Cybersecurity for IoT – FPGA Introduction

Department of Electrical, Computer and Biomedical Engineering of University of Pavia

Master of Science Program in Computer Engineering

Instructor: Paris Kitsos

http://diceslab.cied.teiwest.gr

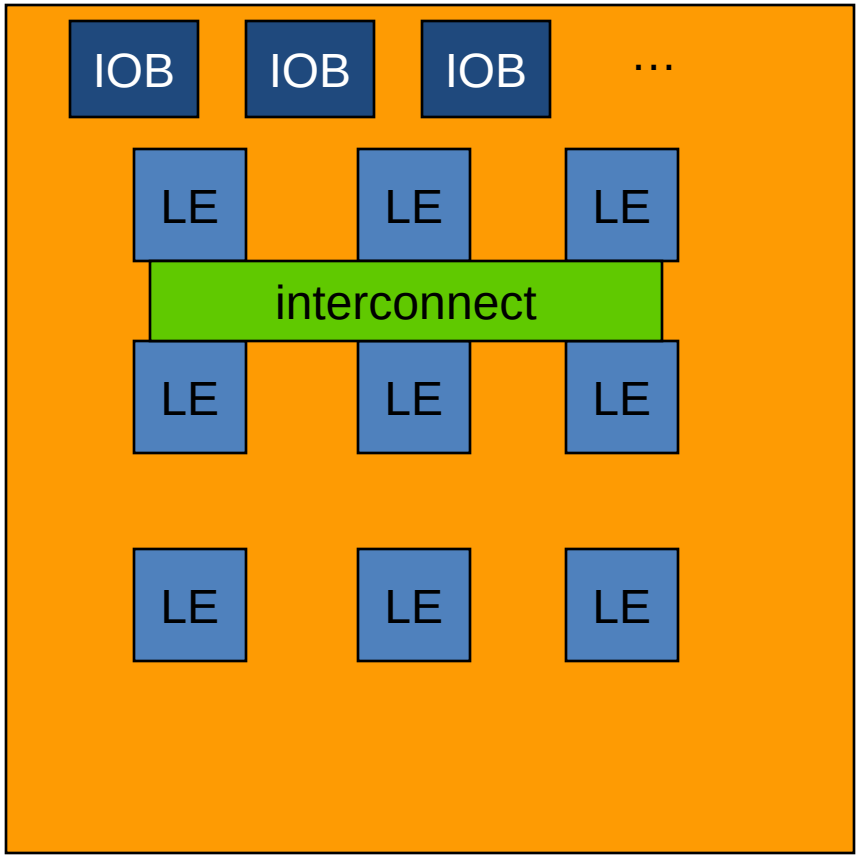
E-mail: pkitsos@teimes.gr

Pavia 2018

This lecture is based on “FPGA – based System Design”, book by Wayne Wolf

Elements of an FPGA fabric

- Logic.
- Interconnect.
- I/O pins.



Terminology

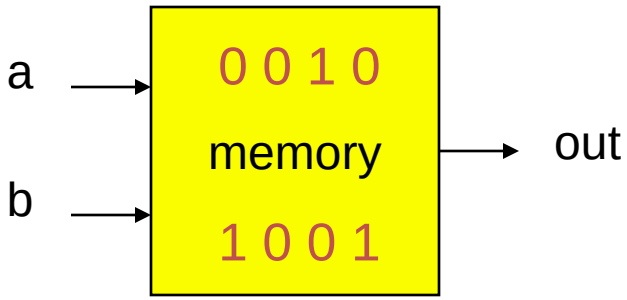
- Configuration: bits that determine logic function + interconnect.
- CLB: combinational logic block = logic element (LE).
- LUT: Lookup table = SRAM used for truth table.
- I/O block (IOB): I/O pin + associated logic and electronics.

Logic element

- Programmable:
  - Input connections.
  - Internal function.
- Generally includes register.
- May provide specialized logic.
  - Adder carry chain.

Example logic element

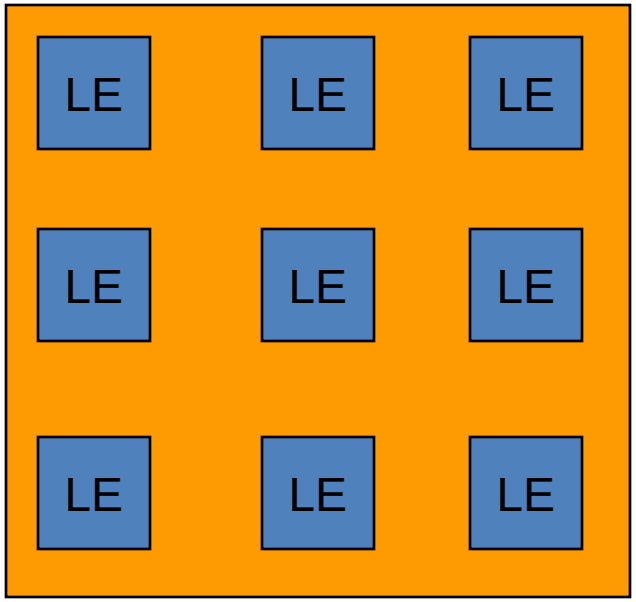
- Lookup table:



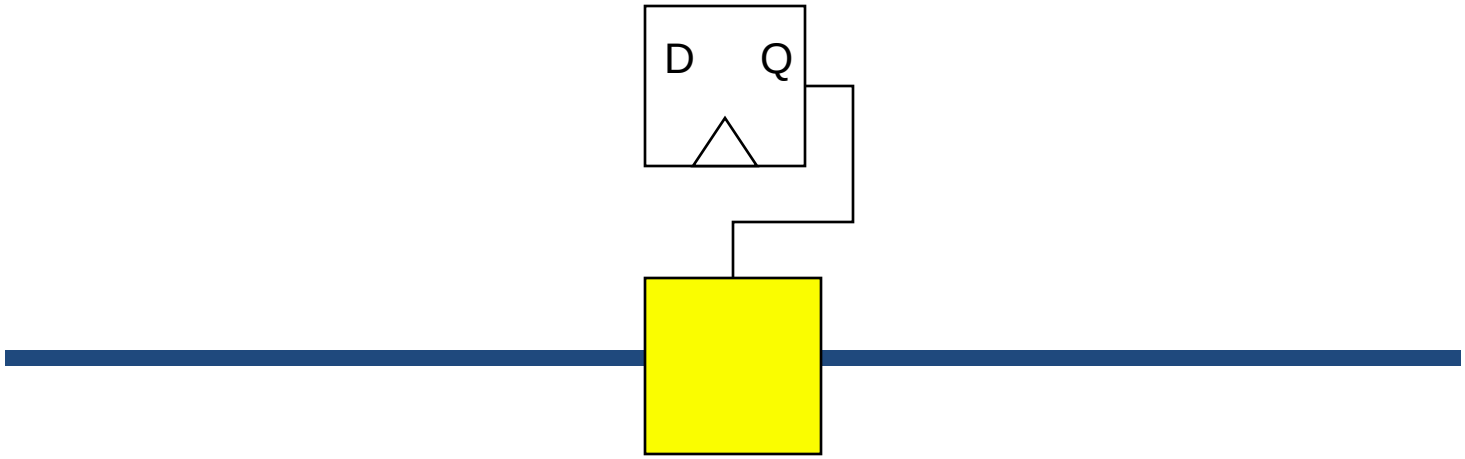
a	b	out
0	0	0
0	1	0
1	0	0
1	1	1

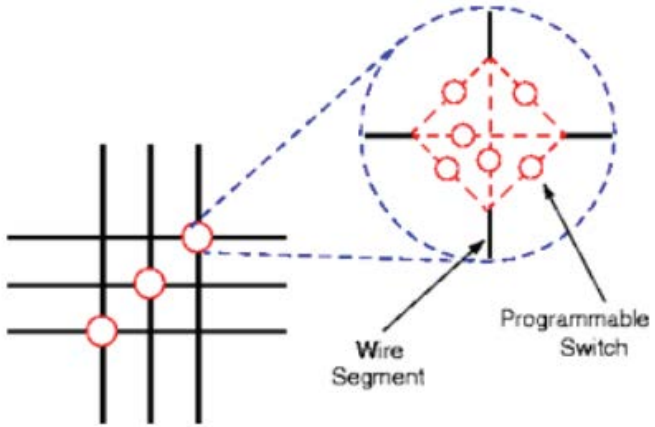
Placement

- Where do we put each piece of logic in the array of logic elements?

