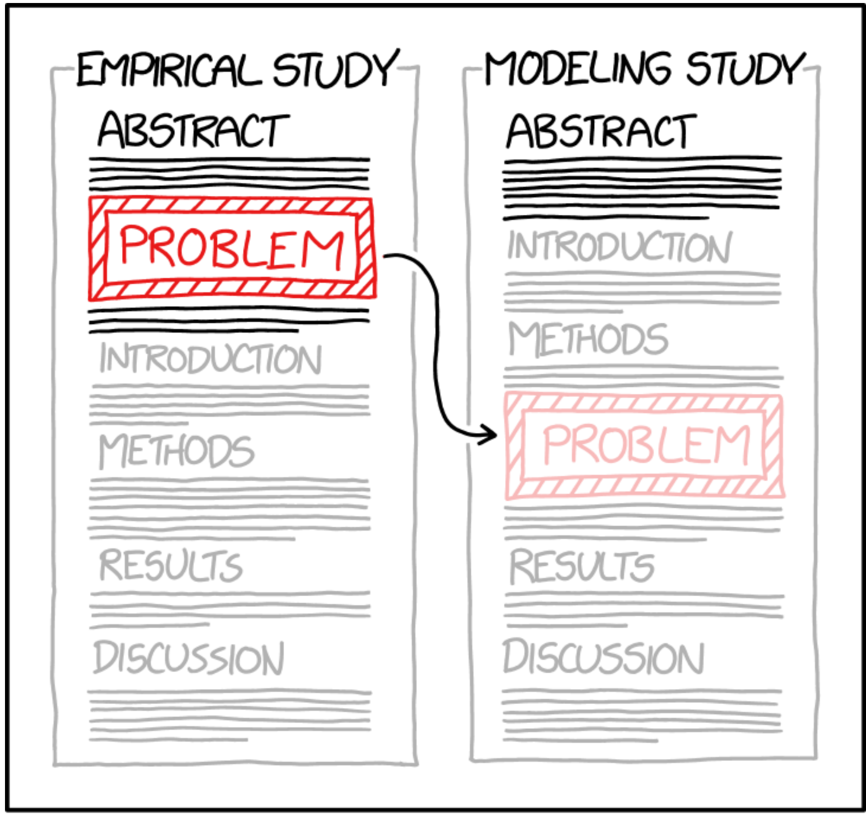
Logic and Computability

Modeling Systems & Symbolic Encoding

Bettina Könighofer
bettina.koenighofer@lamarr.at

Stefan Pranger
stefan.pranger@iaik.tugraz.at

https://xkcd.com/2323/



A MATHEMATICAL MODEL IS A POWERFUL TOOL FOR TAKING HARD PROBLEMS AND MOVING THEM TO THE METHODS SECTION.

Motivation – Modelling Systems

- We want to reason about systems.
  - Does the system satisfy certain properties?
- Model system as transition system
  - Check properties on transition system
- State space is often huge
  - Symbolic Encoding:
    - Represent transition system as formulas
    - Often possible to represent huge sets with relatively small formulas!

Outline

- Transition Systems
- Symbolic Encoding
  - Symbolic representation of sets of states
  - Symbolic representation of the transition relation
  - Symbolic encodings of arbitrary sets
  - Set operations on symbolically encoded sets

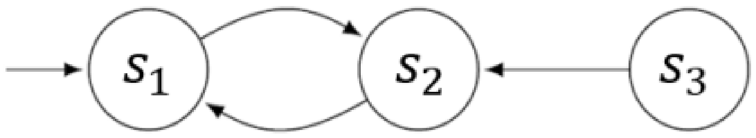
Transition Systems

- Model of a digital system

- T is a triple (S, S_0, R)
  - Finite Set of States S
  - Set of Initial States $S_0 \subseteq S$
  - Transition Relation $R \subseteq S \times S$

