Verification of Combinational and Sequential Circuits in LEAN3

Zahir Bingen| Informatica

Universiteit Leiden
The Netherlands

Index

Introduction

- Motivation
- Simulation vs Formal Verification
- LEAN3
- Specifications and Implementations
- Combinational and Sequential Circuits
  - Logic Gates (Combinational)
  - Multiplexer (Combinational)
  - …
  - Flip Flops (Sequential)
  - …

Methodology

1. Specification creation
2. Specification functionality proof
   - Choose the orientation of input/output
   - Check for existence of output
   - Check whether the output is precisely defined (unique)
3. Implementation of specification
4. Compliance proof
   - Check whether the implementation complies with the specification

Logic Gates

a_1	a_2	o
0	0	0
0	1	0
1	0	0
1	1	1

Table 4: Truth table of a 2-input AND-gate

a_1	a_2	o
0	0	0
0	1	1
1	0	1
1	1	1

Table 3: Truth table of a 2-input OR-gate

a	o
0	1
1	0

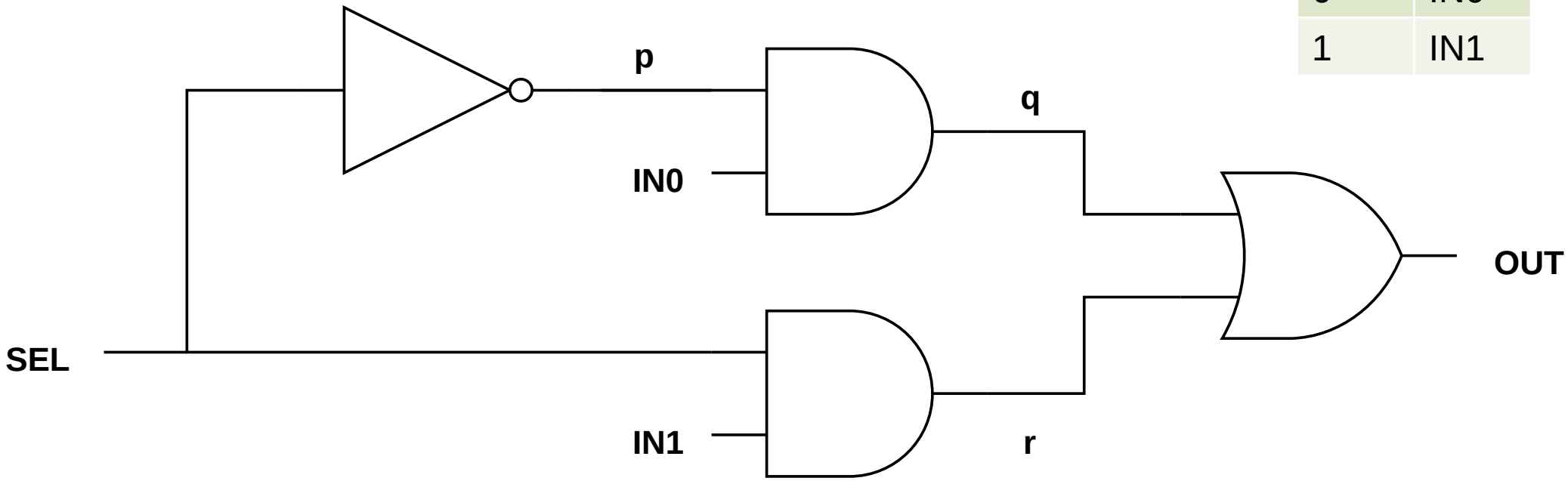
Table 2: Truth table of a NOT-gate

a_1	a_2	a_3	o
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

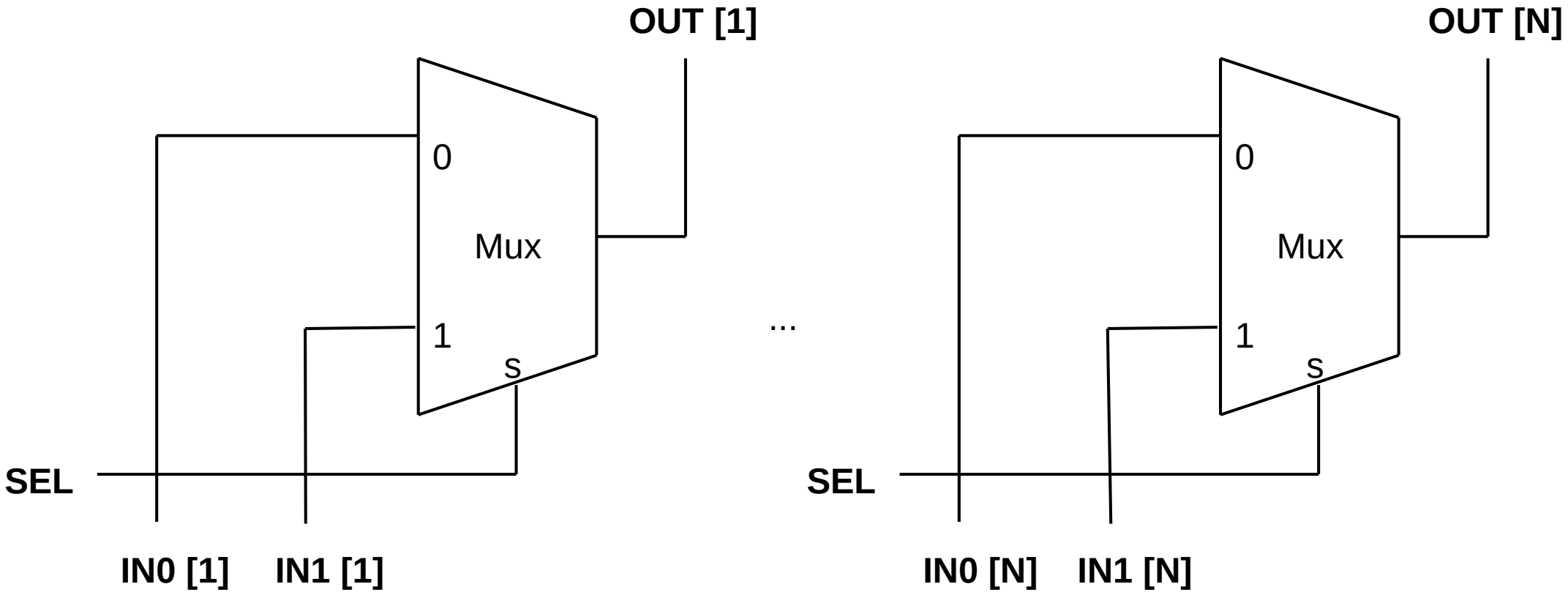
Table 4: Truth table of a 3-input XOR-gate