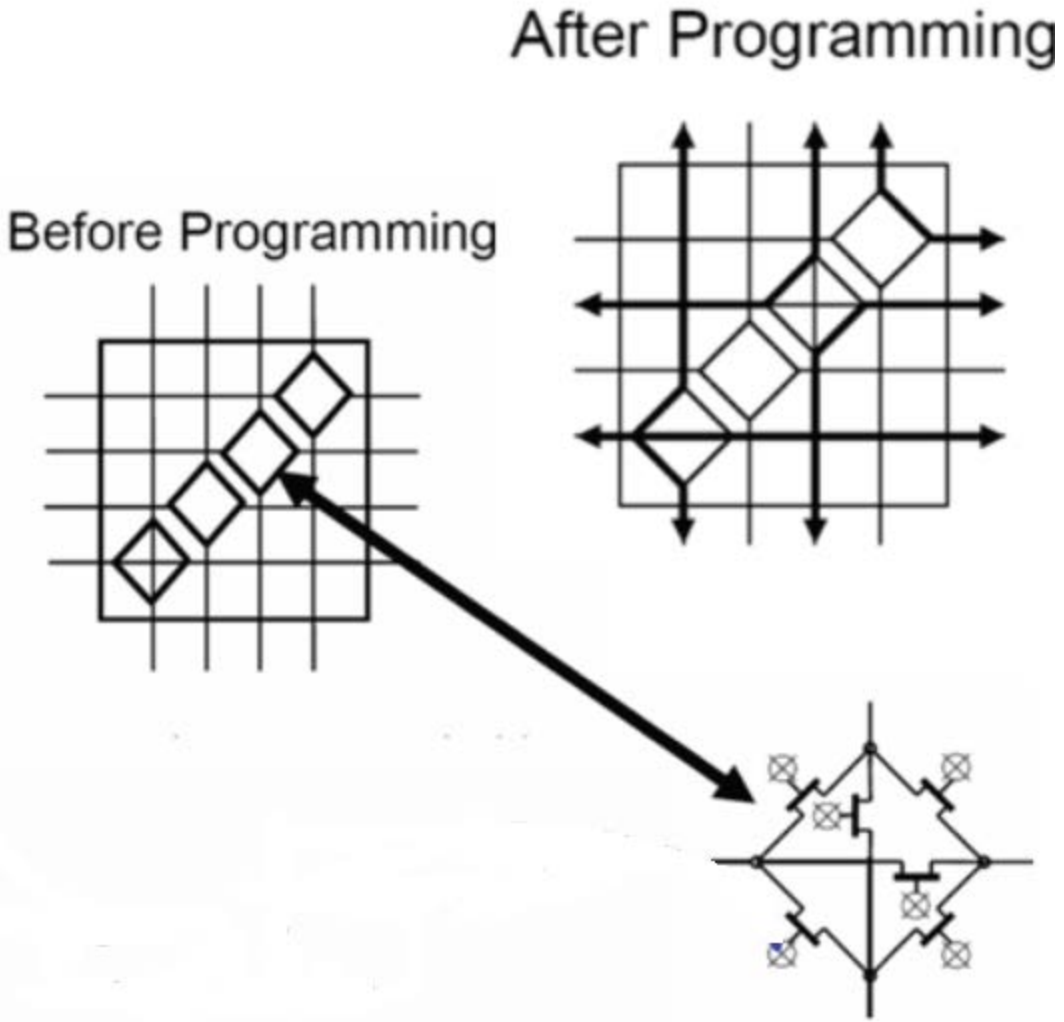


Programmable interconnection point…

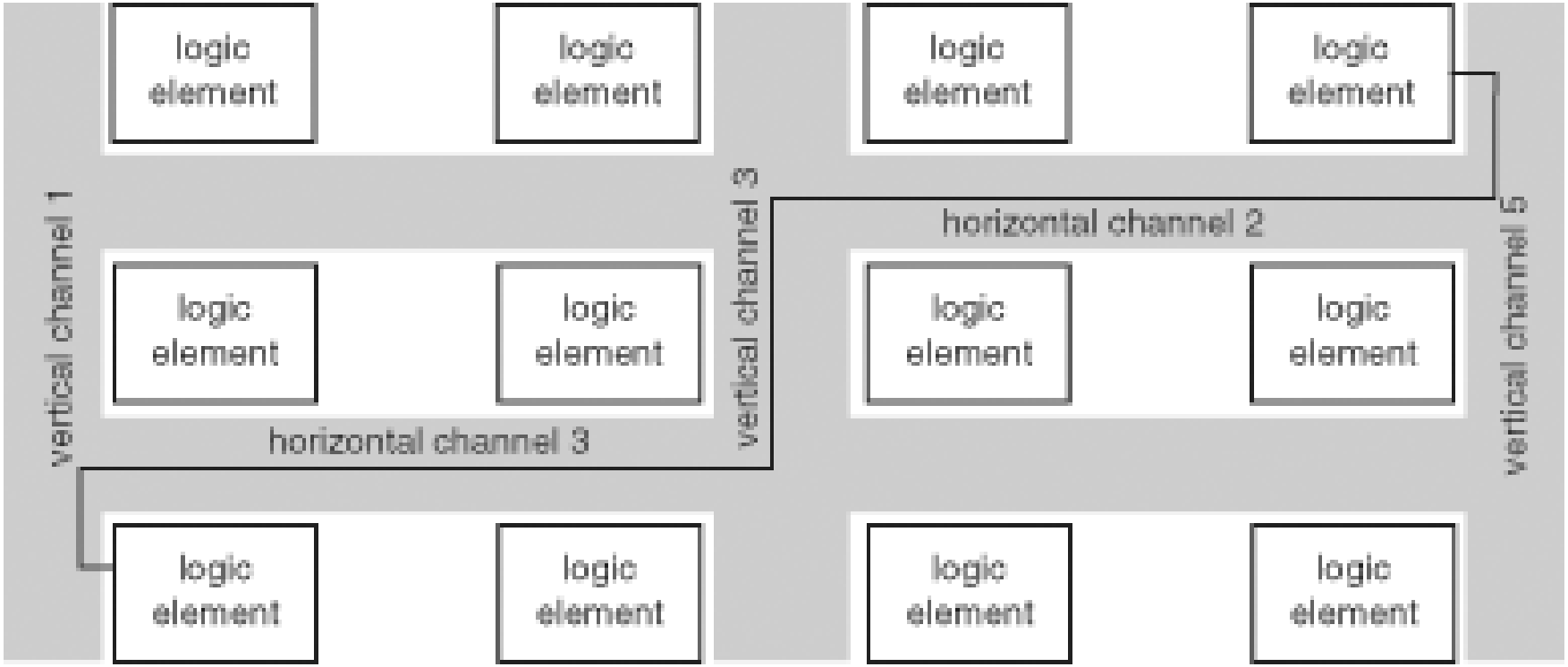




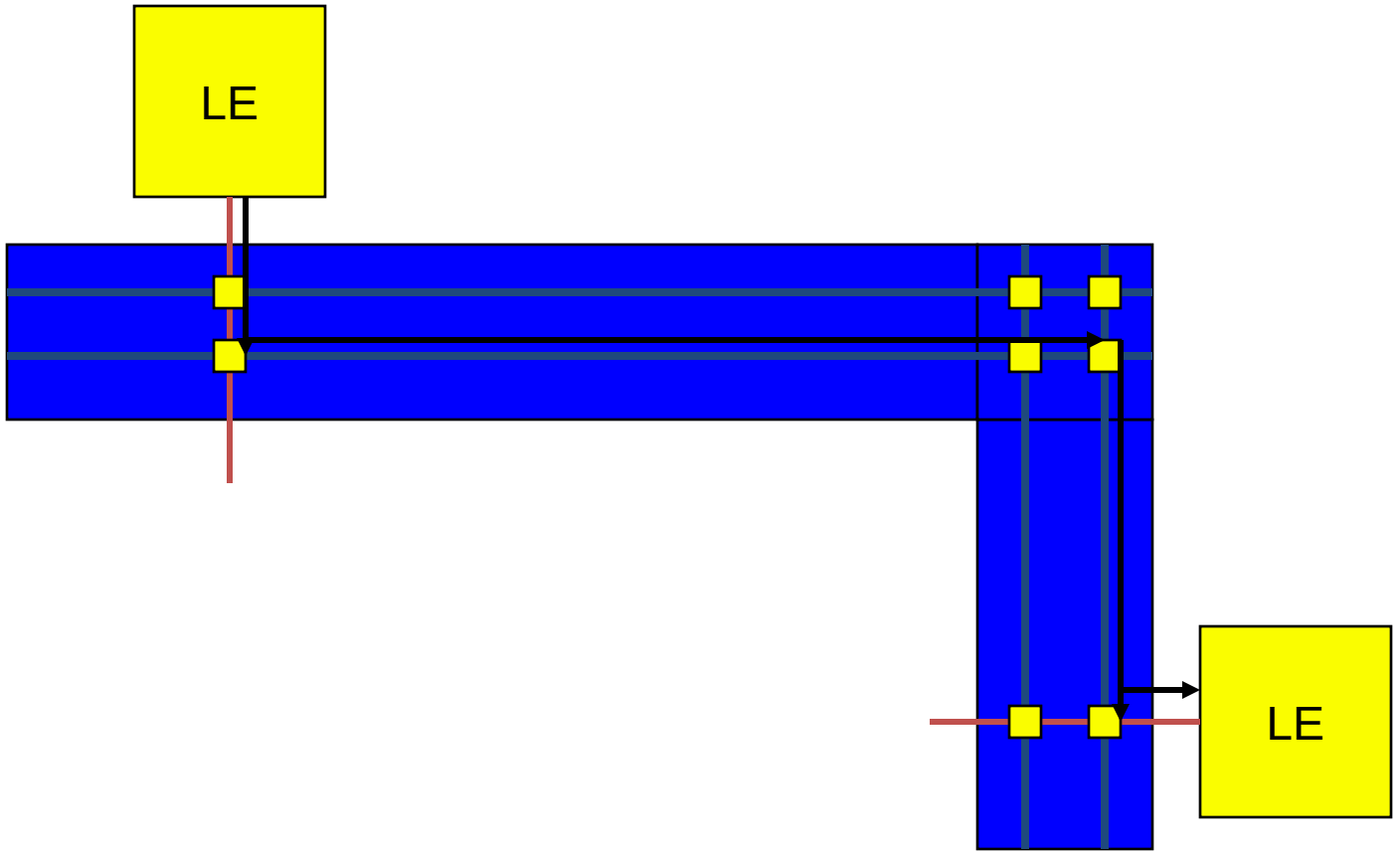
…Programmable interconnection point



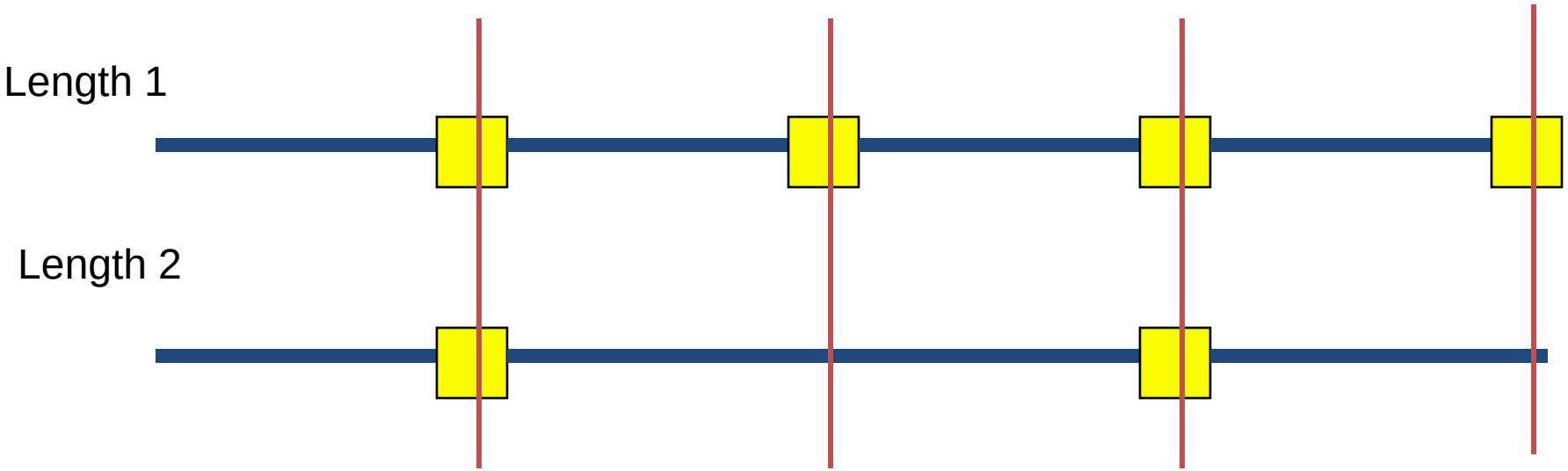
Programmable wiring paths



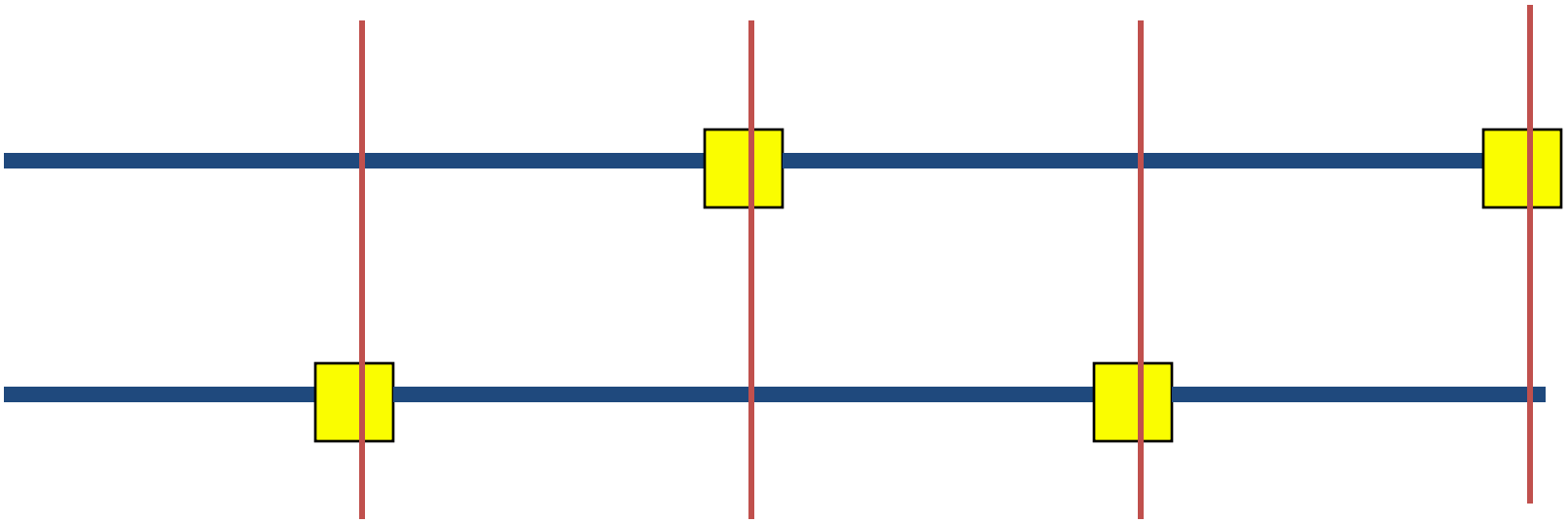
Choosing a path



Segmented wiring



Offset segments



I/O

- Fundamental selection: input, output, three-state?
- Additional features:
  - Register.
  - Voltage levels.
  - Slew rate.

Programming technologies

- SRAM.
  - Can be programmed many times.
  - Must be programmed at power-up.
- Antifuse.
  - Programmed once.
- Flash.
  - Similar to SRAM but using flash memory.

Configuration

- Must set control bits for:
  - LE.
  - Interconnect.
