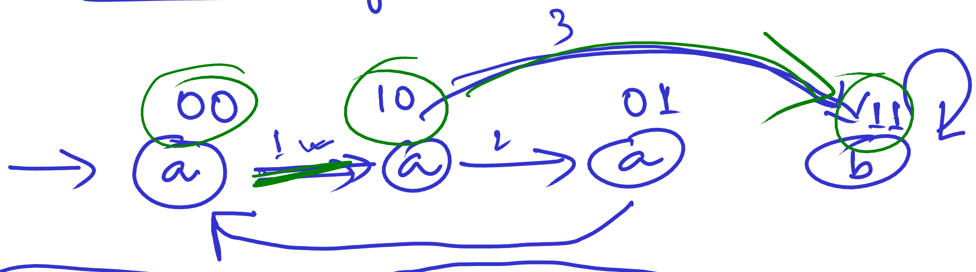
SAT Based Model Checking

Bounded Model Checking

v_0, v_1



$10 \to 01$, 11

Initial state: $\neg v_0 \wedge \neg v_1$

Transition relation

$$T(v_0, v_1, v_0', v_1') = \neg v_0 \wedge \neg v_1 \wedge v_0' \wedge \neg v_1' \quad \to 1$$
$$\vee\ v_0 \wedge \neg v_1 \wedge v_1' \quad \to 2, 3$$
$$\vee\ \neg v_0 \wedge v_1 \wedge \neg v_0' \wedge \neg v_1'$$
$$\vee\ v_0 \wedge v_1 \wedge v_0' \wedge v_1'$$

LTL property (along all paths) a is globally true

$p : (\neg v_0 \vee \neg v_1)$

Interested in paths upto length k where at least one of the states satisfy $\neg p$.

pose question to (SAT) solver; then how can you ensure that the encoding is "friendly" for the solver.

→ paths of length 2 such that one of the states satisfies $\neg p$

→ $s_0 \to s_1 \to s_2$ $\quad \neg p(s_0) \vee \neg p(s_1) \vee \neg p(s_2)$

$s_0 : v_{0,0}, v_{1,0}$
$s_1 : v_{0,1}, v_{1,1}$
$s_2 : v_{0,2}, v_{1,2}$

$I(s_0) \wedge T(s_0, s_1) \wedge T(s_1, s_2) \wedge$ similar

$(\neg v_{0,0} \wedge \neg v_{1,0})$

$\neg v_{0,0} \wedge \neg v_{1,0} \wedge v_{0,1} \wedge \neg v_{1,1}$
$\vee\ v_{0,0} \wedge \neg v_{1,0} \wedge v_{1,1}$
$\vee\ \neg v_{0,0} \wedge v_{1,0} \wedge \neg v_{0,1} \wedge \neg v_{1,1}$
$\vee\ v_{0,0} \wedge v_{1,0} \wedge v_{0,1} \wedge v_{1,1}$

$\neg p(s_0) = \neg(\neg v_{0,0} \vee \neg v_{1,0})$

$\to CNF(\text{———})$

23 SMT

$\boxed{v_{0,0} = 0 \quad v_{1,0} = 0}$ ✓

$\boxed{v_{0,1} = 1 \quad v_{1,1} \quad 0}$ ✓

$\boxed{v_{0,2} = 1 \quad v_{1,2} = 1}$ ✓

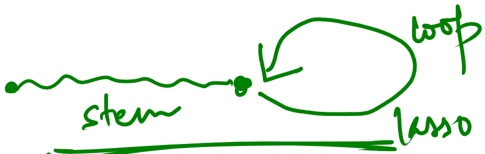
→ exercise

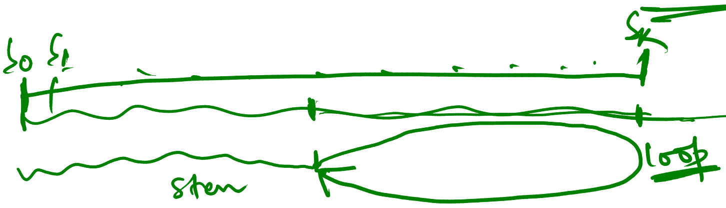
→ What about eventuality properties?

AF p every path must have a state where p is true.

Counterexample: an infinite path where $\neg p$ is always true.

Claim: If a counterexample exists, then a lasso counterexample exists as well.





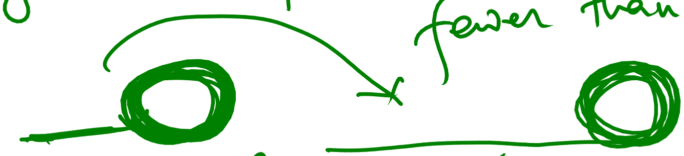
finding a lasso where $\neg p$ always holds.

$$\text{lasso}_k(s_0, \ldots, s_k) \wedge \bigwedge_{i=0}^{k-1} \neg p(s_i)$$ ✓

BMC

$$\text{path}_k(s_0, \ldots, s_k) \wedge \bigvee_{i=0}^{k-1} s_k = s_i$$ ✓ ✓

Why is this formula satisfied by lassos with fewer than k transitions?



