This document contains a summary of the second chapter of the text “Principles of Model checking”, by Baier and Katoen. We list the main formal definitions (with a slightly modified notation).

Transition systems

Definition 1 (Transition system) A transition system is given by a tuple (S, Σ, δ, I) where S is a finite set of *states*, Σ is a finite set of *actions*, $\delta \subseteq S \times \Sigma \times S$ is a *transition relation* and I is a set of initial states.

Program graphs

Let $\mathit{Var} = \{x_1, x_2 \dots, x_n\}$ be a set of variables. Each variable $x_i \in Var$ is associated with a finite set $\mathrm{dom}(x_i)$ called its *domain*. Denote by $\mathrm{dom}(Var)$ the set $\mathrm{dom}(x_1) \times \mathrm{dom}(x_2) \times \cdots \times \mathrm{dom}(x_n)$. Each element $v \in \mathrm{dom}(Var)$ is of the form $(v_1, \dots, v_n)$ such that $v_i \in \mathrm{dom}(x_i)$ for each $i \in \{1, \dots, n\}$ and is called a *valuation* of the variables. Let $2^{\mathrm{dom}(Var)}$ denote the power set of $\mathrm{dom}(Var)$.

Definition 2 (Program graph) A program graph over variables *Var* is a tuple $(\mathit{Loc}, \Sigma, \mathrm{Effect}, \Delta, \mathit{Loc}_0, g_0)$ where *Loc* is a set of *locations*, Σ is a set of actions, $\mathrm{Effect} : \Sigma \times \mathrm{dom}(Var) \mapsto \mathrm{dom}(\mathit{Var})$ is a function which associates a valuation to each action-valuation pair, $\Delta \subseteq \mathit{Loc} \times 2^{\mathrm{dom}(Var)} \times \Sigma \times \mathit{Loc}$ is a transition relation, Loc_0 is the initial location and $g_0 \subseteq 2^{\mathrm{dom}(Var)}$ is a subset of valuations denoting the initial values of the variables.

Each program graph is associated with a transition system. In order to specify a transition system, we need to give four objects: its set of states, actions, transition relation and the initial states. We describe below the transition system corresponding to a program graph $G = (\mathit{Loc}, \Sigma, \mathrm{Effect}, \Delta, \mathit{Loc}_0, g_0)$, denoted as $TS(G)$:

- the states of $TS(G)$ are of the form (l, η) where $l \in \mathit{Loc}$ is a location and $\eta \in \mathrm{dom}(x_1) \times \mathrm{dom}(x_2) \times \cdots \times \mathrm{dom}(x_n)$ is a valuation of the variables,
- the set of actions of $TS(G)$ is Σ as in G,
- for every state (l, η) in the transition system $TS(G)$, and for every transition (l, g, α, l') in G, there is a transition $((l, \eta), \alpha, (l', \eta'))$ in $TS(G)$ provided $\eta \in g$; and in this case η' is given as the effect of α applied on the valuation η, that is: $\mathrm{Effect}(\alpha, \eta)$,
- initial states are $\{(l_0, \eta_0) \mid l_0 \in \mathit{Loc}_0 \text{ and } \eta_0 \in g_0\}$

Exercise: Read Examples 2.12 and 2.14 from the text.

Parallel composition of independent systems

We say that two transition systems $TS_1 = (S_1, \Sigma_1, \delta_1, I_1)$ and $TS_2 = (S_2, \Sigma_2, \delta_2, I_2)$ are *independent* if $\Sigma_1 \cap \Sigma_2 = \emptyset$.

Definition 3 (Interleaving operator) Let $TS_i = (S_i, \Sigma_i, \delta_i, I_i)$, $i = 1, 2$ be two independent transition systems. The transition system $TS_1 \mid\mid\mid TS_2$ is defined as:

$$TS_1 \mid\mid\mid TS_2 = (S_1 \times S_2, \Sigma_1 \cup \Sigma_2, \delta, I_1 \cup I_2)$$

where the transition relation δ is defined as:

$$\begin{aligned} \delta((s_1, s_2), \alpha) &= (\delta_1(s_1, \alpha), s_2) \quad \text{if } \alpha \in \Sigma_1 \\ \delta((s_1, s_2), \alpha) &= (s_1, \delta_2(s_2, \alpha)) \quad \text{if } \alpha \in \Sigma_2 \end{aligned}$$

From each state of the cross product, only one component makes the next transition - the transitions in the product are interleaved. The above definition can be extended naturally to product of any number of systems. The above composition is also known as *asynchronous* product.

