Lecture Notes for

# Logic and Computability

Course Number: IND04033UF

by

Bettina Könighofer
Bernd Grabner
Belinda Uhl

Contact

Bettina Könighofer
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria
bettina.koenighofer@iaik.tugraz.at

March, 2021

# Table of Contents

# 8

# Modelling Systems and Symbolic Encoding

Many digital circuits and programs are examples of reactive systems. Such systems typically exhibit frequent interactions with their environment and often do not terminate. The most important feature of a reactive system that we need to capture is its *state*. A state is a snapshot of the system that captures the values of the variables of the system at a particular instant of time. To analyze system behavior we also need to know how the state of the system changes as the result of some action of the system. Such a pair of states determines a *transition* of the system. Consequently, the behaviors of a reactive system can be defined in terms of its transitions.

In this chapter, we use a type of state transition graph called a *Kripke structure* to model the behavior of reactive systems. A Kripke structure consists of a set of states, a set of transitions between states, and a function that labels each state with a set of properties that are true in this state. Paths in a Kripke structure correspond to behaviors of the system. Although Kripke structures are very simple models, they are sufficiently expressive to capture those aspects of temporal behavior that are most important for reasoning about reactive systems.

Kripke structures are often very large. Therefore, we will use formulas to symbolically represent Kripke structures. We will see that it is straightforward to translate a Kripke structure to a formula, and vise versa.

## 8.1 Transition Systems and Kripke Structures

**Definition - Transition system.** *A transition system $\mathcal{T}$ is a triple $(S, S_0, R)$ where*

1. *$S$ is a set of states.*
2. *$S_0 \subseteq S$ is the set of initial states.*
3. *$R \subseteq S \times S$ is a transition relation.*

In order to make observations about particular states, we define a set of state labels. We refer to these labels as atomic propositions and use AP to denote the set of all atomic propositions. A transition system enriched with such a state-labeling is called a Kripke structure.

**Note:** Kripke structures are often referred to as *models*, because they are models of the system under analysis. The intended meaning of *model* is usually clear from the context.

**Definition - Kripke structure.** *A Kripke structure $M$ is a five tuple $\mathcal{K} = (S, S_0, R, AP, L)$ where*

1. *$S$, $S_0$, and $R$ are defined as above,*
2. *$AP$ is the set of atomic propositions, and*
3. *$L : S \to 2^{AP}$ is a function that labels each state with the set of those atomic propositions that are true in that state.*

Kripke structures are frequently visualized by means of directed graphs.

**Example.** Draw the graph of a Kripke structure $\mathcal{K}_1$ with: $S = \{s_1, s_2, s_3\}$, $S_0 = \{s_1\}$, $R = \{(s_1, s_2), (s_2, s_1), (s_3, s_2)\}$, $AP = \{p, q\}$ and $L = \{s1 \to \{p\}, s2 \to \{p, q\}, s3 \to \emptyset\}$.

**Solution.**

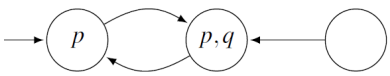



**Figure 8.1:** Graph for Kripke structure $\mathcal{K}_1$.

**Example.** Consider the example of an light switch. Initially, the light is off. Once a button is pressed, the light is turned on. To turn the light off, the button has to be released and pressed again. Model the light switch as Kripke structure.

**Solution.** A state is labeled with the label 1 if the light is on, and with label 0 if the light is off. Similarly, we use the label r for states in which the button is released, and p for those states in which the button is pressed.

In $\mathcal{K}_2$, initially, the button may either be pressed or released. This is modeled by means of two initial states. As example for a transition, consider the state labeled with $(0, r)$: to model the case the button is pressed, there is a transition

to the state labeled $(1, p)$. Otherwise, the system remains in state $(0, r)$ by means of a self-transition.

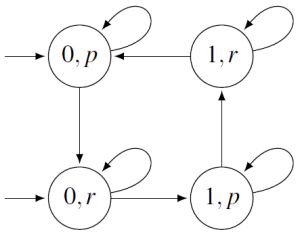



**Figure 8.2:** Graph for Kripke structure $\mathcal{K}_2$.

## 8.2 Symbolic Representation

Our goal is to use propositional logic to represent the set of initial states and the transition relation of Kripke structures symbolically.

