Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen
Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Solution 7 (due 18th June) —

General Remarks

- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via e-mail.
- If a task asks you to justify your answer, an explanation of your reasoning is sufficient. If you are required to prove a statement, you need to give a *formal* proof.

Exercise 1 (3+3 Points)

Let φ and ψ be LTL formulae. Consider the following new operators.

- "At next": $\varphi \,\mathsf{AX}\, \psi \iff$ the next time at which ψ holds, φ also holds.
- "While": $\varphi \,\mathsf{WH}\, \psi \iff \varphi$ holds at least as long as ψ holds.
- "Before": $\varphi \,\mathsf{B}\, \psi \iff$ if ψ holds at some point, φ does so (strictly) before.

(a) Formalize the semantics of these operators on infinite words $\sigma \in (2^{\mathrm{AP}})^\omega$.

(b) Show that these operators are LTL-definable by providing equivalent LTL formulae.
Hint: You may use both the until and weak until operator.

Solution:

In the following, let $\sigma = A_0 A_1 \ldots \in \left(2^{\mathrm{AP}}\right)^\omega$.

(a)

$$\sigma \models \varphi \,\mathsf{AX}\, \psi \iff \forall i \geq 0. \Big((A_i A_{i+1} \ldots \models \psi \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \not\models \psi) \implies A_i A_{i+1} \ldots \models \varphi \Big)$$

$$\sigma \models \varphi \,\mathsf{WH}\, \psi \iff \forall i \geq 0. \Big((\forall 0 \leq j < i. A_j A_{j+1} \ldots \models \psi) \implies \forall 0 \leq k < i. A_k A_{k+1} \ldots \models \varphi \Big)$$

$$\sigma \models \varphi \,\mathsf{B}\, \psi \iff \forall i \geq 0. \, (A_i A_{i+1} \ldots \models \psi \implies \exists 0 \leq j < i. A_j A_{j+1} \ldots \models \varphi)$$

(b)

$$\begin{aligned}
& \sigma \models \varphi \;\mathsf{AX}\; \psi \\
\iff & \forall i \geq 0. \Big((A_i A_{i+1} \ldots \models \psi \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \not\models \psi) \implies A_i A_{i+1} \ldots \models \varphi \Big) \\
\iff & \forall i \geq 0. \Big((A_i A_{i+1} \ldots \models \psi \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \models \neg\psi) \implies A_i A_{i+1} \ldots \models \varphi \Big) \\
\iff & \exists i \geq 0. \, (A_i A_{i+1} \ldots \models \psi \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \models \neg\psi \wedge A_i A_{i+1} \ldots \models \varphi) \vee \forall i \geq 0. A_i A_{i+1} \ldots \models \neg\psi \\
\iff & \sigma \models \Big(\neg\psi \;\mathsf{U}\; (\psi \wedge \varphi) \Big) \vee \Box \neg\psi \\
\iff & \sigma \models \neg\psi \;\mathsf{W}\; (\psi \wedge \varphi)
\end{aligned}$$

$$
\begin{aligned}
&\sigma \models \varphi \;\mathsf{WH}\; \psi \\
\iff &\forall i \geq 0. \Big((\forall 0 \leq j < i. A_j A_{j+1} \ldots \models \psi) \implies \forall 0 \leq k < i. A_k A_{k+1} \ldots \models \varphi \Big) \\
\iff &\exists i \geq 0. \, (A_i A_{i+1} \ldots \models \neg\psi \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \models \varphi \wedge \psi) \vee \forall i \geq 0. A_i A_{i+1} \ldots \models \varphi \wedge \psi \\
\iff &\sigma \models \Big((\varphi \wedge \psi) \;\mathsf{U}\; \neg\psi \Big) \vee \Box (\varphi \wedge \psi) \\
\iff &\sigma \models (\varphi \wedge \psi) \;\mathsf{W}\; \neg\psi
\end{aligned}
$$

$$
\begin{aligned}
&\sigma \models \varphi \;\mathsf{B}\; \psi \\
\iff &\forall i \geq 0. \, (A_i A_{i+1} \ldots \models \psi \implies \exists 0 \leq j < i. A_j A_{j+1} \ldots \models \varphi) \\
\iff &\exists i \geq 0. \, (A_i A_{i+1} \ldots \models \varphi \wedge \forall 0 \leq j \leq i. A_j A_{j+1} \ldots \models \neg\psi) \vee \forall i \geq 0. A_i A_{i+1} \ldots \models \neg\psi \\
\iff &\exists i \geq 0. \Big(A_i A_{i+1} \ldots \models (\varphi \wedge \neg\psi) \wedge \forall 0 \leq j < i. A_j A_{j+1} \ldots \models \neg\psi \Big) \vee \forall i \geq 0. A_i A_{i+1} \ldots \models \neg\psi \\
\iff &\Big(\neg\psi \;\mathsf{U}\; (\varphi \wedge \neg\psi) \Big) \vee \Box \neg\psi \\
\iff &\neg\psi \;\mathsf{W}\; (\varphi \wedge \neg\psi)
\end{aligned}
$$

