Assignment 2 Solutions

March 11, 2002

4.4.9 Suppose S is a (countable) infinite set of expressions over the variables $x_1, x_2, \ldots$, and suppose that each finite subset of S is satisfiable. For each i, let S_i be the subset of S which contains the expressions involving only the variables $x_1, x_2, \ldots, x_i$. Each S_i is finite, thus satisfiable.

Let G be a (not necessarily complete) binary tree with the following properties: Each node at level i represents a truth assignment for S_i. The root node (level 0) represents the empty truth assignment. A node N at level i which represents the truth assignment T_N may have up to two children: a node which represents $T_N \cup \{x_{i+1} = \textbf{true}\}$ as a left child, and/or a node which represents $T_N \cup \{x_{i+1} = \textbf{false}\}$ as a right child. Finally, a node N is only part of the tree G at level i if its truth assignment T_N satisfies S_i.

Since there are infinitely many S_i, and each S_i is satisfiable, there are infinitely many nodes in G. Thus, by Konig's lemma, G contains an infinitely long path which begins at the node. Label this path P. Since P is infinitely long, it contains a node P_i at each level i. Thus, S is satisfiable, and its satisfying truth assignment is as follows: $x_i = \textbf{true}$ if P_i is a left child in G, and $x_i = \textbf{false}$ if P_i is a right child in G. This completes the proof of the compactness theorem.

4.4.13 Suppose F can be expressed as a circuit C using only AND and OR gates. Then proceed by induction on the depth of C. (Assume without loss of generality that each gate only has, at more, two inputs).

The base case is trivial: the depth of C is 0, and F is a constant function. This is clearly monotone.

Inductive step: Case 1: $F = F_1$ **AND** F_2 for monotone functions F_1 and F_2. Changing one of the inputs from F_1 (or F_2) from **false** to **true** cannot change the value of F_1 (or F_2) from **true** to **false** and thus cannot change the value of F from **true** to **false**. Thus F is monotone.

Case 2: $F = F_1$ **OR** F_2 for monotone functions F_1 and F_2. The argument is identical to Case 1.

Now suppose the F is monotone. Proceed by induction on the arity of F.

The base case is trivial. F is a unary function. Since F is monotone, it cannot be the "negation" function, and is thus either the identity function or it is a constant function. In either case, it has a trivial circuit with no gates.

For the inductive step, suppose that F has arity $k+1$, and furthermore suppose that each monotone function of arity k has a circuit using only **and** and **or** games. So, consider the two functions $F(x_1, x_2, \ldots, x_k, \textbf{false})$ and $F(x_1, x_2, \ldots, x_k, \textbf{true})$. Since F is monotone, these must also be monotone. Furthermore, they have only k variables as inputs. Thus, by the induction hypothesis, they have circuits using only **and** and **or** gates as inputs. Call these circuits C_F and C_T respectively. Note that, since F is monotone, if C_F evaluates to true on a certain set of inputs, then C_T must also evaluate to true on those same inputs. So, F can be expressed by the circuit $C = C_F \vee (C_T \wedge x_k)$. This completes the inductive proof.

5.8.3 This proof is **identical** to the proof in the text of Theorem 5.1, except that,in every place where they account for the amount of time taken, you need to account for the amount of space used. The logarithmic space bound will be easily shown in this way.

Each quantifier increases the space used by a constant factor (ie, it increases the constant hidden in the big-O notation of the $O(logn)$ space). Each quantifier also increases the time bound by a factor of n.

5.8.7 $\phi = \forall x(x \text{ LOVES MYBABY}) \wedge \forall y((\text{MYBABY LOVES } y) \Rightarrow (y = \text{ME}))$

(a) Since everybody loves MYBABY, in particular, MYBABY loves MYBABY. Thus, since MYBABY loves nobody but ME, MYBABY = ME.

(b)

$$\{\phi\} \quad \vdash \quad \forall x(x \text{ LOVES MYBABY})$$

$$
\begin{array}{rl}
& \vdash \text{MYBABY LOVES MYBABY} \\
\{\phi\} & \vdash \forall y((\text{MYBABY LOVES } y) \Rightarrow (y = \text{ME})) \\
& \vdash (\text{MYBABY LOVES MYBABY}) \Rightarrow (\text{MYBABY} = \text{ME}) \\
& \vdash (\text{MYBABY} = \text{ME})
\end{array}
$$

(c) $\phi = \forall x(x \text{ LOVES MYBABY}) \wedge \forall y((\text{MYBABY LOVES } y) \Rightarrow ((y = \text{ME}) \vee (y = \text{MYBABY})))$

5.8.10 Suppose that Δ has no model. Than $\Delta \models \phi$ is vacuously true for all ϕ. In particular, $\Delta \models \phi$ and $\Delta \models \neg\phi$ for some arbitrary ϕ. So by the first form of the completeness theorem, $\Delta \vdash \phi$ and $\Delta \vdash \neg\phi$. Thus Δ is inconsistent. This completes the proof.

5.8.13 (a) REACHABILITY can be expressed by the following second–order existential statement:

$$
\begin{array}{rll}
\phi(u,v) = \exists P & (& \forall x \forall y \forall z((\neg P(x,x)) \wedge ((P(x,y) \wedge P(y,z)) \Rightarrow P(x,z)) \\
& \wedge & \forall x \forall y((P(x,y) \wedge \forall z(\neg P(x,z) \vee \neg P(x,y))) \Rightarrow G(x,y)) \\
& \wedge & ((u = v) \vee P(u,v)))
\end{array}
$$

The first line ensures that P is transitive but not reflexive. The second line ensures that consecutive nodes in P are adjacent in G. The third line ensures that the two nodes are either the same node, or are related by P.

