Midterm 2

15-317: Constructive Logic

November 12, 2013

Name: Andrew ID:

Instructions

- This exam is closed-book, but one two-sided sheet of notes is permitted. The last pages of the exam recap some rules you may find useful.
- There are 4 problems on 10 pages. Not all problems are the same size or difficulty. You have 80 minutes to complete the exam.
- When writing proofs, remember to label each inference with the rule used.
- You may find it helpful to construct your proofs on scratch paper (such as the back of a page) before writing it clearly in the space provided.
- Stay cool and good luck!

	Max	Score
1	45	
2	65	
3	15	
4	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.*

Problems

1. **Inversion and G4ip**

   (a) (20 points) Show that in the restrictive sequent calculus (Figure 2), the rule $\supset R$ is invertible, i.e. show that if there is a proof of the conclusion then there is a proof of the premise. You may use the lemmas for weakening, contraction, identity and cut.

(b) (25 points) Recall that the G4ip calculus (Figure 1) is derived from the restrictive sequent calculus (Figure 2) by refining the rules for implication on the left. For instance, we justify the rule $\supset\supset L$ by showing $((D \supset E) \supset B) \wedge D \equiv (E \supset B) \wedge D$ i.e., both directions of implication are provable *in the restrictive calculus*.

Justify the G4ip rule $\wedge\supset L$ in the same way, i.e., give two proofs in the restrictive sequent calculus. Assume that all the propositions are atomic. Use only the rules; do not use weakening or other lemmas.

2. **Prolog programming**

   (It would be a good idea to read all of this section before solving any part.)

   Consider the following program. The intended meaning of `replace(+X,+Y,+Xs,-Ys)` is that `Ys` is derived from the list `Xs` by replacing all occurrences of `X` by `Y`.

```
replace(X,Y,[],[]).
replace(X,Y,[X|Xs],[Y|Ys]) :- replace(X,Y,Xs,Ys).
replace(X,Y,[Z|Xs],[Z|Ys]) :- replace(X,Y,Xs,Ys).
```

   (a) (10 points) Describe the set of all outputs of `replace` (using the intended modes) with standard Prolog depth-first search with backtracking.

   (b) (15 points) Use `cut` to transform the definition of `replace` to obtain the intended meaning.

(c) (15 points) Use \= (but not `cut`) to transform the definition of `replace` to obtain the intended meaning.

(d) (15 points) Use arithmetic to transform the definition of `replace` to define a new predicate `replace_n(+N, +X, +Y, +Xs, -Ys)',`
so that `Ys` is derived from the list `Xs` by replacing `N` occurrences of `X` by `Y`. Don't use any unnecessary non-logical constructs.

(e) (10 points) Here is a Prolog predicate intended to compute the length of a difference list. Assume that the - operator has been declared appropriately.

```
dl_length(X-X, 0).
dl_length([H|T]-T1, N) :- dl_length(T-T1, M), N is M+1.
```

Show that this definition is incorrect in the absence of the occurs check by giving the substitution that would be created as a result of the query `dl_length([a | D] - D, N)`. (It may help to remember that `[a | D]` is internally represented as `cons(a,D)`, and `X-X` is represented as `-(X,X)`). What is the (incorrect) value for `N` that results?

3. (15 points) **Uniform provability**

   Recall the definition of a *uniform proof*: a proof in the (intuitionistic) sequent calculus where each occurrence of a sequent with non-atomic right-hand side is the conclusion of the right rule for its top-level connective. E.g., any sequent of the form

   $$\Gamma \longrightarrow A \wedge B$$

   must be the conclusion of the rule $\wedge R$.

   Show that in the intuitionistic propositional sequent caculus (ipMNPS) of Figure 3 there is no uniform proof of $A \vee B \supset B \vee A$. You may assume A and B are atomic.

4. **Operational semantics of Prolog**

This question concerns the "lifting" of a ground calculus for the operational semantics of pure Prolog.

