclusion requires resources from Δ to be split to produce A and B separately.

$$\dfrac{\dfrac{\dfrac{}{A \Vdash A}\ init \quad \dfrac{}{A \Vdash A}\ init}{A \Vdash A \,\&\, A}\ \&R}{A \Vdash A \otimes A}\ R2$$

should not prove since two A are needed for $A \otimes A$ but only one is supplied.

10 **Task 3**

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

Solution: ⓢ sound since it is acceptable, just unnecessary, to split the unrestricted resources up. $\multimap R$ is invertible so its inverse admissible, which transforms the second premise as expected:

$$\dfrac{\dfrac{\Gamma; \Delta \Vdash A}{\Gamma, \Gamma'; \Delta \Vdash A}\ W \quad \dfrac{\dfrac{\Gamma'; \Delta' \Vdash B \multimap C}{\Gamma'; \Delta', B \Vdash C}\ \multimap R^{-1}}{\Gamma, \Gamma'; \Delta', B \Vdash C}\ W}{\Gamma, \Gamma'; \Delta, \Delta', A \multimap B \Vdash C}\ \multimap L$$

10 **Task 4**

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

Solution: ⓤ unsound since linear implication can be used twice

$$\dfrac{\dfrac{}{A \Vdash A}\ init \quad \dfrac{\dfrac{}{A \Vdash A}\ init \quad \dfrac{\dfrac{}{B \Vdash B}\ init \quad \dfrac{}{B \Vdash B}\ init}{B, B \Vdash B \otimes B}\ \otimes L}{A, A \multimap B \Vdash B \otimes B}\ \multimap R}{A, A, A \multimap B \Vdash B \otimes B}\ R4$$

which should not prove because if there is only one copy of the linear implication rewrite, it should not be possible to use it twice.

10 **Task 5**

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

Solution: ⓤ unsound since Δ eats resources

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

should not prove since it wastes the unsolicited esource B

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:

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

Solution: Correct if the variables of the first argument do not appear in the second argument.

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 $f(t_1, t_2)$.

Solution: The condition implies that since the variables of s_1, t_1 do not occur in s_2, t_2 so neither do the variables of the unifier θ_1 of s_1, t_1 occur in s_2, t_2 such that the unifier θ_1 has no effect there and can be added or removed arbitrarily. In particular $s_2\theta_1 = s_2$ and $t_2\theta_1 = t_2$. Consequently, under the above conditions, the new rule derives from the function application and list application rules as follows:

$$\dfrac{\dfrac{s_1 \doteq t_1 \mid \theta_1 \quad \dfrac{s_2 \doteq t_2 \mid \theta_2}{s_2\theta_1 \doteq t_2\theta_2 \mid \theta_2}\, cond}{(s_1, s_2) \doteq (t_1, t_2) \mid \theta_1\theta_2}\, unify - cons}{f(s_1, s_2) \doteq f(t_1, t_2) \mid \theta_1\theta_2}\, unify - app$$

Semantic proof alternative: def indicates by definition of substitution and $\circ$ indicates use of the composition theorem for substitutions while IH indicates induction hypothesis and $cond$ indicates condition from previous task.
$s_1\theta_1 = t_1\theta_1$ by IH on the first premise.
$s_2\theta_2 = t_2\theta_2$ by IH on the second premise.

$f(s_1, s_2)(\theta_1\theta_2) \overset{def}{=} f\big((s_1, s_2)(\theta_1\theta_2)\big) \overset{def}{=} f\big(s_1(\theta_1\theta_2), s_2(\theta_1\theta_2)\big) \overset{\circ}{=} f\big((s_1\theta_1)\theta_2, (s_2\theta_1)\theta_2\big) \overset{IH}{=} f\big((t_1\theta_1)\theta_2, (s_2\theta_1)\theta_2\big) \overset{cond}{=} f\big((t_1\theta_1)\theta_2, s_2\theta_2\big) \overset{IH}{=} f\big((t_1\theta_1)\theta_2, t_2\theta_2\big) \overset{cond}{=} f\big((t_1\theta_1)\theta_2, (t_2\theta_1)\theta_2\big) \overset{\circ}{=} f\big(t_1(\theta_1\theta_2), t_2(\theta_1\theta_2)\big) \overset{def}{=} f(t_1, t_2)(\theta_1\theta_2)$

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.

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

Solution: This is never sound since function symbols f and g are different, so no substitution of variables can ever make the identical.

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:

$$\begin{array}{rl} & p(\, f(x), x \quad) \;\vee\; q(\, h(f(x), c)) \\ \text{and} \quad & p(\, f(a), g(b)\,) \;\vee\; q(\, h(z, \quad c)) \end{array}$$

Solution: Impossible since x must be a by the first argument but also $g(b)$ by the second argument, which no substitution can make happen for different function symbols a and g.

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

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

Solution:

$$(f(g(b))/z,\ g(b)/x,\ k(f(g(b)))/u,\ f(k(f(g(b))))/y)$$

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.

Solution: Even if most-general unifiers are not unique because they differ by variable renamings, the algorithm in the lecture notes will still give a unique answer, because only one rule ever applies.

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.

Solution: Linear in the size of the result of the substitution (min of both outputs is acceptable)

$$O(|t\theta|)$$

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.

Solution: This is impossible since if CM is complete then it proves the law of excluded middle $A \vee \neg A$. But the law of excluded middle is not provable in intuitionistic logic by the lecture notes.

Blank page for extra answers if needed