Final Exam

15-317/657 Constructive Logic
André Platzer

December 17, 2015

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 16 pages, including blank pages for extra space *at the end*.
- Consider writing out deductions on scratch paper first.

	Max	Score
Sequent Calculus	50	
Proof Checking	50	
Miraculous Sequent Rules	50	
Substitutions	60	
Unification	50	
Prolog	40	
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 Sequent Calculus (50 points)

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

20 **Task 1** Prove the following equivalence using sequent calculus
$(A \wedge B) \supset (C \wedge D) \equiv A \supset ((B \supset C) \wedge (B \supset D))$

Solution: Prove both implications in sequent calculus.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{B, \ldots \longrightarrow B}\,id \quad \dfrac{}{C, B \supset D, A, B \longrightarrow C}\,id}{B \supset C, B \supset D, A, B \longrightarrow C}\,\supset L \quad \dfrac{\dfrac{}{B, \ldots \longrightarrow B}\,id \quad \dfrac{}{B \supset C, D, A, B \longrightarrow D}\,id}{B \supset C, B \supset D, A, B \longrightarrow D}\,\supset L}{B \supset C, B \supset D, A, B \longrightarrow C \wedge D}\,\wedge R}{(B \supset C) \wedge (B \supset D), A, B \longrightarrow C \wedge D}\,\wedge L}{A \supset (B \supset C) \wedge (B \supset D), A, B \longrightarrow C \wedge D}\,\supset L \quad \dfrac{}{A, B \longrightarrow A}\,id}{A \supset (B \supset C) \wedge (B \supset D), A \wedge B \longrightarrow C \wedge D}\,\wedge L}{A \supset (B \supset C) \wedge (B \supset D) \longrightarrow A \wedge B \supset C \wedge D}\,\supset R}{\longrightarrow \big(A \supset (B \supset C) \wedge (B \supset D)\big) \supset \big(A \wedge B \supset C \wedge D\big)}\,\supset R$$

and the converse implication in which both main branches are identical except for D versus C

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A, B \longrightarrow A}\,id \quad \dfrac{}{A, B \longrightarrow B}\,id}{A, B \longrightarrow A \wedge B}\,\wedge R \quad \dfrac{}{C, D, A, B \longrightarrow C}\,id}{C \wedge D, A, B \longrightarrow C}\,\wedge L}{A \wedge B \supset C \wedge D, A, B \longrightarrow C}\,\supset L \quad \dfrac{\dfrac{\dfrac{}{A, B \longrightarrow A}\,id \quad \dfrac{}{A, B \longrightarrow B}\,id}{A, B \longrightarrow A \wedge B}\,\wedge R \quad \dfrac{}{C, D, A, B \longrightarrow D}\,id}{C \wedge D, A, B \longrightarrow D}\,\wedge L}{A \wedge B \supset C \wedge D, A, B \longrightarrow D}\,\supset L}{A \wedge B \supset C \wedge D, A \longrightarrow B \supset C}\,\supset R \quad \dfrac{A \wedge B \supset C \wedge D, A, B \longrightarrow D}{A \wedge B \supset C \wedge D, A \longrightarrow B \supset D}\,\supset R}{A \wedge B \supset C \wedge D, A \longrightarrow (B \supset C) \wedge (B \supset D)}\,\wedge R}{A \wedge B \supset C \wedge D \longrightarrow A \supset (B \supset C) \wedge (B \supset D)}\,\supset R}{\longrightarrow \big(A \wedge B \supset C \wedge D\big) \supset \big(A \supset (B \supset C) \wedge (B \supset D)\big)}\,\supset R$$

10 **Task 2** Prove the following theorem:
Theorem (Disconnection Property): *If* $\Longrightarrow (\neg A \vee B) \wedge C$ *then either* $A \Longrightarrow \bot$ *or* $\Longrightarrow B$ *and, either way, also* $\Longrightarrow C$.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Longrightarrow \bot}{\Longrightarrow \neg A}\supset R}{\Longrightarrow \neg A \vee B}\vee R_1 \qquad \Longrightarrow C}{\Longrightarrow (\neg A \vee B) \wedge C}\wedge R$$

or as

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

Since these are the only options for applicable rules in sequent calculus, the disconnection property follows.