Below are the rules for a system that does not have an explicit goal stack or backtracking, but does have an explicit representation of the program as a context Γ. The judgment $\Gamma \vdash \mathsf{solve}(A)$ means that the interpreter solves the (ground) goal A given program Γ.

$$\frac{}{\Gamma \vdash \mathsf{solve}(\top)} \qquad \frac{\Gamma \vdash \mathsf{solve}(A) \qquad \Gamma \vdash \mathsf{solve}(B)}{\Gamma \vdash \mathsf{solve}(A \wedge B)}$$

$$\frac{\forall \mathbf{x}.\ P' \leftarrow B' \in \Gamma \qquad \begin{array}{l}\mathrm{dom}(\tau) = \mathbf{x} \\ \mathrm{cod}(\tau) = \emptyset \\ P'\tau = P\end{array} \qquad \Gamma \vdash \mathsf{solve}(B'\tau)}{\Gamma \vdash \mathsf{solve}(P)}$$

(a) (8 points) Below is a sketch of the rule for atomic goals in a lifted version of this calculus with judgment $\Gamma \vdash A \mid \theta$. But we have omitted the subgoal to be solved and the answer substitution in the conclusion. Fill in the omitted parts of the rule.

For reference, the unification algorithm is given in Figure 4. As a reminder, we write the application of substitution θ to term t as $t\theta$, and the composition of substitutions θ_1 and θ_2 as $\theta_1\theta_2$.

$$\frac{\forall \mathbf{x}.\ P' \leftarrow B' \in \Gamma \qquad \begin{array}{l}\mathrm{dom}(\rho) = \mathbf{x} \\ \mathrm{cod}(\rho) \cap \mathrm{FV}(P) = \emptyset \\ P'\rho \doteq P \mid \theta_1\end{array} \qquad \Gamma \vdash \mathsf{solve}(\boxed{}) \mid \theta_2}{\Gamma \vdash \mathsf{solve}(P) \mid \boxed{}}$$

(b) (7 points) Give the other rules for the lifted version of the calculus.

(c) (10 points) With the program $\Gamma = \forall x.p(x) \leftarrow q(x) \wedge r(x), q(a) \leftarrow \top, r(a) \leftarrow \top$, here is a deduction in the ground system of $\Gamma \vdash \mathsf{solve}(p(a))$. Since the program Γ never changes, we don't show it explicitly.

$$\dfrac{\dfrac{\dfrac{q(a)(\cdot) = q(a) \qquad \overline{\mathsf{solve}(\top)}}{\mathsf{solve}(q(a))} \qquad \dfrac{r(a)(\cdot) = r(a) \qquad \overline{\mathsf{solve}(\top)}}{\mathsf{solve}(r(a))}}{\mathsf{solve}(q(a) \wedge r(a))} \qquad p(x)(a/x) = p(a)}{\mathsf{solve}(p(a))}$$

Give a corresponding deduction in the same style for the goal $p(y)$ (with the same program) in your lifted system. Note that y is a *variable*. Show unification goals and their answer subsitutions, but omit the unification deductions. For example you might show $p(x) \doteq p(a) \mid (a/x)$. For the sake of brevity, omit both the program Γ and the judgment form solve.

Useful Rules

Note: P always refers to an atomic proposition; A, B, C, etc. refer to arbitrary propositions.

$$\frac{}{\Gamma, P \longrightarrow P}\ \text{init}$$

$$\frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge R \qquad \frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ \wedge L$$

$$\frac{}{\Gamma \longrightarrow \top}\ \top R \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \top \longrightarrow C}\ \top L$$

$$\frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B}\ \vee R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \longrightarrow C \quad \Gamma, B \longrightarrow C}{\Gamma, A \vee B \longrightarrow C}\ \vee L$$

$$\text{no } \bot R \text{ rule} \qquad \frac{}{\Gamma, \bot \longrightarrow C}\ \bot L$$