Exercise 2* (1+2 Points)

Let $\mathrm{AP} = \{a, b\}$. Let $\varphi = (a \to \bigcirc \neg b) \;\mathsf{W}\; (a \wedge b)$.

(a) Transform $\neg\varphi$ into an equivalent LTL formula in PNF using the until operator U and the weak until operator W.

(b) Determine which of the properties $P = \mathit{Words}(\varphi)$ and $P' = \mathit{Words}(\neg\varphi)$ are safety properties. Justify your answer.

Solution:

(a) We use the duality

$$\neg(\varphi \;\mathsf{W}\; \psi) \equiv (\varphi \wedge \neg\psi) \;\mathsf{U}\; (\neg\varphi \wedge \neg\psi).$$

We transform $\neg\varphi$ into PNF as follows:

$$
\begin{aligned}
&\neg\varphi \\
&\equiv \neg \left((a \to \bigcirc \neg b) \;\mathsf{W}\; (a \wedge b) \right) && \text{(* definition of } \varphi \text{ *)} \\
&\equiv \Big((a \to \bigcirc \neg b) \wedge \neg(a \wedge b) \Big) \;\mathsf{U}\; \Big(\neg(a \to \bigcirc \neg b) \wedge \neg(a \wedge b) \Big) && \text{(* duality of W and U *)} \\
&\equiv \Big((\neg a \vee \bigcirc \neg b) \wedge \neg(a \wedge b) \Big) \;\mathsf{U}\; \Big(\neg(\neg a \vee \bigcirc \neg b) \wedge \neg(a \wedge b) \Big) && \text{(* definition of } \to \text{ *)} \\
&\equiv \Big((\neg a \vee \bigcirc \neg b) \wedge (\neg a \vee \neg b) \Big) \;\mathsf{U}\; \Big(a \wedge \neg \bigcirc \neg b) \wedge (\neg a \vee \neg b) \Big) && \text{(* deMorgan *)} \\
&\equiv \Big((\neg a \vee \bigcirc \neg b) \wedge (\neg a \vee \neg b) \Big) \;\mathsf{U}\; \Big(a \wedge \bigcirc b) \wedge (\neg a \vee \neg b) \Big) && \text{(* duality of } \bigcirc \text{ *)} \\
&\equiv \underbrace{\Big(\neg a \vee (\neg b \wedge \bigcirc \neg b) \Big) \;\mathsf{U}\; \Big(a \wedge \neg b \wedge \bigcirc b \Big)}_{=:\varphi'} && \text{(* simplification *)}
\end{aligned}
$$

(b) $P' = \mathit{Words}(\neg\varphi) = \mathit{Words}(\varphi')$ is not a safety property. Consider the word $\sigma = \{a\}^\omega$. We see that $\sigma \notin P'$ as $\sigma \not\models \varphi'$, because, in particular, at no position in σ we have that b holds. However, every prefix $\{a\}^n$ of σ can be completed to a word in P' (satisfying φ') by appending $\{a\}\,\{b\}\,\emptyset^\omega$.

P is a safety property. Consider any word $\sigma = A_0 A_1 \ldots \in \left(2^{\mathrm{AP}}\right)^\omega \setminus P = P' = \mathit{Words}(\varphi')$. From the semantics of LTL, we have

$$\exists i \geq 0. A_i A_{i+1} \ldots \models a \wedge \neg b \wedge \bigcirc b \quad \wedge \quad \forall 0 \leq j < i. A_j A_{j+1} \ldots \models \neg a \vee (\neg b \wedge \bigcirc \neg b).$$

We observe that $\widehat{\sigma} = A_0 A_1 \ldots A_{i+1}$ is a bad prefix of σ with respect to P since any continuation σ' of $\widehat{\sigma}$ also satisfies φ'. Therefore $\sigma' \in \mathit{Words}(\varphi') = P' = \left(2^{\mathrm{AP}}\right)^\omega \setminus P$ and, in particular, $\sigma' \notin P$.

