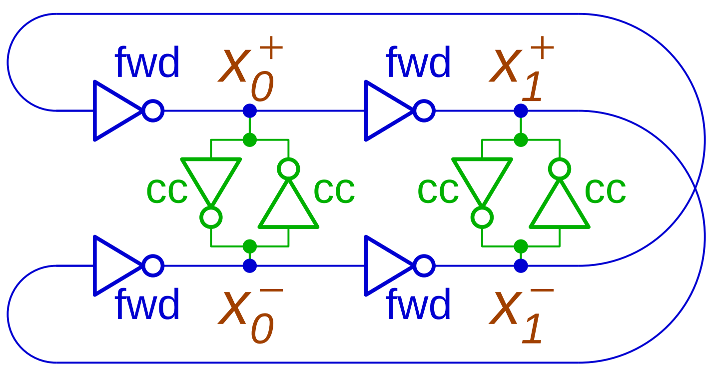
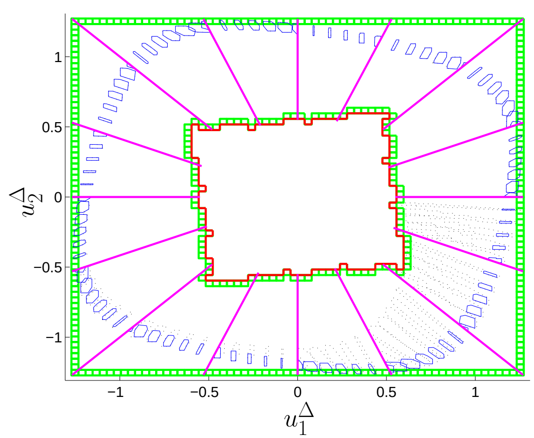
Oscillator Verification with Probability One

Chao Yan, Mark Greenstreet

Intel, The University of British Columbia





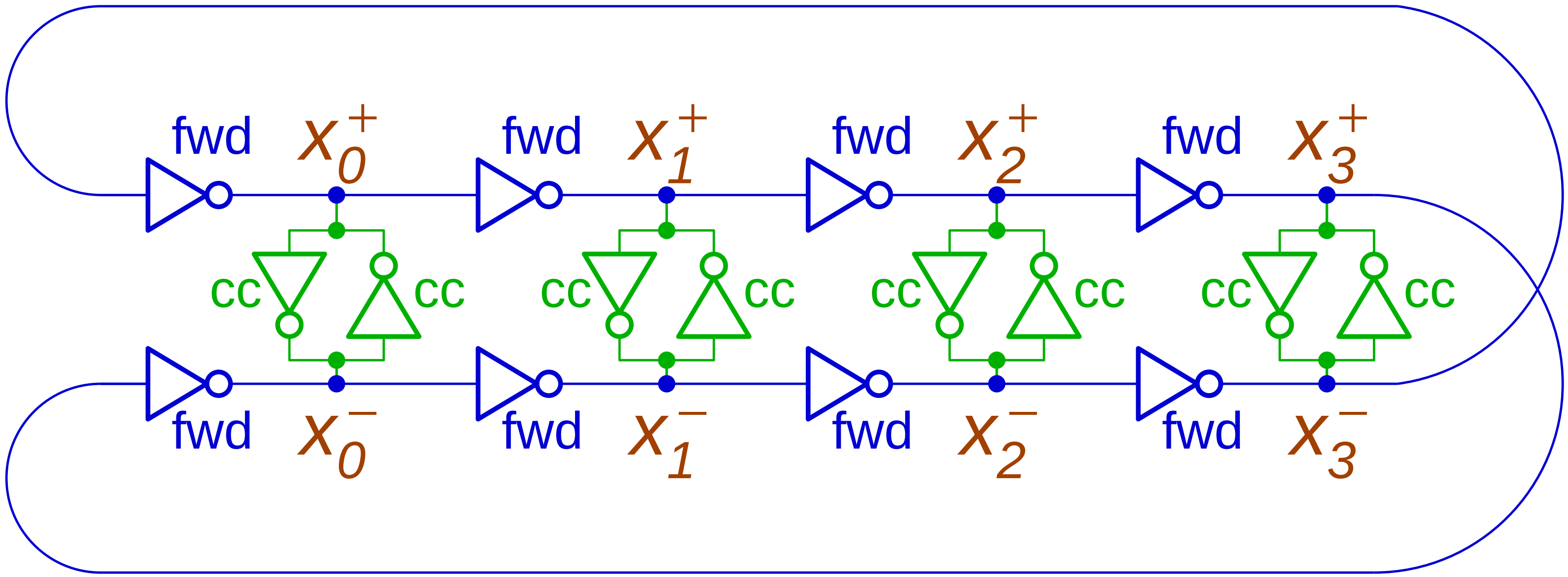
Outline

- Motivation
- Rambus Ring Oscillator
- Our Approach: Reachability Analysis
- Challenge 1: Performance
- Challenge 2: Non-empty Failure Set
- Result
- Conclusion & Future Work

