Specification models and their analysis
–Background Material–

Kai Lampka

December 10, 2010

TIK Institut für Technische Informatik und Kommunikationsnetze
Part I

Introduction
In the following we will develop a concise (mathematical) framework for formally describing systems of interest (→ formal model).

This framework allows one to formally, i.e., mathematically reason about a model’s and hence a system’s correctness w. r. t. dedicated properties, e.g. deadlock-freeness etc.

In principle we could start with any programming language. However, their interpretation is very complicated (address arithmetic, arbitrary data types, ...). Also only certain aspects of a system matter, where one may abstract away many details. Hence it appears useful to follow a more abstract view and speak here only about very simple “languages” for describing systems. Such methods are commonly denoted as high-level model description methods.
There are $N$ philosophers sitting around a circular table either thinking or eating pasta. Each philosopher needs his left and right fork to eat, but there is only one fork between each 2 philosophers. Design an algorithm that the philosophers can follow.

Consider the following protocol (= sequence of interaction)

```c
void philosopher()
{
    while(1) {
        think();
        get_left_fork();
        get_right_fork();
        eat();
        put_left_fork();
        put_right_fork();
    }
}
```

Even though the high-level model description methods appear very simple, they possess clearly defined (execution or operational) semantics. These semantics allow us to map them to graphs.

These graphs represent all possible behaviors of the specified high-level description.

Hence the basic objects which represent the entities to be studied are graphs. Therefore we will briefly re-visit some basic definitions, which you probably have already seen before.

Don’t mind the formal notation, this will be made clear by examples and allows you to understand the resp. literature.
Part II

Basic (formal) Facts about Graphs
Definition 2.1: Graph

A graph \( G \) is a pair \((\mathcal{V}, \mathcal{E})\) where

1. \( \mathcal{V} \) is a discrete set of vertices (or nodes) \( \{v_1, \ldots, v_m\} \)

2. \( \mathcal{E} \subseteq \mathcal{V} \times \mathcal{V} \) is a discrete set of pairs \( \{(v_i, v_j) \mid \text{for some } i, j \in \{1, \ldots, m\}\} \). One commonly denotes these pairs as edges or arcs.
Definition 2.2: Directed Graph (Digraph)

- If the elements of $\mathcal{E}$ are ordered in such a way that $(v, w) \neq (w, v)$ the elements of $\mathcal{E}$ are denoted as directed edges or directed arcs.

- A graph with such a property is denoted directed graph or *digraph* for short.
In a digraph and for an ordered pair \((u, v) \in E\) vertex \(u\) is denoted as **predecessor or parent** of vertex \(v\) and vertex \(v\) is denoted as **successor or child** of vertex \(u\).

This can be extended to the level of sets of children and parent nodes as follows:

\[
\mathcal{P}ost(u) := \{v \in V \mid (u, v) \in E\}
\]

is the set of all **children or direct successors** of a vertex \(u\).

\[
\mathcal{P}re(v) := \{u \in V \mid (u, v) \in E\}
\]

is the set of all **parents or direct predecessors** of a vertex \(v\).

The above sets are very helpful, once we want to operate on graphs.

→ Question 2.1: Please write down an algorithm which check if a node \(n\) is contained in a graph.
Check reachability of a node $n$

(1) $\text{Nodes2beTraversed} := \{v_0\}$, $\text{Nodes} := \emptyset$, $\text{Edges} := \emptyset$

(2) While $\text{Nodes2beTraversed} \neq \emptyset$

(3) $v_s := \text{getElement}(\text{Nodes2beTraversed})$ //get node to be processed next

(4) $\text{Edges} := \text{PostSetEdges}(v)$ //get set of outgoing edges of node $v_s$

(5) While $\text{Edges} \neq \emptyset$ //still edges we did not traverse so far?

