Modeling Systems and Symbolic Encodings

Bettina Könighofer

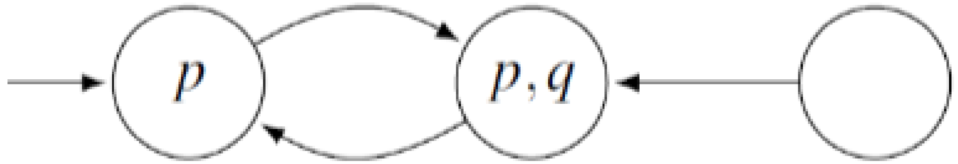
IAIK – Graz University of Technology
bettina.koenighofer@iaik.tugraz.at

Reactive System

- **Set of States**
- Initial State(s)
- State Update Rules
  - aka *Transition Function* (deterministic case)
  - aka *Transition Relation* (non-Deterministic)

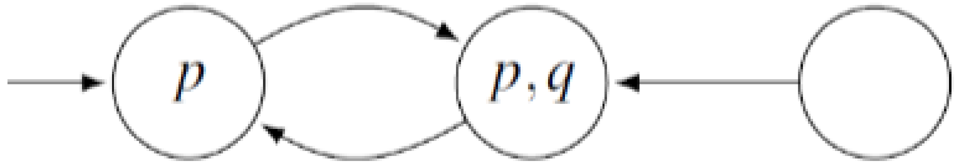
Kripke Structure

- Formalization of Digital System
  - Finite Set of States S
  - Set of Initial States $I \subseteq S$
  - Transition Relation $T \subseteq S \times S$
  - Labeling Function $L: S \rightarrow 2^{AP}$
    - "AP": Set of Atomic Propositions



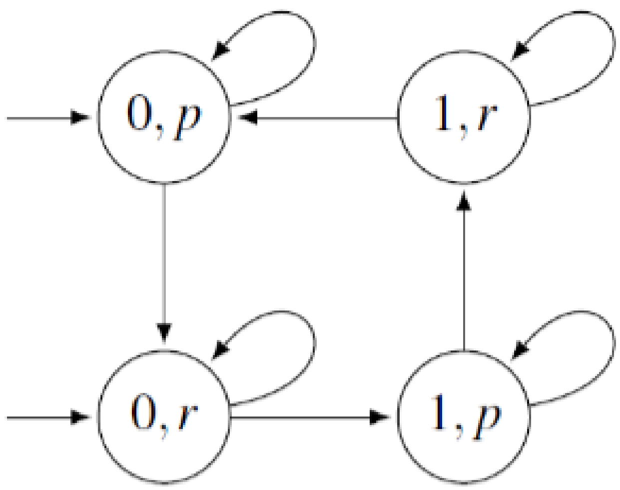
Kripke Structure

- Formalization of Digital System
  - Finite Set of States S
  - Set of Initial States $I \subseteq S$
  - Transition Relation $T \subseteq S \times S$
  - Labeling Function $L: S \rightarrow 2^{AP}$
    - "AP": Set of Atomic Propositions
    - $AP = \{p, q\}$
    - $L = \{s_1 \rightarrow \{p\}, s_2 \rightarrow \{p, q\}, s_3 \rightarrow \emptyset\}$



Kripke Structure

- Light Switch Example:
  - 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
  - Labels:
  - 1 … the light is on
  - 0 … the light is off.
  - r … the button is released
  - p … button is pressed



Symbolic Encoding

- Systems have huge state spaces / number of transitions
- Therefore,
  - Symbolically encode sets
  - Perform set operations symbolically

Boolean Function

- $f\colon \mathbb{B}^n \mapsto \mathbb{B}$
  - $\mathbb{B} = \{True,\ False\}$

- Possible Representations
  - Propositional Formula
  - Truth Table
  - Binary Decision Diagram

Finite Sets vs. Boolean Functions

- **Set:**
  - **Finite Domain of Objects**
    - **Element**
    - **“Non-Element”**