- Often visualized as directed Graph

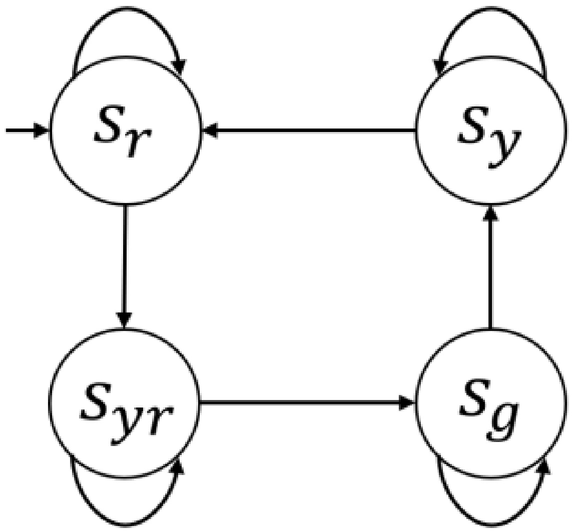
$S = \{s_1, s_2, s_3\}, \quad S_0 = \{s_1\}, \quad R = \{(s_1, s_2), (s_2, s_1), (s_3, s_2)\}$



Transition Systems - Example

- Model a traffic light controller
  - Initially the red light is on. After some time, the red and the yellow light are on. After some time, the controller switches to green, from green to yellow, and from yellow back to red, and so on.

- Draw the transition systems
  - States used:
    - s_r … the red light is on.
    - s_y … the yellow light is on.
    - s_g … the green light is on.
    - s_{ry} … the red and yellow lights are on



Outline

- Transition Systems ✓
- Symbolic Encoding
  - Symbolic representation of sets of states
  - Symbolic representation of the transition relation
  - Symbolic encodings of arbitrary sets
  - Set operations on symbolically encoded sets

Symbolic Encoding

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

Symbolic encoding/representation of sets =
Encode/represent set as formulas

Symbolic Representation of Sets of States

- Symbolic Representation of States via Binary Encoding
  - Given $|S| \leq \mathbf{2^n}$ states, we need $\boldsymbol{n}$ Boolean variables $\{v_0, \ldots, v_{n-1}\}$ to symbolically represent the state space.

- Example: Encode the $S = \{s_0, s_1\}$
  - Use 1 Boolean variable v_0
    - The formula $\neg v_0$ symbolically represents the state s_0
    - The formula v_0 symbolically represents the state s_1

Symbolic Representation of Sets of States

- Symbolic Representation of States via Binary Encoding
  - Given $|S| \leq \mathbf{2^n}$ states, we need $\boldsymbol{n}$ Boolean variables $\{v_0, \ldots, v_{n-1}\}$ to symbolically represent the state space.

- Example: Encode the $S = \{s_0, s_1, s_2, s_3\}$
  - Use 2 Boolean variable v_0 and v_1
    - The formula $\neg v_1 \wedge \neg v_0$ symbolically represents the state s_0
    - The formula $v_1 \wedge \neg v_0$ symbolically represents the state s_1
    - The formula $\neg v_1 \wedge v_0$ symbolically represents the state s_2
    - The formula $v_1 \wedge v_0$ symbolically represents the state s_3

