Lent Term 2008 J. M. E. Hyland

Set Theory and Logic: Example Sheet 3

1. Which of the following propositions are tautologies?
   (a) $(A \to B) \to (B \to A)$. (b) $(A \to (B \to C)) \to (B \to (A \to C))$.
   (c) $(A \to (B \to C)) \to ((A \to B) \to C))$. (d) $((A \to B) \to C)) \to (A \to (B \to C))$. In case the proposition is a tautology, use the Deduction Theorem to show that there is a proof in the propositional calculus.

2. (i) Consider the propositional calculus based on $\to$ and without the constant $\perp$. take a special propositional r and define $\neg A$ to be $A \to r$. Show that the following are all provable.
   (a) $(A \to \neg B) \to ((A \to B) \to \neg A)$. (b) $A \to \neg\neg A$.
   (c) $(A \to B) \to (\neg B \to \neg A)$. (d) $(A \to B) \to ((A \to \neg B) \to \neg A)$.
   Show that $\neg\neg A \to A$ is not in general provable. For which A is $\neg\neg A \to A$ is provable?
   (ii) Suppose that a formula $A(r)$ (where we indicate the occurences of r) is such that $A(\perp)$ is provable in the propositional calculus, while $A(r)$ is not provable. Show that any proof of $A(\perp)$ involves a use of the double negation axiom $\neg\neg A \to A$.

3. A proof $A_1, A_2, \cdots A_n = A$ is said to have n *lines*. Examine the proof of the Deduction Theorem to show that if we have a proof for $\Gamma, A \vdash B$ in n lines, then we have one for $\Gamma \vdash A \to B$ in at most $3n+2$ lines. In lectures we showed $\perp \vdash B$ and then $\neg A \vdash A \to B$. Give sensible upper bounds for the number of lines in proofs of these.

4. Three people each have a set of beliefs: a consistent deductively closed set. Show that the set of propositions that they all believe is also consistent and deductively closed. Must the set of propositions that a majority believe be consistent? Must it be deductively closed?

5. Let $t_1, t_2, \ldots$ be propositions such that, for every valuation v, $v(t_n) = \top$ for some n. Use the Compactness Theorem to show that in fact we may bound the values of n: there must be an N such that, for every valuation v, there exists $n \leq N$ with $v(t_n) = \top$.

6. A set S of propositions is a *chain* if for any distinct $p, q \in S$ we have $p \vdash q$ or $q \vdash p$ but not both. Write down an infinite chain. If the set of primitive propositions is allowed to be uncountable, can there exist an uncountable chain?

7. Formulate sets of axioms in suitable languages (to be specified) for the following.
   (i) Fields of characteristic 2. (ii) Algebraically closed fields.
   (iii) Groups of order 60. (iv) Simple groups of order 60.
   (v) Posets with no maximal element. (vi) Real vector spaces

8. Let T be the theory generated by the following infinite set of axioms.

$$\exists x. x = x \qquad \forall x, y. s(x) = s(y) \to x = y \qquad \forall y \exists x. s(x) = y$$

$$\forall x. s(x) \neq x \qquad \forall x. s^2(x) \neq x \qquad \forall x. s^3(x) \neq x \qquad \cdots .$$

   Show that T has no finite models and describe the countable models of T. Show that T is complete: for every sentence ϕ of the language in question either ϕ or $\neg\phi$ is in T.

9. Show that a theory with arbitrarily large finite models has an infinite model. (So if a theory has only finite models, then there is a bound on the size of a model.)

10. (i) Suppose that a sentence ϕ is true in all fields of characteristic 0. Show that it is true in all fields of sufficiently large prime characteristic.
(ii) Is there a finite set of axioms characterising fields of characteristic 0?
(iii) Is there a set of axioms characterising the fields of characteristic not equal to 0?

11. (i) Suppose that $\vdash \exists x.\phi(x)$, where ϕ is quantifier-free with just x free. Show that the set $\{\neg\phi(t) \mid t \text{ is a closed term}\}$ is inconsistent. Deduce that there are closed terms $t_1, \cdots, t_n$ such that $\vdash \phi(t_1) \vee \cdots \vee \phi(t_n)$.
(ii) Suppose that $\vdash \forall x.\exists y.\phi(x, y)$, where ϕ is quantifier-free with just x and y free. What can you deduce? Can you say anything about $\vdash \exists x.\forall y.\exists z.\phi(x, y, z)$?

12. A graph is bipartite or 2-colourable if we can partition the set of vertices into sets B and R such that the only edges lie between vertices in different sets.
(i) Show that if any finite subgraph of a graph is bipartite, then so is the graph itself.
(ii) Write down a set of axioms characterising bipartite graphs in the language of graphs.
(iii) Is there a single first-order sentence characterising bipartite graphs?

13. Is there a theory in the first order language for groups which axiomatizes the following?
(i) Groups all of whose elements are of finite order.
(ii) Groups all of whose non-unit elements are of infinite order.
(iii) Groups with some non-identity element of finite order.
(iv) Groups with some element of infinite order.

14. A theory T admits elimination of quantifiers just when for every formula $\phi(\mathbf{x})$ there is a quantifier-free formula $\psi(\mathbf{x})$ such that ϕ and ψ are equivalent modulo T.
(i) Let T be a theory. Consider formulae of the form $\exists x.\phi(x, \mathbf{y})$ where $\phi(x)$ is a conjunction of basic formulae. Suppose that any such formula is equivalent modulo T to a quantifier-free formula. Show that T admits elimination of quantifiers.
(ii) Show that both the theory of an infinite set, and the theory of dense linear orders without endpoints admit elimination of quantifiers.

15. Show that there is no first order theory characterising connected graphs.
(If, very wickedly, you look for help on the web, you may find some information about so-called locality properties in finite model theory. You do not need such general theory to answer this question.)

16. (This final question is not the hardest, but is just a curiosity for this course.)
(i) Show that Peirce's Law $((A \to B) \to A) \to A$ is always a tautology. Use the Deduction Theorem to show that $\vdash ((A \to B) \to A) \to A$.
Is $((A \to B) \to A) \to A$ provable without a use of the double negation axiom?
(ii) Consider the Propositional Calculus without the constant $\perp$. Take as axioms the first two axioms viz $A \to (B \to A)$ and $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$, together with Pierce's Law; and take the usual rule MP of modus ponens as rule of inference. State and prove a version of the Completeness Theorem.
(This should throw light on the approach to the Completeness Theorem in lectures. Did we really need to prove Model Existence first?)

Comments, corrections and queries can be sent to me at `m.hyland@dpmms.cam.ac.uk`.