Computer-Aided Formal Verification (Sheet #2)

Marius Gavrilescu

1. If $\varphi \vDash \Diamond\psi$, $\varphi[i..] \vDash \psi$. Then $\varphi[i..] \vDash (\phi \,\mathrm{U}\, \psi)$, so $\varphi \vDash \Diamond(\phi \,\mathrm{U}\, \psi)$.

   If $\varphi \vDash \Diamond(\phi \,\mathrm{U}\, \psi)$, $\varphi[i..] \vDash (\phi \,\mathrm{U}\, \psi)$. Then $\varphi[(i+j)..] \vDash \psi$, so $\varphi \vDash \Diamond\psi$.

   Hence the formulae are equivalent.

   Suppose $\phi = a, \psi = b$ and the trace we are looking at is ac^ω.

   Then $ac^\omega \nvDash \Box\Diamond\phi$ so $ac^\omega \vDash \Box\Diamond\phi \to \Box\Diamond\psi$.

   However, $ac^\omega \vDash \phi$ and $ac^\omega \nvDash \Diamond\psi$ so $ac^\omega \nvDash \phi \to \Diamond\psi$ therefore $ac^\omega \nvDash \Box(\phi \to \Diamond\psi)$.

   $ac^\omega \vDash LHS$ but $ac^\omega \nvDash RHS$.

   Hence the formulae are not equivalent.

   If $\varphi \vDash (\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2)$ then $\varphi[i..] \vDash \Box\phi_1$ and $\varphi[j..] \vDash \Box\phi_2$. But then $\varphi[max(i,j)..] \vDash \Box\phi_1 \wedge \Box\phi_2$, so $\varphi \vDash \Diamond(\Box\phi_1 \wedge \Box\phi_2)$.

   If $\varphi \vDash \Diamond(\Box\phi_1 \wedge \Box\phi_2)$ then $\varphi[i..] \vDash \Box\phi_1$ and $\varphi[i..] \vDash \Box phi_2$. But then $\varphi \vDash \Diamond\Box\phi_1$ and $\varphi \vDash \Diamond\Box\phi_2$, so $\varphi \vDash (\Diamond\Box\phi_1) \wedge (\Diamond\Box\phi_2)$.

   Hence the formulae are equivalent.

   If $\varphi \vDash \phi_1 \,\mathrm{U}\, \phi_2$, then $\varphi \vDash \Diamond\phi_2$ so $\varphi \vDash true \,\mathrm{U}\, \phi_2$ which means (by assumption) $\varphi \vDash (\phi_1 \,\mathrm{U}\, \phi_2) \,\mathrm{U}\, \phi_2$.

   If $\varphi \vDash (\phi_1 \,\mathrm{U}\, \phi_2) \,\mathrm{U}\, \phi_2$ then either $\varphi \vDash \phi_1 \,\mathrm{U}\, \phi_2$ or $\varphi \vDash \phi_2$ (which implies $\varphi \vDash \phi_1 \,\mathrm{U}\, \phi_2$).

   Hence the formulae are equivalent.

2. $TS \nvDash \phi_1$ due to the path $s_1(s_4s_5)^\omega$.

   $TS \vDash \phi_2$ because s_1 can never be reached after the first move, and the only other state that is not labelled c (that is, s_4) does not have a self-loop (so we can't even obtain two consecutive non-"c"s after the first move).

   $TS \vDash \phi_3$. Assume it was false, then $\exists$ a path in TS called φ such that $\varphi \vDash \bigcirc\neg c$ and $\varphi \nvDash \bigcirc\bigcirc c$. The first statement implies the second element in the path is s_4 (the only state reachable in one step that is not labelled c), and note that all states that can come after s_4 are labelled c. Contradiction.

   $TS \nvDash \phi_4$ due to the path $s_1(s_4s_5)^\omega$, note that s_4 is not labelled a.

