Homework Assignment 7 - Hints

Due **Friday 2-04-04**

(Double Assignment)

Part I

1. Define a Non-Deterministic Finite State Automaton N on the alphabet $A = \{0, 1\}$ which accepts exactly the language $\mathcal{L} = \{u \in A^* | u = w0xy\}$, i.e., precisely the words on A where the third letter from the end is 0. Define a Deterministic Finite State Automaton M equivalent to N and find the minimal deterministic automaton equivalent to N.

(*5 points*)

No hint here! (You know how to do this.)

2. Let $f : N \times N \to N$ be a total function. Given an Abacus Machine that computes f, define an Abacus Machine that computes the total function $h(m, n) = \mu y < n.f(m, y) = 0$, i.e., the function which maps the arguments m, n to the least $y < n$ such that $f(m, y) = 0$, if such a y exists, and returns n otherwise.

(*5 points*)

An Abacus Machine is just a register machine! (You know how to do this.)

3. Let $A(x, y)$ be a binary predicate, and consider the following formulas

$B = \forall x.\neg A(x, x)$

$C = \forall x.\forall y.\forall z.(A(x, y) \wedge A(y, z) \to A(x, z))$

$D = \forall x.\exists y.A(x, y)$

Thus $(B \wedge C) \wedge D$ says that the universe of discourse is a strict ordering without maximal points. Show that $(B \wedge C) \wedge D$ has an infinite model but no finite model.

(*5 points*)

Hint: Suppose $\mathcal{M} : (M, <_{\mathcal{M}})$ is an interpretation for the language $\mathcal{L} = \{A^2\}$. What does it means that to say that a pair $\sigma = (\mathcal{M}, \alpha)$ satisfies B, C and D? Work through Tarski's definition, page 8 of Handout 5 (available here). Suppose M is finite and derive a contradiction, by showing that if the relation $<_{\mathcal{M}}$ on M is transitive and has no maximal points then it cannot be irreflexive - i.e., if $C^\sigma = T$ and $D^\sigma = T$ then $B^\sigma = F$.

Part II

4. Apply the "semantic tableaux procedure" to the following formulas. If the formula is not valid, construct an interpretation that falsifies it.

(i) $((A \to B) \to A) \to A$.

(*2.5 points*)

Hint: Apply the "semantic tableaux" procedure (pages 2-5 of Handout 5) to the formula $((\neg A \vee B) \wedge \neg A) \vee A$ which is logically equivalent to (i).

(ii) $(\forall x.\exists y.A(x,y)) \to (\exists y.\forall x.A(x,y))$

(2.5 points)

Hint: Apply the "semantic tableaux" procedure (pages 10-14 of Handout 5) to the formula $(\exists x.\forall y.\neg A(x,y)) \vee (\exists y.\forall x.A(x,y))$ which is logically equivalent to *(ii)*. After some steps you should be able to recognize that the procedure does not terminate, yielding an infinite open branch β. Let $M = \{a_0, a_1, a_2, \ldots\}$ be the set of parameters introduced in β. Set

$$< a_i, a_j > \in <_{\mathcal{M}} \text{ if and only if } \ldots$$

in such a way that both $\exists x.\forall y.\neg A(x,y)$ and $\exists y.\forall x.A(x,y)$ are false in $\mathcal{M}$.

(iii) $(\forall x.A(x)) \to (\forall y.B(y)) \to \exists x.\forall y.(A(x) \to B(y))$

(2.5 points)

Hint: Apply the "semantic tableaux" procedure (pages 10-14 of Handout 5) to the formula $(\forall x.A(x) \wedge \exists y.\neg B(y)) \vee (\exists x.\forall y.\neg A(x) \vee B(y))$ which is logically equivalent to *(ii)*.

(5) Show that there are infinitely many prime numbers of the form $6n - 1$.

(7.5 points)

Hint: Follow the proof of Exercise 1 in Homework 5. Write q_n for the n-th prime of the form $6k - 1$, i.e., equivalent to 5 (mod 6). Clearly $q_1 = 5$. For the inductive step, suppose

$$q_1, \ldots, q_n \text{ are all the prime numbers of the form } 6k - 1 \qquad (*)$$

and let $c = 6(q_1 \cdot \ldots \cdot q_n) - 1$. Notice that $c > q_n > \ldots > q_1$, hence if assumption $(*)$ is true, then c cannot be prime, hence it must be divisible by some prime. Now you have to consider all possible prime divisors p of c; here you have the following cases:

1. $p = 2 \pmod 6$; (*c is odd.*)
2. $p \equiv 1 \pmod 6$; (*c cannot be devided only by prime numbers of this form.*)
3. $p \equiv 3 \pmod 6$; (*can c be divided by a number of the form $6n + 3$?*)
4. $p \equiv 5 \pmod 6$.

You must show that c must be divisible by some q_i and then conclude that this is impossible, hence assumption $(*)$ is false and so there must be a prime $q_{n+1} \leq c$.