Exercise 3 (2+2+2+2 Points)

Let φ, ψ, π be arbitrary LTL formulae. For each of the following pairs of LTL formulae, determine in which relation they are. More specifically, determine whether they are equivalent, one of them subsumes the other or they are incomparable. Prove your claims.

(a) $\Diamond\Box\varphi$ and $\Box\Diamond\varphi$

(b) $\Diamond\Box\varphi \wedge \Diamond\Box\psi$ and $\Diamond(\Box\varphi \wedge \Box\psi)$

(c) $\varphi \wedge \Box(\varphi \rightarrow \bigcirc\Diamond\varphi)$ and $\Box\Diamond\varphi$

(d) $(\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi$ and $\varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi)$

Solution:

(a) $\Diamond\Box\varphi \implies \Box\Diamond\varphi$.

- $\Box\Diamond\varphi$ does not imply $\Diamond\Box\varphi$.

  Counterexample:
  Take $\varphi = a$. Then $(\{a\}\,\emptyset)^\omega \models \Box\Diamond\varphi$, because a is seen infinitely many times. However, $(\{a\}\,\emptyset)^\omega \not\models \Diamond\Box\varphi$, because a is never seen continuously.

- $\Diamond\Box\varphi$ implies $\Box\Diamond\varphi$.

  Proof:

$$
\begin{aligned}
& A_0A_1\ldots \models \Diamond\Box\varphi \\
\Rightarrow & \exists j \geq 0.\ A_jA_{j+1}\ldots \models \Box\varphi \\
\Rightarrow & \exists j \geq 0.\ \forall k \geq j.\ A_kA_{k+1}\ldots \models \varphi \\
\Rightarrow & \exists j \geq 0.\ \forall k \geq j.\ \exists \ell \geq k.\ A_\ell A_{\ell+1}\ldots \models \varphi \\
\Rightarrow & \exists j \geq 0.\ \forall k \geq 0.\ \exists \ell \geq k.\ A_\ell A_{\ell+1}\ldots \models \varphi \\
\Rightarrow & \forall k \geq 0.\ \exists \ell \geq k.\ A_\ell A_{\ell+1}\ldots \models \varphi \\
\Rightarrow & \forall k \geq 0.\ A_kA_{k+1}\ldots \models \Diamond\varphi \\
\Rightarrow & A_0A_1\ldots \models \Box\Diamond\varphi
\end{aligned}
$$

(b) The two formulae are indeed equivalent: $\Diamond\Box\varphi \wedge \Diamond\Box\psi \equiv \Diamond(\Box\varphi \wedge \Box\psi)$.

Proof:

$$
\begin{aligned}
& A_0A_1\ldots \models \Diamond(\Box\varphi \wedge \Box\psi) \\
\Leftrightarrow & \exists j \geq 0.\ A_jA_{j+1}\ldots \models \Box\varphi \wedge \Box\psi \\
\Leftrightarrow & \exists j \geq 0.\ (\forall k \geq j.\ A_kA_{k+1}\ldots \models \varphi \text{ and } \forall k \geq j.\ A_kA_{k+1}\ldots \models \psi) \\
\overset{(*)}{\Leftrightarrow} & (\exists j_1 \geq 0.\ \forall k \geq j_1.\ A_kA_{k+1}\ldots \models \varphi) \text{ and } (\exists j_2 \geq 0.\ \forall k \geq j_2.\ A_kA_{k+1}\ldots \models \psi) \\
\Leftrightarrow & (\exists j_1 \geq 0.\ A_{j_1}A_{j_1+1}\ldots \models \Box\varphi) \text{ and } (\exists j_2 \geq 0.\ A_{j_2}A_{j_2+1}\ldots \models \Box\psi) \\
\Leftrightarrow & (A_0A_1\ldots \models \Diamond\Box\varphi) \text{ and } (A_0A_1\ldots \models \Diamond\Box\psi) \\
\Leftrightarrow & A_0A_1\ldots \models \Diamond\Box\varphi \wedge \Diamond\Box\psi
\end{aligned}
$$

where for $(*)$ and "$\Leftarrow$" we take $j := max\,\{j_1, j_2\}$, and for "$\Rightarrow$" we take $j_1, j_2 := j$.

(c) $\varphi \wedge \Box(\varphi \rightarrow \bigcirc\Diamond\varphi) \implies \Box\Diamond\varphi$.

- $\Box\Diamond\varphi$ does not imply $\varphi \wedge \Box(\varphi \rightarrow \bigcirc\Diamond\varphi)$.

