Additional Exercises for

# The Calculus of Computation

by Aaron R. Bradley and Zohar Manna
(published by Springer)

October 29, 2007

This document contains exercises of two types: those that we failed to think of before publication; and those that address technical errors in the book.

## Chapter 7

1. (**★Divides constraints**) Prove the important direction of Theorems 7.13 and 7.15: that solutions to the original divides constraints are reported as solutions.

## Chapter 10

1. (**Theories with Equality**) In Chapter 10, we failed to appreciate a subtle point: the concept of *stably infinite* theories is typically treated in the context of a variation of FOL in which equality is explicitly part of the logic (see [92]), whereas we treat the predicate $=$ like any other. When equality is explicitly part of the logic, each domain element of an interpretation differs from every other element. However, when $=$ is interpreted (for example, in $T_{\mathsf{E}}$), a domain may have multiple elements that are deemed equal. This situation interferes with the definition of *stably infinite*. ((a) Why?) The following two corrections address the issue:
   - Correction of definition on page 284: A theory $T$ **has equality** if its signature $\Sigma$ includes the binary predicate $=$; its axioms imply reflexivity, symmetry, and transitivity of equality; and *its other functions and predicates obey the* (function congruence) *and* (predicate congruence) *axiom schemata.*
   - Correction of definition on page 270: A theory $T$ that has equality is **stably infinite** if for every quantifier-free $\Sigma$-formula $F$, if $F$ is $T$-satisfiable, then there exists some $T$-interpretation that satisfies $F$ and that has a domain *whose quotient by (the interpretation of)* $=$ *is of infinite cardinality; that is; there is an infinite number of unequal elements.*

   b) Suggest a theory that is not stably infinite but that would be considered "stably infinite" according to the definition in the book. *Hint: See Example 10.2 on page 270, but add the axioms of equality.* Why is it actually stably infinite?

   c) Describe a method for constructing from any interpretation of a theory with equality a similar interpretation but in which each element of the domain differs from every other element according to the interpretation of $=$. *Hint: Recall from Chapter 9 that the quotient of a set by a congruence relation is a set isomorphic to taking one representative per congruence class.*

   d) What problem does the incorrect definition of *stably infinite* cause in the proof of Theorem 10.16?

2. (**★More than two theories**) To extend the Nelson-Oppen procedure to $n$ theories $T_1, \ldots, T_n$, $n > 2$, one could in principle compose the theories incrementally: combine $T_1$ with $T_2$; then combine $T_1 \cup T_2$ with $T_3$, and so on. However, one additional fact is needed: *the combination theory $T_1 \cup T_2$ is stably infinite if both $T_1$ and $T_2$ are stably infinite.* (Please review the previous exercise first.)

   a) Prove that the correct definition of **stably infinite** given in the previous exercise is equivalent to the following statement: A theory $T$ with signature $\Sigma$ is stably infinite if for every quantifier-free $\Sigma$-formula $F$, each $T$-interpretation $I$ of $F$ can be extended to a $T$-interpretation whose domain has infinite cardinality (and in particular is such that the quotient of the domain by $=$ also has infinite cardinality; that is, there is an infinite number of unequal elements). *Hint: Consider constructing a $\Sigma$-formula describing a given interpretation with a finite domain.*

   b) Use this new definition to argue that $T_1 \cup T_2$ is stably infinite when $T_1$ and $T_2$ are.

## Chapter 11

1. (**Sets and Multisets**)

   a) Define a theory $T_{\mathsf{S}}$ of finite sets with signature

   $$\Sigma_{\mathsf{S}} = \{=,\ \cup,\ \setminus,\ \subset,\ \in\}$$

   that includes the basic set operations union ($s_1 \cup s_2$) and set complement ($s_1 \setminus s_2$, which consists of the elements of $s_1$ that are not elements of $s_2$); and predicates subset ($s_1 \subset s_2$), membership ($e \in s_1$), and equality ($s_1 = s_2$). Describe a decision procedure that reduces quantifier-free $\Sigma_{\mathsf{S}}$-formulae to equisatisfiable $\Sigma_{\mathsf{A}}$-formulae in the array property fragment.

   b) Define a theory $T_{\mathsf{M}}$ of finite multisets with signature

   $$\Sigma_{\mathsf{M}} = \{=,\ \uplus,\ \setminus,\ \mathsf{C},\ \subset,\ \mathsf{setof}\}\ .$$

   A multiset is like a set except that it allows multiple occurrences of elements. The *count* function $\mathsf{C}(s, e)$ returns the number of occurrences of $e$ in $s$. $s_1 \uplus s_2$ is the multiset union of $s_1$ and $s_2$: $\mathsf{C}(s_1 \uplus s_2, e) = \mathsf{C}(s_1, e) + \mathsf{C}(s_2, e)$. For multiset complement, $\mathsf{C}(s_1 \setminus s_2, e) = \max(0,\ \mathsf{C}(s_1, e) - \mathsf{C}(s_2, e))$. Similarly, $s_1 \subset s_2$ iff $\mathsf{C}(s_1, e) \leq \mathsf{C}(s_2, e)$ for all elements $e$ of $s_2$. Finally, the $\mathsf{setof}$ function maps multisets to sets: $\mathsf{C}(\mathsf{setof}(s), e) = 1$ iff $\mathsf{C}(s, e) > 0$, and 0 otherwise. Describe a decision procedure that reduces quantifier-free $\Sigma_{\mathsf{M}}$-formulae to equisatisfiable $\Sigma_{\mathsf{A}}$-formulae in the array property fragment.