- **Boolean Function:**
  - **Finite Domain of Truth Assignments**
    - **Map to True**
    - **Map to False**

Characteristic Function

- Function f represents set A
  - $[\![f]\!] = A$

- $a \in A \quad \Leftrightarrow \quad f\big(Enc(a)\big) = \top$
  - Elements give True
  - Non-Elements give False

Encoding Elements

- Domain: e.g. $\mathrm{D} = \{Austria, Germany, Spain, Italy\}$
  - $\#Vars = \lceil ld(|\mathrm{D}|) \rceil$

Element	Encoding	
	x_1	x_0
Austria	0	0
Germany	0	1
Spain	1	0
Italy	1	1

Example

- $f = \neg x_0 \wedge \neg x_1$

  $[\![f]\!] = \{Austria\}$

- $g = \neg x_0$

  $[\![g]\!] = \{Austria, Spain\}$

Element	Encoding	
	x_1	x_0
Austria	0	0
Germany	0	1
Spain	1	0
Italy	1	1

Example

Element	Encoding	
	x_1	x_0
Austria	0	0
Germany	1	0
Spain	1	1
Italy	0	1

Element	Encoding	
	x_1	x_0
Austria	0	0
Germany	1	0
Spain	0	1
Italy	1	1

- Which encoding gives the shorter characteristic function for the set B={Germany, Spain}?

$f = x_1$

$g = x_1 \oplus x_0$

Example

1. Consider the set $A = \{Apple,\ Banana,\ Orange,\ Pear\}$. Find a symbolic encoding for its elements. Using this encoding, determine the characteristic functions of the sets B= $\{Apple, Pear\}$, C= $\{Orange\}$, and $D = \{\,\}$.

Element	Encoding	
	x_1	x_0
Apple	0	0
Banana	0	1
Orange	1	0
Pear	1	1

$$b = (\neg x_1 \land \neg x_0) \lor (x_1 \land x_0)$$
$$c = x_1 \land \neg x_0$$
$$d = \bot$$

Encoding Natural Numbers

- Binary Representation
- Domain D: Usually Power of 2
  - E.g.: $\mathrm{D} = \{\mathrm{x} \in \mathbb{N} \mid \mathrm{x} < 2^{12}\}$

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

$$x_{11} \cdots\cdots\cdots\cdots \; x_3 \; x_2 \; x_1 \; x_0$$

Example

- Domain: $A = \{x \in \mathbb{N} | 0 \leq x \leq 1023\}$
  - 10 bit binary repräsentation $x_9 x_8 \ldots . x_0$
- $B = \{x \in A | x < 512\}$, $b = ?$
- $C = \{x \in A | 256 \leq x < 768\}$, $c = ?$

256 010....0
511 011....1
512 100....0
767 101....1

$c = (\neg x_9 \wedge x_8) \vee (x_9 \wedge \neg x_8)$

Symbolic Operations

- **Intersection:** $F \cap G =$

$$= [\![f \land g]\!]$$

- **Union:** $F \cup G =$

$$= [\![f \lor g]\!]$$

- **Difference:** $F \setminus G =$

$$= [\![f \land \neg g]\!]$$

Symbolic Relations

- **Equality:** $F = G \Leftrightarrow$

  $\Leftrightarrow f \equiv g$

- **Subset:** $F \subseteq G \Leftrightarrow$

  $\Leftrightarrow f \rightarrow g$

Example

- Domain: $A = \{x \in \mathbb{N} | 0 \leq x \leq 1023\}$
- $b = \neg x_9$ $\quad c = (\neg x_9 \land x_8) \lor (x_9 \land \neg x_8)$
- $D = B \cup C$

$d = \neg x_9 \lor [(\neg x_9 \land x_8) \lor (x_9 \land \neg x_8)] = \neg x_9 \lor (x_9 \land \neg x_8)$

- $E = B \cap C$

$e = \neg x_9 \land [(\neg x_9 \land x_8) \lor (x_9 \land \neg x_8)] = \neg x_9 \land x_8$