  Counterexample:
  Take $\varphi = a$. Then $\emptyset\,\{a\}^\omega \models \Box\Diamond\varphi$, because a is seen infinitely many times. However, $\emptyset\,\{a\}^\omega \not\models \varphi \wedge \Box(\varphi \rightarrow \bigcirc\Diamond\varphi)$, because a does not hold in the beginning.

- $\varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi)$ implies $\square \lozenge \varphi$.

  Proof (by contrapositive):
  We show that $A_0 A_1 \ldots \not\models \square \lozenge \varphi$ implies $A_0 A_1 \ldots \not\models \varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi)$.

  We start with $A_0 A_1 \ldots \not\models \square \lozenge \varphi$.

  $$\begin{aligned} & A_0 A_1 \ldots \not\models \square \lozenge \varphi \\ \Rightarrow & A_0 A_1 \ldots \models \neg \square \lozenge \varphi \\ \Rightarrow & A_0 A_1 \ldots \models \lozenge \square \neg \varphi \\ \Rightarrow & \exists j^* \geq 0.\ \forall k \geq j^*.\ A_k A_{k+1} \ldots \models \neg \varphi \end{aligned}$$

  - Case 1: there exists no $j \geq 0$ with $A_j A_{j+1} \ldots \models \varphi$, then $A_0 A_1 \ldots \not\models \varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi)$ and nothing remains to show.
  - Case 2: there exists $j \geq 0$ with $A_j A_{j+1} \ldots \models \varphi$ and we conclude $j < j^*$.
    Let $j\uparrow < j^*$ be the highest such index.

    We assume $A_0 A_1 \ldots \models \varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi)$ for the purpose of a contradiction. Then

    $$\begin{aligned} & A_0 A_1 \ldots \models \varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi) \\ \Rightarrow & (A_0 A_1 \ldots \models \varphi) \text{ and } (\forall j \geq 0.\ A_j A_{j+1} \ldots \models \varphi \rightarrow \bigcirc \lozenge \varphi) \\ \Rightarrow & \forall j \geq 0.\ A_j A_{j+1} \ldots \models \varphi \rightarrow \bigcirc \lozenge \varphi \\ \Rightarrow & \forall j \geq 0.\ \big((A_j A_{j+1} \ldots \models \varphi) \implies (A_j A_{j+1} \ldots \models \bigcirc \lozenge \varphi)\big) \end{aligned}$$

    The last statement holds for all $j \geq 0$ and in particular for $j\uparrow \geq 0$. Then

    $$\begin{aligned} & A_{j\uparrow} A_{j\uparrow+1} \ldots \models \varphi \\ \Rightarrow & A_{j\uparrow} A_{j\uparrow+1} \ldots \models \bigcirc \lozenge \varphi \\ \Rightarrow & A_{j\uparrow+1} A_{j\uparrow+2} \ldots \models \lozenge \varphi \\ \Rightarrow & \exists k \geq j\uparrow{+}1.\ A_k A_{k+1} \ldots \models \varphi \\ \Rightarrow & \exists k > j\uparrow.\ A_k A_{k+1} \ldots \models \varphi \end{aligned}$$

    which contradicts that $j\uparrow$ is the largest index such that $A_{j\uparrow} A_{j\uparrow+1} \ldots \models \varphi$.
    We can therefore conclude $A_0 A_1 \ldots \not\models \varphi \wedge \square(\varphi \rightarrow \bigcirc \lozenge \varphi)$.

(d) The two formulae $(\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi$ and $\varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi)$ are incomparable.

- $(\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi$ does not imply $\varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi)$.

  Counterexample:
  Take $\varphi = a$, $\psi = b$ and $\pi = c$. Let $A_0 = \{a\}, A_1 = \{b\}, A_2 = \{a\}, A_3 = \{b\}$ and $A_i = \{c\}, i \geq 4$. Then

  $$A_0 A_1 A_2 A_3 A_4 A_5 \ldots = \{a\}\,\{b\}\,\{a\}\,\{b\}\,\{c\}^\omega \models (\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi.$$

  In detail it is $A_4 A_5 \ldots \models \pi$. Moreover $A_0 A_1 \ldots \models \varphi \,\mathsf{U}\, \psi$, $A_1 A_2 \ldots \models \varphi \,\mathsf{U}\, \psi$, $A_2 A_3 \ldots \models \varphi \,\mathsf{U}\, \psi$, $A_3 A_4 \ldots \models \varphi \,\mathsf{U}\, \psi$. Therefore

  $$A_0 A_1 A_2 A_3 A_4 A_5 \ldots \models (\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi.$$

  However,

  $$A_0 A_1 A_2 A_3 A_4 A_5 \ldots \not\models \varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi).$$

  In detail, $A_0 A_1 \ldots \models \varphi$, but $A_1 A_2 \ldots \not\models \varphi$ and $A_1 A_2 \ldots \not\models \psi \,\mathsf{U}\, \pi$.