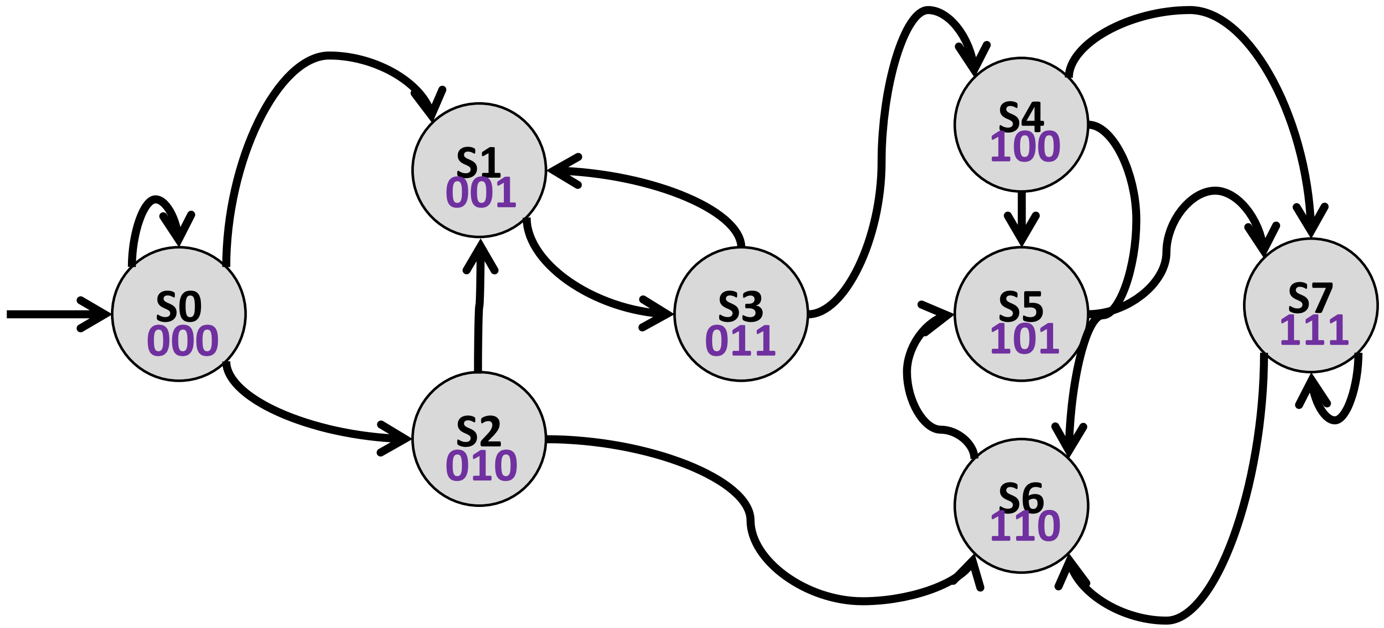
Symbolic Representation of Sets of States

- Symbolic Representation of States via Binary Encoding
  - Given $|S| \leq \mathbf{2^n}$ states, we need $\boldsymbol{n}$ Boolean variables $\{v_0, \ldots, v_{n-1}\}$ to symbolically represent the state space.

- Example: Encode the $S = \{s_0, s_1, s_2, s_3, s_4, \ldots, s_7\}$
  - Use 3 Boolean variable v_0 , v_1 and v_2
    - The formula $\neg v_2 \wedge \neg v_1 \wedge \neg v_0$ symbolically s_0
    - .....
    - The formula $v_2 \wedge v_1 \wedge v_0$ symbolically s_7