- $F = A \setminus E$

$f = T \land \neg[\neg x_9 \land x_8] = x_9 \lor \neg x_8$

$|A| = 1024$
$|E| = 256$
$|F| = 768$
$|B| = 512$

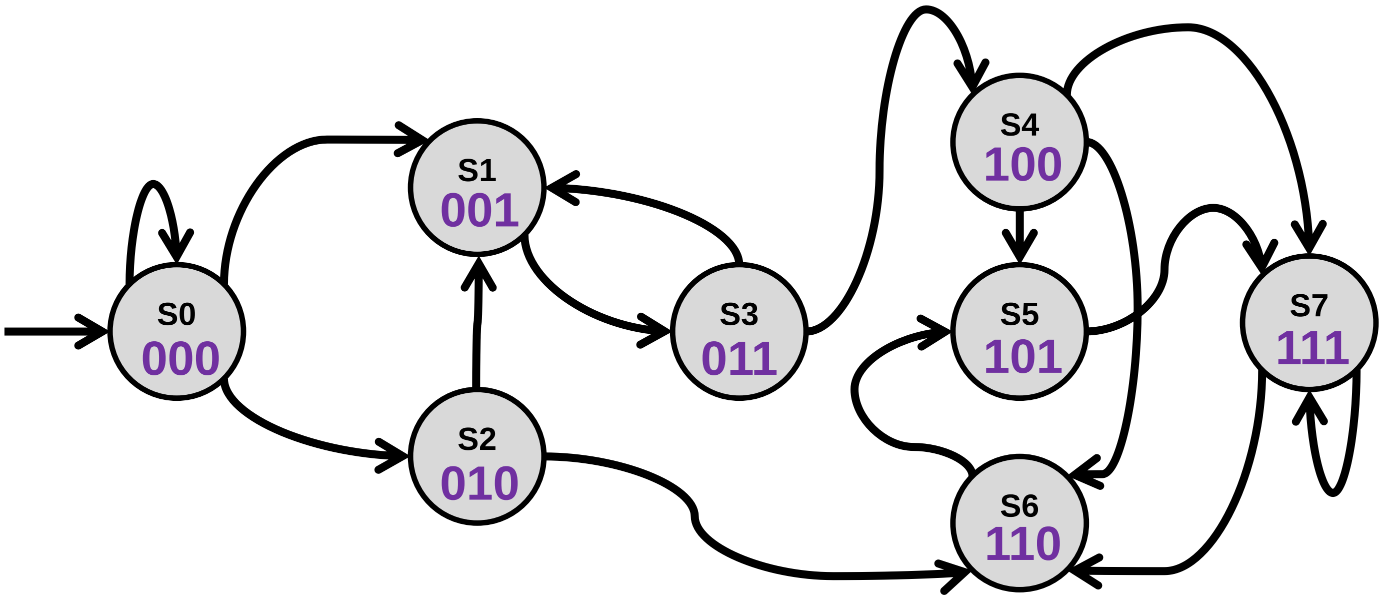
Symbolic Encoding of Kripke Structures

- Systems have huge state spaces / number of transitions

- Therefore:
  - Symbolically encode sets of states
  - Symbolically encode sets of transitions
  - Perform set operations symbolically