Motivation

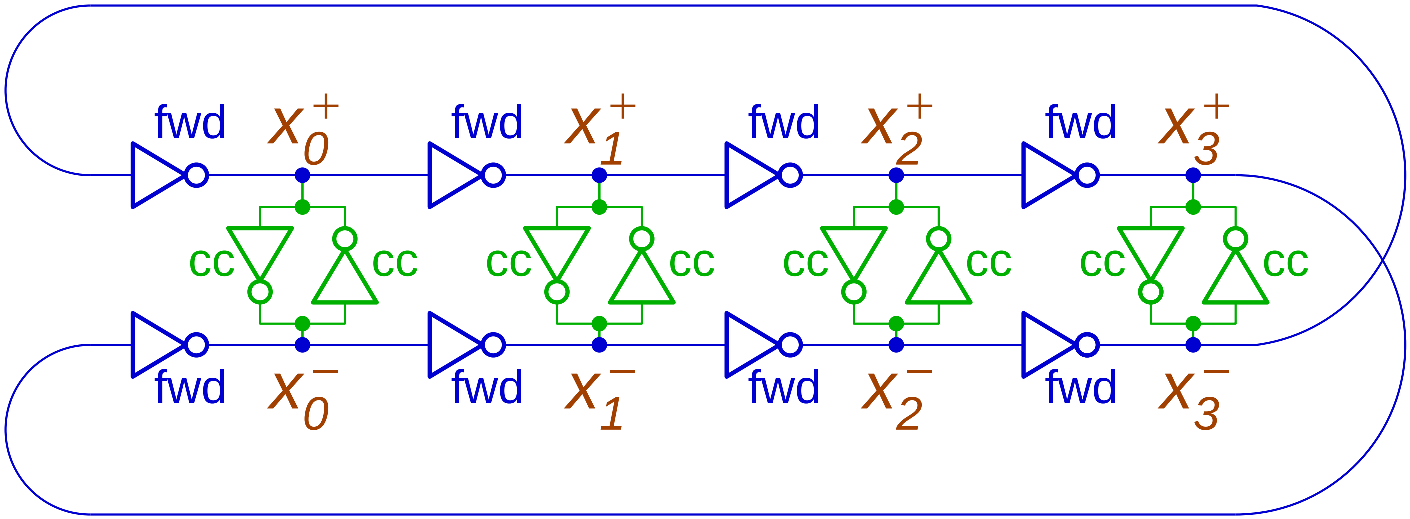
- AMS bugs account for large percent of re-spin bugs in industry
  - Analog or Mixed Signal Circuits are widely used, e.g. Cells, IO, DFx
  - Digital design has become relatively low error, e.g. formal property verification
  - Analog design relies on designers' intuition and expertise
- Simulation based methods are not good enough
  - Expensive: solve continuous ordinary differential equations (ODEs)
  - Low coverage: impossible to cover all corner cases
  - Start-up failures: most simulations assume intended operating conditions
- Formal verification is an attractive approach
- But, not as successful as digital FV
  - Computation is more expensive than simulation: solve nonlinear ODEs from an initial set
  - Accuracy is a big problem: approximation techniques must be applied
  - Analog are complicated, unexpected problems: e.g. metastability behaviors

Rambus Ring Oscillator



- Even-stage differential oscillator
  - Forward inverters (fwd), cross-couple inverters (cc).
  - Forward inverters and cross-couple inverters fight each other to make the circuit oscillate
  - Generates multiple, evenly spaced, differential phases.