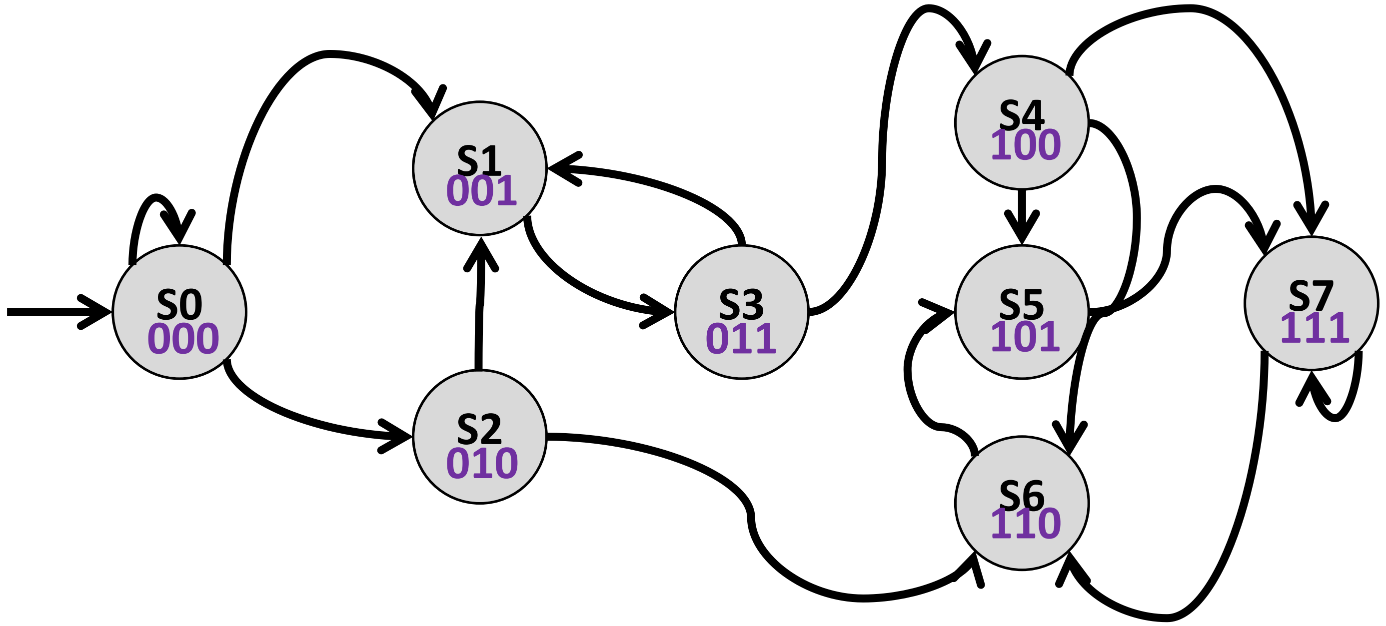
Symbolic Encoding of the State Space

- Use variables $V = \{v_1, \ldots, v_n\}$ for binary representations of 2^nstates



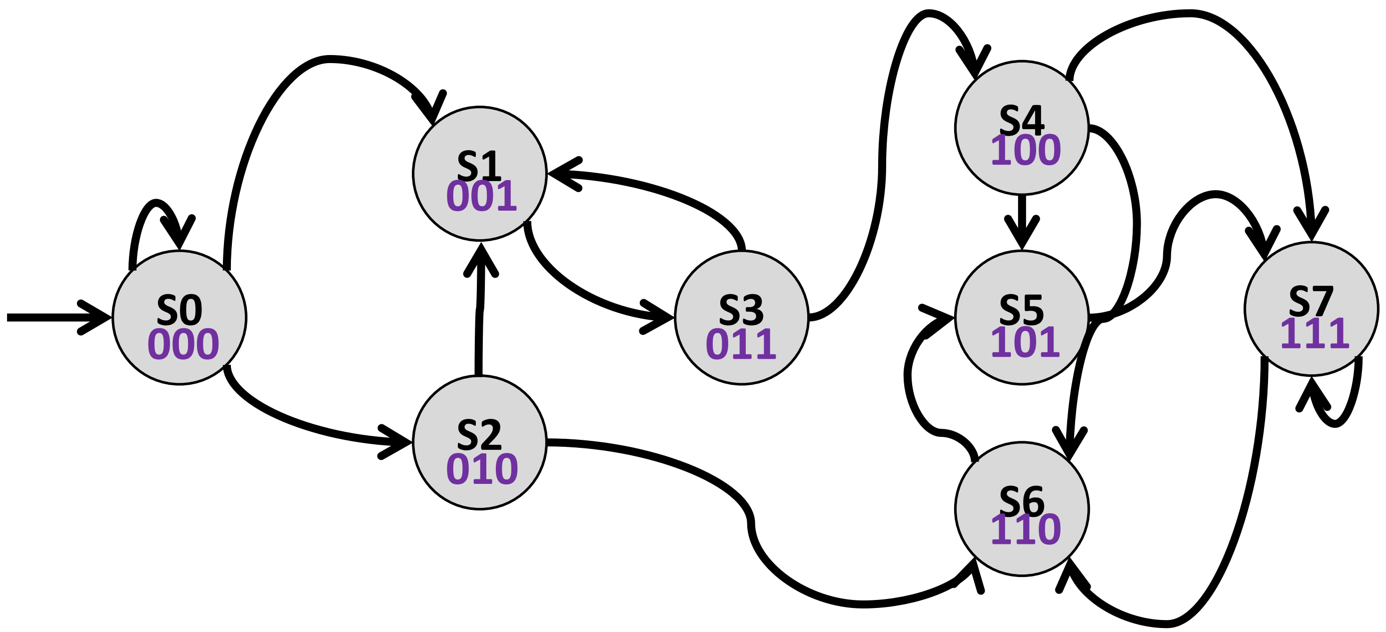
Symbolic Encoding of a Single State

- Single State
  - Apply binary encoding
    - E.g. State s_2 is encoded as $\neg v_2 \land v_1 \land \neg v_0$



