

Introduction to Model Checking 2015:

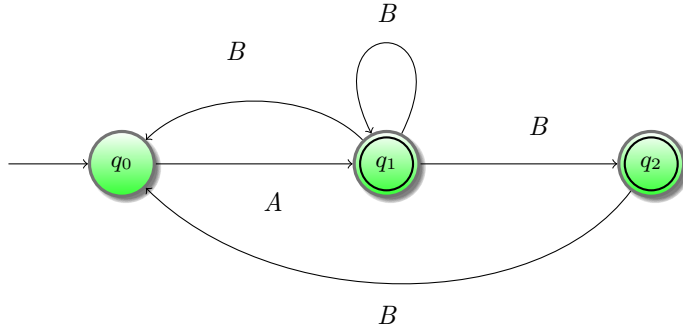
Exercise 5.

Supervised by: Dr. Prof. Joost-Pieter Katoen

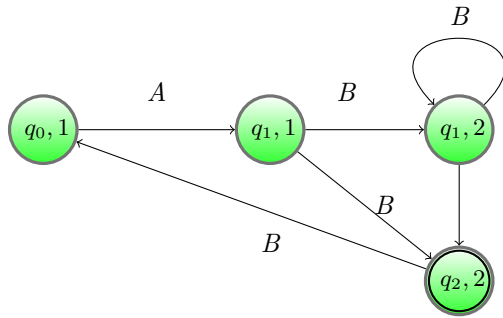
Hand in before: 3rd June

Assisted by: Dr. N. Jansen & S. Chakraborty

Solution 1 The GNBA is:



The equivalent NBA is:



Solution 2 If L is ω -regular then there exists a non-deterministic Büchi automaton $A = (Q, \Sigma, \delta, q_0, F)$, such that $\mathcal{L}(A) = L$. A state of an NBA is deemed useless iff there is no accepting run containing the state. W.l.o.g assume that A does not have any useless state, since they can be safely removed from Q .

1. Define $A_{cl} = (Q, \Sigma, \delta, q_0, F')$, where $F' = Q$. We will see that $cl(L) = \mathcal{L}(A_{cl})$.

To prove: $\mathcal{L}(A_{cl}) \subseteq cl(L)$. Consider any arbitrary word $w \in \mathcal{L}(A_{cl})$. Let ρ be an accepting run for the word w . For any prefix u of w , there is a prefix σ of ρ . Since A does not have any useless state, there exists an accepting run ρ' from $\text{last}(\sigma)$. Thus, $\sigma \cdot \rho'$ is an accepting run of A . Or, there exists a word $w' \in \mathcal{L}(A) = L$, such that u is prefix of w' (where $w' = \delta^{-1}(\sigma \cdot \rho')$). Rephrasing in familiar terms:

For every prefix u of w there exists a $w' \in L$ with u as prefix of w' .

Or, $\mathcal{L}(A_{cl}) \subseteq L$.

To prove: $cl(L) \subseteq \mathcal{L}(A_{cl})$. For any arbitrary word w such that $w \in cl(L)$ it follows that for every prefix u of w , there exists a word w' such that $u \cdot w' \in L$. We will show that $w \in \mathcal{L}(A_{cl})$. Since, any infinite run of A_{cl} is accepting, it suffices to show that for any prefix $u \cdot a$, (where $a \in \Sigma$) of w , $\delta(q_0, ua) \neq \emptyset$.

We know that for every ua there exists a w' such that $uaw' \in L$. Thus there exists an accepting run ρ in A for the word uaw' . Since, ρ is also run A_{cl} , it follows that $\delta(q_0, ua) \neq \emptyset$. Q.E.D.

2. Any NBA can be considered as NFA. Thus given a structure A , let $\mathcal{L}_f(A)$ denote the set of finite path of the NFA A and $\mathcal{L}(A)$ be the set of infinite path of the NBA A . Let $A = (Q, \Sigma, \delta, q_0, F)$ be the structure without useless states such that $\mathcal{L}(A) = L$. Define $A_p = (Q, \Sigma, \delta, q_0, Q)$. It follows immediately,

$$\text{Prefixes of } \mathcal{L}(A) \text{ is } \mathcal{L}_f(A_p) \tag{1}$$

Construct A_p^c such that $\mathcal{L}_f(A_p^c) = \overline{\mathcal{L}_f(A_p)}$. This is easy to build, since we are interested in only finite paths and hence A_p is considered as an NFA, whose complement is obtained by subset construction. We will see that $\mathcal{L}(A_p^c) = \overline{cl(L)}$.

