Technische Universität München (I7) **Summer Semester 2016**
J. Křetínský / D. Suwimonteerabuth **12.05.2016**

Model Checking – Sample Solution 4

Exercise 4.1

(a) Not equivalent. A counterexample is $\sigma = \{\}\{p,q\}\{q\}^\omega$, because $\sigma \not\models \phi$ but $\sigma \models \psi$.

(b) Not equivalent. A counterexample is $\sigma = \{p,q\}\{q\}^\omega$, because $\sigma \models \phi$ but $\sigma \not\models \psi$.

(c) Equivalent.

"$\Rightarrow$" Let $\sigma \models (p \mathbf{U} q) \mathbf{U} q$ and i be the first position where q holds. If $i = 0$, then $q \in \sigma(0)$ and trivially $\sigma \models p \mathbf{U} q$. If $i > 0$, then $\sigma^k \models p \mathbf{U} q$ for all k between 0 and $i-1$, and therefore $\sigma \models p \mathbf{U} q$, since $\sigma^0 = \sigma$.

"$\Leftarrow$" Let $\sigma \models p \mathbf{U} q$ and i be the first position where q holds. If $i = 0$, then trivially $\sigma \models (p \mathbf{U} q) \mathbf{U} q$. If $i > 0$, then $\sigma^k \models p$ for all k between 0 and $i-1$. Since $\sigma^i \models q$, we have $\sigma^k \models p \mathbf{U} q$ also, and consequently $\sigma \models (p \mathbf{U} q) \mathbf{U} q$.

(d) Not equivalent. A counterexample is $\sigma = \{p,q\}\{q\}\{r\}\{\}^\omega$, because $\sigma \models \phi$ but $\sigma \not\models \psi$.

Exercise 4.2

(a) Let $\sigma \models \phi$. We define $n_\phi(\sigma)$ inductively over $\mathbf{NNF_{-R}}$ formulae:

- If $\phi = a$, where $a \in AP$, then $a \in \sigma(0)$ and $\forall \sigma' : \sigma(0)\sigma' \models \phi$. So, $n_\phi(\sigma) = 0$.
- If $\phi = \neg a$, where $a \in AP$, we have similarly $n_\phi(\sigma) = 0$.
- If $\phi = \phi_1 \wedge \phi_2$, then $\sigma \models \phi_1$ and $\sigma \models \phi_2$. We have $n_\phi(\sigma) = \max(n_{\phi_1}(\sigma), n_{\phi_2}(\sigma))$.
- If $\phi = \phi_1 \vee \phi_2$, then $\sigma \models \phi_1$ or $\sigma \models \phi_2$. If $\phi \models \phi_1$, then $n_\phi(\sigma) = n_{\phi_1}(\sigma)$. Otherwise, $n_\phi(\sigma) = n_{\phi_2}(\sigma)$.
- If $\phi = \mathbf{X}\,\phi_1$, then $\sigma^1 \models \phi_1$. So, $n_\phi(\sigma) = n_{\phi_1}(\sigma^1) + 1$.
- If $\phi = \phi_1 \mathbf{U} \phi_2$, then $\exists i : \sigma^i \models \phi_2 \wedge \forall k < i : \sigma^k \models \phi_1$. We take $n_\phi(\sigma) = \max\left(i + n_{\phi_2}(\sigma^i), \max_{k=0}^{i}(k + n_{\phi_1}(\sigma^k))\right)$.

(b) We prove by induction that

$$\sigma \models \phi \;\Leftrightarrow\; D(\sigma) \models \phi \;\Leftrightarrow\; D(\sigma)^1 \models \phi$$

- If ϕ is a or $\neg a$, where $a \in AP$, the property trivially holds, because $\sigma(0) = D(\sigma)(0) = D(\sigma)^1(0)$.
- If ϕ is $\phi_1 \wedge \phi_2$ or $\phi_1 \vee \phi_2$, the proof trivially follows from the induction hypothesis.

- If $\phi = \phi_1 \mathbf{U} \phi_2$, we prove each direction as follows:

  $\underline{\sigma \models \phi_1 \mathbf{U} \phi_2 \;\Rightarrow\; D(\sigma) \models \phi_1 \mathbf{U} \phi_2}$

  From the definition, $\exists i : \sigma^i \models \phi_2 \wedge \forall k < i : \sigma^k \models \phi_1$. We need to prove that $\exists i' : D(\sigma)^{i'} \models \phi_2 \wedge \forall k' < i' : D(\sigma)^{k'} \models \phi_1$.

  Let $i' = 2i$. By induction hypothesis, we have $D(\sigma)^{i'} \models \phi_2$. Also, for all $k < i$ where $\sigma^k \models \phi_1$, we know that $D(\sigma)^{2k} \models \phi_1$ and $D(\sigma)^{2k+1} \models \phi_1$. We can conclude that $D(\sigma)^{k'} \models \phi_1$ for all $k' < i'$.

  $\underline{D(\sigma) \models \phi_1 \mathbf{U} \phi_2 \;\Rightarrow\; D(\sigma)^1 \models \phi_1 \mathbf{U} \phi_2}$

  If $D(\sigma) \models \phi_2$, then $D(\sigma)^1 \models \phi_2$.

  Otherwise, $\exists i \geq 1 : D(\sigma)^i \models \phi_2 \wedge \forall k < i : D(\sigma)^k \models \phi_1$. This implies that $\exists i' \geq 0 : D(\sigma)^{1+i'} \models \phi_2 \wedge \forall k' < i' : D(\sigma)^{1+k'} \models \phi_1$, which means $D(\sigma)^1 \models \phi_1 \mathbf{U} \phi_2$ by definition.