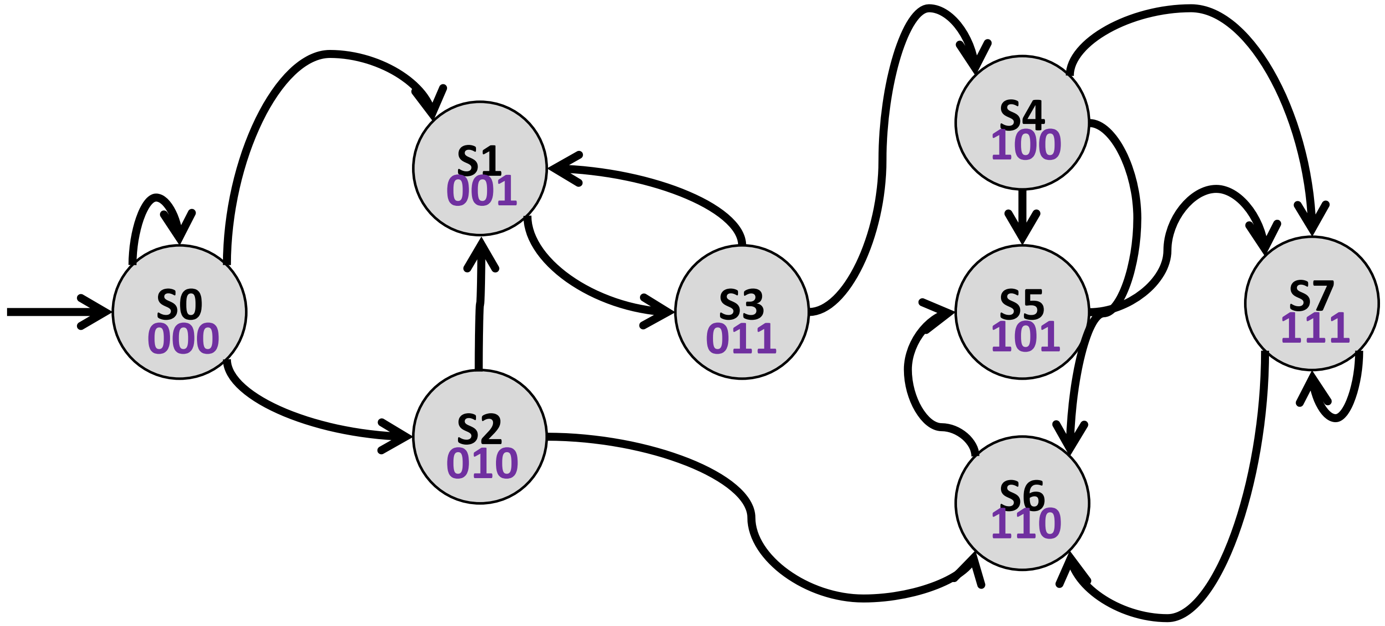
Symbolic Encoding of Sets of States

- Single State
  - Example: Symbolically encode the set of states $\{s_5, s_1\}$
    - Solution: $(v_1 \wedge \neg v_2 \wedge v_3) \vee (\neg v_1 \wedge \neg v_2 \wedge v_3) = (\neg v_2 \wedge v_3)$



Symbolic Encoding of Sets of States

- Single State
  - Example: Symbolically encode all even numbered states
    - Solution: $\neg v_0$
  - Remember goal of symbolic encoding:
    Encode large sets with relatively small formulas.