  - I/O blocks.
- Usually configured off-line.
  - Separate burn-in step (antifuse).
  - At power-up (SRAM).

SRAM-based FPGAs

- Program logic functions, interconnect using SRAM.
- Advantages:
  - Re-programmable;
  - dynamically reconfigurable;
  - uses standard processes.
- Disadvantages:
  - SRAM burns power.
  - Possible to steal, disrupt configuration bits.

Logic elements

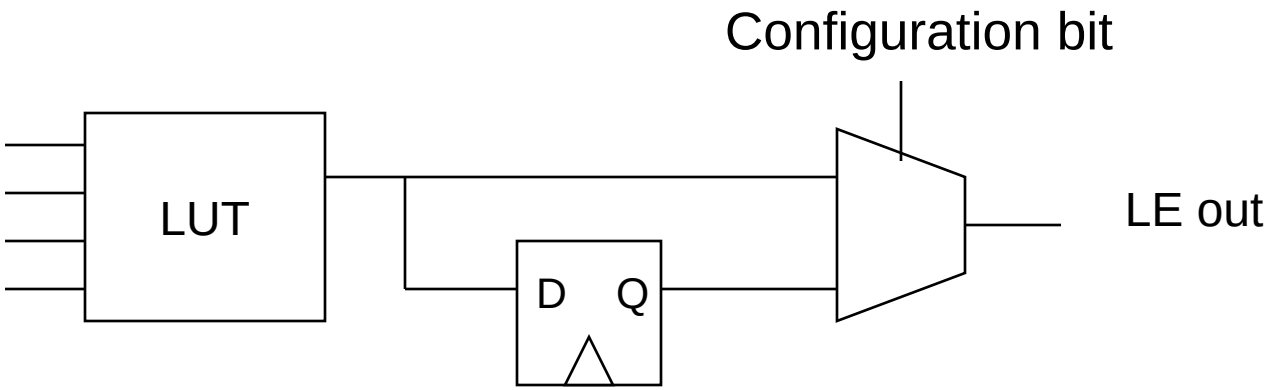
- Logic element includes combinational function + register(s).
- Use SRAM as lookup table for combinational function.

Evaluation of SRAM-based LUT

- N-input LUT can handle function of 2^n inputs.
- All logic functions take the same amount of space.
- All functions have the same delay.
- SRAM is larger than static gate equivalent of function.