(b) UNREACHABILITY can be expressed by the following second–order existential statement:

$$\phi(u,v) = \exists P(P(u) \wedge \forall x \forall y((P(x) \wedge G(x,y)) \Rightarrow P(y)) \wedge \neg P(v))$$

In this case, $P(x)$ if and only if x is reachable from u.

5.8.14 (a) $P^M \subseteq P^{M'}$, so $M \models P(\mathbf{x}) \rightarrow M' \models P(\mathbf{x})$ for any $\mathbf{x}$. Since P occurs only positively in ϕ, and M and M' are identical in all other respects, $M \models \phi \Rightarrow M' \models \phi$.

(b) Since P is taken to be the set of even natural numbers, it is clear that "$\exists z \neg P(z)$" is satisfied, since our universe contains non-even (ie, odd) numbers.

To see that $(\mathbf{N}, 2\mathbb{N})$ is P–minimal, suppose that there is some proper subset S of $2\mathbb{N}$ such that $(\mathbf{N}, S) \models P(x) \Leftrightarrow (x = 0 \vee \exists y(P(y) \wedge x = y + 2))$. Since S is a proper subset of $2\mathbb{N}$, let v be the smallest even natural number not in S (it must exist). Clearly, v cannot be 0, since $(v = 0) \Rightarrow P(v)$. But, since $v = (v - 2) + 2$, it is also true that $(P(v - 2) \Rightarrow P(v)$. Thus $P(v - 2)$ must also be false, which contradicts the minimality of v.

(c) First, note that if F is taken to be the reflexive–transitive closure of G, then $(G, F) \models P(x, y) \Leftrightarrow ((x = y)) \vee \exists z(P(x, z) \wedge G(z, y)))$. This is clear by inspection.

Also, suppose that there is a path between nodes u and v in G. Then, by induction on the length of the path, it is clear that for any model (G, F') which satisfies the given fixpoint expression, $(u, v) \in F'$. So the reflexive–transitive closure is in fact P–minimal, as desired.

Also, since for any model (G, F') which satisfies the fixpoint expression, the reflexive–transitive closure F of G must be a subset of F', it is clear that no other model can be $P--minimal$. So, indeed, (G, F) is the only model that satisfies the expression, as desired.

(d) By induction on i: $F_0 = \emptyset$, so clearly $F_0 \subseteq F_1$.

Now say $F_{i-2} \subseteq F_{i-1}$. Also suppose $(v_1, v_2, \ldots v_r) \in F_{i-1}$. So, by definition of F_{i-1}, $(G, F_{i-2}) \models \psi[x_1 \leftarrow v_1, \ldots, x_r Rightarrow v_r]$. So, since $F_{i-2} \subseteq F_{i-1}$, it is also true that $(G, F_{i-1}) \models \psi[x_1 \leftarrow v_1, \ldots, x_r Rightarrow v_r]$ (by part (a)), and so $(v_1, v_2, \ldots v_r) \in F_i$ by definition of F_i. Thus $F_{i-1} \subseteq F_i$ as desired.

(e) By induction on i: $F_0 = \emptyset$ so clearly $F_0 \subseteq F$.

Now say $F_{i-1} \subseteq F$. Suppose $(v_1, v_2, \ldots v_r) \in F_i$ So by definition, $(G, F_{i-1}) \models \psi[x_1 \leftarrow v_1, \ldots, x_r Rightarrow v_r]$. So $(G, F) \models \psi[x_1 \leftarrow v_1, \ldots, x_r Rightarrow v_r]$. (Since $F_{i-1} \subseteq F$, and by part (a)), and so $(v_1, v_2, \ldots v_r) \in F$. Thus $F_i \subseteq F$, as desired.

(f) At each stage we add at least one r–tuple to F (we stop when we reach a stage where nothing is added). So there can be no more steps then there are r–tuples. The number of different r–tuples is n^r, which is polynomial in n (remember that r is a constant). So we terminate in polynomial time.

To see that our result (F) is the unique minimal model of ψ, we use an argument similar to that used in part (c). Note that at each stage, the tuples that we add *must* be a subset of any model F' of ψ. Thus, if F' is a correct model, $F \subseteq F'$. So F' cannot be P–minimal unless if $F' = F$, otherwise ψ would be modeled by a proper subset of F'.

(g) To solve an instance of $(\phi : P = \psi^*)$–GRAPHS in polynomial time, simply run the polynomial–time algorithm developed above to get a list of tuples in the relation P, and then check to see if the first–order relation ψ is true (also in polynomial time). Output "yes" or "no" accordingly.

(h) In the REACHABILITY example, each F_i is the set of pairs of nodes which have a path of length less than or equal to i joining them.

1. 6.4.3 We know that number theory (NT) is not axiomatizable, but if it were, then it would be decidable. That is, using Goedel's Incompleteness theorem, we notice that all proofs in number theory can be derived from logical axioms, number theory axioms or from modus ponens.

   We also know that group theory (GT) is axiomatizable, since there are axioms (**GR1-GR3**) for group theory. Notice that we can prove all properties of groups from these axioms. However, in order to be decidable, we would need to allow proofs from an arbitrarily large number of premises: that is, in order to show, for example, that groups are finitely generated, we would need to use *mathematical induction*, which is a technique stronger than modus ponens, and would require infinitely many premises.