

DUE: Tue 5 February 2008

**READING**

See Web page for current reading assignments.

**PROBLEMS****1. Hofstadter's Function**

Recursion can be very complex, including arbitrarily “nested” recursions. Here is an interesting one. In Computer Science, “discovery” is usually done by computing examples, and then leaping to a conclusion. But “proof” usually requires a careful induction.

Consider the following recursively (i.e., inductively) defined function, where  $n$  is a *non-negative* integer.

$$g(n) = \begin{cases} n - g(g(n - 1)) & n \geq 1 \\ 0 & n \leq 0 \end{cases}$$

- (a) *Discovery* or **scientific induction**.<sup>†</sup> Discover a simple closed-form (i.e., non-recursive) arithmetic expression for the function  $g$ , of the form  $g(n) = \lfloor \dots n \dots \rfloor$ . Here  $\lfloor x \rfloor$  means “floor of  $x$ , i.e., the largest non-negative integer less than or equal to  $x$ . (*HINT*: it’s “almost” a straight line. Start by approximating it by a straight line and then work on the subtleties. The hint about “floor” is crucial.)

If you cannot determine the expression by the weekend before due date, mail me to receive the answer, so you can proceed to part (b) and receive partial credit.

- (b) *Proof or Formal Deduction*. Prove by **mathematical** induction that your expression is correct.

**2. CNF**

Results like this say that something is true of all possible strings (formulas) of a given language (in this case all propositional formulas.) Such an argument for an “infinite number of cases” calls for induction—induction of the structure of a formula. Note that the set of propositional formulas is defined inductively, and so this makes for a natural way of proving results like this.

Homer & Selman, Homework 1.3.

**3. Tautology and Negation**

- (a) Homer & Selman, Homework 1.2. Note: In AI, automated theorem provers try to prove an assertion  $A$  by negating it, and trying to show that  $\neg A$  is *unsatisfiable*.
- (b) Give an example of a formula  $F$  such that both  $F$  and  $\neg F$  are satisfiable.
- (c) Give an example of a formula  $F$  that is unsatisfiable (i.e., that has *no* satisfying assignments to its variables.)
- (d) Give an example of a formula  $F$  that is satisfied by *all* assignments to its free variables.
- (e) Give an example of a formula  $F$  that has *exactly one* satisfying assignment.
- (f) Give an example of a formula  $F$  that has *exactly two* satisfying assignments.

**4. Enumerable  $\equiv$  Countable**

Homer & Selman, Homework 1.4. One direction is trivial. The other way is harder, and here are some ideas. Assume you have an enumeration of the set  $A$

$$a_0, a_1, a_2, \dots \tag{*}$$

(which might contain some elements repeated many times), you have to show how to construct a 1-1

<sup>†</sup>Also called *scientific inference*.

correspondence from  $N$  onto  $A$  (a bijection.  $h : N \rightarrow A$ ). Note that the enumeration (\*) is really just a function  $a : N \rightarrow_{\text{onto}} A$ , but, because of possible repeats, it is not necessarily a bijection—there could be  $i$  and  $j$  such that  $a(i) = a(j)$ , or in other words one might have  $a_i = a_j$ .

## 5. A Formal System

The following formal system will give you some experience with the process of formal derivation. Think of it as a puzzle that doesn't "mean" anything, so you will not be misled into jumping to conclusions which are outside the system, or not provable in the system itself. If you are having trouble using formal reasoning, I suggest dressing in a tuxedo and black tie ...

**Symbols**†:  $\wedge, \vee, \neg, (, ), p, q, r, \dots$

The symbols  $p, q, r, \dots$  are sometimes called "propositional symbols" or "propositional variables". There are as many propositional symbols as are needed.