Registers in logic elements

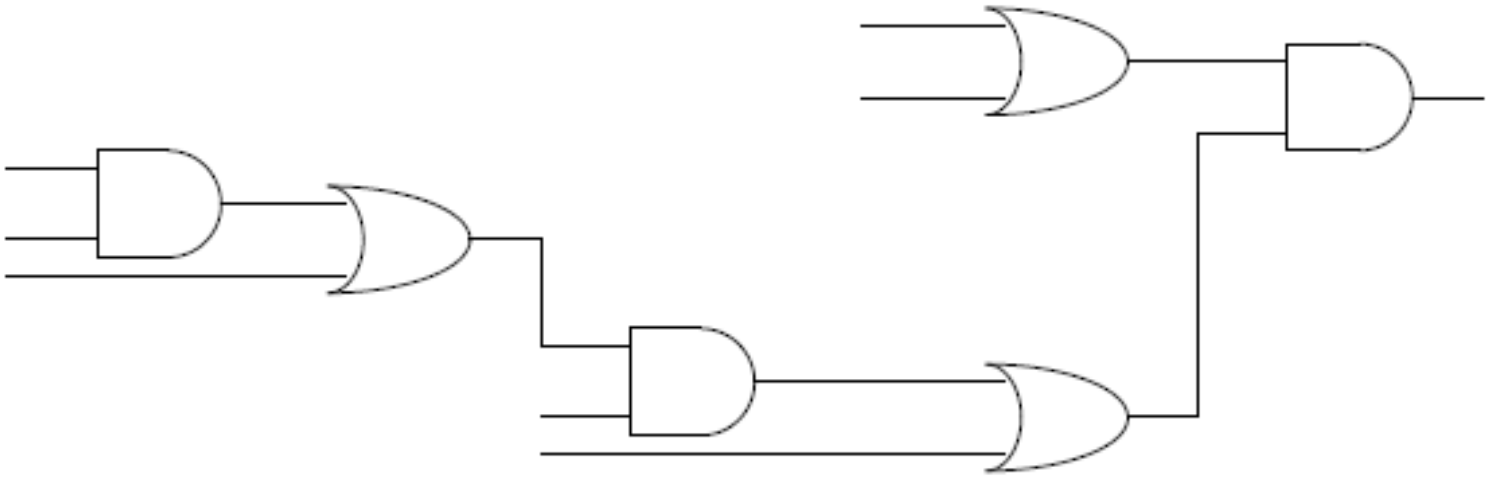
- Register may be selected into the circuit:



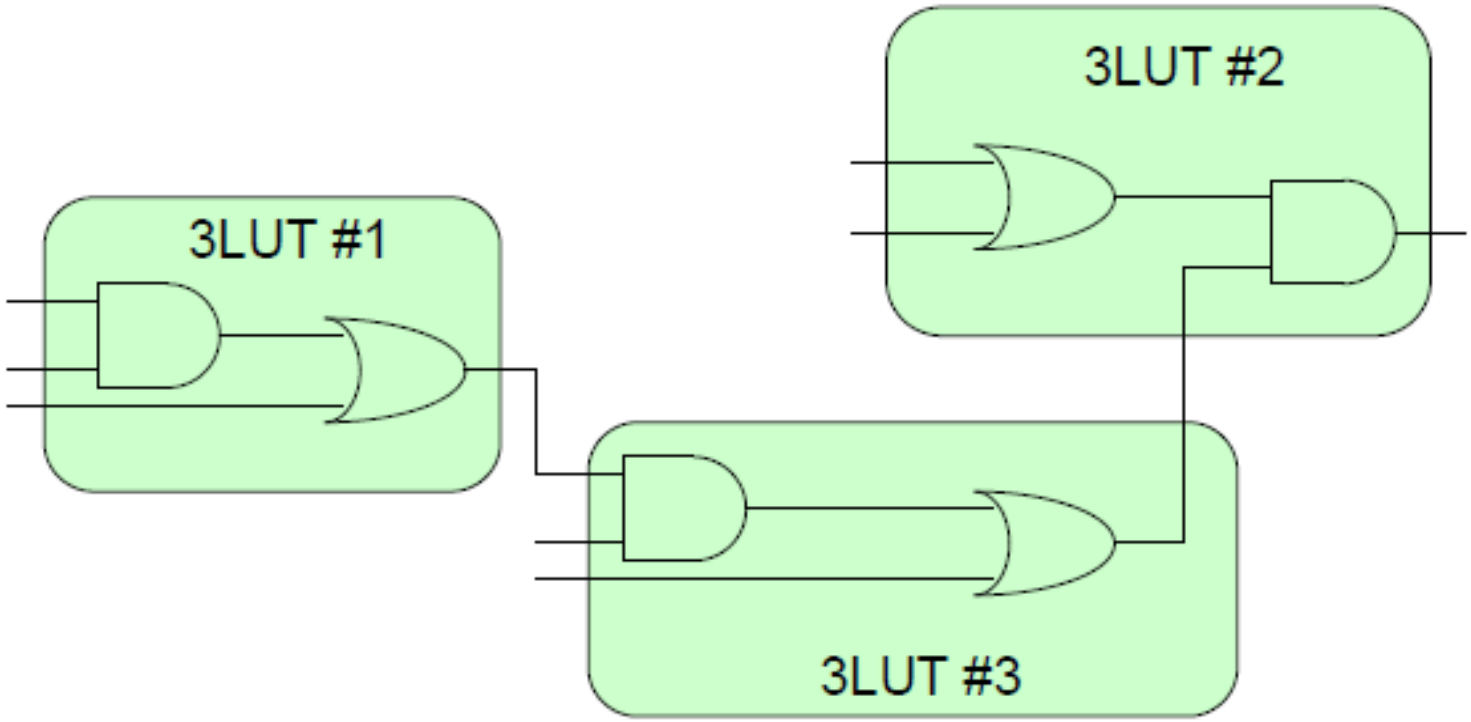
Other LE features

- Multiple logic functions in an LE.
- Addition logic:
  - carry chain.
- Partitioned lookup tables.

