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

Solution of Exercise sheet 2

Prequels

We give a few important logical equivalences: let ξ, ζ and ν some logical statements,

$\xi \to \zeta$	$\iff$	$\neg\xi \vee \zeta$	*(definition of implication)*
$\xi \wedge \zeta$	$\iff$	$\neg(\neg\xi \vee \neg\zeta)$	*(de Morgan's law)*
$\nu \vee (\xi \wedge \zeta)$	$\iff$	$(\nu \vee \xi) \wedge (\nu \vee \zeta)$	*(distributivity of $\wedge$ over $\vee$)*
$\forall x\ \xi$	$\iff$	$\neg\exists x\ (\neg\xi)$	*(duality between $\forall$ and $\exists$)*
$\forall x > k,\ \xi$	$\iff$	$\forall x\ ((x > k) \to \xi)$	a widely used notation
$\neg\forall x > k,\ \xi$	$\iff$	$\exists x > k,\ \neg\xi$	not hard to prove

$$\xi \iff \zeta \quad \Longrightarrow \quad \begin{cases} \exists x\ \xi \iff \exists x\ \zeta \\ \nu \wedge \xi \iff \nu \wedge \zeta \\ \neg\xi \iff \neg\zeta \end{cases} \quad \text{we can rewrite within formulas}$$

This list is not exhaustive, especially concerning the $\vee$ and $\wedge$ operators, which are also associative, commutative, idempotent; false is neutral for $\vee$ and is the zero of $\wedge$ and conversely for true.

Structural Induction over LTL Formulas

For a formal and accurate definition, it is well-founded induction over the set of formulas using the well-order "is a subformula". The boring details may be inspected in the Wikipedia article on well-founded induction.

Assume we want to show some property P holds for any LTL formula, for that we need to show:

- Property P holds for atomic LTL formulas,
- The operators preserve the property. For any LTL formulas φ and ψ such that φ and φ satisfy the property P we have to show that:
  - $\varphi\ \mathcal{U}\ \psi$ satisfies P
  - $\varphi \vee \psi$ satisfies P
  - $\mathbf{X}\varphi$ satisfies P
  - $\neg\varphi$ satisfies P

Intuitively this ensures any formula will satisfy property P, as as formula can be seen as a tree whose leaves satify property P and each node preserves the property P.

This technique can be generalized to other type of inductively defined formulas. Remark that it is crucial that property P is the same everywhere in the prove.

(tiny) LTL cheat sheet

p		$p \in AP$ and $p \in w(0)$	p holds **now**
$\neg\varphi$		$w \not\models \varphi$	φ doesn't hold
$\varphi \vee \psi$		$w \models \varphi$ or $w \models \psi$	needs not be always the same
$\mathbf{X}\varphi$	$\neg\mathbf{X}\neg\varphi$	$w^1 \models \varphi$	next φ
$\varphi\,\mathcal{U}\,\psi$	$\psi \vee (\varphi \wedge \mathbf{X}(\varphi\,\mathcal{U}\,\psi))$	$\exists i (w^i \models \psi \wedge \forall k < i,\, w^k \models \varphi)$	ψ may hold right away
$\mathbf{G}\varphi$	$\neg(\top\,\mathcal{U}\,\neg\varphi)$	$\forall n\; w^n \models \varphi$	φ is always true
$\mathbf{F}\varphi$	$\neg\mathbf{G}\neg\varphi$	$\exists n\; w^n \models \varphi$	φ is true (at least) once
$\varphi\,\mathbf{R}\,\psi$	$\neg(\neg\varphi\,\mathcal{U}\,\neg\psi)$	$\forall i\; (\forall j < i,\, w^j \not\models \varphi) \rightarrow w^i \models \psi$	ψ may get false only after φ does
$\mathbf{FG}\varphi$	$\mathbf{GFG}\varphi$	$\exists t\; \forall n > t,\, w^n \models \varphi$	φ will always hold
$\mathbf{GF}\varphi$	$\mathbf{FGF}\varphi$	$\forall t\; \exists n > t,\, w^n \models \varphi$	φ holds infinitely often

$\mathbf{G}(p \rightarrow \mathbf{F}q)$	Each p is eventually followed by a q
$\mathbf{G}(p \rightarrow \mathbf{X}(\mathbf{G}\neg q))$	After the first p, q no longer occurs