Two program graphs PG_1 and PG_2, over variables Var_1 and Var_2 respectively are said to be independent if $Var_1 \cap Var_2 = \emptyset$. The joint behaviour of such independent programs is described by $TS(PG_1) \,|||\, TS(PG_2)$.

Communication via shared variables

Let $PG_1 = (Loc_1, \Sigma_1, \text{Effect}_1, \Delta_1, Loc_{0,1}, g_{0,1})$ and $PG_2 = (Loc_2, \Sigma_2, \text{Effect}_2, \Delta_2, Loc_{0,2}, g_{0,2})$ be two program graphs over variables Var_1 and Var_2. Assume that they share some variables in common, that is, $Var_1 \cap Var_2 \neq \emptyset$. Without loss of generality, we can assume that $\Sigma_1 \cap \Sigma_2 = \emptyset$. In order to give the joint behaviour of these two programs, we need to first interleave the program graphs, and then consider the transition system of this interleaved program graph.

Definition 4 (Interleaving of program graphs) Let $PG_i = (Loc_i, \Sigma_i, \text{Effect}_i, \Delta_i, Loc_{0,i}, g_{0,i})$, $i = 1, 2$ be a program graph over Var_i. The program graph $PG_1 \,|||\, PG_2$ is defined over $Var_1 \cup Var_2$ as:

$$PG_1 \,|||\, PG_2 := (Loc_1 \times Loc_2, \Sigma_1 \cup \Sigma_2, \text{Effect}, \Delta, Loc_{0,1} \times Loc_{0,2}, g_{0,1} \cap g_{0,2})$$

where Δ is given by the following rules:

$$(\langle l_1, l_2 \rangle, \alpha, g, \langle l_1', l_2 \rangle) \in \Delta \text{ if } (l_1, \alpha, g, l_1') \in \Delta_1$$
$$(\langle l_1, l_2 \rangle, \alpha, g, \langle l_1, l_2' \rangle) \in \Delta \text{ if } (l_2, \alpha, g, l_2') \in \Delta_2$$

and $\text{Effect}(\alpha, \eta) = \text{Effect}_i(\alpha, \eta)$ if $\alpha \in \Sigma_i$.

The transition system $TS(PG_1 |||PG_2)$ gives the joint behaviour of the two programs running concurrently. The inter

Exercise: Read examples 2.22, Remark 2.23, Examples 2.24 and 2.25 from the text.

Communication via shared actions

We now consider the case when there are two transition systems communicating with each other through shared actions. All actions which are not shared can be interleaved. Actions that are shared can be taken only when both the systems are able to perform the action.

Definition 5 (Handshake operator) Let $TS_i = (S_i, \Sigma_i, \delta_i, I_i)$, $i = 1, 2$ be two transition systems and let $\Sigma_1 \cap \Sigma_2$ be non-empty. The transition system $TS_1 \parallel TS_2$ is defined as:

$$TS_1 \parallel TS_2 := (S_1 \times S_2, \Sigma_1 \cup \Sigma_2, \delta, I_1 \times I_2)$$

where δ is defined as:

$$\begin{aligned}
&\delta((s_1, s_2), \alpha) = (\delta_1(s_1, \alpha), s_2) && \text{if } \alpha \in \Sigma_1 \setminus \Sigma_2 \\
&\delta((s_1, s_2), \alpha) = (s_1, \delta_2(s_2, \alpha)) && \text{if } \alpha \in \Sigma_2 \setminus \Sigma_1 \\
&\delta((s_1, s_2), \alpha) = (\delta_1(s_1, a), \delta_2(s_2, \alpha)) && \text{if } \alpha \in \Sigma_1 \cap \Sigma_2
\end{aligned}$$

Exercise: Read Section 2.2.3 from the text