Formal Methods

M. Nimalan

December 2, 2023

Let's start with some questions

- Given integers x and y can the this equation be solved?
- How did we know that this does not have a solution?
- Can we generalize the way we solve this?
- Given any set of equations is there a way to know if the exists a solution that **satisfies** the equations

$$x + y = 5$$

$$2x + 2y = 15$$

Valid and Satisfiable

- **Valid** An set of equations are valid if they are true for all assignment of values to its variables.
- **Satisfiable** An set of equations are satisfiable if it is true for some assignment of values to its variables.
- ...
- We can prove a set of equations to be **Invalid**, by proving that the opposite is **Satisfiable**

Satisfiability Modulo Theory

Formal Solvers

- Satisfiability Modulo Theory is the problem of determining whether a mathematical formula is satisfiable.
- Theorm Provers are tools that test whether given model is satisfiable eg) z3
- Models are written SMT Lib, and a Theorm Provers solves these models.

SMT Lib

```
(declare-const x Int)
(declare-const y Int)

(assert (= (+ x y) 5))
(assert (= (+ (* 2 x) (* 2 y))

(check-sat)
```

SAT and SMT

- Boolean Satisfiability problem (SAT) solvers find variable assignments that solve boolean formula
- Satisfiability Modulo Theory (SMT) solvers has theories beyond boolean formulas

Application of Formal Methods

If you want to prove a design/algorithm/model correct, you model it in SMT lib and use a theorm solver to prove it.

- Formal Verification of hardware
- Contraint problems
- Security Research
- Design of Cryptographic Algorithms

Formal Verification of Hardware

Are the bad states reachable from the initial states ?