20 **Task 3** Recall that $\neg\neg A \supset A$ is not provable in the (intuitionistic) sequent calculus. Give a simple proof that the law of excluded middle $A \vee \neg A$ is not provable in the (intuitionistic) sequent calculus either.

Solution: Prove DNE, which isn't provable, from the law of excluded middle to show that the law of excluded middle cannot be provable either.

$$\dfrac{\dfrac{\Longrightarrow A \vee \neg A \qquad \dfrac{\dfrac{}{A, \neg\neg A \longrightarrow A}\,id \qquad \dfrac{\dfrac{}{\neg A \longrightarrow \neg A}\,id \qquad \dfrac{}{\neg A, \bot \longrightarrow A}\,\bot L}{\neg A, \neg\neg A \longrightarrow A}\supset L}{A \vee \neg A, \neg\neg A \longrightarrow A}\vee L}{\dfrac{\neg\neg A \Longrightarrow A}{\Longrightarrow \neg\neg A \supset A}\supset R}\,cut$$

Since cut elimination and identity are admissible, if the above proof of an unprovable $\Longrightarrow \neg\neg A \supset A$ were possible with a cut and identity from $\Longrightarrow \neg\neg A \supset A$, it would also be possible without cut and identity. But $\Longrightarrow \neg\neg A \supset A$ is not provable, so there cannot be a proof, with or without cut and identity, of $\Longrightarrow A \vee \neg A$ either.

2 Proof Checking (50 points)

30 **Task 1** Commodore Horgiatiki performed one case of a cut elimination proof for sequent calculus. But he is missing some parts and is unsure whether he got a correct proof. Fill in literally **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, identify and clearly mark all errors and explain carefully **why** they are incorrect arguments.

If $\Gamma \Longrightarrow A_1$		(1)
$\Gamma \Longrightarrow A_2$		(2)
$\Gamma \Longrightarrow A_1 \wedge A_2$	by $\wedge R$ on (1) and (2)	(3)
$\Gamma, A_1 \wedge A_2, A_2 \Longrightarrow C$		(4)
$\Gamma, A_1 \wedge A_2 \Longrightarrow C$	by $\wedge L_2$ on (4)	(5)

Then

$\Gamma, A_1 \Longrightarrow C$	by i.h. on $A_1 \wedge A_2$ and (3) and (4)	(6)
$\Gamma, A_1 \wedge A_2 \Longrightarrow C$	by i.h. on A_2 and (2) and (4)	(7)
$\Gamma \Longrightarrow C$	by i.h. on $A_1 \wedge A_2$ and (3) and (7)	(8)

Solution:

(6) needs $\Gamma, A_2 \Longrightarrow C$ instead and weaken (3) but is actually useless (dead code)

(7) is missing a weakening justification since (2) is not of the form $\Gamma, A_1 \wedge A_2 \Longrightarrow A_2$ (which, on top of that, is trivially provable on its own even without Γ so not helpful).

(8) induction hypothesis is not applicable since the proof resulting by induction hypothesis via cut elimination from (7) is bigger than the induction hypothesis permits on same-size cut formula $A_2 \wedge A_2$.

