Yasmeen Osama & Aya Mahmoud

Lec 3 : Static Verification

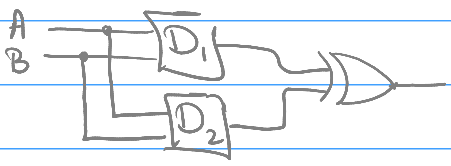
[I] Formal verification

- It's a method by which we Prove or disprove a design implementation against a formal specification or Property
- Uses mathimatical reasoning
- works well for small designs where the number of inputs, outputs and states are small.
- Methods of formal verification (Equivalence checking - Model checking)

* Equivalence Checking :-

- prove or disprove the logical equivalence between the final version of the netlist and the initial RTL. زي بعض مش مهم صح ولا غلط، المهم إنهم equivalent

2 ways → SAT solver (بيدور على الـ inputs اللي تطلع 1 في الـ output) or ATPG
ATPG : Automatic Test Pattern Generation
→ Miter Circuit

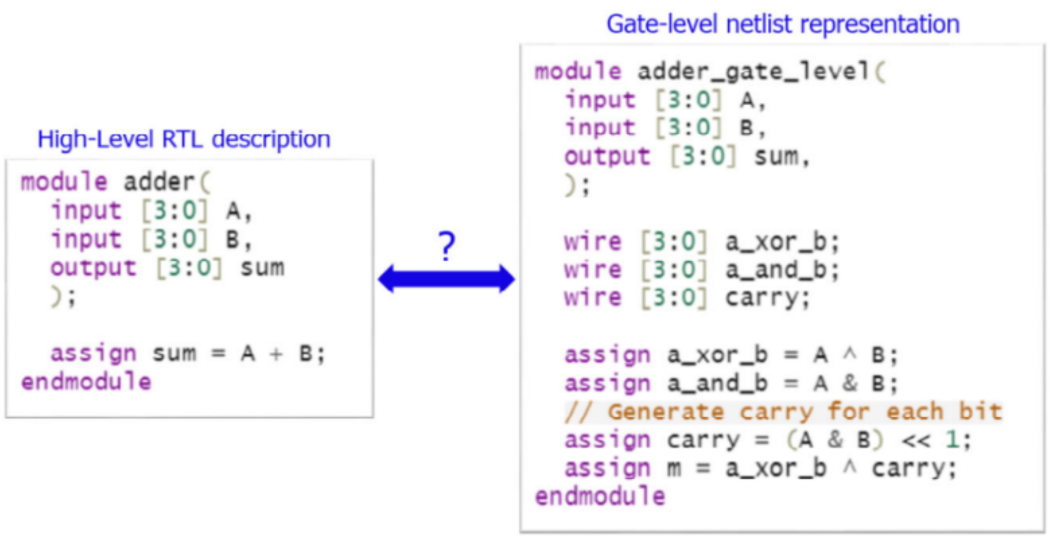


1 لو طلع 1 معناه الـ XOR كده الـ designs مش زي بعض

لو ملقتش أي Pattern بيطلعلك 1 عند الـ output بتاع الـ XOR كده equivalent لبعض وده مفهوم الـ Miter Circuit

- is crucial in the design flow of digital circuits to ensure that optimizations, التحسينات, transformations, التحويلات, or synthesis التوليف, steps haven't introduced errors.

Ex:-



High-Level RTL description

```
module adder(
   input  [3:0] A,
   input  [3:0] B,
   output [3:0] sum
  );

   assign sum = A + B;
endmodule
```

?

Gate-level netlist representation

```
module adder_gate_level(
   input  [3:0] A,
   input  [3:0] B,
   output [3:0] sum,
   );

   wire [3:0] a_xor_b;
   wire [3:0] a_and_b;
   wire [3:0] carry;

   assign a_xor_b = A ^ B;
   assign a_and_b = A & B;
   // Generate carry for each bit
   assign carry = (A & B) << 1;
   assign m = a_xor_b ^ carry;
endmodule
```

We compare the outputs of these two representations for all possible combinations of inputs A and B.

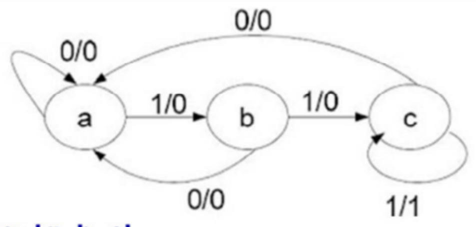
* Model Checking :-

- used to verify whether a system meets a certain property or specification

Categories of Properties
- → Safety : means an undesirable state would never happen.
- → liveness : the system keeps making progress within a reasonable timeframe
- → fairness : all processes or components of the system are given a fair chance to progress or access shared resources.

- involves exploring all possible states of a finite-state model of the system to determine if there a state that violates the property to be verified

Ex:-



States: {a, b, c}
Transitions: {(a,a), (a,b), (b,a), (b,c), (c,c), (c,a)}
Initial state: a

Explored states:
– a (initial)
Unexplored transitions:
– (a,a)
– (a,b)

وهو عند الـ a
شاف الـ 2 tran.
دول بس

↓

Explored states:
– a (initial, from a)
Unexplored transitions:
– (a,b)

جرب مشى واحد منهم (a,a) يبقى الـ a
عمله نروحلها من a
برده ولسه ماشوفتش (a,b)

→

Explored states:
– a (initial, from a)
– b (from a)
Unexplored transitions:
– (b,a)
– (b,c)

لما روحت لـ b عرفت إنى أقدر أشوف دول
دا إلى الـ b عمله أوصلها من a

↓

Explored states:
– a (initial, from a, from b)
– b (transition from a)
Unexplored transitions:
– (b,c)

لما مشيت من الـ (b,a) عرفت إن الـ a عمله أوصلها من الـ b وبالتالي بزود كل شوية
أقدر أروح لـ a منهم a (initial, from a, from b) وهكذا

→

Explored states:
– a (initial, from a, from b)
– b (transition from a)
– c (transition from b)
Unexplored transitions:
– (c,a)
– (c,c)

↓

Explored states:
– a (initial, from a, from b, from c)
– b (transition from a)
– c (transition from b)
Unexplored transitions:
– (c,c)

↓

Explored states:
– a (initial, from a, from b, from c)
– b (transition from a)
– c (transition from b, from c)
Unexplored transitions:
– None

Advantages:-

- **Completeness:** explores all behaviors and corner cases. الاكتمال صارم ميبقوش أى state عندى
- **Rigor:** based on mathematical principles providing rigorous proofs of correctness or violation of properties. الدقة لازم كلهم explored
- **Automation:** tools automate the process of verification.
- **Formal Guarantees:** it provides a formal proof of correctness. الضمانات الرسمية
- **Coverage:** can achieve higher coverage of design space.
- **Debugging Support:** tools often provide detailed counterexamples or traces when a property is violated. دعم تصحيح الأخطاء
- **Regulatory Compliance:** In safety-critical industries formal verification is often required to comply with standards and certification processes. الامتثال التنظيمي