### 8.2.1 Symbolic Representation of Sets of States

Since states are instantaneous descriptions of a system, it is natural to identify states with valuations of the system variables. To this end, let $V = \{v_1, \ldots, v_n\}$ be the set of system variables. *To make it simpler, since this is an introductory course, we assume that all variables $v \in V$ are Boolean variables.* Thus, state $s$ defines a valuation for all variables $v \in V$; it assigns truth values to all variables.

**Representation of a single state:** For a given valuation, we can write a formula that is true for exactly that valuation. For instance, the valuation $v_1 \to \mathit{true}$, $v_2 \to \mathit{false}$, and $v_3 \to \mathit{true}$ can be represented by the formula

$$v_1 \wedge \neg v_2 \wedge v_3.$$

**Example.** Given a state space of the size $|S| = 2^{12} = 4096$. Give the symbolic encoding for the state $s_{457}$.

**Solution.** For the symbolic encoding we need 12 Boolean variables, $\{v_{11}, \ldots, v_0\}$. Let $v_{11}$ be the most significant bit, and $v_0$ the least significant bit.

We have that

$$(457)_{10} = (0001\ 1100\ 1001)_2$$

therefore, we get the symbolic encoding

$$\neg v_{11} \wedge \neg v_{10} \wedge \neg v_9 \wedge v_8 \wedge v_7 \wedge v_6 \wedge \neg v_5 \wedge \neg v_4 \wedge v_3 \wedge \neg v_2 \wedge \neg v_1 \wedge v_0.$$

**Representation of sets of states:** *A formula precisely represents the set of all valuations that make it true.* Therefore, we can describe certain subsets

of the set of states by means of propositional formulas. Thus, a formula can be viewed as the *characteristic function* or *symbolic representation* of a set of states. In particular, the set of *initial states* of the system can be described by a formula $S_0$ over the variables in $V$.

**Example.** Consider the following set of states defined by the valuations

$$\{(v_1 \to true, v_2 \to false, v_3 \to true), (v_1 \to false, v_2 \to false, v_3 \to true)\}.$$

Represent this set of states symbolically using a propositional logic formula.

**Solution.** This set can be represented by means of a propositional formula with disjunction:

$$(v_1 \wedge \neg v_2 \wedge v_3) \vee (\neg v_1 \wedge \neg v_2 \wedge v_3) = (\neg v_2 \wedge v_3)$$

**Example.** Given a state space of the size $|S| = 1024$. Symbolically represent the sets of states $B = \{s_0, s_1, s_2, \ldots, s_{511}\}$ and $C = \{s_{256}, s_{257}, \ldots, s_{767}\}$.

**Solution.** Using the variables $\{v_9, \ldots, v_0\}$ the encoding of $B$ is simply given by $b = \neg v_9$.

In order to find a simple formula $c$ for $C$, we can analyze the Binary representations of the contained states.

- The binary encoding of 256 is 0100000000.
- The binary encoding of 256 is 0100000001.
- ...
- The binary encoding of 767 is 1011111111.

We can only the values of $v_9$ and $v_8$ are important to distinguish whether a state is included in $C$ or not. We get the final formula:

$$c = (\neg v_9 \wedge v_8) \vee (v_9 \vee \neg v_8) = (v_9 \oplus v_8).$$

### Set Operations on Symbolically Encoded Sets

When using formulas to characterize sets, we can perform the usual set operations by appropriate transformations to symbolic operations. Let $A$ and $B$ denote subsets of a set $S$ and $a$ and $b$ denote the respective characteristic functions of $A$ and $B$. Then we have:

| | | |
|---|---|---|
| Intersection | $A \cap B$ | $a \wedge b$ |
| Union | $A \cup B$ | $a \vee b$ |
| Difference | $A \backslash B$ | $a \wedge \neg b$ |

Similar transformations apply in the case of relational operators over sets. As an instance, we can check $A \subseteq B$ by determining whether the formula $a \to b$ evaluates to true.

| Equality | $A = B$ | $a \equiv b$ |
|---|---|---|
| Subset | $A \subseteq B$ | $a \rightarrow b$ |

**Example.** Given the sets of states $S$, $A$ and $B$ from the previous example. Compute the characteristic functions for the sets $D = B \cup C$, $E = B \cap C$, and $F = S \setminus E$.