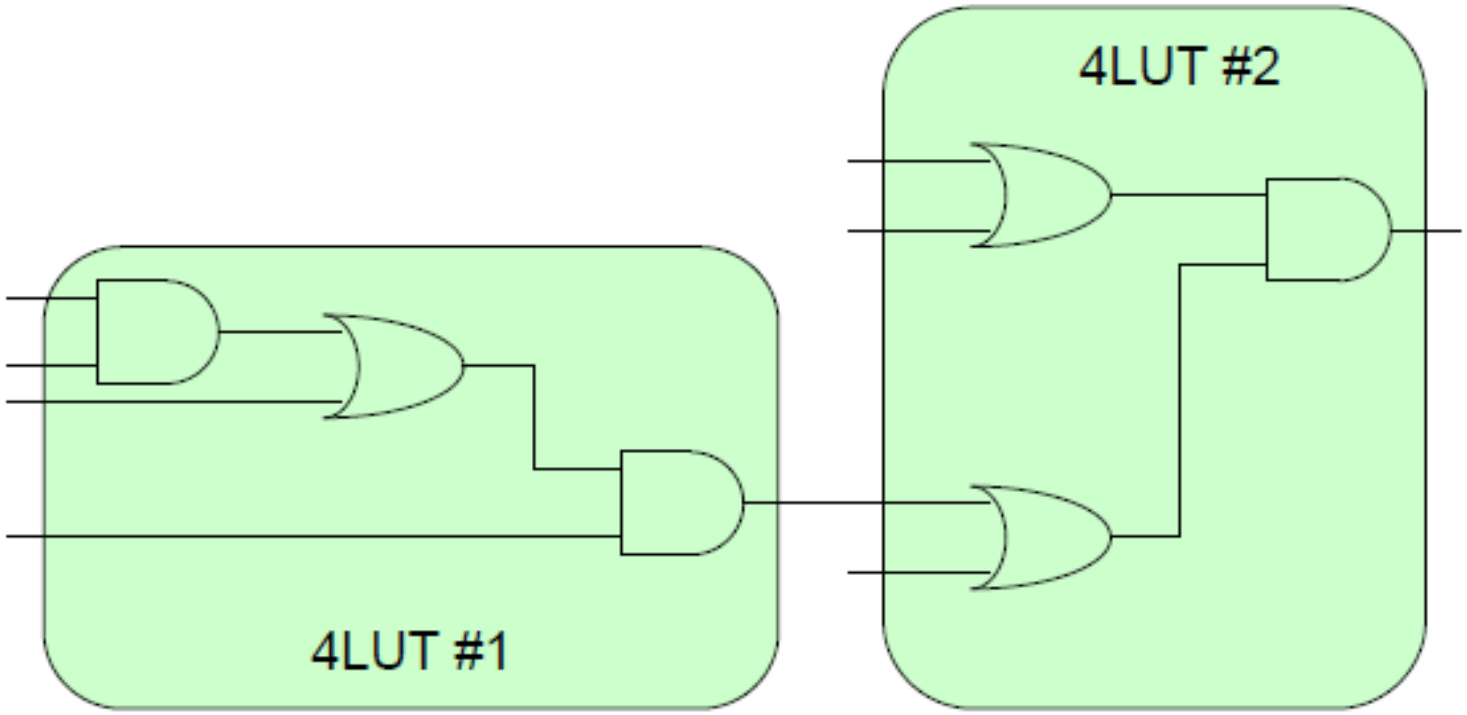
Logic correspondence in a LUT…



…Logic correspondence in a LUT…

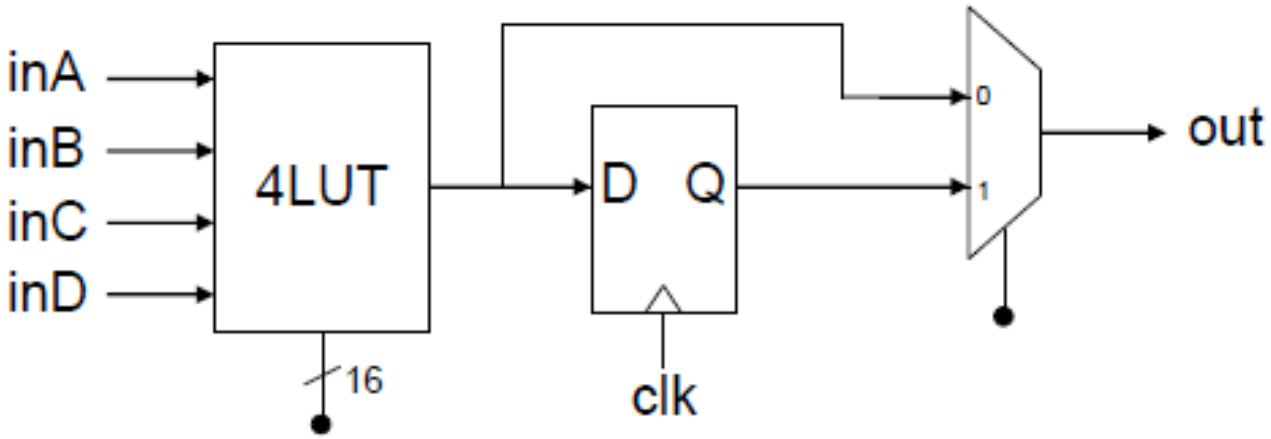


…Logic correspondence in a LUT



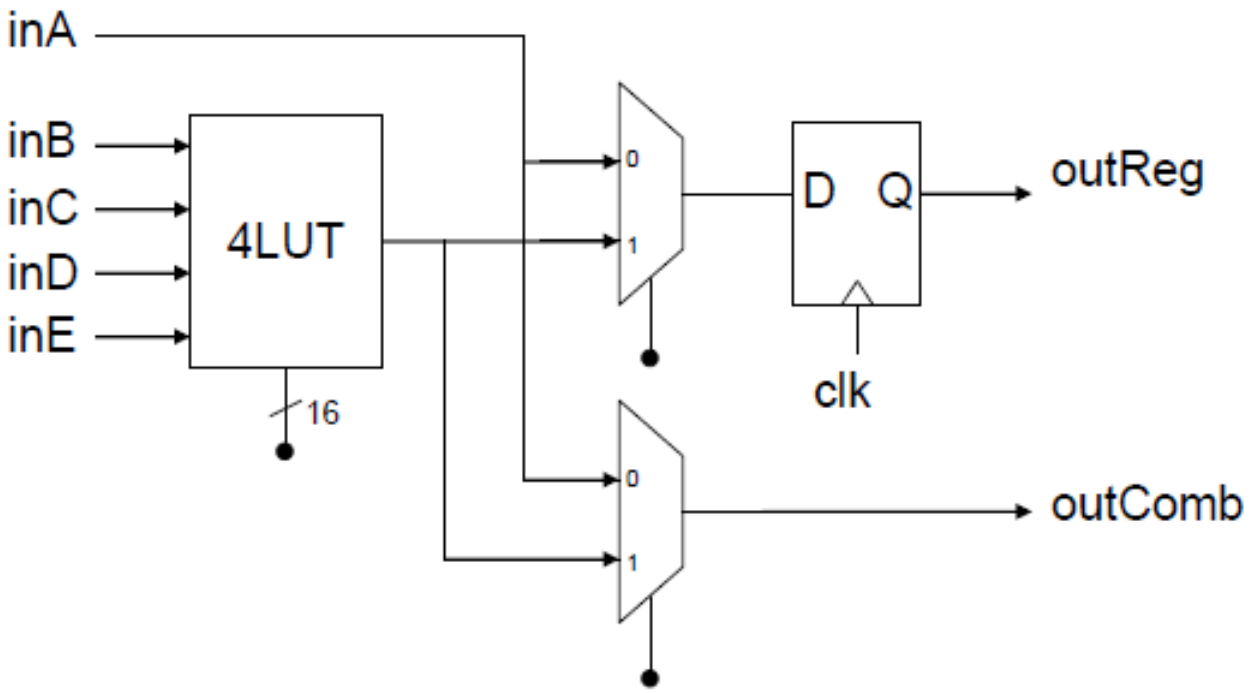
Configurable Logic Element (or Logic Element)…

