Technische Universität München **Summer Semester 2015**
I7
J. Esparza / A. Durand-Gasselin / D. Suwimonteerabuth **June 2015**

Model Checking – Exercise sheet 4

Exercise 4.1: Solution

$\varphi = \mathbf{G}\neg q \vee \mathbf{F}(q \wedge (\neg p \ \mathbf{W}\, s))$ and $\psi = \mathbf{G}((q \wedge \neg r \wedge \mathbf{F}r) \rightarrow ((p \rightarrow (\neg r\ \mathcal{U}(s \wedge \neg r)))\ \mathcal{U}\, r))$

1. $\{p,q\}\{p,q,r,s\}\{s\}\{p,q,r\}\{q,r,s\}\{p,q\}\{p\}\{\}\{p,q\}^\omega$ $\quad \models \varphi \models \psi$
2. $\{p,q\}\{p,q,s\}\{s\}\{p,q,r\}\{q,r,s\}\{p,q\}\{p\}\{\}\{p,q\}^\omega$ $\quad \models \varphi \models \psi$
3. $\{p,q\}\{q\}\{p,q,s\}\{p,q,s\}\{p,s\}\{q,r,s\}\{q,r\}\{q,r,s\}\{r,s\}\{q,r,s\}^\omega$ $\quad \models \varphi \models \psi$
4. $\{p,q\}\{p,q,s\}\{p,r,s\}\{q,s\}\{p,s\}\{r,s\}\{r\}^\omega$ $\quad \models \varphi \models \psi$
5. $(\{p\}\{s\}\{r\}\{q\})^\omega$ $\quad \not\models \varphi \models \psi$

Exercise 4.2: Solution

(a) (1) by definition of $\mathbf{G}$, $w \models \mathbf{G}\varphi$ iff $\forall n\ w^n \models \varphi$, fixing $n = 0$ yields $w \models \varphi$. Thus $w \models \mathbf{G}\varphi \implies w \models \varphi$
(2) by definition of $\mathbf{F}$, $w \models \mathbf{F}\varphi$ iff $\exists n\ w^n \models \varphi$. If $w \models \varphi$, then $w^0 \models \varphi$, hence $w \models \mathbf{F}\varphi$.

(b) (3) by (1), since $\mathbf{G}\psi \implies \psi$. (typically when $\psi = \mathbf{F}\varphi$)
(5) by (2), since $\psi \implies \mathbf{F}\psi$. (when $\psi = \mathbf{G}\varphi$).

(c) Clearly if $w \models \mathbf{F}\varphi$ then $\exists n\ w^n \models \varphi$, thus $w^n \models \varphi$, hence $w \models \mathbf{F}\psi$

(d) If $\varphi \implies \psi$ then $\neg\psi \implies \neg\varphi$ thus $\mathbf{F}\neg\psi \implies \mathbf{F}\neg\varphi$, so $\neg\mathbf{F}\neg\varphi \implies \neg\mathbf{F}\neg\psi$, which can be rewritten as $\mathbf{G}\varphi \implies \mathbf{G}\psi$.

(e) We rely on the fact that $\exists i\, \forall j\, \xi \implies \forall j\, \exists i\, \xi$. More intuitively if we can find an i that works for all j, then for all j, we can find an i (and it will even be the same i for all j). Thus $\exists i\, \forall j\, w^{i+j} \models \varphi$ (i.e. $w \models \mathbf{FG}\varphi$) implies $\forall i\, \exists j\, w^{j+i} \models \varphi$, (i.e. $w \models \mathbf{GF}\varphi$).

(f) If $\exists i\, \exists j\, w^{i+j} \models \varphi$, then we could have directly existentially quantified the sum: $\exists s\, w^s \models \varphi$.

(g) (3) gives us $\mathbf{F}\varphi \implies \mathbf{FF}\varphi$. (f) allows to conclude.