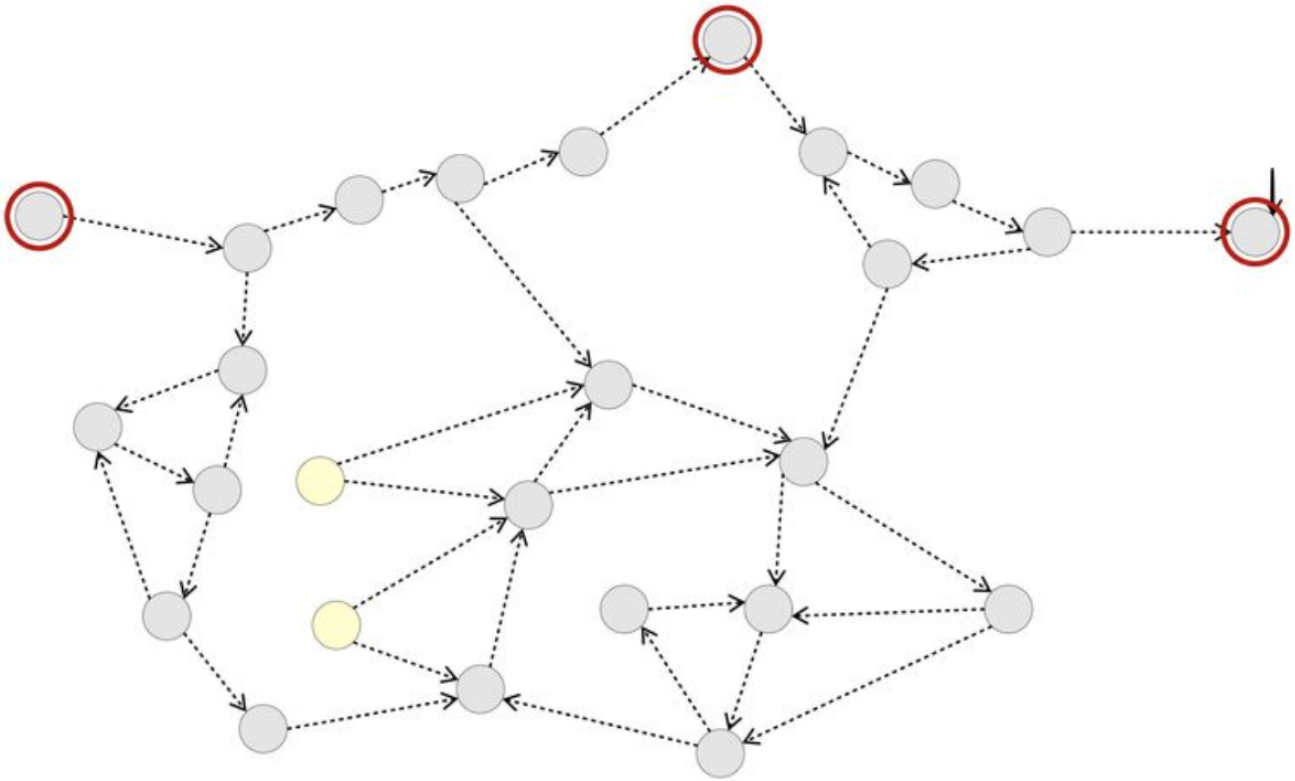


Image Credit: Clifford Wolf, Formal Verification with SymbiYosys and Yosys-SMTBMC

Formal Verification of Hardware

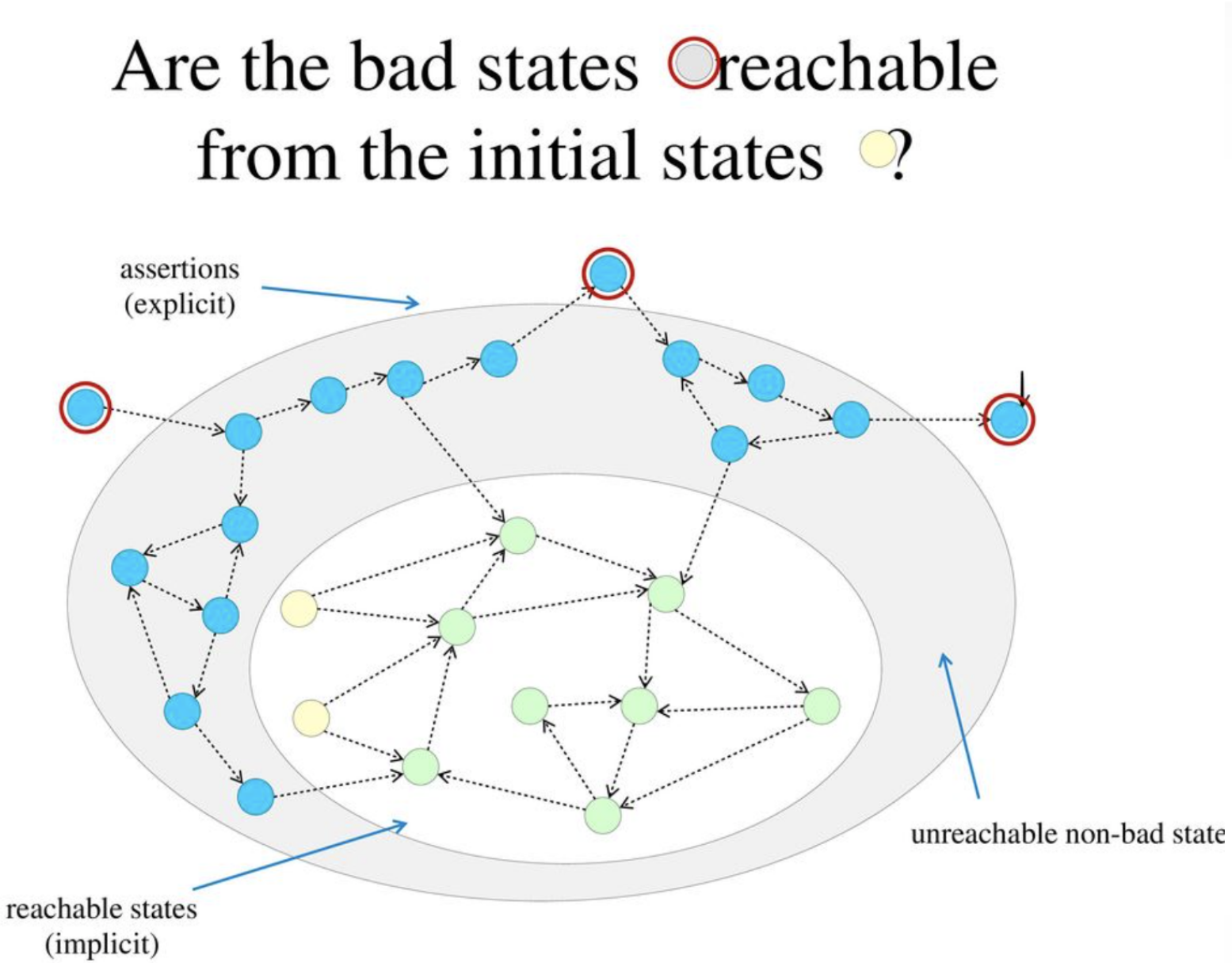


Image Credit: Clifford Wolf, Formal Verification with SymbiYosys and Yosys-SMTBMC