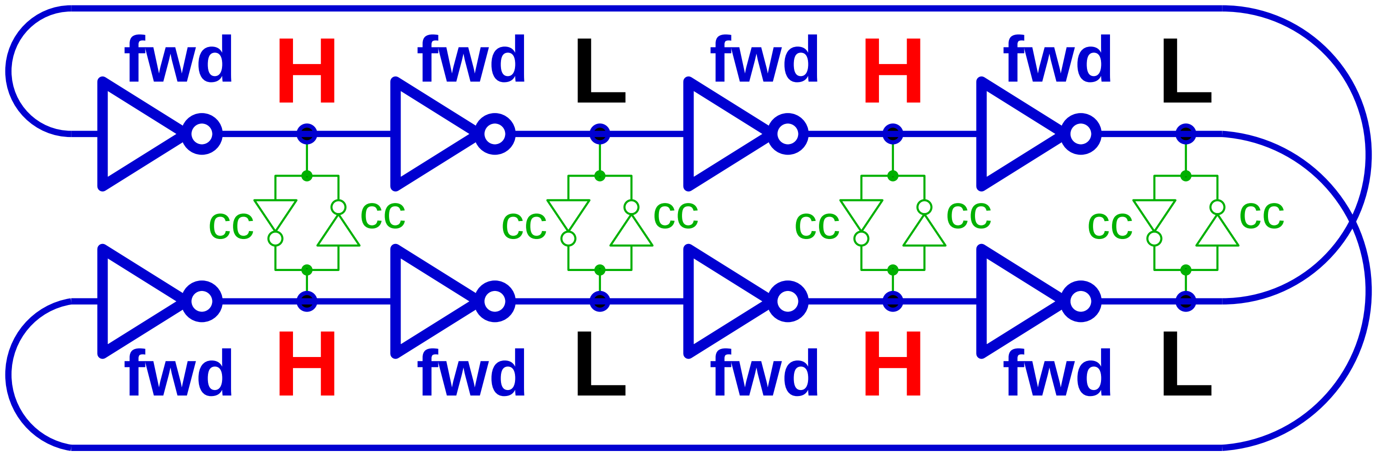
Start-up Failures



- Will it start-up reliably?
  - Proposed by Jones et al.
  - Easy to show that the oscillation mode is stable once the oscillator is running.
  - Start-up failures have been observed for real chips in spite of extensive simulation.
  - Known to depend on the transistor sizes in the inverters.

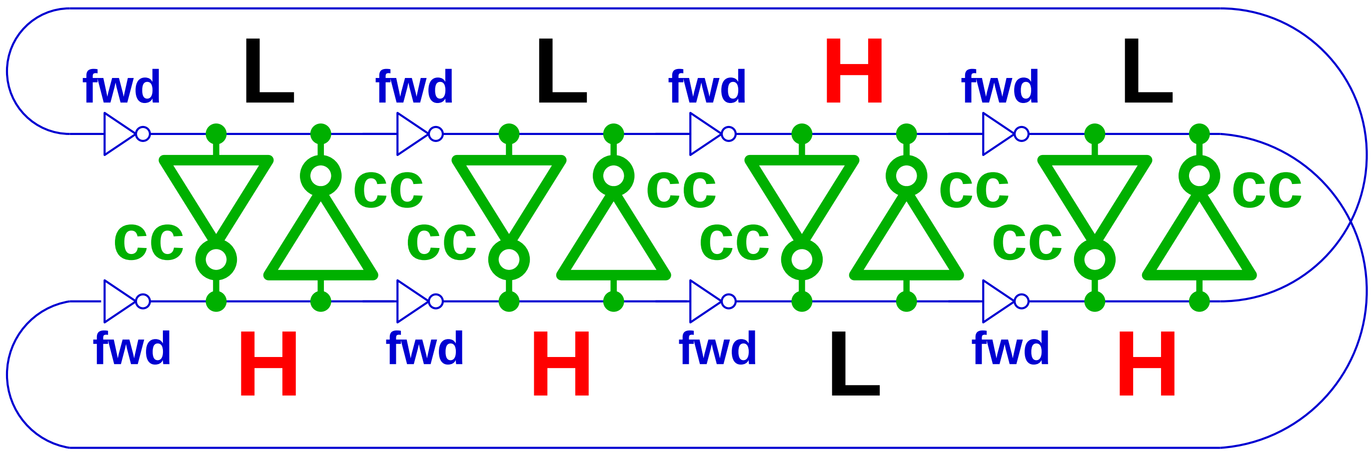
$$s = \frac{\text{size of cross coupling inverters}}{\text{size of forward inverters}}$$

Start-up Failures



- If the fwd inverters are much larger than the cc's,
  - then the circuit acts like an 8-inverter ring,
  - and the circuit may lock-up.

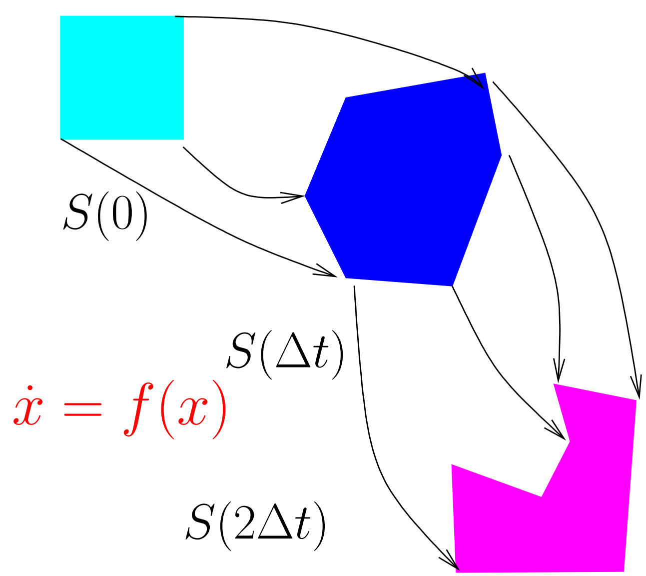
Start-up Failures



- If the cc inverters are much larger than the fwd's,
  - then the circuit acts like 4 SRAM cells,
  - and the circuit may lock-up.