20 **Task 2** Mark all errors in the following sequent calculus proof and subsequently explain whether and why they are soundness-critical or why they could be accepted with a different argument.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{⑦}}{⑥\ a(x) \supset p(x,x) \Longrightarrow a(x) \supset p(x,x)}\ init}{⑤\ a(x) \supset p(x,x), a(x) \Longrightarrow p(x,x)}\ \supset R}{④\ a(x), a(x) \supset p(x,x) \Longrightarrow \forall y\, p(y,x)}\ \forall R}{③\ a(x), \forall x\,(a(x) \supset p(x,x)) \Longrightarrow \forall y\, p(y,x)}\ \supset L}{②\ \forall x\,(a(x) \supset p(x,x)) \Longrightarrow a(x) \supset \forall y\, p(y,x)}}{①\ \forall x\,(a(x) \supset p(x,x)) \Longrightarrow \forall y\,(a(y) \supset \forall x\, p(x,y))}\ \forall R}{⓪\ \Longrightarrow \forall x\,(a(x) \supset p(x,x)) \supset \forall y\,(a(y) \supset \forall x\, p(x,y))}\ \supset L$$

Refer to the line numbers in your answers below. Where ① refers to the whether the sequent in line ① can result by applying the given proof rule to the sequent in ⓪ etc.

Solution:

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

② variables have been shuffled by bound renaming, which is unlike the rule but would be acceptable. The parameter is supposed to be fresh, which it is not here, but acceptable since not occurs free.

③ missing $\supset R$

④ $\forall L$ and weakening missing

⑤ unsound, should have chosen fresh name for y not reuse parameter x, which is unsound and renders this proof unsound

⑥ $\supset R$ is the wrong rule. It is invertible, though, so its inverse $(\supset R)^{-1}$ that is used here would be admissible.

⑦ $init$ is the wrong rule since not atomic. The identity rule would be admissible, though.

3 Miraculous Sequent Rules (50 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**

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

Solution: unsound, since this gives a proof of falsehood:

$$\dfrac{\dfrac{\dfrac{}{\Longrightarrow \top}\ \top R \quad \dfrac{}{\bot \Longrightarrow \bot}\ init}{\top \supset \bot \Longrightarrow \bot}\ \supset L \qquad \dfrac{\dfrac{\dfrac{}{\bot \Longrightarrow \bot}\ init/\bot L}{\Longrightarrow \bot \supset \bot}\ \supset R \qquad \dfrac{\dfrac{}{\bot \vee \top \Longrightarrow \top}\ \top R}{\bot \supset \bot \Longrightarrow \top \supset \bot}\ R1}{\Longrightarrow \top \supset \bot}\ cut}{\Longrightarrow \bot}\ cut$$

Consider linear logic now.

10 **Task 2**

$$\frac{\Gamma; \cdot \Vdash A \multimap B}{\Gamma; \Delta \Vdash\ !(A \multimap B)}\ R2$$

Solution: unsound as too much resource consumption (Δ) in the conclusion. The following example eliminates resourceful $\top$, which should not have a left rule

$$\dfrac{\dfrac{\dfrac{\dfrac{}{; A \Vdash A}\ id}{; \cdot \Vdash A \multimap A}\ \multimap R}{; \top \Vdash\ !(A \multimap A)}\ R2 \qquad \dfrac{\dfrac{}{A \multimap A; \cdot \Vdash \mathbf{1}}\ \mathbf{1}L}{; !(A \multimap A) \Vdash \mathbf{1}}\ !L}{; \top \Vdash \mathbf{1}}\ cut$$

10 **Task 3**

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

Solution: unsound because resource duplication of Δ in both branches

$$\dfrac{\dfrac{}{A \Vdash A}\ init/id \qquad \dfrac{\dfrac{\dfrac{}{A \Vdash A}\ init/id \quad \dfrac{}{A \Vdash A}\ init/id}{A, A \Vdash A \otimes A}\otimes R}{A \Vdash A \multimap A \otimes A}\multimap R}{A, A \multimap A \Vdash A \otimes A}\ R3$$

This sequent should not be provable, because having one A and a way of turning one A back into an A does not give two A.