To prove: $\mathcal{L}(A_p^c) \subseteq \overline{\text{cl}(\mathcal{A})}$. Consider an arbitrary $w \notin \overline{\text{cl}(\mathcal{L}(A))}$. Thus, for any $u \prec w$, there exists w' , such that $uw' \in \mathcal{L}(A)$. This implies any prefix of w is a prefix of $\mathcal{L}(A)$, or equivalent $\forall u \prec w : u \notin \mathcal{L}_f(A_p^c)$. Thus no prefix of w has a run that visits the final state of A_p^c . Which means w is not accepted by A_p^c . The statement follows from contra-position.

To prove: $\overline{\text{cl}(\mathcal{L}(A))} \subseteq \mathcal{L}(A_p^c)$. Consider an arbitrary $w \notin \mathcal{L}(A_p^c)$. Then w does not visit the accepting states finitely often (if at all). Thus, there exists a prefix u such that for all v with $u \prec v$, $\text{last}(v)$ is not a final state. That is $\forall v : u \prec v \prec w, v \notin \mathcal{L}_f(A_p^c)$. Or, $\forall v : u \prec v \prec w, v \in \mathcal{L}_f(A_p)$. Which implies, that the final states of A_p are visited infinitely often. Hence $w \in \mathcal{L}(A_p) = \text{cl}(\mathcal{L}(A))$. Consequently, $w \notin \overline{\text{cl}(\mathcal{L}(A))}$. The statement follows from contra-position. Q.E.D.

Solution 3 The topology of the transition system $T_{e,f}$ with property (1) is a ring with 2^n states $\{s_0, \dots, s_{2^n-1}\}$. Thus, infinitely often a boils down to the existence of state with a label a . Since the labeling function is monotonic, that is for $i \leq j$: $f(i, a) \implies f(j, a)$, we can use binary search. Thus the worst case computation will need $\log(2^n)$ checks whether a state s_i has the label a . Each check is accomplished by solving a circuit value problem, $f(i, a)$, which can be done $(n + m)^k$. This gives the required complexity bounds.

Solution 4 1. $\Diamond \Box a \rightarrow \Box \Diamond b \equiv \Box(a \cup (\sim a \vee b))$

For any word w there are two choices:

(a) $w \models \Diamond \Box a$: if $w \models \Diamond \Box a \rightarrow \Box \Diamond b$ then $w \models \Box \Diamond b$. Let index i be such that $w[i \dots] \models \Box a$. For indices $j < i$ Either $w_j \models b$, in which case $w[j \dots] \models a \cup (\sim a \vee b)$, or $w_j \models a$. In which case, there exists a $k > j$, such that $w_k \models \sim a$ (where $k \leq i$). Hence, $w[j \dots] \models a \cup (\sim a \vee b)$. For $j \geq i$, $w[j \dots] \models a \cup b$. Thus, $w \models \Box(a \cup (\sim a \vee b))$.

Now let $w \models \Box(a \cup (\sim a \vee b))$ and suppose $w \not\models \Box \Diamond b$. That is there exists a i' , such that $w[i' \dots] \models \Box \sim b$. Thus for $k \geq \max(i, i')$, $w[k \dots] \not\models a \cup (\sim a \vee b)$. Contradiction, hence $w \models \Box \Diamond b$.

(b) $w \models \Box \Diamond \sim a$. Then $w \models \Diamond \Box a \rightarrow \Box \Diamond b$ vacuously. For every index j , $w[j \dots] \models a \cup \sim a$. Or, $w \models \Box(a \cup (\sim a \vee b))$.

2. $\Box \Diamond a \rightarrow \Box \Diamond b \not\equiv \Box(a \rightarrow \Diamond b)$

Consider the word $w = \begin{pmatrix} a \\ \sim b \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \end{pmatrix} \dots$

3. $(a \cup b) \cup c \not\equiv a \cup (b \cup c)$

$\begin{pmatrix} a \\ \sim b \\ \sim c \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \\ c \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \\ \sim c \end{pmatrix} \begin{pmatrix} \sim a \\ \sim b \\ \sim c \end{pmatrix} \dots$

4. $\Box a \rightarrow a$.

$$\begin{array}{ll} \Box a & \text{Premises} \\ \implies a \wedge X(\Box a) & \text{Expansion rule of } \Box \\ \implies a & \text{Elimination rule for } \wedge \end{array}$$

And $\Box a \rightarrow \Box \Box a$. If $w \models \Box a$, then for all indices i , $w[i \dots] \models \Box a$. Hence $w \models \Box \Box a$.