2_1 Multiplexer 1-bit

SEL	OUT
0	IN0
1	IN1



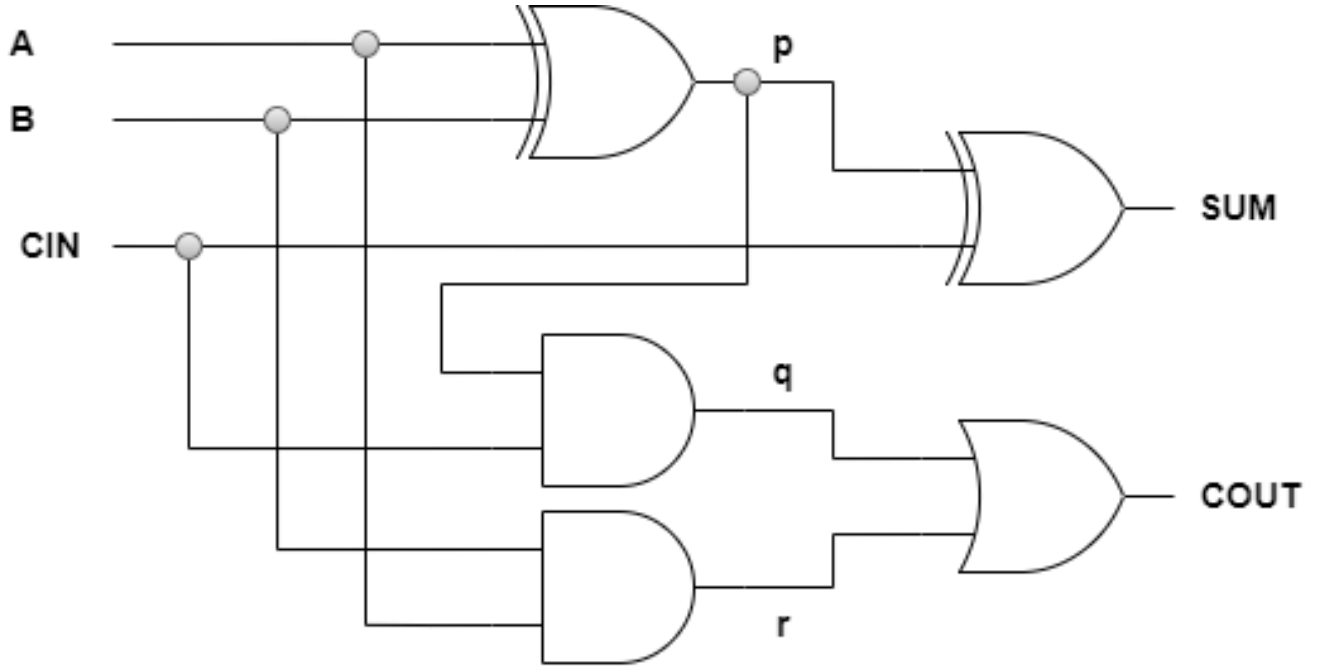
2_1 Multiplexer n-bit



Full-Adder 1-bit