  $\underline{D(\sigma)^1 \models \phi_1 \mathbf{U} \phi_2 \;\Rightarrow\; \sigma \models \phi_1 \mathbf{U} \phi_2}$

  From the definition, $\exists i : D(\sigma)^{1+i} \models \phi_2 \wedge \forall k < i : D(\sigma)^{1+k} \models \phi_1$. We need to prove that $\exists i' : \sigma^{i'} \models \phi_2 \wedge \forall k' < i' : \sigma^{k'} \models \phi_1$. We proceed by proving that such i' and k' exist as follows:

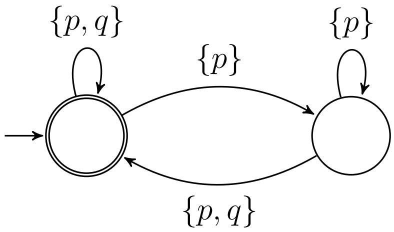
  If i is even, $D(\sigma)^{1+i} = D(\sigma^{i/2})^1 \models \phi_2$, hence by induction hypothesis $\sigma^{i/2} \models \phi_2$. Furthermore, for any even $k < i$, we have $D(\sigma)^{1+k} = D(\sigma^{k/2})^1$, and by induction hypothesis $\sigma^{k/2} \models \phi_1$. Therefore, $\forall k' < i/2 : \sigma^{k'} \models \phi_1$.

  If i is odd, $D(\sigma)^{1+i} = D(\sigma^{(i+1)/2}) \models \phi_2$, hence by induction hypothesis $\sigma^{(i+1)/2} \models \phi_2$. Furthermore, for any even $k < i$, we have $D(\sigma)^{1+k} = D(\sigma^{k/2})^1$, and by induction hypothesis $\sigma^{k/2} \models \phi_1$. Therefore, $\forall k' < (i+1)/2 : \sigma^{k'} \models \phi_1$.

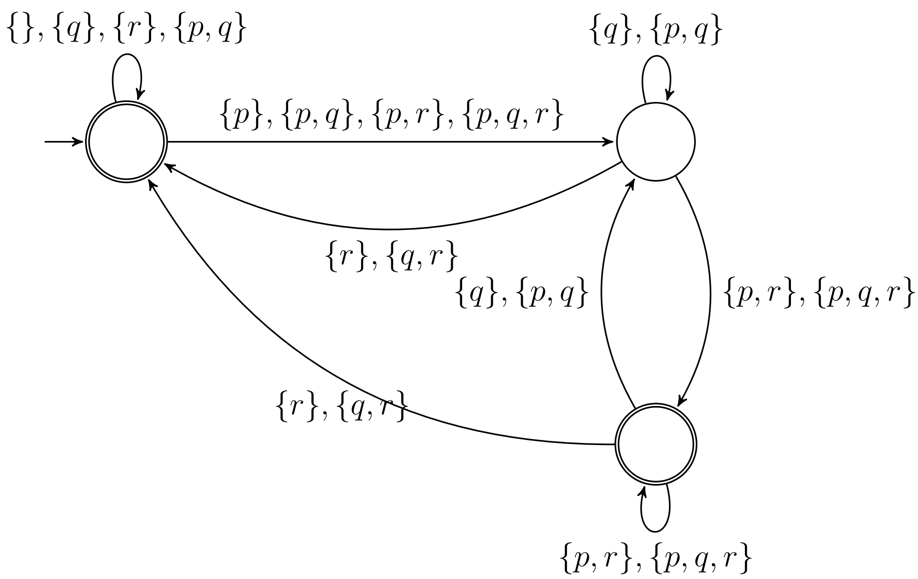
- If $\phi = \phi_1 \mathbf{R} \phi_2$, the proof is similar to the previous case.

Exercise 4.3

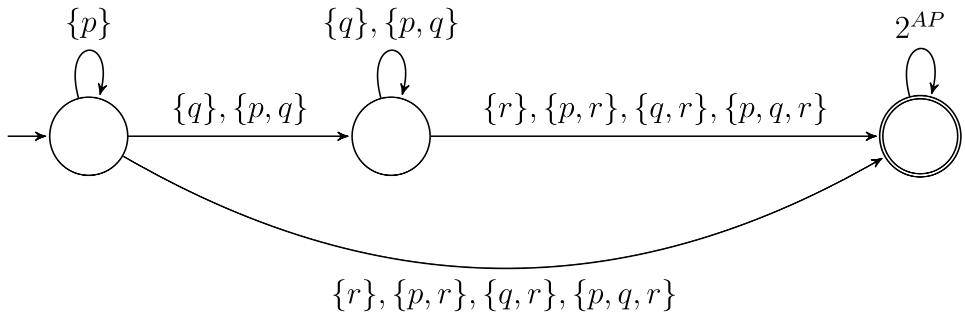
(a)



(b)


{}, {q}, {r}, {p, q}
{q}, {p, q}
{p}, {p, q}, {p, r}, {p, q, r}
{r}, {q, r}
{q}, {p, q}
{p, r}, {p, q, r}
{r}, {q, r}
{p, r}, {p, q, r}

(c)


{p}
{q}, {p, q}
2^AP
{q}, {p, q}
{r}, {p, r}, {q, r}, {p, q, r}
{r}, {p, r}, {q, r}, {p, q, r}