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\ \supset R$$

$$\frac{P \in \Gamma \quad \Gamma, B \longrightarrow C}{\Gamma, P \supset B \longrightarrow C}\ P \supset L$$

$$\frac{\Gamma, D \supset (E \supset B) \longrightarrow C}{\Gamma, (D \wedge E) \supset B \longrightarrow C}\ \wedge \supset L \qquad \frac{\Gamma, B \longrightarrow C}{\Gamma, \top \supset B \longrightarrow C}\ \top \supset L$$

$$\frac{\Gamma, D \supset B, E \supset B \longrightarrow}{\Gamma, (D \vee E) \supset B \longrightarrow C}\ \vee \supset L \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \bot \supset B \longrightarrow C}\ \bot \supset L$$

$$\frac{\Gamma, E \supset B, D \longrightarrow E \quad \Gamma, B \longrightarrow C}{\Gamma, (D \supset E) \supset B \longrightarrow C}\ \supset \supset L$$

Figure 1: Rules for G4ip.

$$\frac{}{\Gamma, P \longrightarrow P}\ \text{init}$$

$$\frac{\Gamma \longrightarrow A \quad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge R \qquad \frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ \wedge L$$

$$\frac{}{\Gamma \longrightarrow \top}\ \top R \qquad \frac{\Gamma \longrightarrow C}{\Gamma, \top \longrightarrow C}\ \top L$$

$$\frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B}\ \vee R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\ \vee R_2 \qquad \frac{\Gamma, A \longrightarrow C \quad \Gamma, B \longrightarrow C}{\Gamma, A \vee B \longrightarrow C}\ \vee L$$

$$\text{no } \bot R \text{ rule} \qquad \frac{}{\Gamma, \bot \longrightarrow C}\ \bot L$$

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\ \supset R \qquad \frac{\Gamma, A \supset B \longrightarrow A \quad \Gamma, B \longrightarrow C}{\Gamma, A \supset B \longrightarrow C}\ \supset L$$

Figure 2: Rules for the restrictive sequent calculus

$$\frac{}{\Gamma, P \longrightarrow P}\ \text{init} \qquad \frac{}{\Gamma, \bot \longrightarrow C}\ \bot L$$

$$\frac{\Gamma, A, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\ \wedge L \qquad \frac{\Gamma \longrightarrow A \qquad \Gamma \longrightarrow B}{\Gamma \longrightarrow A \wedge B}\ \wedge R \qquad \frac{}{\Gamma \longrightarrow \top}\ \top \mathsf{R}$$

$$\frac{\Gamma, A \longrightarrow C \qquad \Gamma, B \longrightarrow C}{\Gamma, A \vee B \longrightarrow C}\ \vee L \qquad \frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B}\ \vee R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\ \vee R_2$$

$$\frac{\Gamma \longrightarrow A \qquad \Gamma, B \longrightarrow C}{\Gamma, A \supset B \longrightarrow C}\ \supset L \qquad \frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\ \supset R$$

Figure 3: Rules for the intuitionistic propositional sequent calculus ipMNPS

$$\frac{\mathbf{t} \doteq \mathbf{s} \mid \theta}{f(\mathbf{t}) \doteq f(\mathbf{s}) \mid \theta} \qquad \frac{}{(\cdot) \doteq (\cdot) \mid (\cdot)} \qquad \frac{t \doteq s \mid \theta_1 \quad \mathbf{t}\theta_1 \doteq \mathbf{s}\theta_1 \mid \theta_2}{(t, \mathbf{t}) \doteq (s, \mathbf{s}) \mid \theta_1\theta_2}$$

$$\frac{}{x \doteq x \mid (\cdot)} \qquad \frac{x \notin \mathrm{FV}(t)}{x \doteq t \mid (t/x)} \qquad \frac{t = f(\mathbf{t}), x \notin \mathrm{FV}(t)}{t \doteq x \mid (t/x)}$$

Figure 4: Rules for unification