10 **Task 4**

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

Solution: unsound because even if the second premise appears to need $\Delta = (\cdot)$ to prove its resource independent succedent, the duplication of Δ still enables unsound resource duplication using the with operator:

$$\dfrac{\dfrac{\dfrac{}{A \Vdash A}\ init/id}{A \,\&\, !(B \multimap C) \Vdash A}\,\&L_1 \quad \dfrac{\dfrac{}{!(B \multimap C) \Vdash !(B \multimap C)}\ id}{A \,\&\, !(B \multimap C) \Vdash !(B \multimap C)}\,\&L_2}{A \,\&\, !(B \multimap C), A \multimap B \Vdash C}\ R4$$

This sequent is not provable in linear logic because the proof of A after $\multimap L$ needs the with resource but then the second premise will not succeed and vice versa.

10 **Task 5** Recall natural deduction rules for intuitionistic propositional logic such as

$$\frac{B\ true}{A \vee B\ true}\ \vee I_R$$

Can you give such a natural deduction proof calculus for linear logic? Briefly justify why or why not.

Solution: no since resource management / assumption management is impossible in this two-dimensional notation. This notation for rules is not explicit about what assumptions are available, so does not provide explicit ways of dividing them up.

4 Substitutions (60 points)

Recall that a *substitution* is a function σ from terms to terms that satisfies

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

and has a finite domain $\mathrm{dom}(\sigma) = \{x \,:\, x\sigma \neq x\}$ of variables. Recall that $\tau\sigma$ denotes the substitution that is the composition of substitution σ after τ. Finally recall that a *variable renaming* is a substitution whose only effect is to replace variables by variables, not by arbitrary terms, and that, moreover, never renames two different variables to the same variable.

20 **Task 1** Let σ and τ be substitutions such that $\tau\sigma = (\cdot)$ is the identity substitution. Then is σ a variable renaming? Prove or disprove.

Solution: INCOMPLETE SOLUTION: Yes.
It might seem as if this was a counterexample:

$$(z/x)(f(x)/x) = (z/x)$$

but only almost, since their composition (z/x) is not the identity substitution, but, rather, a variable renaming.

20 **Task 2** Let σ and τ be any substitutions such that $\tau\sigma = \tau$. Then is σ a variable renaming? Prove or disprove.

Solution: No if τ replaces everything away that σ would have replaced.

$$(f(a)/x)(g(b)/x) = (f(a)/x)$$

The effect of the compositions of substitutions is indeed equivalent to the effect of the single substitution, but still the substitution σ would have had an effect on its own that is not just a variable renaming.

Recall that a *representation ℓ for a substitution* is of the form, e.g.:

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

For any such representation ℓ of a substitution, let $\hat{\ell}$ denote the substitution belonging to that representation ℓ.

20 **Task 3** Let ℓ, k be representations of substitutions $\hat{\ell}$ and $\hat{k}$, respectively. Under what condition on ℓ and k is $\ell \cup k$ a representation of the composition $\hat{k}\hat{\ell}$ of $\hat{\ell}$ after $\hat{k}$? Prove correctness of the condition you identified or prove why no such condition exists.

Solution: $\mathrm{dom}(\hat{k}) \cap \mathrm{cod}(\hat{l}) = \emptyset$ and $\mathrm{dom}(\hat{l}) \cap \mathrm{cod}(\hat{k}) = \emptyset$
INCOMPLETE SOLUTION: proof

5 Unification (50 points)

Unification specified the judgment $t \doteq s \mid \theta$ where θ is the most-general unifier for terms t and s. But, with some caveats, it works for formulas, too. In this question, we construct the judgment $F \doteq G \mid \theta$ with most-general unifier θ for formulas F and G.

10 **Task 1** Augment the judgment by writing new inference rules to also cover the case $p(\bar{t})$ for predicate symbol p with a sequence of terms $\bar{t}$ as arguments.

Solution:

$$\frac{\bar{t} \doteq \bar{s} \mid \theta}{p(\bar{t}) \doteq p(\bar{s}) \mid \theta}$$

10 **Task 2** Augment the judgment further to the case of formulas of the form $F \vee G$.

