Automated Reasoning and Program Verification

Final Assignment
Due March 27, 2015

Problem 1. (20 points) Consider the following formula:

$$x = a \rightarrow x = b$$

where x is a variable and a, b are constants.

Describe the class of interpretations that makes this formula valid.

Problem 2. (20 points)
Consider a signature Σ with a single sort s, with two constants a and b, and with a unary function symbol f. Let I be an interpretation of Σ and D is the domain of s in I. We know the following about I:

- the formulas $a \neq b,\ x = f(f(x))$, and $x \neq y \rightarrow f(x) \neq f(y)$ are valid in I;
- for every u in D, there is a term t of s such that t has no variables and $t^I = u$.

Find all possible values for the number of elements in D.

Problem 3. (20 points) Use the decision procedure of $\mathcal{T}_E$ to decide satisfiability of the following formula:

$$(a = b \ \vee \ f(a) = b) \ \wedge \ f(f(a)) \neq b \ \wedge \ f(b) = b.$$

Provide a level of details.

Problem 4. (20 points) Apply the decision procedure of $\mathcal{T}_A$ to decide satisfiability of the following formula:

$$read(write(write(A, i, e), j, f), k) = g \ \wedge \ j \neq k \ \wedge i = j \ \wedge read(A, k) \neq g.$$

Provide a level of details.

Problem 5. (20 points)
Establish the satisfiability or the unsatisfiability of the following formula:

$$a = b + 2 \wedge \big(read(write(B, a + 1, 4), b + 3) = 2 \ \vee \ f(a - 1) \neq f(b + 1)\big),$$

where a, b are constants, f is an uninterpreted function symbol, B is an array constant, and $+, -, 1, 2, 3, 4$ are interpreted in the standard way over the integers.

Use reasoning in the combination of the theories of arrays, uninterpreted functions, and linear arithmetic. Use the decision procedures for the theory of arrays and the theory of uninterpreted functions, and use simple mathematical reasoning for deriving new equalities among the constants in the theory of arithmetic. Provide a sufficiently detailed explanation of your work.