Exercise 5

Given two FA $A_I$ and $A_S$ describing an implementation $I$ and specification $S$, respectively. Explain in detail how to check whether $I$ conforms to $S$, given $A_I$ and $A_S$. Illustrate your explanations using set diagrams.

Exercise 6

Check conformance of implementation $I$ and specification $S$ given as FA on the right.

Exercise 7

Let $f_1 := (x \lor y \lor z) \land (\neg x \lor y \lor z) \land (\neg x \lor y \lor \neg z) \land (\neg x \lor y \lor \neg z)$ and $f_2 := (\neg x \lor \neg z) \land (x \lor y)$ be propositional formulae in conjunctive normal form (CNF) over a set of Boolean variables $V := \{x, y, z\}$. Assume that $f_1$ characterizes an implementation and $f_2$ a specification.

Does $f_1$ conform to $f_2$? Is $f_1 \land \neg f_2$ satisfiable? Justify your answers by constructing a truth table.

Exercise 8

a) Read sections I and III “Software Model Checking” in the survey on software verification\(^1\) and describe the approach of counterexample-guided abstraction refinement (CEGAR).

b) Given variables $i, n \in \mathbb{Z}$ (integers), the predicate $a \leftrightarrow (i \leq n)$ and the action $\alpha := i++$. Predicate $a$ defines two abstract states $a$ and $\neg a$, i.e. $a$ can hold or not. Draw an abstract transition system by adding all possible transitions between states $a$ and $\neg a$ when action $\alpha$ is executed: how does executing $\alpha$ influence the value of predicate $a$? What is the difference when interpreting $i, n$ and $\alpha$ over 32-bit Java integers with overflow semantics?

\(^1\)V. D’Silva, D. Kroening, G. Weissenbacher: A Survey of Automated Techniques for Formal Software Verification. IEEE TCAD 27(7), 2008. The article can be found in KUSSS.