Exercise 2.1: Solution

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

word	$w \models \varphi$	$w \models \psi$
$\{p\}\{p\}\{p\}^\omega$	no	yes
$\{q\}\{q\}\{q\}^\omega$	yes	yes
$\{s\}\{s\}\{s\}^\omega$	no	yes
$\{q,r\}\{q,r\}\{q,r\}^\omega$	yes	yes
$\emptyset\emptyset\emptyset^\omega$	no	yes
$\{r\}\{r\}\{q\}\{q\}(\{r\}\{q\})^\omega$	yes	yes
$\{r\}\{s\}\{r\}\{q\}\{q\}(\{r\}\{q\}\{q\})^\omega$	yes	yes
$\{r\}\{r\}\{q\}\{s\}\{q\}(\{r\}\{r\}\{q\})^\omega$	yes	yes
$rprqqq(rrrqqq)^\omega$	yes	yes
$rprqqqs(rrrqqq)^\omega$	yes	yes
$rrpqqqs(rrrqqq)^\omega$	yes	yes
$rrpqqsq(rrrqqq)^\omega$	yes	yes
$rrpqqqrsr(qqrr)^\omega$	yes	yes
$qqqrrpqqqqsqqq^\omega$	yes	yes
$qqqrrpqpqpqqsqqrq^\omega$	yes	yes

Exercise 2.2: Solution

1. If a program $P \models \mathbf{F}g$ then any trace of that program will give a result. For instance $\{g\}\emptyset^\omega$ is an example of a valid trace and $\emptyset^\omega$ is not.

2. $p \rightarrow \mathbf{G}(\neg r \wedge \neg s)$ would only ensure the desired property if the program first gives a result, for instance $\{s\}\{r\}\{g\}(\{s\}\{r\})^\omega$ would satisfy this LTL formula. Thus the property is $\mathbf{G}(p \rightarrow \mathbf{G}(\neg r \wedge \neg s))$, or depending on the semantics of the english word

"after", only $\mathbf{G}(p \to \mathbf{XG}(\neg r \land \neg s))$ may be considered correct. Typically $\{g, s, r\}\emptyset^\omega$ is only satisfying the second formula.

3. $\mathbf{GF}s$ indicates that s holds infinitely often ($\{s\}^\omega$ satsifies this property, $\{s\}(\{e\}^\omega)$ does not.

4. This time we need the next operator, (otherwise, we would have $g \to \mathbf{G}\neg g$, which implies $g \to \neg g$, thus $\neg g$), $\mathbf{F}g \land \mathbf{G}(g \to \mathbf{XG}\neg g)$.

5. It is not possible to express in LTL that property if we consider that every send can only match one receive: that language would not be regular. However if we consider that a send responds to every preceding receive, then the property is equivalent to every receive there will later be a send. $\mathbf{G}(r \to X\mathbf{F}s)$.

6. The most succint way to write this property is $(\neg s \land \neg g)\ \mathbf{W}\, r$.

Exercise 2.3: Solution

Remark that $\emptyset^\omega$ satisfies none of the following formulas, while $\{p, q, r, s\}^\omega$ satisfies all of them.

1. $p\,\mathcal{U}(q \lor \mathbf{G}q)$: since $\mathbf{G}q \implies q$, this formula is equivalent to $p\,\mathcal{U}\,q$.

2. $\mathbf{G}(q \to \mathbf{F}s)$ is s responds to q.

3. $\mathbf{G}((q \land \neg r \land \mathbf{F}r) \to (\neg p\,\mathcal{U}\,r))$ is p is false between q and r.

4. $p\,\mathcal{U}\,\mathbf{G}q$, this formula state that the word consists of a finite prefix of p (other predicates may hold) followed by an infinite suffix of q (other predicates may hold).

5. $p\,\mathcal{U}\,\mathbf{F}q$: this formula is equivalent to $\mathbf{F}q$. (eventually q will hold).

6. $\mathbf{G}(p\,\mathcal{U}\,\mathbf{G}q)$: this formula is equivalent to $p\,\mathcal{U}\,\mathbf{G}q$, indeed if that formula holds at the first position, it holds at every position.

7. $(\mathbf{G}p)\,\mathcal{U}\,\mathbf{G}q$: this formula is equivalent to $p\,\mathcal{U}\,\mathbf{G}(p \land q)$.