(h) by taking the negation of (g) over $\neg\varphi$, we obtain $\neg\mathbf{FF}\neg\varphi \equiv \neg\mathbf{F}\neg\varphi$. $\neg\mathbf{FF}\neg\varphi \equiv \mathbf{G}\neg\mathbf{F}\neg\varphi \equiv \mathbf{GG}\neg\neg\varphi \equiv \mathbf{GG}\varphi$.

(i) (2) gives $\mathbf{GF}\varphi \implies \mathbf{FGF}\varphi$.

by (4) we have $\mathbf{FG}\psi \implies \mathbf{GF}\psi$. With $\psi = \mathbf{F}\varphi$, we obtain, $\mathbf{FGF}$ $varphi \implies \mathbf{GFF}\varphi$. With (9), we conclude that $\mathbf{FGF}\varphi \implies \mathbf{GF}\varphi$.

The other equivalence can be obtained by definition of $\mathbf{G}\varphi = \neg\mathbf{F}\neg\varphi$.

Exercise 4.3: Solution

1. We will show a more general property on **LTL** formulas: For any **LTL** formula φ, there exists 2 formulas $\mathcal{P}(\varphi)$ and $\mathcal{N}(\varphi)$ of **NF-LTL** such that $w \models \varphi \iff w \models \mathcal{P}(\varphi)$ and $w \models \neg\varphi \iff w \models \mathcal{N}(\varphi)$.

   We show this property by structural induction over formulas:

   - the atomic case is when φ is of the form p, $p \in AP$, clearly $\mathcal{P}(\varphi) = p$ and $\mathcal{N}(\varphi) = \neg p$ are both in **NF-LTL**. The property therefore holds for the atomic case
   - if $\varphi = \varphi_1 \wedge \varphi_2$, by induction hypothesis, we have $\mathcal{P}(\varphi_1), \mathcal{P}(\varphi_2), \mathcal{N}(\varphi_1), \mathcal{N}(\varphi_2)$, clearly we can define the two **NF-LTL** formulas $\mathcal{P}(\varphi) = \mathcal{P}(\varphi_1) \wedge \mathcal{P}(\varphi_2)$ and $\mathcal{N}(\varphi) = \mathcal{N}(\varphi_1) \vee \mathcal{N}(\varphi_2)$, which are equivalent to φ and $\neg\varphi$ respectively. Therefore, conjunction preserves the property.
   - if $\varphi = \neg\psi$, then by induction we have two **NF-LTL** formulas $\mathcal{P}(\psi)$ and $\mathcal{N}(\psi)$, that are equivalent to ψ and $\neg\psi$. Clearly, it suffices to take $\mathcal{P}(\varphi) = \mathcal{N}(\psi)$ and $\mathcal{N}(\varphi) = \mathcal{P}(\psi)$. Therefore negation preserves the property.
   - if $\varphi = \mathbf{X}\psi$, we take $\mathcal{P}(\varphi) = \mathbf{X}\mathcal{P}(\psi)$ and $\mathcal{N}(\varphi) = \mathbf{X}\mathcal{N}(\psi)$. Let us emphasize that $\mathcal{N}(\varphi)$ is indeed equivalent to $\neg\varphi$. Let us show for any word w, $w \models \mathcal{N}(\varphi)$ iff $w \not\models \mathbf{X}\psi$. $w \models \mathcal{N}(\varphi)$ iff $w \models X\mathcal{N}(\psi)$ iff $w^1 \models \mathcal{N}(\psi)$ (By induction hypothesis, we have that for any u, $u \models \mathcal{N}(\psi)$ iff $u \not\models \psi$, typically when $u = w^1$) iff $w^1 \not\models \psi$ iff $w \not\models \mathbf{X}\psi$ iff $w \not\models \varphi$.
   - The last case is when $\varphi = \psi_1 \,\mathcal{U}\, \psi_2$. $\mathcal{P}(\varphi)$ is easy to define: $\mathcal{P}(\varphi) = \mathcal{P}(\psi) \,\mathcal{U}\, \mathcal{P}(\psi_2)$. To define $\mathcal{N}(\varphi)$, we use the following equivalence: $w \models \neg(\psi_1 \,\mathcal{U}\, \psi_2) \iff w \models \mathbf{G}\neg\psi_2 \vee (\neg\psi_2 \,\mathcal{U}(\neg\psi_1 \wedge \neg\psi_2))$, then we get that $\mathcal{N}(\varphi) = \mathbf{G}\mathcal{N}(\psi_2) \vee (\mathcal{N}(\psi_2) \,\mathcal{U}(\mathcal{N}(\psi_1) \wedge \mathcal{N}(\psi_2))$.