**Solution.**

- $d = b \vee c \;\equiv\; (x_9 \oplus x_8) \vee \neg x_9 \;\equiv\; (x_9 \wedge \neg x_8) \vee \neg x_9$
- $e = ((x_9 \wedge \neg x_8) \vee (\neg x_9 \wedge x_8)) \wedge \neg x_9 \;\equiv\; \neg x_9 \wedge x_8$
- $f = true \wedge \neg(\neg x_9 \wedge x_8) \;\equiv\; x_9 \vee \neg x_8$

### 8.2.2 Symbolic Representation of the Transition Relation

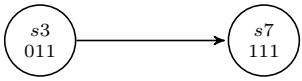
To represent the transition relation of Kripke structures symbolically, we extend the idea used for symbolic representation of sets of states above. This time, we use a formula to represent *a set of ordered pairs of states*. Therefore, we create a second set of variables $V'$. We think of the variables in $V$ as *present state variables* and the variables in $V'$ as *next state variables*. Each variable $v$ in $V$ has a corresponding next state variable $v'$ in $V'$. A valuation for the variables in $V \cup V'$ can be viewed as a transition. We can represent sets of these valuations using formulas as above.

For instance, the formula

$$(v_1 \wedge v_2 \wedge v_3 \wedge v_1' \wedge v_2' \wedge v_3')$$

represents a transition which is a self loop for the state with the valuation $(v_1 \rightarrow true, v_2 \rightarrow true, v_3 \rightarrow true)$ (state $s_7$).

**Example.** Given a state space of the size $|S| = 2^3 = 8$. Give the formula for the transition from state $s3$ to state $s7$ as shown below.

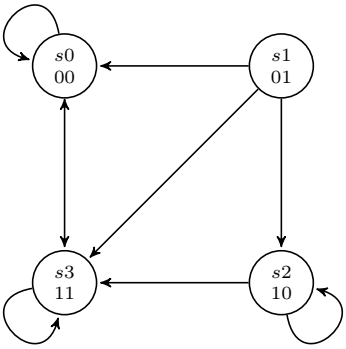



**Solution.** The transition can be encoded via:

$$\neg v_2 \wedge v_1 \wedge v_0 \wedge \; v_2' \wedge v_1' \wedge v_0'.$$

Sets of transitions can again be formed using disjunctions to connect the encodings for the individual transitions, which can then be further simplified. For Kripke structures with dense transition relations, a simple way to get a short formula for the transition relation is to encode the edges that are *not* contained in the transition relation, and to *negate* the resulting formula.

**Example.** Consider the following Kripke structure with $|S| = 4$. Give the symbolic transition relation for this Kripke structure.




**Solution:** Using the variables $v_1$ (MSB), $v_0$ (LSB), we can define the transition relation using the following formula:

$$\begin{aligned}
\neg v_1 \wedge \neg v_0 \quad &\wedge \quad (\neg v_1' \wedge \neg v_0' \ \vee \ v_1' \wedge v_0') \quad \vee \\
\neg v_1 \wedge v_0 \quad &\wedge \quad (\neg v_1' \wedge \neg v_0' \ \vee \ v_1' \wedge \neg v_0' \ \vee \ v_1' \wedge v_0') \quad \vee \\
v_1 \wedge \neg v_0 \quad &\wedge \quad (v_1' \wedge \neg v_0' \ \vee \ v_1' \wedge v_0') \quad \vee \\
v_1 \wedge v_0 \quad &\wedge \quad (v_1' \wedge \neg v_0' \ \vee \ v_1' \wedge v_0')
\end{aligned}$$

We can further simplify the formula to:

$$\begin{aligned}
(v_1 \leftrightarrow v_0) \quad &\wedge \quad (v_1' \leftrightarrow v_0') \quad \vee \\
\neg v_1 \wedge v_0 \quad &\wedge \quad (v_1' \vee \neg v_0') \quad \vee \\
v_1 \wedge \neg v_0 \quad &\wedge \quad v_1'
\end{aligned}$$

### Symbolic Representations of the Set of Atomic Propositions and the Labeling Function

We will use a similar mechanism to define the set of atomic propositions $AP$. Recall that $AP$ is a fixed finite set of labels which contain information about the system states. Essentially, $AP$ can contain arbitrary properties whose truth or falsity is uniquely determined by the state, i.e., by the variable valuation. *In particular, a label in $AP$ can be defined as a propositional formula using the variables in $V$.*

## 8.3 Exercises

### 8.3.1 Examples

**Example 1.** Given the state space $S = \{s_0, \ldots, s_{256}\}$.

(a) Symbolically encode the set of states $A = \{s_{71}, \ldots, s_{255}\}$.

