Problem Sheet 8: Model Checking

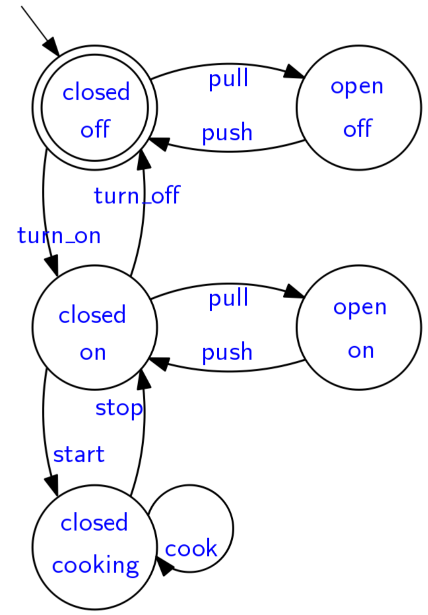
Chris Poskitt and Carlo A. Furia
ETH Zürich

The exercises in this problem sheet are all based on the first set of lecture slides on model checking:

http://se.inf.ethz.ch/courses/2013b_fall/sv/slides/11-ModelChecking.pdf

1 Evaluating LTL Formulae on Automata

Consider the the following automaton:



Do the following properties hold? Justify your judgements.

i. $\Box$ (start $\rightarrow \Diamond$ stop)

ii. $\Box \Diamond$ turn_off

iii. $\Box \Diamond$ (turn_off $\vee$ push)

iv. $\Diamond$ (turn_off $\vee$ push)

v. ($\Box$ false) $\vee \Diamond$ (turn_off $\vee$ push)

vi. (turn_on U start) $\vee$ (pull U push)

2 Equivalence of LTL Formulae

These exercises are about proving the equivalence of LTL formulae. In the first two of these exercises, you will be proving that the operators $\Diamond$ and $\Box$ are *derived*, i.e. they can be defined entirely in terms of the core LTL operators.

i. Recall that $w, i \models \Diamond F$ if there exists some j such that $i \leq j \leq n$ and $w, j \models F$.

   Prove that this is also the case for $w, i \models \text{true} \ \mathsf{U} \ F$ (i.e. that this is an equivalent way of expressing $\Diamond F$ as a derived operator).

ii. Recall that $w, i \models \Box F$ if for all j such that $i \leq j \leq n$, $w, j \models F$.

   Prove that this is also the case for $w, i \models \neg\Diamond\neg F$ (i.e. that this is an equivalent way of expressing $\Box F$ in terms of other LTL operators).

iii. Prove that $\Diamond$ is *idempotent*, i.e. that $\Diamond p$ is equivalent to $\Diamond\Diamond p$.

3 Automata-Based Model Checking

Let us prove by *model checking* that $\Box \ \Diamond$ turn_off is not a property of the microwave oven automaton in Section 1.

i. Build an automaton with the same language as $\neg(\Box \ \Diamond$ turn_off$)$.

   Hint: start with the non-negated formula and then invert the accepting and non-accepting states of its automaton.

ii. Compute the intersection of the automaton you built in part (i) and the microwave oven automaton.

iii. Check the intersection automaton for accepting runs, using them to prove that $\Box \ \Diamond$ turn_off is not a property of the microwave oven automaton.