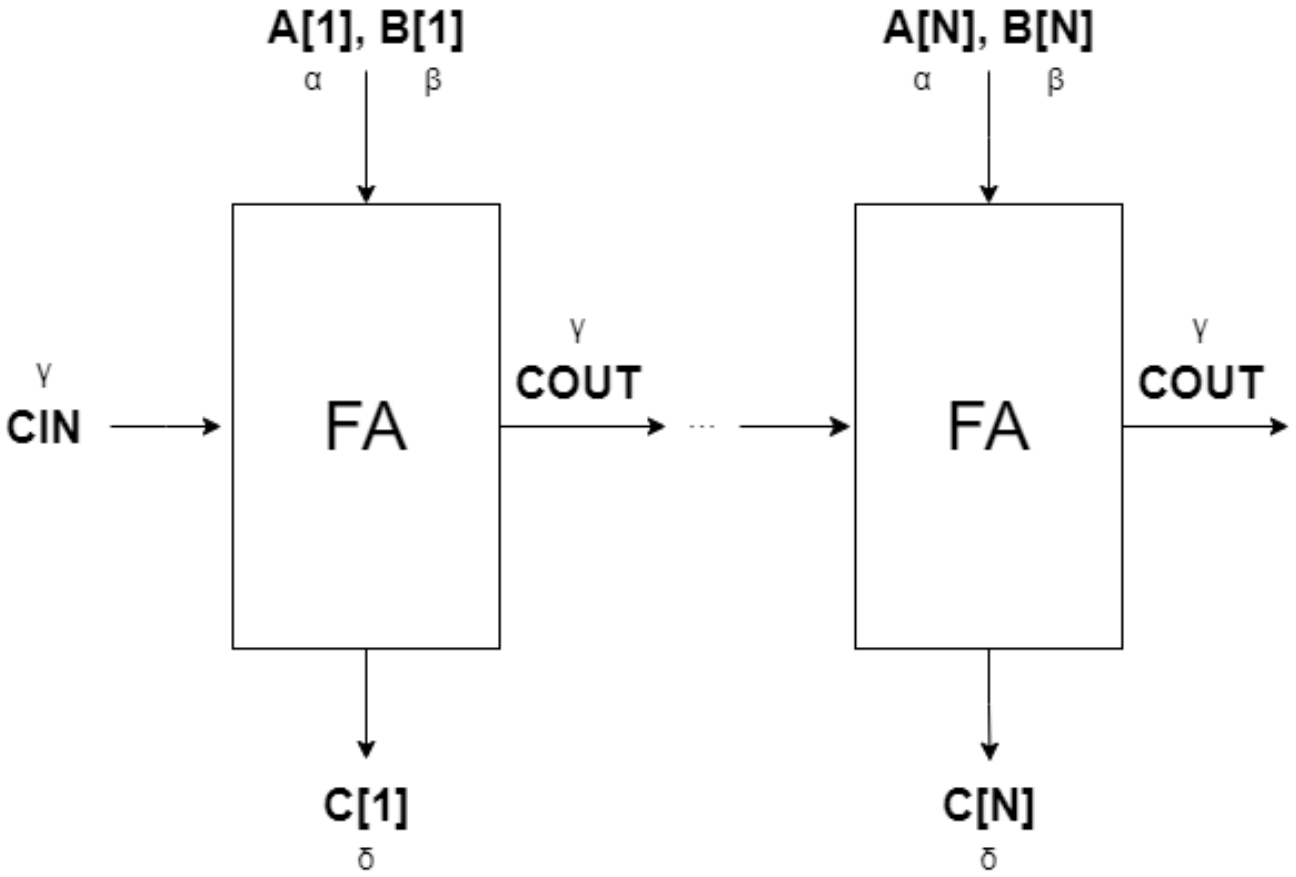
A	B	CIN	SUM	COUT
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