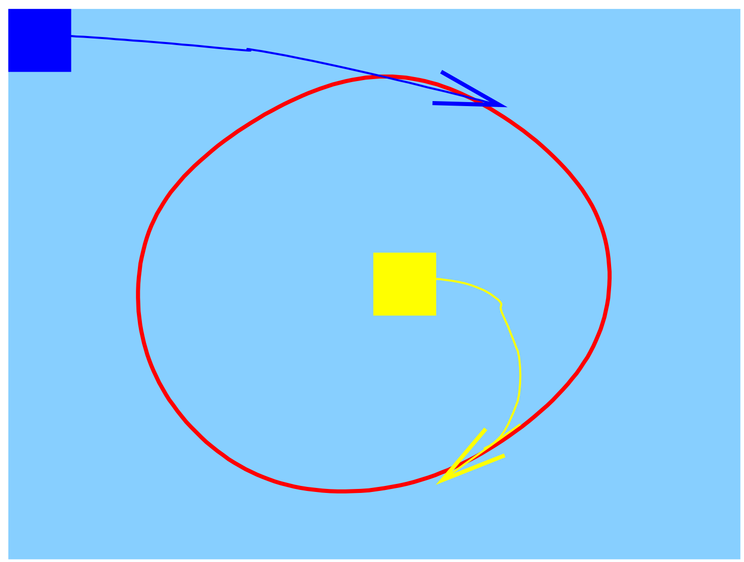
Our Approach: Reachability Analysis

- Reachability analysis
  - Given an initial set $S(0)$
  - and a dynamical system $\dot{x} = f(x)$
  - compute forward reachable set $S(\Delta t)$ after time Δt
  - $S(\Delta t)$ contains all trajectories from $S(0)$
  - repeat for $S(2\Delta t)$, $S(3\Delta t) \cdots$



Our Approach: Reachability Analysis

- Reachability analysis
- Global convergence by reachability computation
  - Split the entire initial state space into small cubes
  - Compute forward reachable states from these cubes
  - Show reachable sets from “all“ cubes converge to one invariant set.



COHO: Reachability Computation Tool

- Construct accurate ODE models from net-list automatically

$$\dot{v} = f(v)$$

- Solving dynamic systems: linear differential inclusions

$$\dot{v} = Av + b \pm u$$

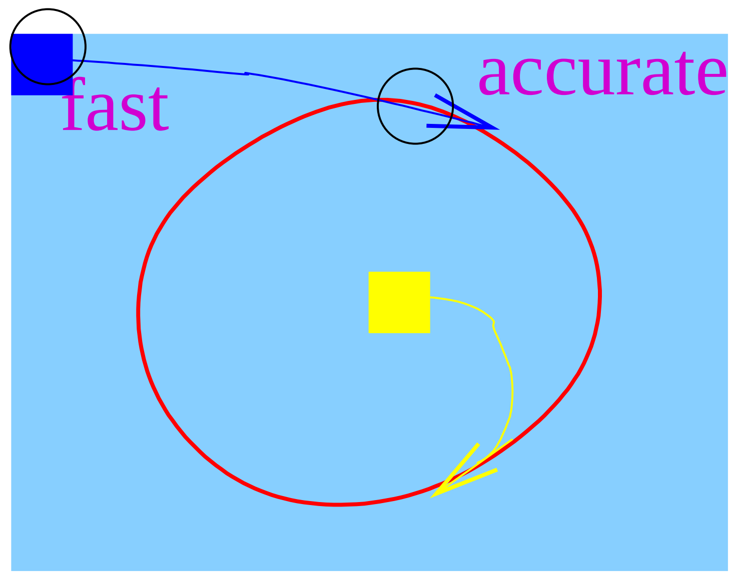
- Efficient representation of high dimensional space: projectagon
  - Exploits extensive algorithms for 2D computational geometry.
  - Support non-convex regions for accuracy
- COHO is sound for verifying safety properties
- Available at http://coho.sourceforge.net

Challenge 1: Performance

- Reachability computation using circuit-level model is expensive
  - Each reachable computation in 4D may take 10 minutes or several hours.
  - There are $16^4 = 64k$ cubes for the two-stage oscillator
  - Requires at least 450 days computation
- Reachability computation can't show convergence if using simple models with large approximation
  - E.g. interval
  - Reachable sets blow up rapidly

Dynamical System Analysis

- Apply “quick“ reachability computation with large over-approximation when the dynamical system converges quickly
- Apply “accurate“ reachability computation to minimize error otherwise