- $\varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi)$ does not imply $(\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi$.

  Counterexample:
  Take $\varphi = a$, $\psi = b$ and $\pi = c$. Let $A_0 = \{a\}$ and $A_i = \{c\}, i \geq 1$. Then

  $$A_0 A_1 A_2 \ldots = \{a\}\,\{c\}^\omega \models \varphi \,\mathsf{U}\, (\psi \,\mathsf{U}\, \pi).$$

  In detail $A_1 A_2 \ldots \models \psi \,\mathsf{U}\, \pi$ and $A_0 A_1 \ldots \models \varphi$.

  However,

  $$A_0 A_1 A_2 \ldots \not\models (\varphi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \pi.$$

  In detail, $A_0 A_1 \ldots \not\models \varphi \,\mathsf{U}\, \psi$ and $A_0 A_1 \ldots \not\models \pi$.

Exercise 4 (2+1 Points)

We consider the release operator R which is defined by

$$\varphi \,\mathsf{R}\, \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \,\mathsf{U}\, \neg\psi).$$

(a) Prove the expansion law

$$\varphi \,\mathsf{R}\, \psi \equiv \psi \wedge \big(\varphi \vee \bigcirc (\varphi \,\mathsf{R}\, \psi)\big).$$

(b) Prove the equivalence

$$\varphi \,\mathsf{R}\, \psi \equiv (\neg\varphi \wedge \psi) \,\mathsf{W}\, (\varphi \wedge \psi).$$

Solution:

(a) The expansion law for the release operator R is given by:

$$\begin{aligned} \varphi \,\mathsf{R}\, \psi &\equiv \psi \wedge \big(\varphi \vee \bigcirc (\varphi \,\mathsf{R}\, \psi)\big) \\ &\equiv (\psi \wedge \varphi) \vee \big(\psi \wedge \bigcirc (\varphi \,\mathsf{R}\, \psi)\big) \end{aligned}$$

According to the release semantics, either ψ holds at the current state and on the next state, $\varphi \,\mathsf{R}\, \psi$ holds again, or ψ is released because in the current state, both ψ and φ are satisfied.

The correctness of the expansion law can be proven as follows:

$$\begin{aligned} \varphi \,\mathsf{R}\, \psi &\equiv \neg(\neg\varphi \,\mathsf{U}\, \neg\psi) && \text{(* definition of R *)} \\ &\equiv \neg\left(\neg\psi \vee (\neg\varphi \wedge \bigcirc\, (\neg\varphi \,\mathsf{U}\, \neg\psi))\right) && \text{(* expansion law of U *)} \\ &\equiv \psi \wedge \neg\left(\neg\varphi \wedge \bigcirc\, (\neg\varphi \,\mathsf{U}\, \neg\psi)\right) && \text{(* deMorgan *)} \\ &\equiv \psi \wedge \left(\varphi \vee \neg \bigcirc\, (\neg\varphi \,\mathsf{U}\, \neg\psi)\right) && \text{(* deMorgan *)} \\ &\equiv \psi \wedge \left(\varphi \vee \bigcirc \neg\, (\neg\varphi \,\mathsf{U}\, \neg\psi)\right) && \text{(* duality of } \bigcirc \text{ *)} \\ &\equiv \psi \wedge (\varphi \vee \bigcirc\, (\varphi \,\mathsf{R}\, \psi)) && \text{(* definition of R *)} \end{aligned}$$

(b) The duality of the until operator U and the weak until operator W is given as

$$\neg(\varphi \,\mathsf{U}\, \psi) \equiv (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi).$$

Then the correctness of the given equivalence can be proven as follows:

$$\begin{aligned} \varphi \,\mathsf{R}\, \psi &\equiv \neg(\neg\varphi \,\mathsf{U}\, \neg\psi) && \text{(* definition of R *)} \\ &\equiv \big(\neg\varphi \wedge \neg(\neg\psi)\big) \,\mathsf{W}\, \big(\neg(\neg\varphi) \wedge \neg(\neg\psi)\big) && \text{(* duality of U and W *)} \\ &\equiv \big(\neg\varphi \wedge \psi\big) \,\mathsf{W}\, \big(\varphi \wedge \psi\big) && \text{(* Duality of } \neg \text{ *)} \end{aligned}$$