SUM = (A + B + CIN) % 2
COUT = ((A + B + CIN) >= 2)



Full-Adder n-bit

SUM = (A + B + CIN) % 2^n
COUT = ((A + B + CIN) >= 2^n)

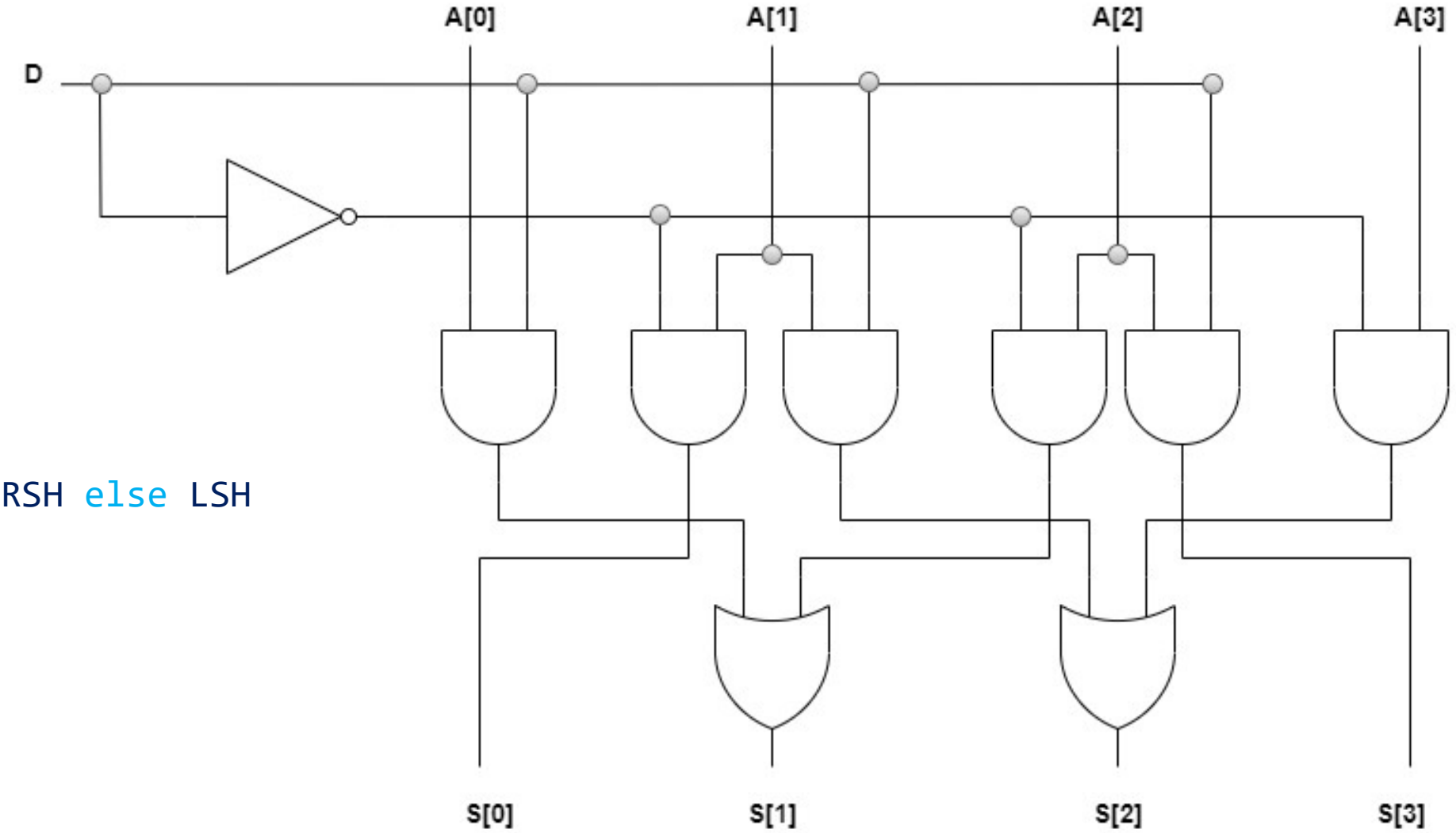


Shifter

- Right shift: shift all bits to the right, left-most bit is 0
- Left shift: shift all bits to the left, right-most bit is 0

```
def lsh_spec {n : ℕ} (A OUT : array n bool) : Prop :=
       OUT = ⟨λ i, if h : i.val + 1 < n then A.read ⟨i.val + 1, h⟩ else ff⟩
def rsh_spec {n : ℕ} (A OUT : array n bool) : Prop :=
       OUT = ⟨λ i, if h : i.val > 0 ∧ i.val - 1 < n then A.read ⟨i.val - 1, h.right⟩
              else ff⟩
```