- Consists of a LUT, a Flip-flip and a Mutiplexer

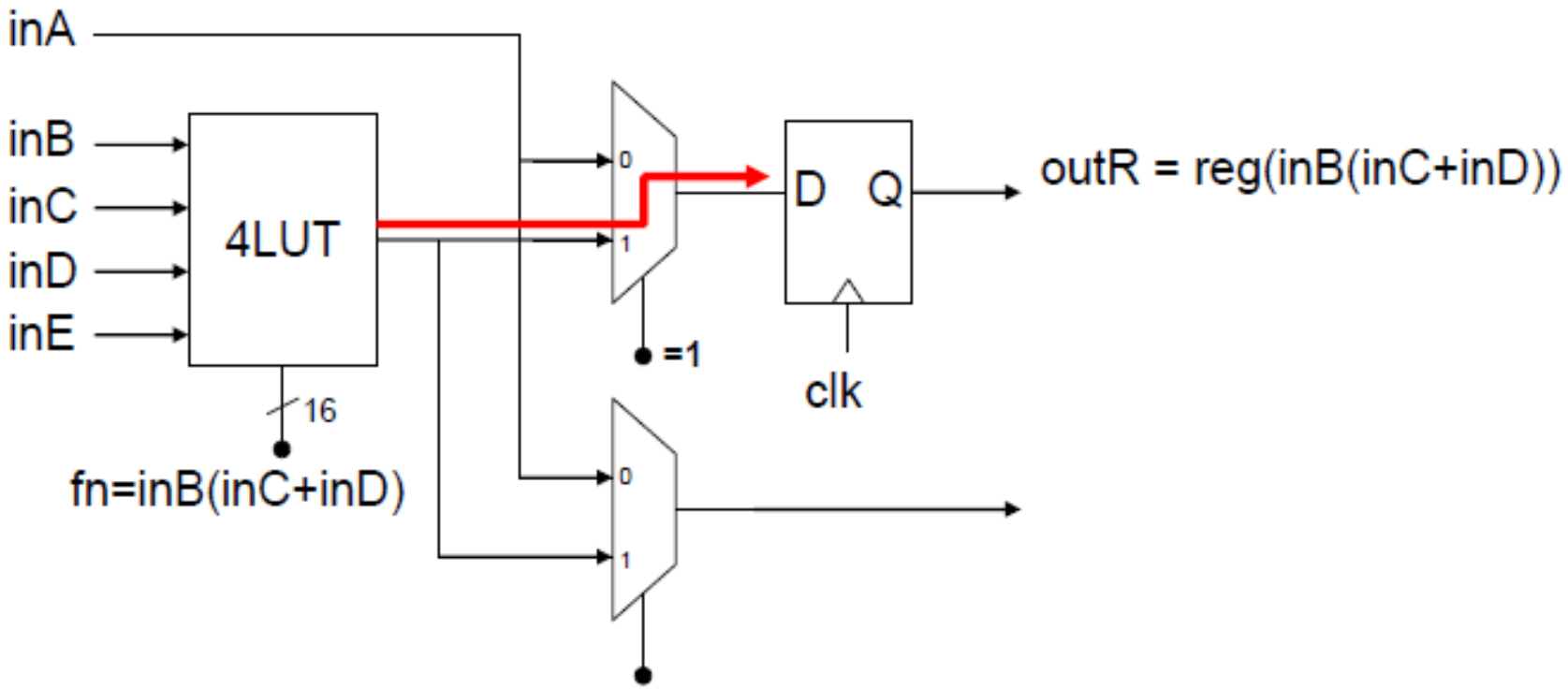


…Configurable Logic Element (or Logic Element)…

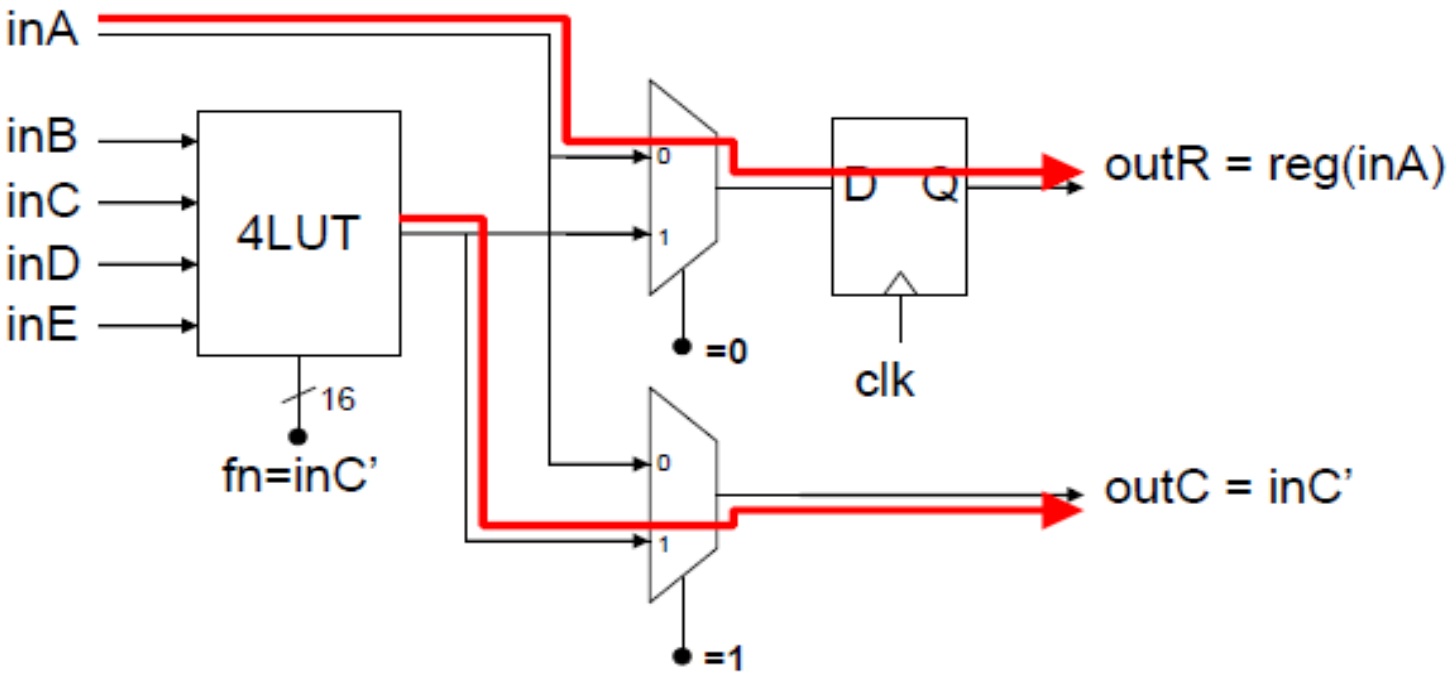
- Two outputs
  - Output of the combinatorial logic
  - Output of a register