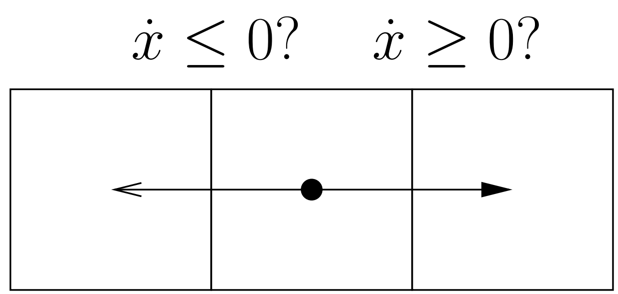


Step 1. Differential Operation

- Change coordinate system

$$u_i^{\Delta} = \frac{x_i^+ - x_i^-}{\sqrt{2}}, \quad \text{“differential” component}$$
$$u_i^{\Sigma} = \frac{x_i^+ + x_i^-}{\sqrt{2}}, \quad \text{“common mode” component}$$

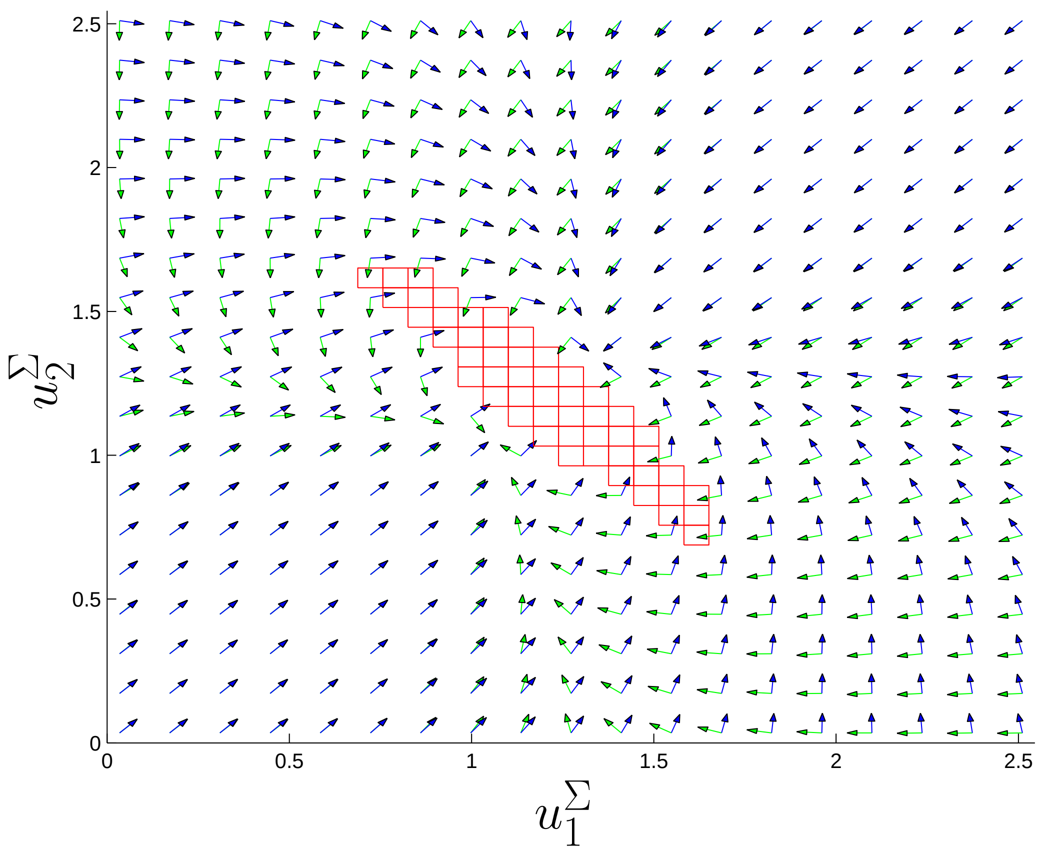
- Partition u space into small boxes and determine flows between boxes



- Eliminate boxes from future consideration
  - if the node has no incoming edges
- Refine the partition and repeat above steps

Step 1. Differential Operation

- All initial conditions lead to boxes with u_0^Σ and u_1^Σ close to $V_{dd}/\sqrt{2}$.
- With $m = 64$, only 0.45% of total space remains