Outline

- Transition Systems ✓
- Symbolic Encoding
  - Symbolic representation of sets of states ✓
  - Symbolic representation of the transition relation
  - Symbolic encodings of arbitrary sets
  - Set operations on symbolically encoded sets

Symbolic Representation of a Single Transition

- Create a second set of variables V' (Duplicate variables)
  - variables in $v_0, v_1, v_2, \ldots \in V$ represent **present state** variables
  - variables in $v_0', v_1', v_2', \ldots \in V'$ represent **next state** variables

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

Symbolic Representation of Sets of Transition

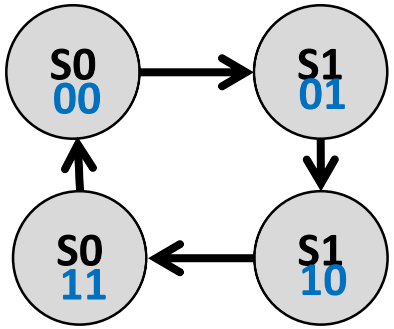
- Union of all Edges
  - Disjunction
  - Good for sparse sets of edges

- $[\![\top]\!] \setminus \{missing\ edges\}$
  - Good for dense sets of edges

- Recognize Patterns
  - E.g. even numbered states have edges to (all) odd numbered states
  - $\neg x_0 \land x_0'$

Symbolic Representation of Sets of Transition

- Example:
  - Symbolically encode the transition relation



$$(\neg v_1 \wedge \neg v_0 \wedge \neg v'_1 \wedge v'_0) \vee$$
$$(\neg v_1 \wedge v_0 \wedge v'_1 \wedge \neg v'_0) \vee$$
$$(v_1 \wedge \neg v_0 \wedge v'_1 \wedge v'_0) \vee$$
$$(v_1 \wedge v_0 \wedge \neg v'_1 \wedge \neg v'_0)$$

Symbolic Representation of Sets of Transition

- 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
  - $\neg x_0 \land x_0'$

Outline

- Transition Systems ✓
- Symbolic Encoding
  - Symbolic representation of sets of states ✓
  - Symbolic representation of the transition relation ✓
  - Symbolic encodings of arbitrary sets
  - Set operations on symbolically encoded sets

Symbolic Encoding of arbitrary Sets

- 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

Symbolic Encoding of arbitrary Sets

- $F = \{Austria\}$
- $f = \neg x_0 \land \neg x_1$

- $G = \{Austria, Spain\}$
- $g = \neg x_0$

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

Symbolic Encoding of arbitrary Sets

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

Element	Encoding x_1	Encoding 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}?

$f = x_1$ $g = x_1 \oplus x_0$

Encoding Natural Numbers

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

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

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

Outline

- Transition Systems ✓
- Symbolic Encoding
  - Symbolic representation of sets of states ✓
  - Symbolic representation of the transition relation ✓
  - Symbolic encodings of arbitrary sets ✓
  - Set operations on symbolically encoded sets

Symbolic Operations

- **Intersection:** $F \cap G \Leftrightarrow f \wedge g$
- **Union:** $F \cup G \Leftrightarrow f \vee g$
- **Difference:** $F \setminus G \Leftrightarrow f \wedge \neg g$
- **Equality:** $F = G \Leftrightarrow f \equiv g$
- **Subset:** $F \subseteq G \Leftrightarrow f \rightarrow g$