Solution:

$$\frac{F_1 \doteq G_1 \mid \theta_1 \quad F_2\theta_1 \doteq G_2\theta_1 \mid \theta_2}{F_1 \vee F_2 \doteq G_1 \vee G_2 \mid \theta_1\theta_2}$$

10 **Task 3** Give a most-general unifier of

$$\begin{array}{rr} & p(f(x), x) \vee q(g(u, x)) \\ \text{and} & p(z, g(b, c)) \vee q(g(z, y)) \end{array}$$

Solution:

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

20 **Task 4** Prove *soundness* of your answers from Tasks 1 and 2, i.e. that the result, θ, of $F \doteq G \mid \theta$ indeed is a unifier for formulas F and G.

Solution:

The conditions for substitutions are extended to formulas as:

$$p(t_1, \ldots, t_n)\sigma = p(t_1\sigma, \ldots, t_n\sigma) \qquad \text{for all predicate symbols } p \text{ and terms } t_i$$
$$(\phi \vee \psi)\sigma = (\phi\sigma) \vee (\psi\sigma) \qquad \text{likewise for other connectives}$$

Case: $\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{E}\\ \mathbf{t} \doteq \mathbf{s} \mid \theta\end{array}}{p(\mathbf{t}) \doteq p(\mathbf{s}) \mid \theta}$ where $t = p(\mathbf{t})$ and $s = p(\mathbf{s})$.

$\mathbf{t}\theta = \mathbf{s}\theta$	By soundness of unification for terms on $\mathcal{E}$
$p(\mathbf{t})\theta = p(\mathbf{s})\theta$	By definition of substitution

Case: $\mathcal{E} = \dfrac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{E}_2\\ F_1 \doteq G_1 \mid \theta_1 & F_2\theta_1 \doteq G_2\theta_1 \mid \theta_2\end{array}}{F_1 \vee F_2 \doteq G_1 \vee G_2) \mid \theta_1\theta_2}$ where $\theta = \theta_1\theta_2$.

$F_1\theta_1 = G_1\theta_1$	By i.h.(i) on $\mathcal{D}_1$
$(F_1\theta_1)\theta_2 = (G_1\theta_1)\theta_2$	By equality reasoning
$F_1(\theta_1\theta_2) = G_1(\theta_2\theta_2)$	By substitution composition
$(F_2\theta_1)\theta_2 = (G_2\theta_1)\theta_2$	By i.h.(ii) on $\mathcal{E}_2$
$F_2(\theta_1\theta_2) = G_2(\theta_1\theta_2)$	By substitution composition
$(F_1 \vee F_2)(\theta_1\theta_2) = (G_1 \vee G_2)(\theta_1\theta_2)$	By defn. of substitution

6 Prolog (40 points)

In this question we will study ways of computing the derivative of polynomials in one variable with Prolog. Assume that polynomial expressions are represented as data structures of type `poly` built in an arbitrary shape from these constructors:

```
plus(S,T)  represents the sum of S and T
times(S,T) represents the product of S and T
var        indicates the variable (only one variable occurs so no need for a name)
num(N)     represents the number literal N (say as an integer)
```

In this problem you will define a predicate `diff/2` to compute the derivative of a polynomial expression represented in this way. For example, the following query is expected to succeed:

```
?- diff(plus(var,num(5)), plus(num(1), num(0))).
```

Modes in Prolog describe the intended ways of using a predicate. Mode `+poly` refers to an input argument of type `poly` that needs to be provided. Mode `-poly` refers to an output argument of type `poly` that will be computed by the predicate when all inputs are provided.

20 **Task 1** Write a Prolog program `diff(+poly,-poly)` that takes the polynomial as an input in the first argument and produces its derivative as an output in the second argument.

10 **Task 2** With mode `diff(+poly,-poly)`, the predicate from Task 1 computes a derivative. Is there a mode with which the predicate from Task 1 computes antiderivatives (also known as indefinite integrals)? Justify.

10 **Task 3** Is there a mode with which the predicate from Task 1 can be used to check whether a given polynomial expression is the integral of another given polynomial expression? Justify.

Blank page for extra answers if needed