Space reduction

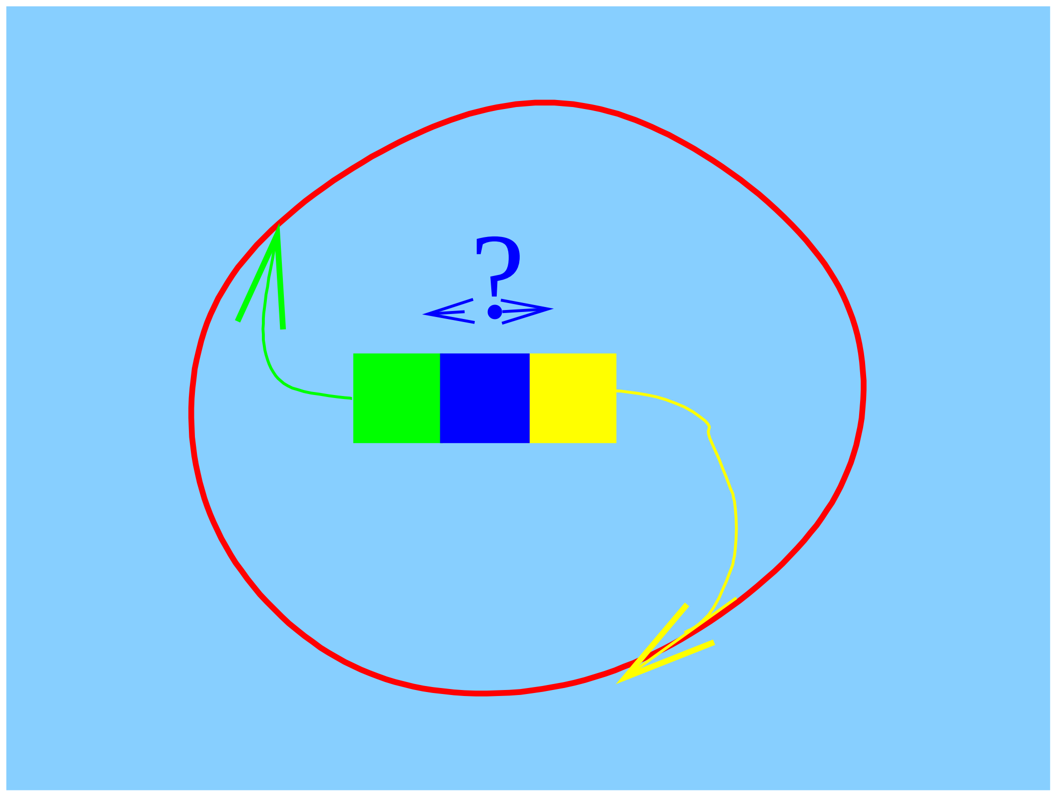
- Common-mode components converges to a small range
- 2-dimensional interval model

$$\dot{u} = f(u) \implies \dot{u}^{\Delta} \in f(u^{\Delta}) \pm err(u^{\Sigma})$$

- Reachability computation for 2-dim system is much more efficient for 4-dim systems.
- Computation error is much smaller although the model error is larger

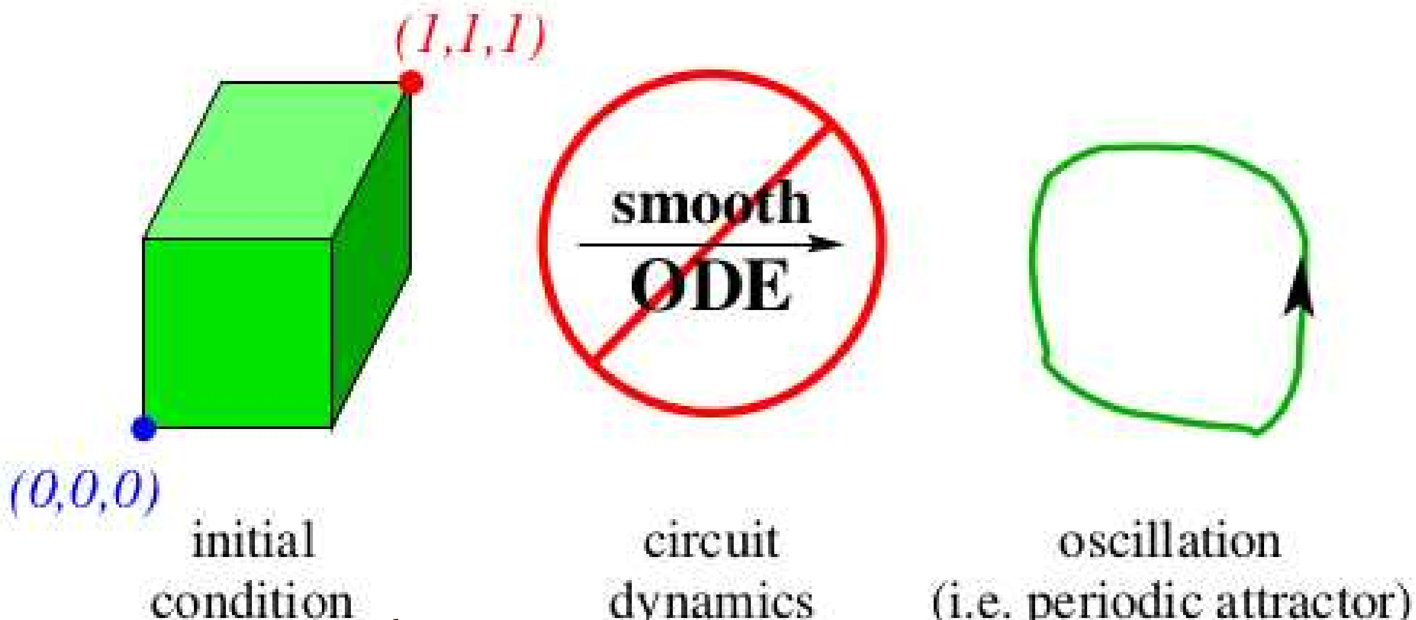
Challenge 2: No Ideal Oscillator

- Reachability analysis can't show escape from the metastable region



Challenge 2: No Ideal Oscillator

- Reachability analysis can't show escape from the metastable region
- Theorem 1: It is impossible to design an oscillator that starts from all initial conditions.
- A common feature in many analog systems, e.g. arbiter, synchronizer