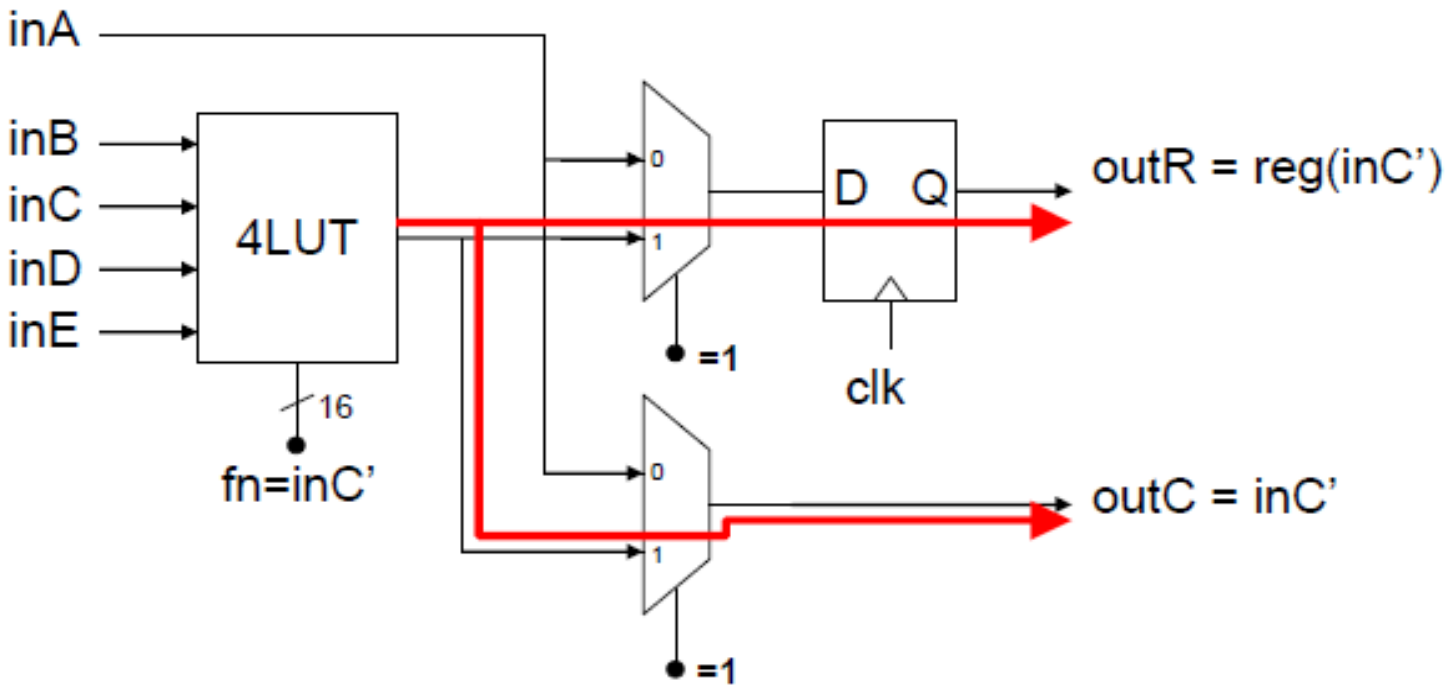
An Example of Configuration



Another Example of Configuration

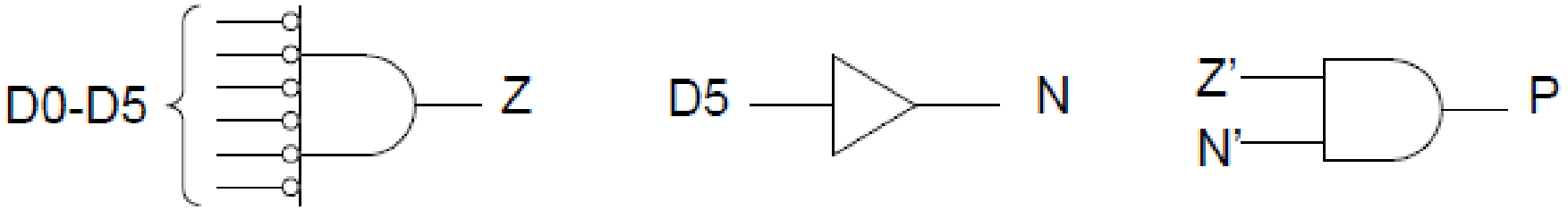


One More Example of a Configuration

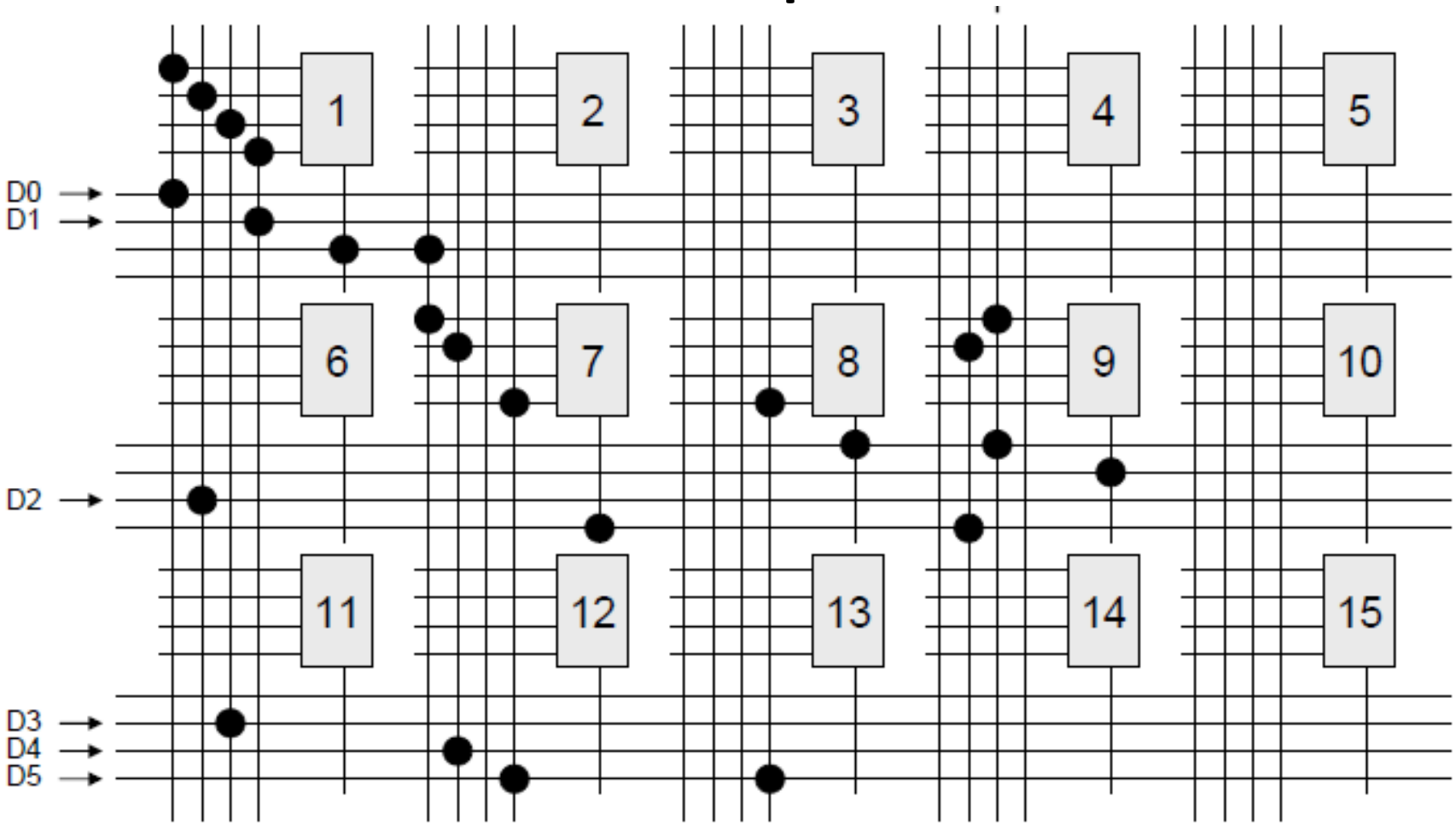


Example…

- Let is consider we want to generate the signals N, Z, P according to the bellow logic



… Example…



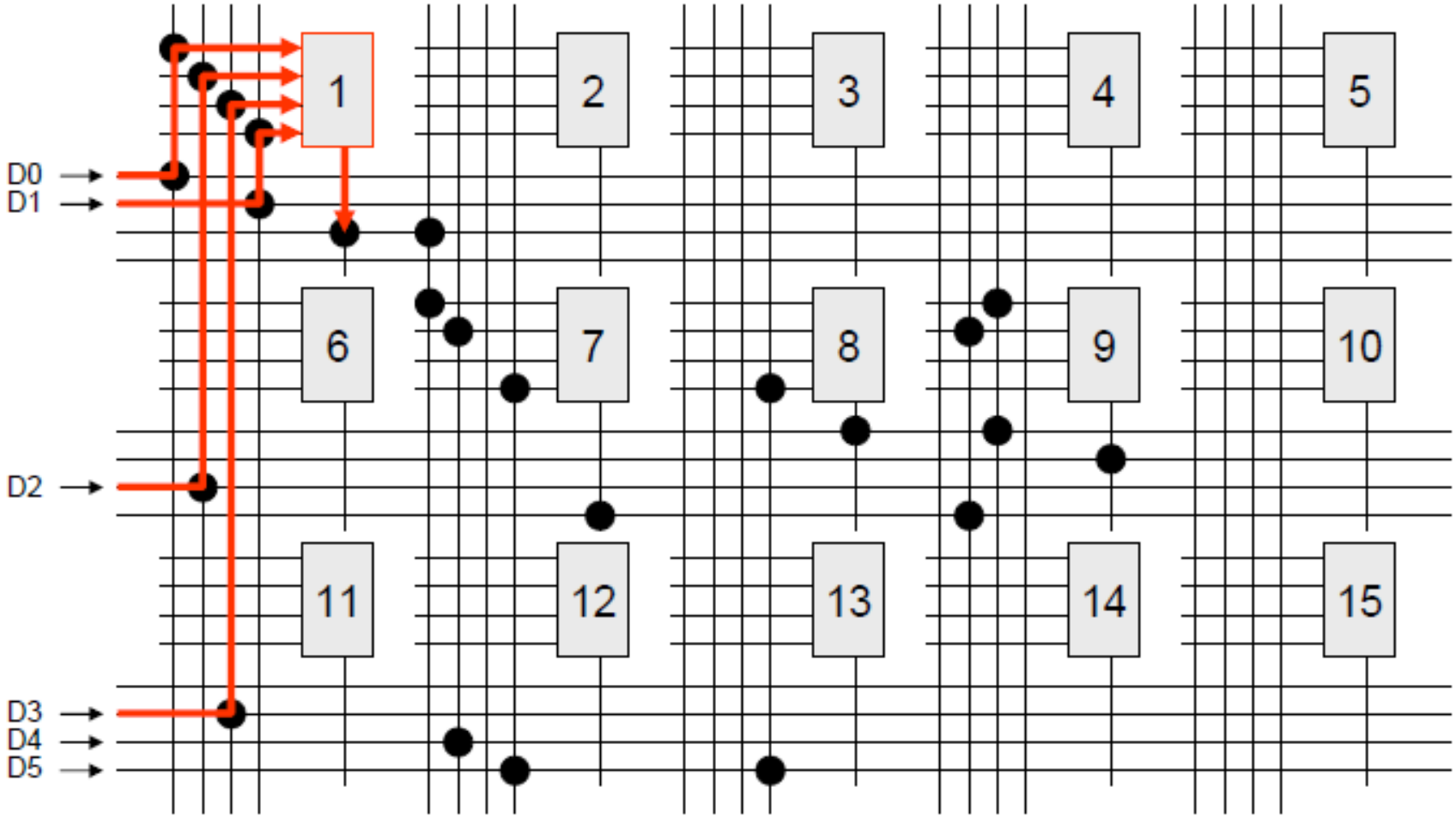
LUT #1: F1 = D0’• D1’• D2’• D3’

LUT #8: F3 = D5 έξοδος N

LUT #7: F2 = F1•D4’•D5’ έξοδος Z

LUT #9: F4 = Z’ • N’ έξοδος P

…Example…



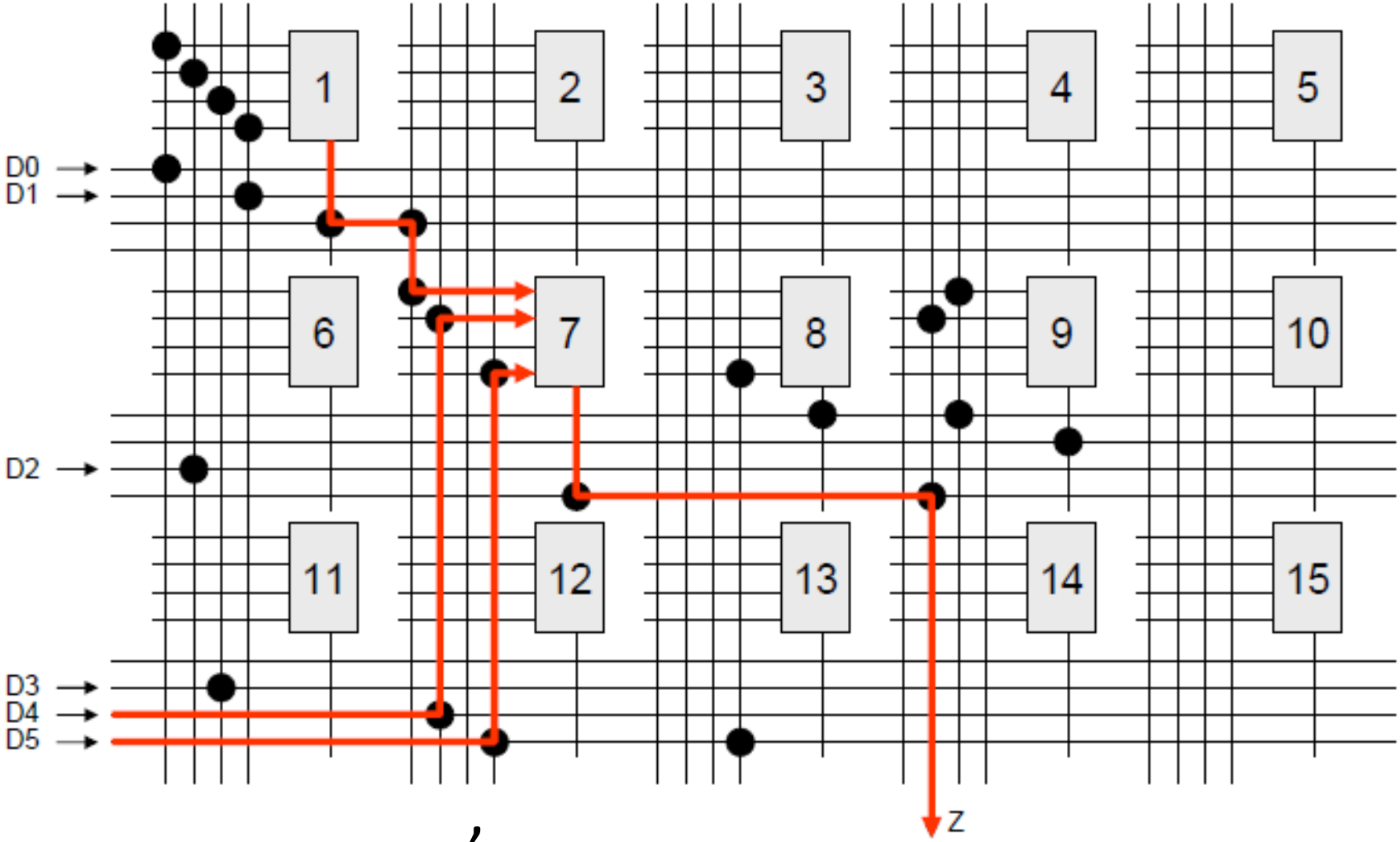
LUT #1: F1 = D0’• D1’• D2’• D3’