2. We define $N_\varphi(w)$ inductively over **NF-LTL**$_{-G}$ formulas:

   - If φ is atomic and $w \models \varphi$, then clearly for any word $w' \in \Sigma^\omega$, $w(0)w' \models \varphi$. Therefore in this case $N_\varphi(w) = 0$.
   - If $\varphi = \psi_1 \wedge \psi_2$, let $w \models \varphi$, then as $w \models \psi_1$ and $w \models \psi_2$, we can write $N_\varphi(w) = \max(N_{\psi_1}(w), N_{\psi_2}(w))$. We have then for all $w' \in \Sigma^\omega$, $w(0)\dots w(N_\varphi(w))w' \models \varphi$.
   - If $\varphi = \psi_1 \vee \psi_2$, let $w \models \varphi$. Then if $w \models \psi_1$, we take $N_\varphi(w) = N_{\psi_1}(w)$, and we have that for any $w' \in \Sigma^\omega$, $w(0)\dots w(N_\varphi(w))w' \models \psi_1$, hence is also validates φ. Otherwise we take $N_\varphi(w) = N_{\psi_2}(w)$, in that case we know that $w \models \psi_2$ and for all $w' \in \Sigma^\omega$, $w(0)\dots w(N_\varphi(w))w' \models \psi_2$ hence it also validates φ.
   - If $\varphi = \mathbf{X}\psi$, let $w \models \varphi$, then $w^1 \models \psi$, hence we take $N_\varphi(w) = N_\psi(w^1) + 1$.
   - If $\varphi = \psi_1 \,\mathcal{U}\, \psi_2$, let $w \models \varphi$, then we know that there exists an integer i such that $\forall j < i$, $w^j \models \psi_1$ and $w^i \models \psi_2$.
     We take $N_\varphi(w) = \max(i + N_{\psi_2}(w^i), \max_{j=0}^{i}(j + N_{\psi_1}(w^j)))$.
     We remark, by induction hypothesis that for any w',
     $\forall j < i$, $w(j)\dots w(N_\varphi(w))w' \models \psi_1$ and $w(i)\dots w(N_\varphi(w))w' \models \psi_2$,
     as for any $j < i$, $w(j)\dots w(N_\varphi(w))w'$ is $w^j(0)\dots w^j(N_\varphi(w)-j)w'$ and as $N_\varphi(w)-j \geq N_{\psi_1}(w^j)$, we have that $w^j(0)\dots w^j(N_\varphi(w)-j)w' \models \psi_1$; also as $N_\varphi(w)-i \geq N_{\psi_2}(w^i)$, $w^i(0)\dots w(N_\varphi(w))w' \models \psi_2$.

3. By induction we show that for any **NF-LTL**$_{-X}$ formula, we have

$$w \models \varphi \iff D(w) \models \varphi \iff D(w)^1 \models \varphi$$

- The case of atomic formulas is trivial: only the first letter matters. As $w(0) = D(w)(0) = D(w)^1(0)$, this property holds for atomic **NF-LTL**$_{-X}$
- The case of disjunction and conjunctions is trivially true.
- If $\varphi = \mathbf{G}\psi$, let us first show that $w \models \varphi \implies D(w) \models \varphi$. For that we need to show that $\forall i$, $D(w)^i \models \psi$. If i is even, $D(w)^i = D(w^{i/2})$. Since $w \models \varphi$, $w^{i/2} \models \psi$ hence by induction hypothesis $D(w^{i/2}) \models \psi$ therefore $D(w)^i \models \psi$. If i is odd, then $D(w)^i = D(w^{i/2})^1$, since $w \models \varphi$, $w^{i/2} \models \psi$ hence by induction hypothesis $D(w^{i/2})^1 \models \psi$ therefore $D(w)^i \models \psi$.