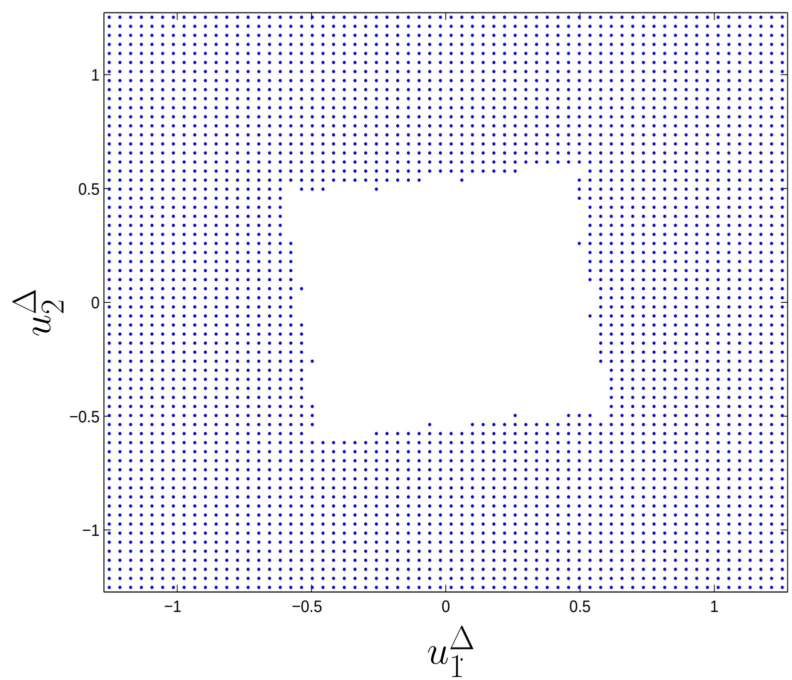


Negligible Failure Set

- The failure set is not empty, instead, show it’s negligible
  - Perfectly reasonable for real designers.
  - But, reachability analysis can’t solve the problem
  - A formal correctness proof must include some notion of probability.
- Theorem 2
  - Generalization of the ”cone” argument (Mitchell *et al.*)
  - A sufficient condition to show the failure set has lower dimension than the full space
  - All trajectories leave the failure set with probability one
  - Details in the paper

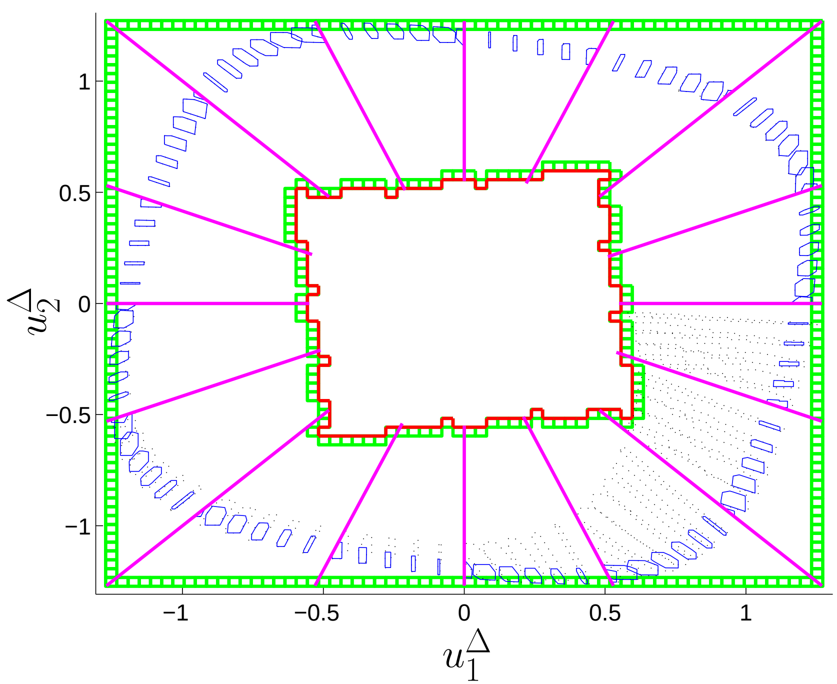
Step 2. Divergence from Metastability

- Prove trajectories escape from the metastable region with probability one by Theorem 2.
- Set $H = diag([+1, +1, -1, -1])$
  - ”1” for the growing differential components, trajectories diverge
  - ”-1” for the diminishing common-mode components, trajectories converge