Bounded Model Check (BMC)

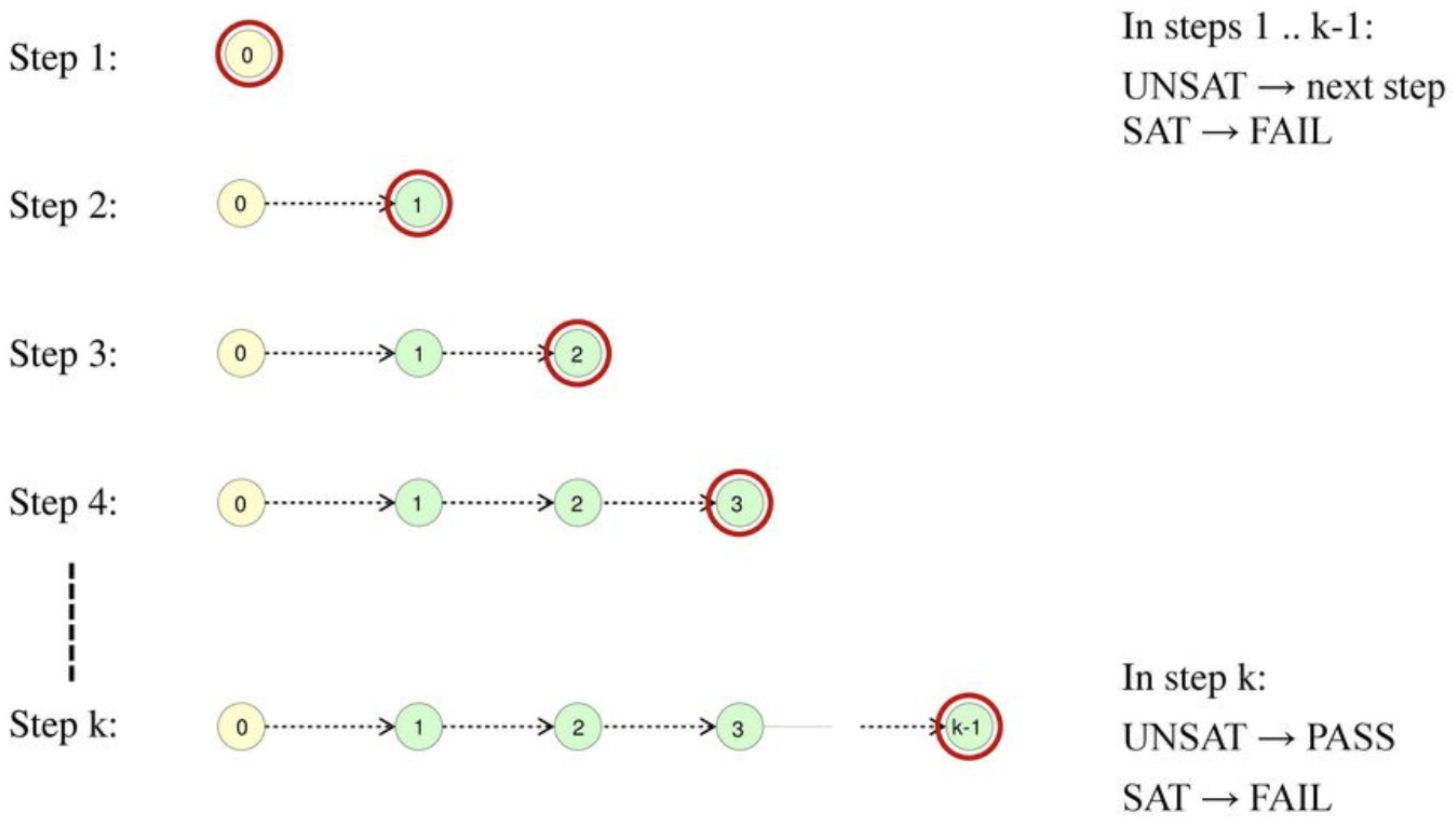
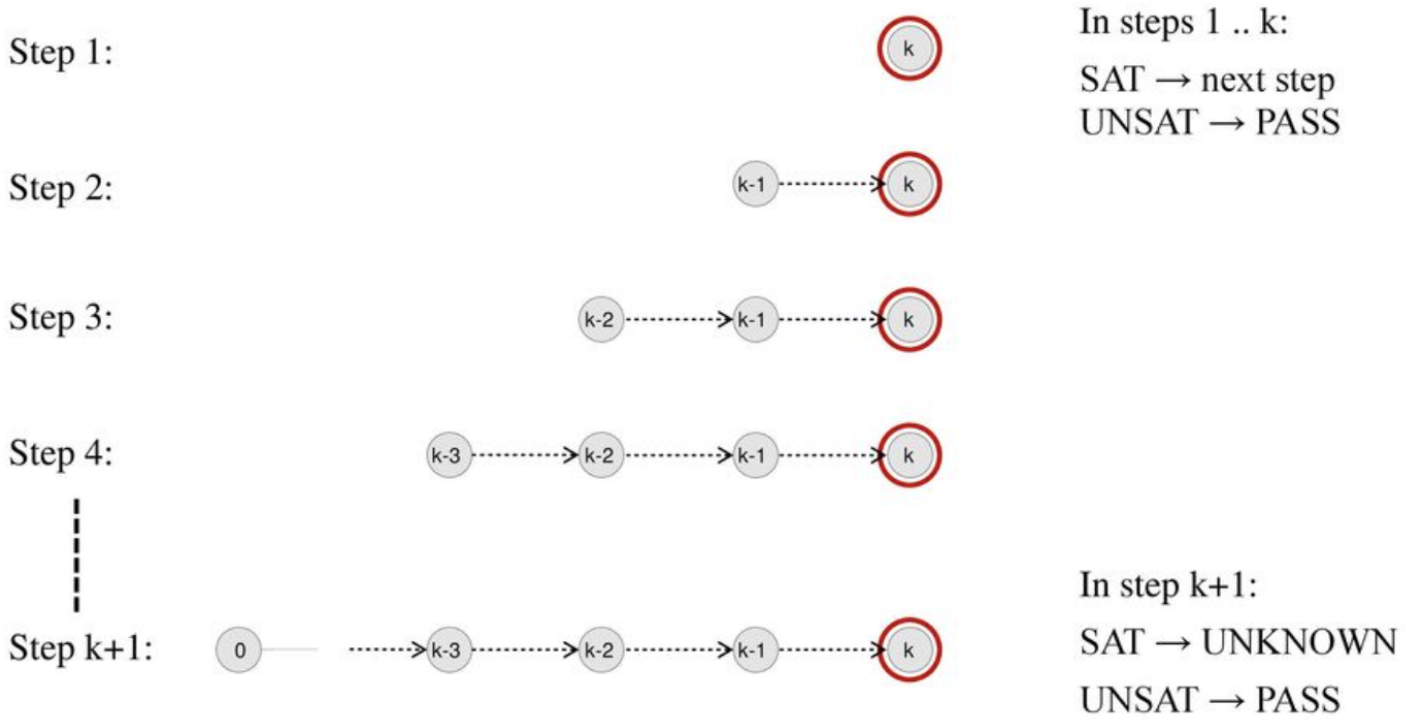


Image Credit: Clifford Wolf, Formal Verification with SymbiYosys and Yosys-SMTBMC

k-Induction



k-induction proves that a sequence of k non-bad states is always followed by another non-bad stat
for a valid complete proof.

Image Credit: Clifford Wolf, Formal Verification with SymbiYosys and Yosys-SMTBMC

Reading

- https://theory.stanford.edu/~nikolaj/programmingz3.html
- https://slideplayer.com/slide/11950984/
- https://link.springer.com/chapter/10.1007/978-3-642-22110-1_46
- https://www.microsoft.com/en-us/research/wp-content/uploads/2013/07/SMT13.pdf
- https://davidsherenowitsa.party/2018/09/19/solving-logic-puzzles-with-z3.html
- https://stackoverflow.com/questions/14547087/extracting-bits-with-a-single-multiplication/14551792

Thank You

A presentation by M.Nimalan (@mark1626)