Decision Procedures and Verification

Seminar 9

1. (1 point) [Manual proof] Show the validity of the following formula with the help of read-over-write axiom:

$$(\forall x \in \mathbb{N}. x < i \Rightarrow a[x] = 0) \land (\forall j. a'[j] = a\{i \leftarrow 0\}[j]) \Rightarrow (\forall x \in \mathbb{N}. x \leq i \Rightarrow a[x] = 0)$$

2. (1 point) [Decision procedure for quantifier-free fragment of array theory] Decide the satisfiability of the following formula using the decision procedure for quantifier-free fragment:

$$i_1 = j \land i_1 \neq i_2 \land a[j] = e_1 \land a\{i_1 \leftarrow e_1\}\{i_2 \leftarrow e_2\}[j] \neq a[j]$$

3. (1 point) [Decision procedure for array property fragment] Decide the validity of the formula from exercise 1 using the decision procedure for array property fragment.

4. (1 point) [Pointer formulas] Determine if the following pointer logic formulas are valid using the semantic translation:

   - $x = y \Rightarrow \&x = \&y$
   - $\&x \neq x$
   - $\&x \neq y + i$
   - $p = \&x \land x = 1 \Rightarrow *p = 1$
   - $*p = x \Rightarrow p = \&x$