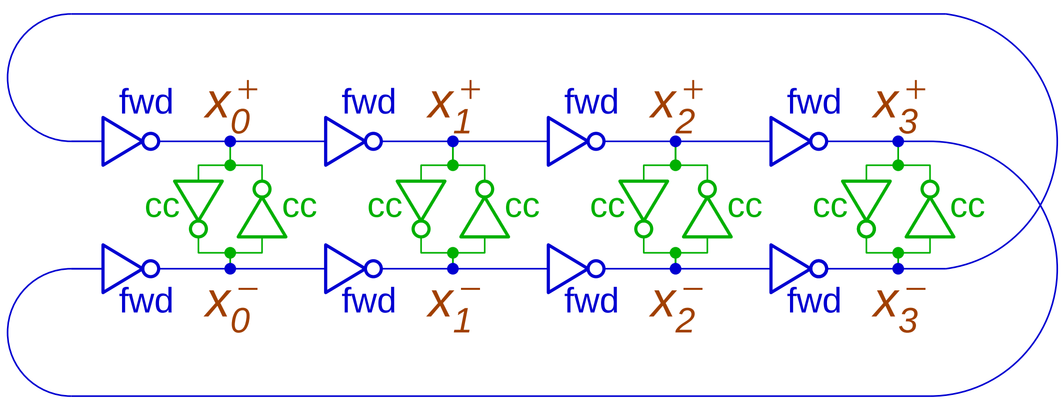
Step 3. Put it all together

- Perform reachability computations from remaining cubes only.
- Note we use 2-dim inclusion models
- Avoid repeated computations
  - Only check cubes on boundaries: trajectories can't cross
  - Partition the state space by 16 "spokes"



Results

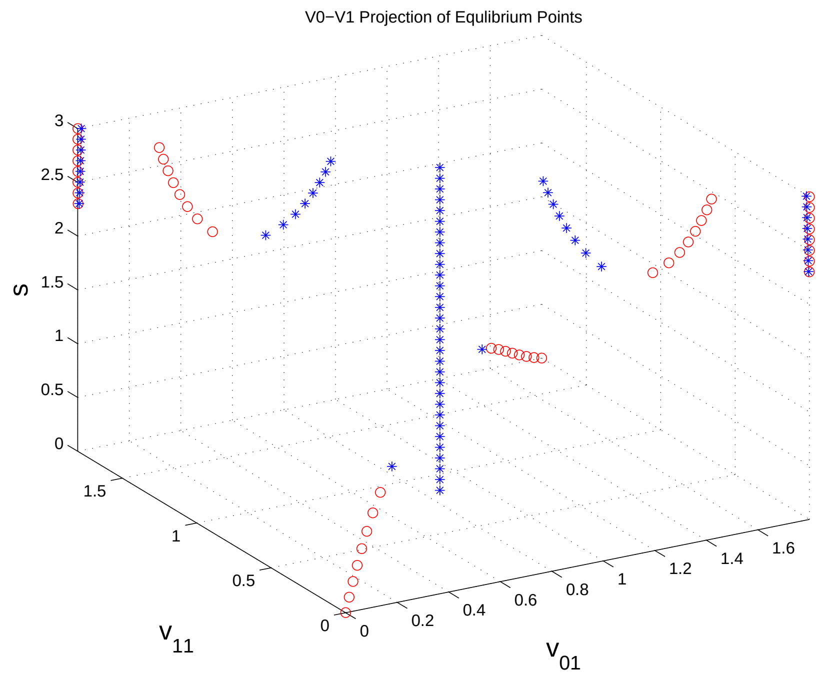
- Verification with equal-size inverters
  - The oscillator is formally verified, i.e. no higher harmonic oscillations or chaotic behavior
  - Reachability computation is less than 5 minutes
- Verification for a range of sizes
  - Use conservative over-approximation to guarantee soundness of the results
  - Oscillators with $0.67 \leq s \leq 2.0$ are formally verified
    $s = \frac{\text{size of cross coupling inverters}}{\text{size of forward inverters}}$



Conclusion

- Measure-theory can be combined with standard reachability methods to formally verify real analog circuits.
  - Reachability analysis can be combined efficiently with dynamical system analysis to show global convergence
  - No physically plausible oscillator starts from all initial conditions
  - Present a general method to prove that the failures occur with probability zero
  - Differential operations can be exploited for model reductions
- Future Work
  - Apply our method to more state-of-the-art process (e.g. PTM models)
  - Use interval-arithmetic for Phase II
  - Verify ring oscillator with more (6+) stages (may have higher harmonic modes)
  - Parameterized verification
  - Verify other practical analog circuits from industry

Prior Work



- Small Signal Analysis [Greenstreet *et al.*]
  - Finds all DC equilibrium points and detects if any are stable.
  - The oscillator is free from lock-up for $0.625 < s < 2.25$
  - A necessary condition but is NOT sufficient to prove correct operation
  - Can not ensure no global convergence failures, e.g. harmonic behaviors?