Exercise 2.4: Solution

$$
\begin{array}{lll}
- & w \models \mathbf{G}\varphi & \iff w \models \neg(\top\, \mathcal{U}\, \neg\varphi) \\
 & & \iff \neg(\exists i (w^i \models \neg\varphi \wedge \forall k < i,\ w^k \models \top)) \\
 & & \iff \forall i\ \neg w^i \models \neg\varphi \vee \neg\forall k < i,\ w^k \models \top \\
 & & \iff \forall i \in \mathbb{N}\ w^i \models \varphi \\
- & w \models \varphi\, \mathbf{R}\, \psi & \iff \neg(\neg\varphi\, \mathcal{U}\, \neg\psi) \\
 & & \iff \neg\exists i (w^i \models \neg\psi \wedge \forall j < i,\ w^j \models \neg\varphi) \\
 & & \iff \forall i (\neg w^i \models \neg\psi) \vee \neg(\forall j < i,\ w^j \not\models \varphi) \\
 & & \iff \forall i \in \mathbb{N}\ (\forall j < i,\ w^j \not\models \varphi) \rightarrow w^i \models \psi \\
- & w \models \neg(\varphi\, \mathcal{U}\, \psi) & \iff w \models \neg\varphi\, \mathbf{R}\, \neg\psi \\
- & w \models \varphi\, \mathcal{U}\, \psi & \iff \exists i (w^i \models \psi \wedge \forall j < i,\ w^j \models \varphi) \\
 & & \iff (i = 0 \wedge w \models \psi) \vee \left(\exists i > 0, \begin{cases} w^i \models \psi \wedge (j = 0 \wedge w^0 \models \varphi) \\ \wedge \forall 0 < j < i,\ w^j \models \varphi \end{cases} \right) \\
 & & \iff w \models \psi \vee \exists i'\ w^{i'+1} \models \psi \wedge w \models \varphi \wedge \forall j' < i',\ w^{j'+1} \models \varphi) \\
 & & \iff w \models \psi \vee (\varphi \wedge \mathbf{X}(\varphi\, \mathcal{U}\, \psi)) \\
- & w \models \varphi\, \mathbf{R}\, \psi & \iff w \models \neg(\neg\varphi\, \mathcal{U}\, \neg\psi) \\
 & & \iff \neg\exists i\ (w^i \not\models \psi) \wedge (\forall j < i,\ w^j \not\models \varphi) \\
 & & \iff \forall i\ (w^i \models \psi \vee \exists j < i,\ w^j \models \varphi) \\
 & & \iff \forall i\ (w^i \not\models \psi \rightarrow \exists j < i,\ w^j \models \varphi)
\end{array}
$$

We need to remark that if $\forall i\ w^i \models \psi$, then $w \models \varphi\, \mathbf{R}\, \psi$. If, on the contrary, ψ does not always hold, we can find a smallest position k, such that ψ doesn't hold: that is $\exists k\ \forall j < k,\ w^j \models \psi \wedge w^k \not\models \psi$. $\varphi\, \mathbf{R}\, \psi$ therefore implies (by instanciating the universal quantification with k), that $\exists j < k,\ w^j \models \varphi$. Thus we have that ($w \not\models \mathbf{G}\psi$ and $w \models \varphi\, \mathbf{R}\, \psi$) implies $\exists j < k,\ w \models \varphi$, and as $\forall i < k,\ w \models \psi$, we deduce that it implies $w \models \psi\, \mathcal{U}(\varphi \wedge \psi)$. Therefore ($w \models \varphi\, \mathbf{R}\, \psi$ and $w \models \mathbf{G}\psi$) or ($w \models \varphi\, \mathbf{R}\, \psi$ and $w \not\models \mathbf{G}\psi$) implies either $w \models \mathbf{G}\psi$ or $w \models \psi\, \mathcal{U}(\varphi \wedge \psi)$ thus $w \models \varphi\, \mathbf{R}\, \psi \implies w \models \mathbf{G}\psi \vee (\psi\, \mathcal{U}(\varphi \wedge \psi))$.

To show the converse implication, assume that $w \models \mathbf{G}\psi \vee (\psi\, \mathcal{U}(\varphi \wedge \psi))$. Let us show that for any i, $w^i \not\models \psi \implies \exists j < i,\ w^j \models \varphi$. If i is such that $w^i \not\models \psi$, then by hypothesis $w \models \psi\, \mathcal{U}(\varphi \wedge \psi)$ so this i is necessarily greater than the position where $\varphi \wedge \psi$ hold, hence there is a position before i where φ holds.

Exercise 2.5: Solution

Any trace of K_1 is also a trace K_2, therefore $K_2 \models \varphi$ is equivalent to $\forall w \in K_2, w \models \varphi$. As $\forall w \in K_1, w \in K_2$, we have $\forall w \in K_1, w \models \varphi$, hence $K_2 \models \varphi \implies K_1 \models \varphi$.