  Then we remark that $w \models \varphi \implies D(w)^1 \models \varphi$, as $\varphi = \mathbf{G}\psi$.

  Finally we need to show that $D(w)^1 \models \mathbf{G}\psi$ implies $w \models \mathbf{G}\psi$. The former is equivalent to $\forall i, D(w)^{1+i} \models \psi$, noticeably it holds for any even value of i. Furthermore, if i is even, $D(w)^{1+i} = D(w^{i/2})^1$. By induction hypothesis, it implies that for any even value of i, $w^{i/2} \models \psi$, therefore $w \models \mathbf{G}\psi$.
- Finally we treat the case where $\varphi = \psi_1 \,\mathcal{U}\, \psi_2$. First we show that $w \models \psi_1 \,\mathcal{U}\, \psi_2 \implies D(w) \models \psi_1 \,\mathcal{U}\, \psi_2$. There is a k s.t. $w^k \models \psi_2$ and $\forall l < k$, $w^l \models \psi_2$, we need to show that $\exists i\ D(w)^i \models \psi_2 \wedge \forall j < i,\ D(w)^j \models \psi_1$. Let $i = 2 * k$, by induction hypothesis $D(w)^i \models \psi_2$. Take $j < i$, either j is even, in which case $D(w)^j = D(w^{j/2})$ and by induction hypothesis (as $j/2 < k$) $D(w)^j \models \psi_1$, or j is odd, and then $D(w)^j = D(w^{j/2})^1$ and the induction hypothesis (as $j/2 < k$) also allows us to conclude that $D(w)^j \models \psi_1$.

  Then we show that $D(w) \models \psi_1 \,\mathcal{U}\, \psi_2 \implies D(w)^1 \models \psi_1 \,\mathcal{U}\, \psi_2$. If $D(w) \models \psi_2$, by induction hypothesis $D(w)^1 \models \psi_2$, hence $D(w)^1 \models \psi_1 \,\mathcal{U}\, \psi_2$, if $D(w) \not\models \psi_2$, then $\exists i > 1,\ D(w)^i \models \psi_2 \wedge \forall j < i,\ D(w)^j \models \psi_1$, which implies that $\exists i',\ D(w)^{1+i'} \models \psi_2 \wedge \forall j' < i',\ D(w)^{1+j'} \models \psi_1$, that is $D(w)^1 \models \psi_1 \,\mathcal{U}\, \psi_2$.

  Finally we show that $D(w)^1 \models \psi_1 \,\mathcal{U}\, \psi_2 \implies w \models \psi_1 \,\mathcal{U}\, \psi_2$. By assumption, $\exists i\ D(w)^{1+i} \models \psi_2 \wedge \forall j < i,\ D(w)^{1+j} \models \psi_1$. If i is even then $D(w)^{i+1} = D(w^{i/2})^1$, hence $w^{i/2} \models \psi_2$, furthermore, for any $j < i$, noticeably for any even j strictly smaller than i, we have $D(w)^{j+1} \models \psi_1$, as j is even $D(w)^{j+1} = D(w^{j/2})^1$, hence by induction hypothesis $w^{j/2} \models \psi_1$, thus for any $k < (i/2)$, $w^k \models \psi_1 \wedge w^{i/2} \models \psi_2$. Now if i is odd $D(w)^{i+1} = D(w^{i/2+1})$, hence $w^{i/2+1} \models \psi_2$, furthermore for any even $j < i$, (which also include the case $j = (i/2)$ as i is odd), we have $D(w)^{j+1} \models \psi_1$. As $D(w)^{j+1} = D(w^{j/2})^1$, by induction hypothesis, we deduce that $w^k \models \psi_1$ for any $k \leq i/2$. Therefore $w \models \psi_1 \,\mathcal{U}\, \psi_2$, which concludes the induction.