Example

- Domain: $A = \{x \in \mathbb{N} | 0 \leq x \leq 1023\}$

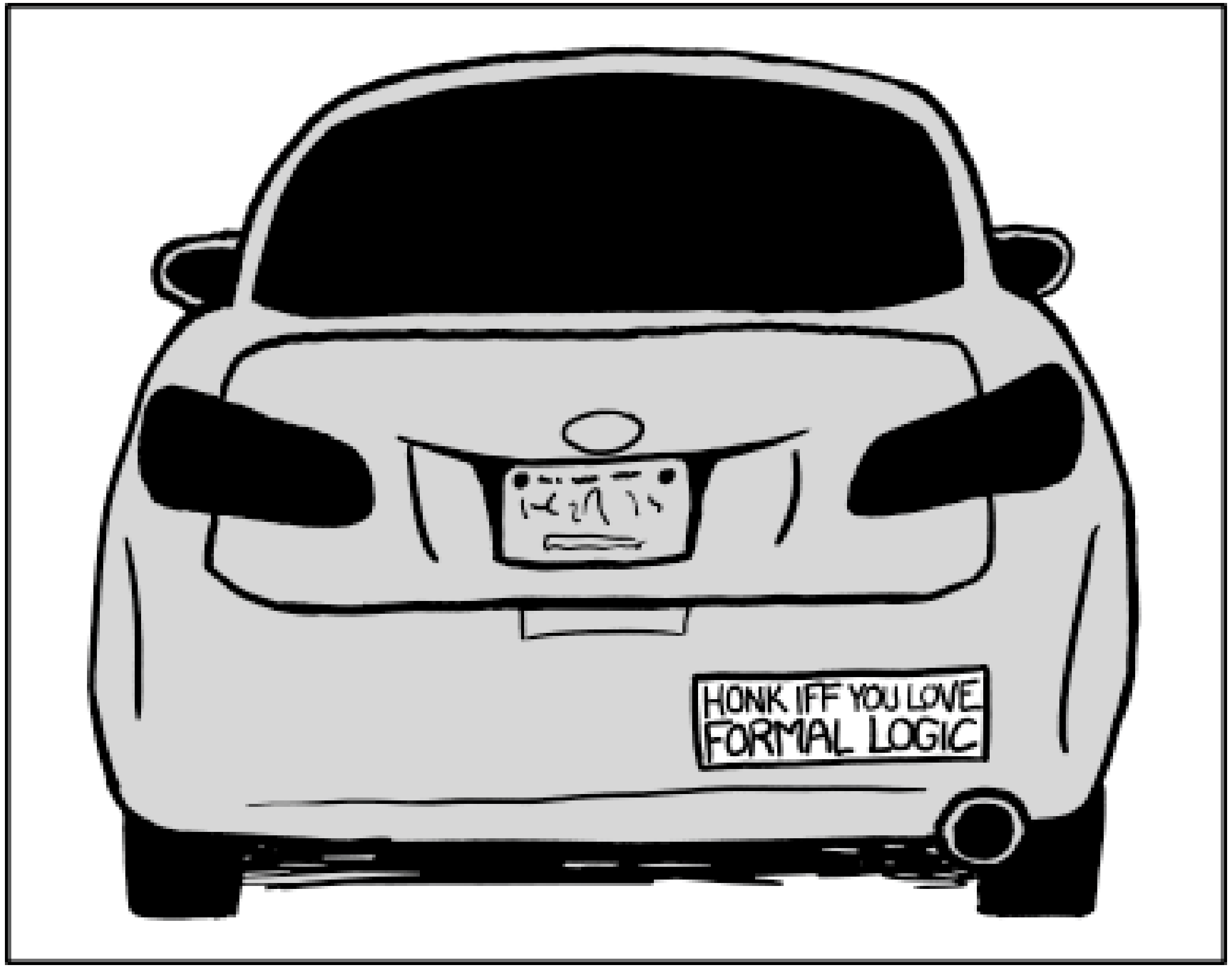
  10 bit binary repräsentation $x_9 x_8 \ldots . x_0$

- $B = \{x \in A | x < 512\}, b = \neg x_9$
- $C = \{x \in A | 256 \leq x < 768\}, c = (\neg x_9 \wedge x_8) \vee (x_9 \wedge \neg x_8)$?

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

- $D = B \cup C \quad d = \neg x_9 \vee \big((\neg x_9 \wedge x_8) \vee (x_9 \wedge \neg x_8)\big) = \neg x_9 \vee (x_9 \wedge \neg x_8)$
- $E = B \cap C \quad e = \neg x_9 \wedge \big((\neg x_9 \wedge x_8) \vee (x_9 \wedge \neg x_8)\big) = \neg x_9 \wedge x_8$
- $F = A \mid E \quad f = T \wedge \neg(\neg x_9 \wedge x_8) = x_9 \vee \neg x_8$

Thank You



https://xkcd.com/1033/