   $TS \vDash \phi_5$: every state that is not s_1 satisfies $b \vee c$; s_1 cannot be reached after the first step, so any path will satisfy $\Box(b \vee c)$ from the second step onwards. Paths that satisfy $\Box(b \vee c)$ from the first step are fine, and paths that do not satisfy it from the first step must start with s_1 which satisfies a.

   $TS \nvDash \phi_6$ due to the path $s_1s_4s_2..$ which satisfies neither $\bigcirc\bigcirc b$ nor $b \vee c$.

3. 1. are not equivalent: take the TS having states s_1, s_2, s_3 labelled q, q, p respectively, with initial state s_1, transitions from s_1 to s_2, s_3, from s_2 to itself, and from s_3 to itself. Clearly $s_1 \vDash LHS$ because the path $s_1 s_3^\omega$ satisfies $\Diamond p$, and the path $s_1 s_2^\omega$ satisfies $\Box q$. However $s_1 \nvDash RHS$ because no suffix of the path $s_1 s_2^\omega$ satisfies $\exists \Box q$, and no suffix of $s_1 s_3^\omega$ satisfies p.

   2. are not equivalent: take the TS having states s_1, s_2 labelled $r, p+q$ respectively, with initial state s_1, transitions from s_1 to s_2 and from s_2 to itself. The only paths starting from the beginning are therefore $s_1 s_2^\omega$. Here $s_1 \vDash RHS$ because $\pi[1..]$ satisfies $p \wedge \forall \Box q$ but $s_1 \nvDash LHS$ because it does not satisfy $\forall \Box q$.

   3. are not equivalent: take the TS having states s_1, s_2 labelled $p+q, q$ respectively with the initial state s_1 and same transitions as before. Paths are as before: $s_1 s_2^\omega$. Here $s_1 \vDash LHS$ because all paths start with p (hence satisfying $\Diamond p$) and every state is labelled q; but $s_1 \nvDash RHS$ because $\pi[1..] \nvDash \forall \Diamond p$ (there is no way to reach p from the second step onwards).

   4. are equivalent. LHS says that any path starting from the beginning reaches a subtree of all ps, and any path starting from the beginning reaches a subtree of all qs. From here we can determine that any path starting from the beginning reaches a subtree of all ps AND reaches a subtree of all qs (i.e. $\forall(\Diamond(\forall \Box p) \wedge \Diamond(\forall \Box q))$).

   But if a path can reach a subtree of all ps we know it must also be able to reach a subtree of all qs. So from this subtree of all ps we must be able to reach a subtree of all qs. Of course, this second subtree is included in the subtree of all ps so we just found a subtree of all $p+q$s.

   Hence if the LHS is true then from all paths starting from the beginning we can reach a subtree of all ps AND a subtree of all qs, which means we can reach a subtree of all $p+q$s, which is the RHS.

   5. and 6. are not equivalent: Take the two-state TS having states s_1, s_2 labelled p, r respectively with the initial state s_1 and the same transitions as in 3. Here $s_1 \vDash RHS$ but $s_1 \nvDash LHS$ because no path starting from s_1 satisfies $q \,\mathrm{U}\, r$ as there is no state labelled q and s_1 is not labelled r.

4. Not equivalent. Take a two-state TS having states s_1 labelled b and s_2 labelled a, with transitions from each state to both states and initial state s_1, then take $r = b \wedge \circ a$ and $a = a$.

   Now observe that $s_1 \vDash \forall \Box(b \wedge \circ a \rightarrow \Diamond a)$ because every path starting somewhere in the tree (not necessarily at the beginning) where $b \wedge \circ a$ is true (that is, the path starts with $s_1 s_2$) satisfies $\Diamond a$ (because the second element of the path is labelled a).

   However, $s_1 \nvDash \forall \Box(b \wedge \circ a \rightarrow \forall \Diamond a)$ because paths which start $s_1 s_2$ do not satisfy $\forall \Diamond a$ since one of the paths starting from s_1 is s_1^ω which does not satisfy $\Diamond a$.