Shifter




```
IF D then RSH else LSH
```

Memory

- Signals (functions of $\mathbb{N} \to \alpha$)
- Underspecified (initial value?)
- Uniqueness of output?

T	D	S	M	O
T	*	0	0	0
T+1			0	
…				
…	d	1	*	*
…			d	d
…				

```
def stream (α : Type) := ℕ → α

def signal := ℕ → bool

def sig_n (n : ℕ) := ℕ → array n bool
```

```
∀ t : ℕ,
(S t = tt → M (t+1) = D t) ∧
(S t = ff → M (t+1) = M t)
```

Program Counter

- Memory component attached with an adder
- Hard to implement in LEAN3
- Create a single component like the memory implementation
- If reset signal is true at time t, then at t+1 counter is reset
- If reset signal is false at time t, then at t+1 counter is incremented by 1

Case Study: Sequence Recognizer

- Verification of Binary Sequence Detector design by Alberto I. Leibovich and Pablo E. Leibovich
- Recognizes the sequence binary sequence “101”
- Changes to state diagram

Actual State	Next State		Output
	X = 0	X = 1	
S_0	S_0	S_1	0
S_1	S_2	S_1	0
S_2	S_0	S_3	0
S_3	S_0	S_3	1

Table 1. Transition Table

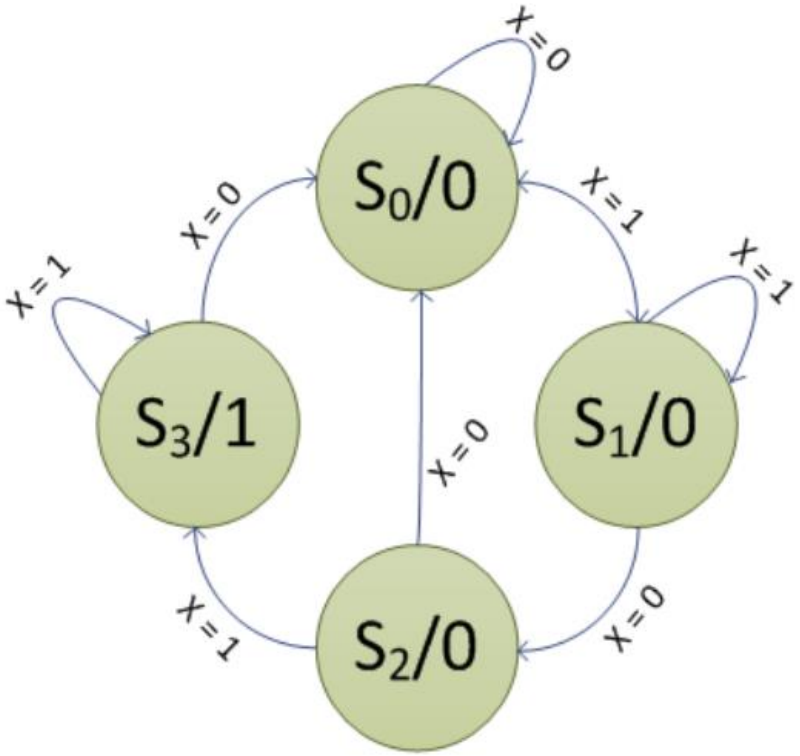
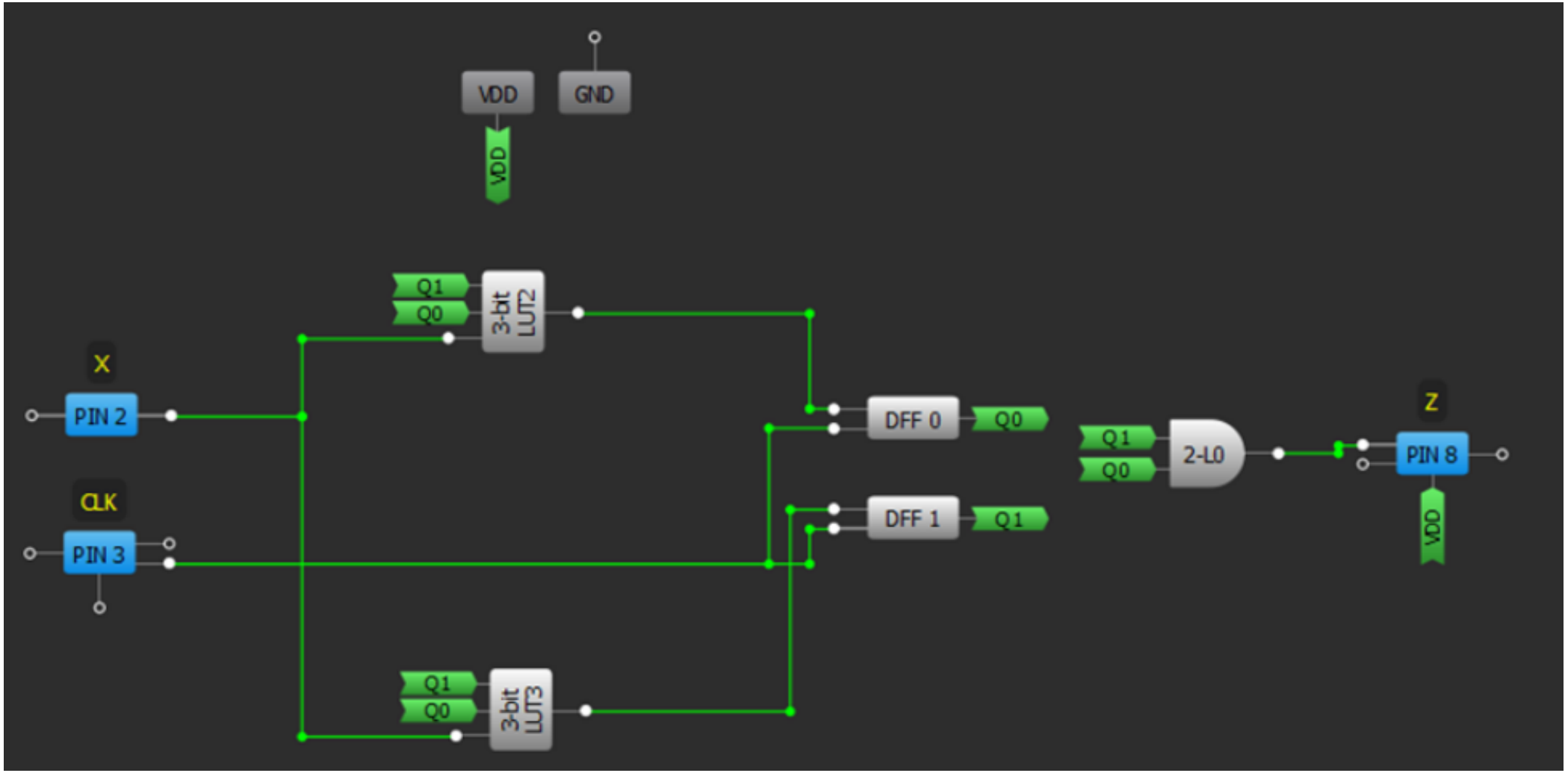


Figure 1. State Diagram

Case Study: Sequence Recognizer



Case Study: Sequence Recognizer

Q1	Q0	X	D0
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Table 2. D0 Truth Table

Q1	Q0	X	D1
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Table 3. D1 Truth Table

Q1	Q0	Z
0	0	0
0	1	0
1	0	0
1	1	1

Table 4. Z Truth Table

Conclusion

- Simulation of simple circuits might be preferred over formal verification
- Formal verification
  - Highly time consuming
  - Error prone
  - Can provide guarantees for correctness
- LEAN3 is a useful proof assistance but not perfect
  - No easy forward recursion (termination must be guaranteed)
  - High memory usage
  - Handling arrays in proofs too complex
  - Limitations in automation
  - Great library of existing tactics

Challenges and Future Work

- Challenges
  - Learning how to use LEAN3 in a short time (steep learning curve)
  - Translating specifications into implementations

- Future Work:
  - Proof optimization (lower memory footprint)
  - Improving Automation
  - Specific library for Circuit Verification

Questions?

Universiteit
Leiden
The Netherlands