# CSC2108: Automated Verification
# Assignment 2, part 2 – Solutions

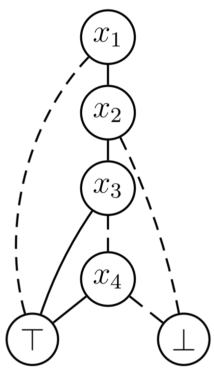
Due: Oct. 24, classtime.
Do not work on this part of the assignment in groups.

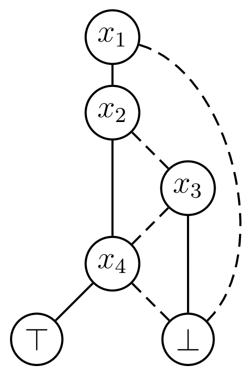
1. Let the following two expressions be given:

$$x_1 \Rightarrow (x_2 \ \wedge \ (x_3 \vee x_4)) \quad (exp_1)$$
$$(x_2 \vee \neg x_3) \ \wedge \ (x_1 \ \wedge \ x_4) \quad (exp_2)$$

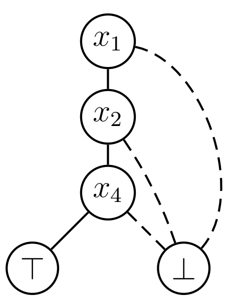
Let the order of variables $x_1 < x_2 < x_3 < x_4$ be given.

(a) Build BDDs for the two expressions, referring to them as $BDD_1$ and $BDD_2$.

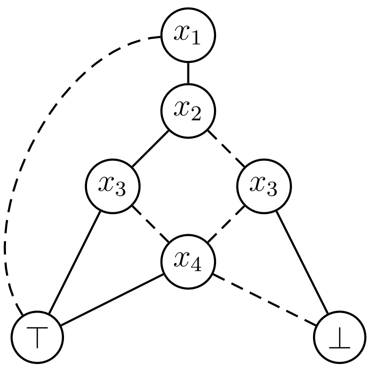



(b) Compute Apply('$\wedge$', $BDD_1$, $BDD_2$). You may compare your answers with computing $exp_1 \ \wedge \ exp_2$ and building a BDD from it (this is not part of the assignment – it is for your benefit only).




(c) Compute Apply($\vee$, $BDD_1$, $BDD_2$).




(d) Compute Quantify($x_1$, $BDD_1$), i.e., compute $\exists x_1 \cdot exp_1$.
The result is $\top$.

2. Prove the duality

$$\mu Z.f(Z) = \neg \nu Z.\neg f(\neg Z)$$

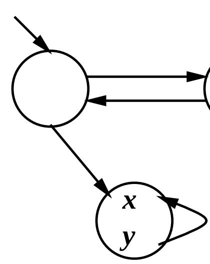
Proof sketch: Assume that $f : 2^S \rightarrow 2^S$ is a monotone function over subsets of a finite set $S$. In this case, negation is set complement. Let $g(Z) = \neg f(\neg Z)$, show by induction that $g^i(S) = \neg f^i(\emptyset)$. The rest follows from the fact that fixpoint computation must converge after finitely many iterations.

3. Prove that $AF\varphi = \mu Z.\varphi \vee AXZ$, i.e., prove

(a) $\varphi \vee AXAF\varphi = AF\varphi$
Need to show that for any state $s$, $[\![\varphi \vee AXAF\varphi]\!](s) \Leftrightarrow [\![AF\varphi]\!](s)$, which follows directly from the definition of $AF$.

(b) $\forall Y \cdot (Y = \varphi \vee AXY) \Rightarrow (Y \supseteq AF\varphi)$
Let $F(Z) = \varphi \vee AXZ$. Note that if $s \in [\![AF\varphi]\!]$ then there exists a bound $k$ such that along every path from $s$, a state in $[\![\varphi]\!]$ is reached in at most $k$ steps. Let $s$ be such that $s \in [\![AF\varphi]\!]$ and $s \notin Y$. Show by induction that $s \in F^k(Y) = Y$.

4. Consider this model:




(a) Compute the transition relation $R$ for this model.

$$
\begin{aligned}
R \;=\;& (x \wedge \neg y \wedge \neg x' \wedge \neg y') \vee (\neg x \wedge \neg y \wedge x' \wedge y') \vee \\
& (\neg x \wedge \neg y \wedge \neg y' \wedge x') \vee (x \wedge y \wedge x' \wedge y')
\end{aligned}
$$

(b) Symbolically, compute the value of $AGEFy$. Check that the computation is correct by executing the explicit-state model-checking algorithm.

We make use of the following laws

$$
\begin{aligned}
\exists x \cdot f \vee g &= (\exists x \cdot f) \vee (\exists x \cdot g) \\
\exists x \cdot f \wedge x &= f
\end{aligned}
$$

First step is to compute $EFy = \mu Z \cdot y \vee EXZ$

$$
\begin{aligned}
& EF_0 y \\
=\;& y \vee EX\bot \\
=\;& y \vee \exists x', y' \cdot R \wedge \bot \\
=\;& y \vee \bot \\
=\;& y
\end{aligned}
$$

$$
\begin{aligned}
& EF_1 y \\
=\;& y \vee EXEF_0 y \\
=\;& y \vee EXy \\
=\;& y \vee \exists x', y' \cdot R \wedge y' \\
=\;& y \vee \exists x', y' \cdot (\neg x \wedge \neg y \wedge x' \wedge y') \vee (x \wedge y \wedge x' \wedge y') \\
=\;& y \vee (\neg x \wedge \neg y) \vee (x \wedge y) \\
=\;& y \vee (\neg x \wedge \neg y)
\end{aligned}
$$

$$
\begin{aligned}
& EF_2 y \\
=\;& y \vee EXEF_1 y \\
=\;& y \vee EX(y \vee (\neg x \wedge \neg y)) \\
=\;& y \vee (EXy) \vee EX(\neg x \wedge \neg y) \\
=\;& y \vee (EXy) \vee \exists x', y' \cdot R \wedge \neg x' \wedge \neg y' \\
=\;& y \vee (EXy) \vee (x \wedge \neg y) \\
=\;& y \vee (\neg x \wedge \neg y) \vee (x \wedge \neg y) \\
=\;& y \vee \neg y \\
=\;& \top
\end{aligned}
$$

Now we need to compute $AG(EFy) = AG\top = \nu Z \cdot \top \wedge AXZ$

$$
\begin{aligned}
& AG_0 \top \\
=\;& \top \wedge AX\top \\
=\;& \top \wedge \forall x', y' \cdot \neg R \vee \top \\
=\;& \top \wedge \forall x', y' \cdot \top \\
=\;& \top
\end{aligned}
$$

(c) Symbolically, compute $EGy$.

We need to compute $EGy = \nu Z \cdot y \land EXZ$

$$\begin{aligned}
& EG_0 y \\
= \;& y \land EX\top \\
= \;& y \land \exists x', y' \cdot R \land \top \\
= \;& y \land \exists x', y' \cdot R \\
= \;& y \land (x \land y) \\
= \;& y \land x
\end{aligned}$$

$$\begin{aligned}
& EG_1 y \\
= \;& y \land EXEG_1 y \\
= \;& y \land EX(x \land y) \\
= \;& y \land \exists x', y' \cdot R \land (x' \land y') \\
= \;& y \land ((\neg x \land \neg y) \lor (x \land y)) \\
= \;& y \land x
\end{aligned}$$