(6) $e := \text{pop}(\text{Edges})$ //pick one of the outgoing edges of node $v_s$

(7) $v_t := \text{get2ndElement}(e)$ //extract children node w. r. t. edge $e$

(8) if ($v_t == n$) return(YES) //did we reach node $n$?

(9) if ($v_t \notin \text{Nodes}$) // did we reach a new node $v_t$ to be traversed; avoid being trapped in cycles.

(10) $\text{insert}(v_t, \text{Nodes})$ // put $v_t$ in set of known states

(11) $\text{insert}(v_t, \text{Nodes2beTraversed})$ // put $v_t$ in set of states to be traversed

(12) $\text{remove}(e, \text{Edges})$ //done with edge $e$

(13) $\text{remove}(v_s, \text{Nodes2beTraversed})$ //done with node $v_s$

(14) return(NO)

Please clarify the functions PostSetEdges.

Order of traversal: depth-first-search or breadth first search?
Definition 2.3: Weighted Graphs

- If the edges of a graph are labelled with elements from \( \mathbb{R} \) one speaks of a *weighted graph*.
- In fact the set of edges of a weighted digraph is a ternary relation (set of triples):
  \[ E \subseteq V \times \mathbb{R} \times V. \]
- Function \( \mathcal{W} : V \times V \to \mathbb{R} \) gives one the weight associated with the respective edge \((u, x, v)\): \((u, x, v) \in E \Rightarrow \mathcal{W}(u, v) = x\) and \(\mathcal{W}(u, v) := 0\) for all triples not contained in \(E\).
Definition 2.4: Labelled Graphs

- If the edges of a graph are labelled with elements from a finite set, e.g. \( l \in Act \) one speaks commonly of a labelled graph.

- In fact the set of edges of a labelled digraph is once again a ternary relation: \( E \subseteq V \times Act \times V \).

Note:

A labelled graph is also often referred to as labelled transition system (LTS), where instead of vertices one speaks of states.
Definition 2.5: Labelled Transition System (LTS)

A LTS is a quadruple \( \mathcal{T} := (S, S_0, Act, E) \), where

1. \( S := \{s_1, \ldots, s_n\} \) is an ordered (indexed) set of states with
2. \( S_0 \) as the set of initial states.
3. \( Act \) is the discrete set of transition labels,
4. \( E \subseteq S \times Act \times S \) is an ordered (indexed) set of labelled state-to-state transitions.
Preliminaries – Labelled Transition system

\[ S := \{ \} \]

\[ S_0 := \]

\[ Act := \{ \} \]

\[ E := \{ \} \]
Note:

LTS are essentially the semantics of the here discussed high-level modelling techniques, where the techniques of model checking allow us to reason about their properties. In the following we briefly strive some important definitions.

- A LTS $\mathcal{T}$ is defined non-terminal if each state has at least one out-going edge otherwise $\mathcal{T}$ is called terminal.

- A LTS $\mathcal{T}$ is defined deterministic if each state has at most one out-going edge with the same edge label otherwise $\mathcal{T}$ is denoted as non-deterministic.

Are non-deterministic finite LTS more expressive than deterministic ones?
Preliminaries – Termination and Determinism (Examples)

1. Deterministic?
   - yes
   - no

2. Non-terminal?
   - yes
   - no
Part III

Backus-Naur-Form
BNF is a method for compactly writing down production rules (of a context-free grammar). The production rules employ variables (capital letters) and terminal symbols (lower case letters).

\[ A ::= true \mid \alpha \in \mathcal{AP} \mid \neg A \mid A \land A \mid (A) \]

is read as follows: each occurrence of variable \( A \) can be replaced by the constant \( true \), a terminal symbol of set \( \mathcal{AP} \) or \( \neg A \) or \( A \land A \) or \( (A) \). One may note that \( A \) may not only be a non-terminal symbol (variable), it can also be a word produced by the above grammar. This is, because it also appears on the left-hand side.

\[ \text{Question 3.1: What does we above rule define?} \]