LUT #8: F3 = D5 έξοδος N

LUT #7: F2 = F1•D4’•D5’ έξοδος Z

LUT #9: F4 = Z’ • N’ έξοδος P

… Example …



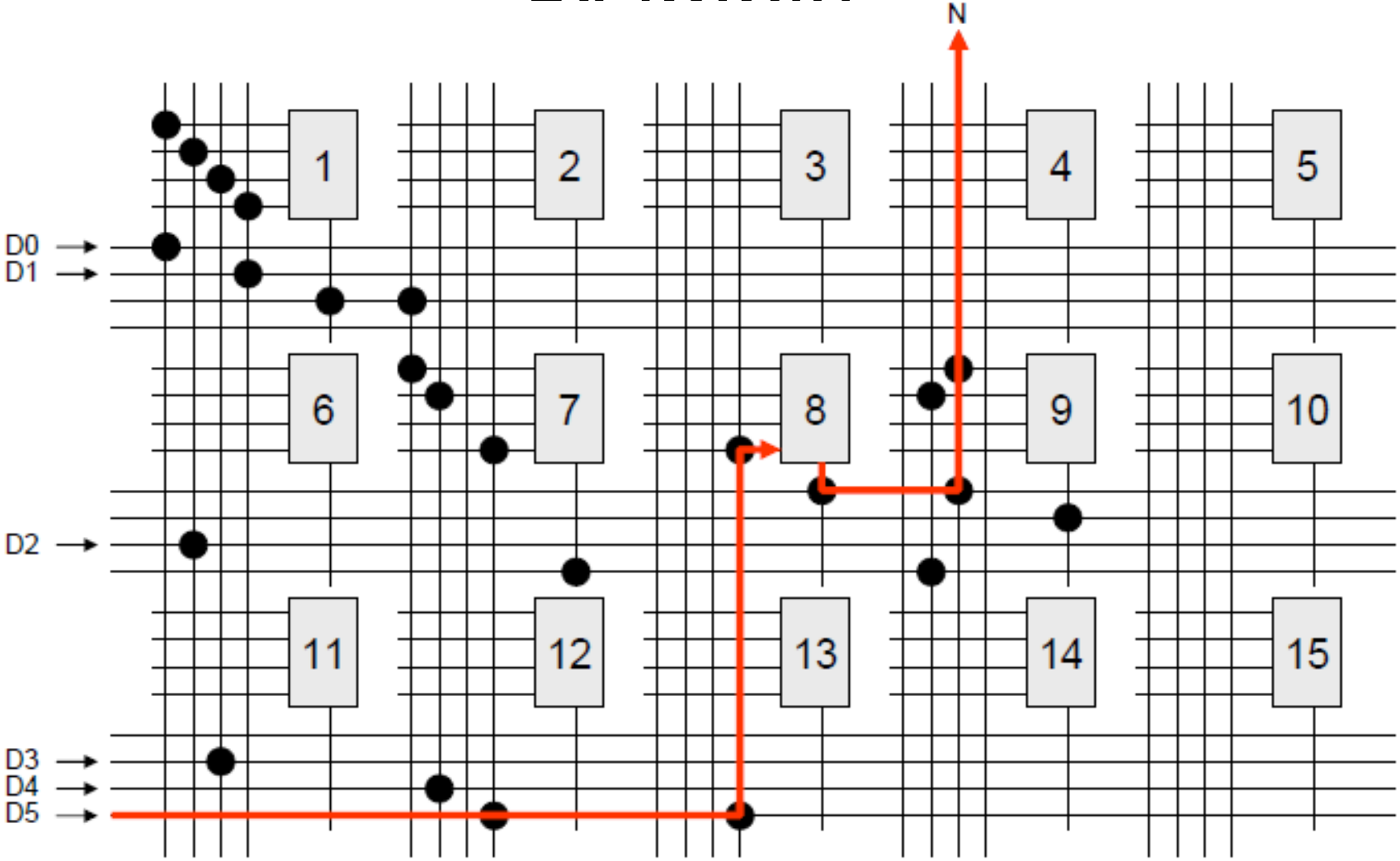
LUT #1: F1 = D0'• D1'• D2'• D3'

LUT #8: F3 = D5 output N

LUT #7: F2 = F1•D4'•D5' output Z

LUT #9: F4 = Z' • N' output P

Example



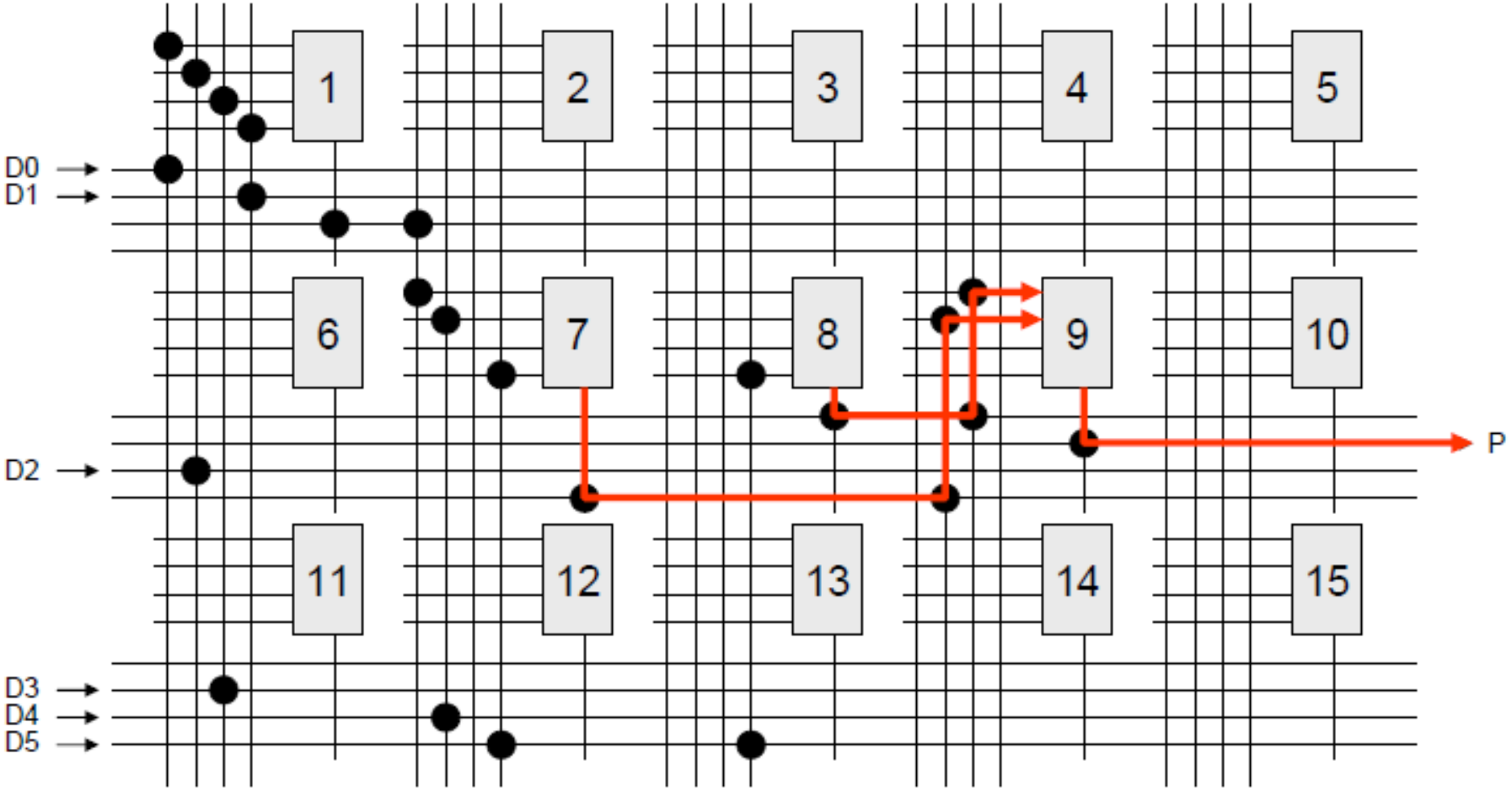
LUT #1: F1 = D0'• D1'• D2'• D3'

LUT #8: F3 = D5 output N

LUT #7: F2 = F1•D4'•D5' output Z

LUT #9: F4 = Z' • N' output P

… Example



LUT #1: F1 = D0'• D1'• D2'• D3'

LUT #7: F2 = F1•D4'•D5' output Z

LUT #8: F3 = D5 output N

LUT #9: F4 = Z' • N' output P

Questions??