15-399 Constructive Logic

Final Examination

December 19, 2000

Name: ______________________________

Andrew ID: ______________________________

- This is an open-book exam; both handouts and personal notes are allowed. Computers are not permitted.
- Write your answer legibly in the space provided.
- There are 20 pages in this exam, including 5 worksheets.
- It consists of 5 questions worth a total of 300 points.
- You have three hours for this exam.
- Unless otherwise indicated, proofs should be informal, but rigorous and detailed. Clearly state the induction principle you use, the cases you distinguish, and the reasoning in each case.

Problem 1	**Problem 2**	**Problem 3**	**Problem 4**	**Problem 5**	**Total**
60	**60**	**60**	**60**	**60**	**300**

1. Proofs and Proof Terms (60 points)

In this problem we write $B(x)$ for a proposition x which may contain occurrences of x while A stands for a proposition without any free occurrence of x. We are in the setting of first-order logic, so all quantifiers range over a type τ about which we make no assumptions.

1. (20 pts) Give a formal constructive proof of $(A \vee \forall x.\, B(x)) \supset (\forall x.\, A \vee B(x))$. You may use a proof tree representation, or a linear form.

2. (10 pts) Give a proof term reflecting your proof.

3. (20 pts) Prove that the converse, $(\forall x.\ A \vee B(x)) \supset (A \vee \forall x.\ B(x))$, is not intuitionistically valid for arbitrary A and $B(x)$. An informal explanation on why it should not be true will receive partial credit.

4. (10 pts) Prove that $(\forall x.\ A \vee B(x)) \supset (A \vee \forall x.\ B(x))$ is classically true, using the law of excluded middle as only classical rule. [Hint: In classical proofs, the law of excluded middle only needs to be applied to subformulas of the theorem.]

2. Data Representation (60 points)

In this problem we consider the representation of an editor buffer containing some characters and a current cursor position. A buffer state is represented by two lists: one containing the characters before the cursor *in reverse order*, the second containing the characters after the cursor. For example, the buffer

$$\mathrm{a\ b\ c}_{\uparrow}\,\mathrm{d\ e\ f}$$

where the cursor position is marked by '↑', is represented as

$$\langle (\mathrm{c} :: \mathrm{b} :: \mathrm{a} :: \mathbf{nil}), (\mathrm{d} :: \mathrm{e} :: \mathrm{f} :: \mathbf{nil}) \rangle.$$

Therefore, given a type **char** of characters, we have

$$\mathit{buffer} = (\mathbf{char\,list}) \times (\mathbf{char\,list})$$

Fill in the following definitions. In each case give a fully explicit definition in type theory and not an equational specification, although you might write such a specification for our own benefit or for partial credit.

1. (10 pts) $\mathit{insert} \in \mathbf{char} \to \mathit{buffer} \to \mathit{buffer}$
   where *insert* c b inserts c just before the cursor.

2. (10 pts) $\mathit{begin} \in \mathit{buffer} \to \mathbf{bool}$
   where *begin* b returns **true** iff the cursor is at the beginning of the buffer.

3. (10 pts) $\mathit{delete} \in \mathit{buffer} \rightarrow (\mathit{buffer} + \mathbf{1})$
   where *delete b* deletes the character just before the cursor, or indicates that the cursor was at the beginning of the buffer.

4. (10 pts) $\mathit{bob} \in \mathit{buffer} \rightarrow \mathit{buffer}$
   which sends the cursor all the way to the beginning of the buffer.

5. (20 pts) Prove in detail that

$$\forall b \in \mathit{buffer}.\ \mathit{begin}\ (\mathit{bob}\ b) =_B \mathbf{true}$$

If you need to generalize the proposition, clearly state the generalized form and prove carefully that it implies the claim above. If your proof is inductive, clearly state the induction principle you use.

3. Boolean Functions (60 points)

In this problem we explore the representation of Boolean functions by ordered binary decision diagrams. Throughout this problem with assume the ordering $x_i < x_j$ iff $i < j$.

1. (10 pts) Give an explicit definition of the exclusive-or function in type theory.

   $xor \quad \in \quad \mathbf{bool} \rightarrow \mathbf{bool} \rightarrow \mathbf{bool}$

2. (10 pts) In the following we write $b_1 \oplus b_2$ for $xor\ b_1\ b_2$. Show the OBDD for $x_1 \oplus x_2$.

3. (20 pts) Show the OBDD for $((x_1 \oplus x_2) \oplus x_3) \oplus x_4$.

4. (20 pts) In expressing various problems as Boolean satisfiability, a frequently used function is

$$oneof(x_1, \ldots, x_n)$$

which is 1 if and only if *exactly one* of $x_1, \ldots, x_n$ is 1.

Show the OBDD for $oneof(x_1, x_2, x_3, x_4)$.

4. Boolean Satisfiability (60 points)

Let G and H be two graphs, both with the nodes numbered $1, 2, \ldots, n$. We say G and H are *isomorphic* if there is a bijection between their nodes such that there is an edge between two nodes in G if and only if there is an edge between the corresponding nodes in H.

For given graphs G and H, we map this to a Boolean satisfiability problem with variables x_{ij}, with the intention that $x_{ij} = 1$ if and only the bijection relates node i of graph G to node j of graph H.

1. (20 pts) Write down a Boolean formula b involving x_{ij} that is satisfiable if and only if the relation is a bijection between the nodes.

2. (20 pts) Construct a Boolean formula c that guarantees that there is an edge between nodes in G if and only if there is an edge between the corresponding nodes in H. You may introduce additional variables, but you should make sure to constrain them properly.

3. (10 pts) Is the satisfiability of $b \cdot c$ equivalent to the existence of an isomorphism between G and H? Confirm this or state any additional conditions that may be necessary.

4. (10 pts) Analyze the size of your final Boolean formula in big-O notation as a function of n.

5. Computation Tree Logic (60 points)

There are generalizations of CTL that permit reasoning about past states. In this problem we explore such a logic. The intended meaning of the new operators AP ϕ and EP ϕ is

- AP ϕ in state s' if ϕ is true in all states immediately preceding s'.
- EP ϕ in state s' if ϕ is true in some state immediately preceding s'.

In giving introduction and elimination rules below, please make sure to clearly mark new parameters or new assumptions that are introduced.

1. (5 pts) Give the introduction rule for AP.

2. (5 pts) Give the elimination rule for AP.

3. (5 pts) Give the introduction rule for EP.

4. (5 pts) Give the elimination rule for EP.

5. (40 pts) For each of the following propositions, indicate if it is true or not (parametrically in ϕ, the current state, the set of states, and the transition relation). If true, give a formal proof using your rules. If false, provide a finite countermodel with a state s_0 in which the proposition is false.

   (a) (10 pts) $\phi \supset \mathrm{AX}\,(\mathrm{EP}\;\phi)$

   (b) (10 pts) $\phi \supset \mathrm{AX}\,(\mathrm{AP}\;\phi)$

(c) (10 pts) EX (AP ϕ) $\supset \phi$.

(d) (10 pts) EX (EP ϕ) $\supset \phi$.

Worksheet

Worksheet

Worksheet

Worksheet

Worksheet