Model Checking by Implicit State Traversal

Given a set of propositional atoms, $P = \{p, q, r\}$ a model is a finite state, labeled transition system, consisting of a set of states ($S$), a transition relation ($T$) and a labeling function ($L$).

$$M = \langle S, T \subseteq S \times S, L: S \rightarrow 2^P \rangle$$

As a running example, we’ll use

In which $S = \{X, Y, Z\}$,

$$
T: \begin{align*}
X &\mapsto \{Y, Z\} \\
Y &\mapsto \{X, Z\} \\
Z &\mapsto \{Z\}
\end{align*}
$$

$$
L: \begin{align*}
X &\mapsto \{p, q\} \\
Y &\mapsto \{q, r\} \\
Z &\mapsto \{r\}
\end{align*}
$$
Represent $s \in S$ by two boolean variables $(s_1, s_0)$ enumerating the three elements, say by

\[
X \leftrightarrow 00 \\
Y \leftrightarrow 01 \\
Z \leftrightarrow 10
\]

So the statement “$s = X$” becomes $\bar{s}_1 \land \bar{s}_0$, and so forth. The elementary propositions for this model become

\[
p \equiv (s = X) \rightarrow \bar{s}_1 \land \bar{s}_0 \\
q \equiv (s = X) \lor (s = Y) \rightarrow \bar{s}_1 \\
r \equiv (s = Y) \lor (s = Z) \rightarrow s_1 \oplus s_0
\]

We can now build a representation of the transition relation, $T$ using two state-variables, $s$ representing the current state (or set of states), and $s'$ representing the next state (or set of states).

\[
s T s' \equiv [ (s = X) \land ((s' = Y) \lor (s' = Z)) \\
\lor (s = Y) \land ((s' = X) \lor (s' = Z)) \\
\lor (s = Z) \land (s' = Z) ]
\]
Quantification
\[ \forall x: \phi \equiv \phi^{1}[x] \land \phi^{0}[x] \]
\[ \exists x: \phi \equiv \phi^{1}[x] \lor \phi^{0}[x] \]

Model Checking
\[ M, s \models AG \phi \]
\[ AG_{\phi}(s) \triangleq \phi(s) \land [\forall s': s T s' \Rightarrow AG_{\phi}(s')] \]
\[ AG_{\phi}(s) \triangleq \phi(s) \land AG_{\phi}(Xs) \]
\[ AG_{\phi}(s) \triangleq \phi(s) \land \forall s' \in Xs: \phi(s') \]
\[ \land \forall s' \in XXs: \phi(s') \]
\[ \vdots \]
\[ \land \forall s' \in X^{i}(s): \phi(s') \]
\[ \vdots \]
\[ until \forall s' \in X^{i}(s): \phi(s') \equiv \forall s' \in X^{i+1}(s): \phi(s') \]

Boolean functions are represented by Binary Decision Diagrams (BDDs).