unrolled into a bigger lasso

→ BMC for full LTL

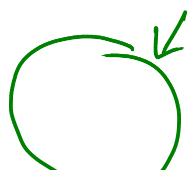
LTL → Buchi

→ Product construction

→ Acceptance

→ counterexamples

lasso



counterexample

Counterexamples of a fixed length — Bounded Model Checking

k ←

Build BMC formula of bound k

↓ SAT solver

UNSAT → k = k+1

SAT → counterexample found

Completeness Threshold (CT) ← tight CT is as hard as the MC problem itself

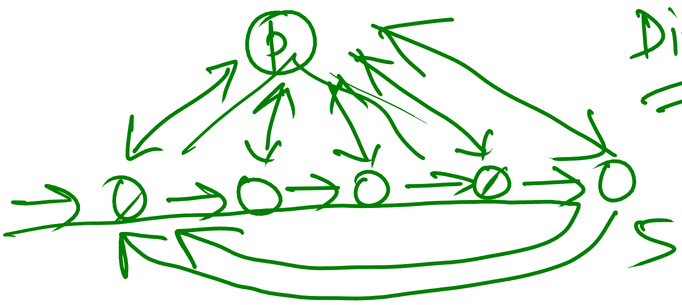
stop if k ≥ CT

|S| is a CT for properties of the form AG p ← smaller condition

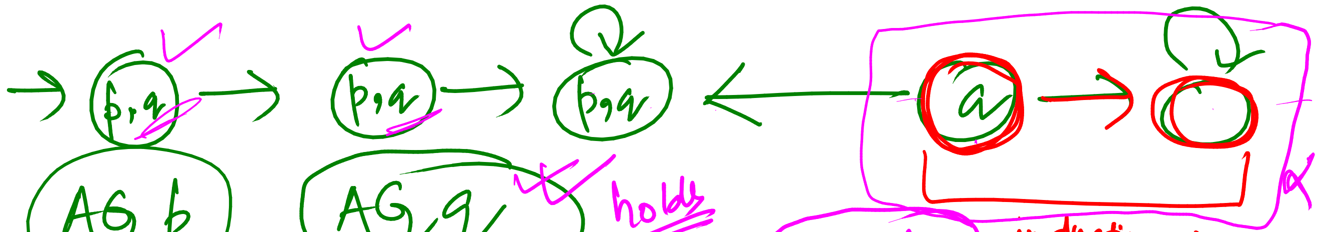
state space explosion

Diameter of the transition graph (length of the longest shortest path between two states)

Not for properties of the form AF p



Dia = 2



AG p ‖ AG q holds

BMC (diameter = 2)

2-induction

inductiveness check fails

Induction

1. All initial states satisfy p

2. If we are in a state where p is true, it is impossible to get to a state where p is not true.

SAT solver

$I(s) \wedge \neg p(s) \rightarrow$ SAT?

unSAT $\boxed{1}$ holds

$P(s) \wedge T(s, s') \wedge \neg p(s') \rightarrow$ SAT?

inductiveness check

will appear later also

unSAT $\boxed{2}$ holds.

claim AG q is true but not inductive

&

k-induction

$P(0) \wedge \forall n \, (P(n) \Rightarrow P(n+1))$

$\Rightarrow \forall n \, P(n)$

stronger base case check

$P(0) \wedge P(1) \wedge \forall n \, (P(n) \wedge P(n+1) \Rightarrow P(n+2))$

strength the premise for this check

$\Rightarrow \forall n \, P(n)$

k-induction principle

k steps

$\bigwedge_{i=0}^{k-1} P(i) \quad \forall n \left(\bigwedge_{i=0}^{k-1} P(n+i) \Rightarrow P(n+k) \right)$

$\Rightarrow \forall n \, P(n)$

$$fib(n) = \begin{cases} n & \text{if } n \leq 1 \\ fib(n-1) + fib(n-2) & \text{otherwise} \end{cases}$$

$fib(n) \geq n$ for $n \geq 5$.

$fib(5) = 5 \geq 5$

$fib(n+1) = fib(n) + fib(n-1)$

2-induction can be useful in this case

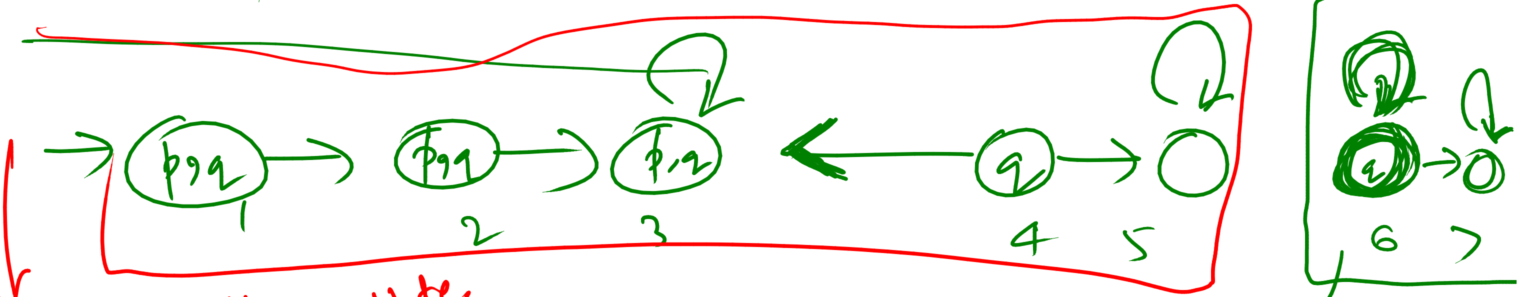
Counterexample Proof

AGq inductive

2 inductive

not k-inductive for any k

AGq not



k-induction

-> how to make k-ind complete for AGq

slides of last 3 lectures. ← 21st after