(b) Symbolically encode the set of states $B = \{s_{16}, \ldots, s_{63}\}$.

(c) Symbolically encode the set of states $C = \{s_0, \ldots, s_7\} \cup \{s_{128}, \ldots, s_{255}\}$.

**Example 2.** Given are the sets $A = \{x \in \mathbb{N} \mid x < 8\}$, and $B = \{x \in \mathbb{N} \mid 4 \leqslant x \leqslant 15\}$.

(a) Find a symbolic encoding for the sets $A$ and $B$.

(b) Find a symbolic encoding for the set $C = A \cup B$.

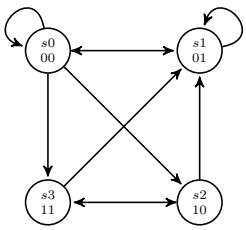
(c) Find a symbolic encoding for the set $D = A \cap B$.

(d) Find a symbolic encoding for the set $E = A \backslash B$.

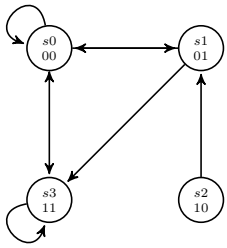
(e) Find a symbolic encoding for the set $F = B \backslash A$.

**Example 3.** For the following Kripke strcutures, give the symbolic transition relations.

(a)




(b)




**Example 4.** Given the following symbolically encoded transition functions, draw the corresponding Kripke strictures.

(a) $(\neg v_1 \wedge \neg v_0 \wedge \neg v_1' \wedge v_0') \vee (\neg v_1 \wedge x_0 \wedge v_1' \wedge v_0') \vee (v_1 \wedge \neg v_0 \wedge \neg v_1' \wedge v_0) \vee (v_1 \wedge v_0 \wedge v_1')$

(b) $v_1' \wedge \neg v_0' \vee \neg(v_1 \oplus \neg v_0) \wedge v_0'$

### 8.3.2 Solutions

**Solution 1.** Eight bit Binary representation $v_7, v_8, ..., v_0$

(a) $a = v_6 \wedge v_2$

(b) $b = \neg v_7 \wedge \neg v_6 \wedge (v_5 \vee v_4)$

(c) $c = v_7 \vee (\neg v_7 \wedge \neg v_6 \wedge \neg v_5 \wedge \neg v_4 \wedge \neg v_3)$

**Solution 2.** (a) Four bit Binary representation $v_3, v_2, v_1, v_0$
$a = \neg v_3, \quad b = v_3 \vee v_2$

(b) $c = a \vee b \quad \equiv \quad \neg v_3 \vee v_3 \vee v_2 \quad \equiv \quad \top$

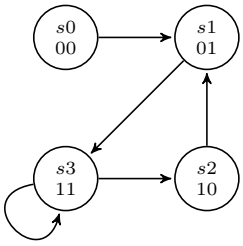
(c) $d = a \wedge b \quad \equiv \quad \neg v_3 \wedge (v_3 \vee v_2) \quad \equiv \quad \neg v_3 \wedge v_2$

(d) $e = a \wedge \neg b \quad \equiv \quad \neg v_3 \wedge \neg(v_3 \vee v_2) \quad \equiv \quad \neg v_3 \wedge \neg v_2$

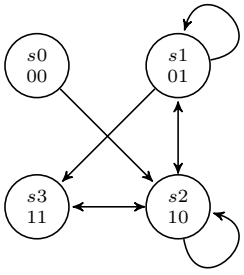
(e) $f = b \wedge \neg a \quad \equiv \quad (v_3 \vee v_2) \wedge \neg\neg v_3 \quad \equiv \quad v_3$

**Solution 3.** (a) $\neg v_1 \wedge \neg v_0 \vee$
$(v_1 \oplus v_0) \wedge \neg v_1' \vee$
$v_1 \wedge v_0 \wedge (v_1' \oplus v_0')$

(b) $(\neg v_1 \vee v_0) \wedge (v_1' \leftrightarrow v_0')$
$v_1 \wedge \neg v_0 \wedge \neg v_1' \wedge v_0'$




**Solution 4.** (a)




(b)

### Declaration of Sources

Chapter 7 was based on the following book.

Edmund M. Clarke Jr., Orna Grumberg, Daniel Kröning, Doron Peled, Helmut Veith: *Model Checking*. Second edition. MIT Press. ISBN-13: 978-0262038836. ISBN-10: 0262038838