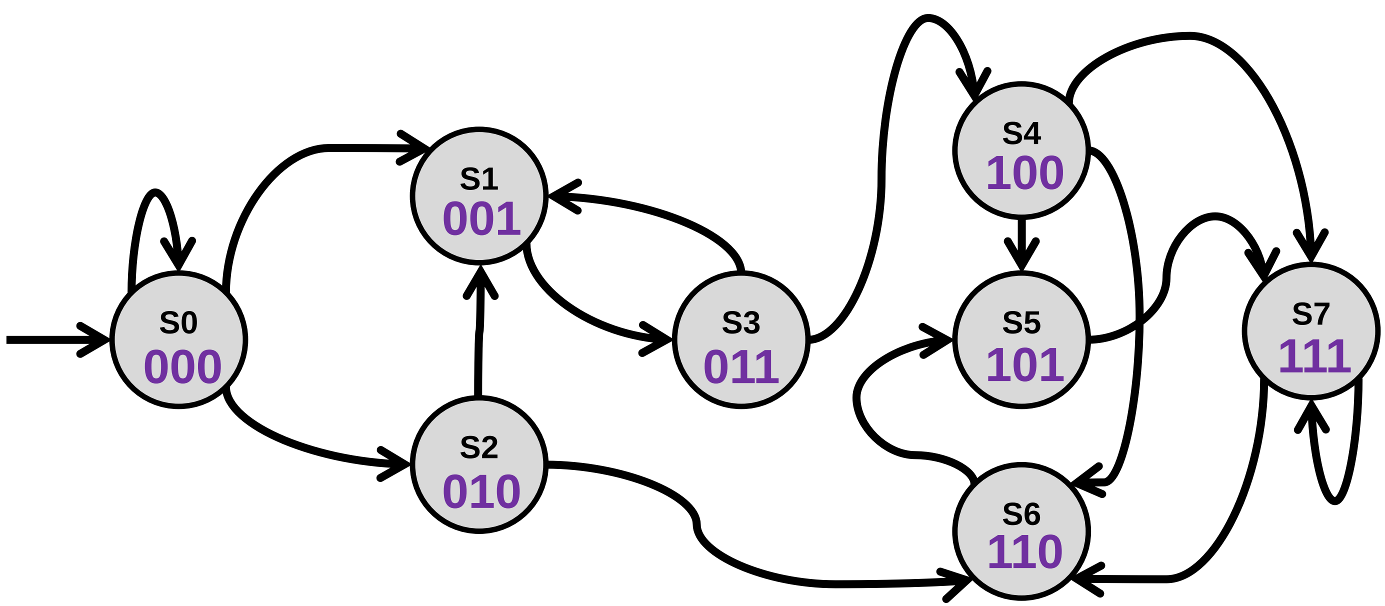
Encoding Kripke Structures – States

- Use variables $V = \{v_1, ..., v_n\}$ for binary representations of states



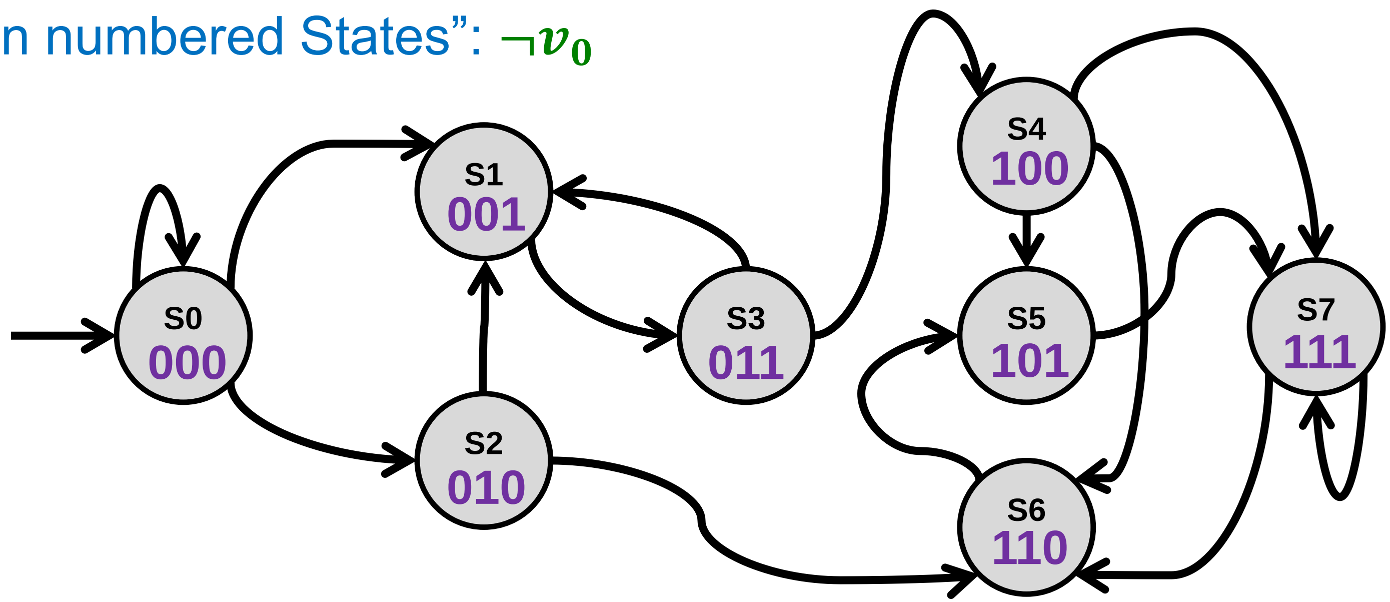
Encoding Kripke Structures – States

- Single State
  - Labeling $v_2 v_1 v_0$
    - E.g. State S_2: $\neg v_2 \land v_1 \land \neg v_0$



Encoding Kripke Structures – States

- Single State
  - Labeling $v_2 v_1 v_0$
    - E.g. State S_2 : $\neg v_2 \wedge v_1 \wedge \neg v_0$
- Sets
  - E.g. "Even numbered States": $\neg \boldsymbol{v_0}$



Encoding Kripke Structures – Edges

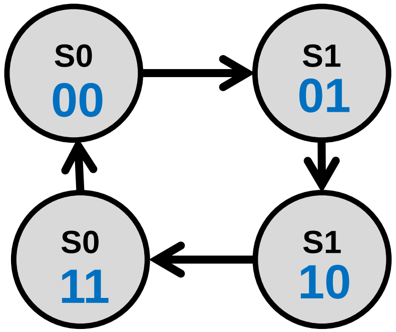
- "Duplicate" Variables
  - "Present" State variables $v_0, v_1, v_2, \ldots$
  - "Next" State variables $v_0', v_1', v_2', \ldots$

$$\neg v_2 \land \neg v_1 \land \neg v_0 \quad \land \quad \neg v_2' \land \neg v_1' \land v_0{}'$$

Symbolic encoding for given transition-relation

- Draw the Kripke Structure for the following transition relation:

$$(\neg v_1 \land \neg v_0 \land \neg v'_1 \land v'_0) \lor$$
$$(\neg v_1 \land v_0 \land v'_1 \land \neg v'_0) \lor$$
$$(v_1 \land \neg v_0 \land v'_1 \land v'_0) \lor$$
$$(v_1 \land v_0 \land \neg v'_1 \land \neg v'_0)$$

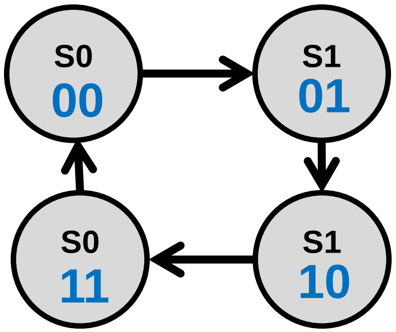


Transition Function/Relation

- Union of all Edges
  - Disjunction
  - Good for sparse sets of edges
- $[\![T]\!] \setminus \{missing\ edges\}$
  - Good for dense sets of edges
- Recognize Patterns
  - E.g. even numbered states have edges to (all) odd numbered states
  - $\neg x_0 \wedge x_0'$

Example

- Symbolic encoding for given transition-relation?



$$(\neg x_1 \land \neg x_0 \land \neg x'_1 \land x_0') \lor$$
$$(\neg x_1 \land x_0 \land x_1' \land \neg x_0') \lor$$
$$(x_1 \land \neg x_0 \land x'_1 \land x_0') \lor$$
$$(x_1 \land x_0 \land \neg x'_1 \land \neg x_0')$$

Summary

- Symbolic Sets
  - Encodings, Operations
- Kripke Structures
  - Graphs that represent digital systems, Symbolic Encoding