**Sentences**‡: any string of symbols described by the following context-free-grammar, having terminal alphabet  $\{p, q, r, \dots\}$  and a single non-terminal  $S$ :

$$\begin{aligned} S &\rightarrow (S \Rightarrow S) \\ S &\rightarrow \neg S \\ S &\rightarrow p \\ S &\rightarrow q \\ &\dots \end{aligned}$$

**Axioms:** The axioms are the following sentences:

1.  $(p \Rightarrow (q \Rightarrow p))$
2.  $((s \Rightarrow (p \Rightarrow q)) \Rightarrow ((s \Rightarrow p) \Rightarrow (s \Rightarrow q)))$
3.  $((\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p))$

**Rules of Inference:** Let  $\phi$  and  $\psi$  be sentences\*.

- I. Any axiom is a theorem.
- II. If  $\phi$  and  $(\phi \Rightarrow \psi)$  are theorems, then  $\psi$  is a theorem\*\*.
- III. If  $\phi$  is a theorem, and if  $\pi$  is obtained from  $\phi$  by substitution [by consistently substituting any sentences for propositional letters in  $\phi$ ], then  $\pi$  is a theorem.

**Theorem:** any sentence which is an axiom, or follows from axioms or other theorems by application of a Rule of Inference.

*Example:* Here is an example derivation of the theorem " $((p \Rightarrow q) \Rightarrow (p \Rightarrow p))$ ":

<i>step</i>	<i>derived sentence</i>	<i>reason</i>
(1)	$((s \Rightarrow (p \Rightarrow q)) \Rightarrow ((s \Rightarrow p) \Rightarrow (s \Rightarrow q)))$	axiom 2
(2)	$((p \Rightarrow (q \Rightarrow p)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow p)))$	by III, substituting $p$ for $s$ , $q$ for $p$ , $p$ for $q$ in (1)
(3)	$(p \Rightarrow (q \Rightarrow p))$	axiom 1
(4)	$((p \Rightarrow q) \Rightarrow (p \Rightarrow p))$	from (2),(3) by II

- (a) Give a derivation for (i.e., prove) the theorem  $(p \Rightarrow p)$
- (b) Prove the *metatheorem*: "if  $(\neg \phi \Rightarrow \neg \psi)$  is a theorem in the system, then  $(\psi \Rightarrow \phi)$  is also a theorem in the system." A metatheorem is a theorem *about* theorems in the formal system; it is not a theorem *in* the formal system, since such "results" just say nonsensical things like  $(p \Rightarrow (p \Rightarrow p))$  [which perhaps can be given meaning but this does not interest us for now].

†The set of symbols is also called the *alphabet*.

‡Sentences are also called *formulas* or *well-formed-formulas (wffs)*

\*Symbols like  $\phi$  that stand for arbitrary sentences are known as *metavariables*.

\*\*Rule II is also known as the rule of *modus ponens*.

## 6. Another Formal System

The following formal system will give you some experience with the process of formal derivation. Since it is just a puzzle, and doesn't "mean" anything, you will not be misled into jumping to conclusions which are outside the system itself.

**Symbols:**  $m \ i \ u$

**Sentences:** any string of symbols

**Axiom:**  $mi$

**Rules of Inference:** Let  $X$  be a sentence.

- I. If  $Xi$  is a theorem, so is  $Xiu$
- II. If  $mX$  is a theorem, so is  $mXX$
- III. In any theorem,  $iii$  can be replaced by  $u$  to yield another theorem
- IV. In any theorem,  $uu$  can be dropped to form another theorem

**Theorems:** any string which follows from the axiom or other theorem by application of a Rule of Inference.

*Remarks:* Rules are one-way; for example, from string  $mu$  you cannot conclude  $mii$ . However, the other direction is legal. Here is an example derivation of a theorem:

<i>step</i>	<i>derived sentence</i>	<i>reason</i>
(1)	$mi$	axiom
(2)	$mii$	from (1) by II
(3)	$miiii$	from (2) by II
(4)	$miiiu$	from (3) by I
(5)	$muiiu$	from (4) by III
(6)	$muiuuuu$	from (5) by II
(7)	$muiiu$	from (6) by IV

So  $muiiu$  is a theorem of this system (as are  $muiiu$  and  $miiii$  for that matter). The axiom is, of course, considered a theorem.

- (a) Give a derivation for (i.e., prove) the theorem  $miiiiiu$
- (b) Prove the *metatheorem*: "every theorem of the system begins with the letter  $m$ ". A metatheorem is a theorem *about* theorems in the formal system; it is not a theorem *in* the formal system, since such "results" just say nonsensical things like  $muiiu$  (which perhaps have meaning to cats).
- (c) Prove the metatheorem: " $mu$  is not a theorem of the system." [HINT: examine how many occurrences of symbol  $i$  can be in any theorem.]