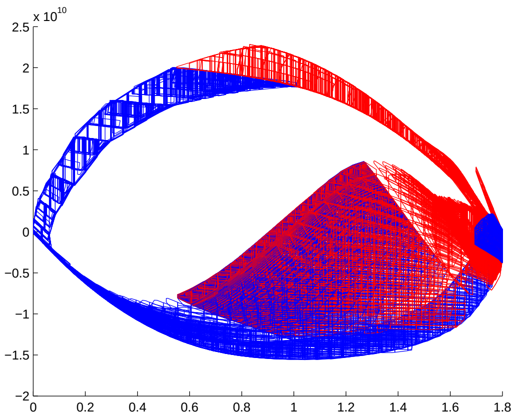
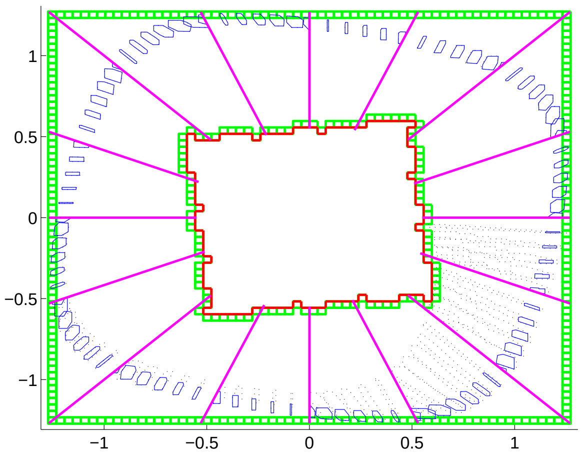
Circuit Verification by Projectagon Based Reachability Analysis

Chao Yan

The University of British Columbia





Outline

- Motivation
- Related Work
- COHO and Verification Flow
- Examples
  - Synchronous: Toggle Circuit, Latch and Flip-Flop
  - Asynchronous: Arbiter Circuit
  - Analog: Rambus Ring Oscillator
- Conclusion and Future Work

Overview

- Motivation
  - Simulation: coverage, expensive
  - Formal verification
  - Circuit-level verification
- Challenges
  - How to model circuits?
  - How to specify properties?
  - How to represent regions?
  - How to compute system states?
- Our Approach
  - Model circuit as non-linear ODEs
  - Brockett's annulus
  - Projectagon
  - COHO algorithm

Related Tools

- Related Work
  - Real-time System: UPPAAL, KRONOS
    - verify safety and liveness properties of timed automata
    - discrete states
  - Hybrid System: HYTECH, PHAver, d/dt, CheckMate, etc.
    - model systems with switched, continuous dynamics
    - models must be either linear or very low dimension
  - Control System: VeriSHIFT, Level Set
    - VeriSHIFT uses ellipsoidal methods, only works with linear systems
    - level sets limited to low dimensions because boundary must be computed explicity.

Related Techniques

- System Model
  - Hybrid automata
    - state machine augmented with continuous dynamics
    - timed automata, linear hybrid automata, nonlinear hybrid automata, etc.
  - Transition system
    - abstracted as states and transition
    - bisimulation
  - Hybrid Petri net
    - combine discrete Petri nets and continuous Petri nets
- Specification
- Space Representation
- Reachability Techniques

Related Techniques

- System Model
- Specification
  - Temporal logic
    - digital systems
    - LTL, CTL,etc
  - Timed logic
    - dense time
    - RTCTL, TCTL, MITL,etc
  - Real-value logic
    - uncountable state space
    - AnaCTL, CTL-AT, CTL-AMS, ICTL, etc.
  - Others
    - digital or analog circuits
    - PSL, ASL, etc.
- Space Representation
- Reachability Techniques

Related Techniques

- System Model
- Specification
- Space Representation
  - Symbolic data structure
    - discrete states
    - BDD, CDD, etc.
  - Polyhedra
    - large number of faces, expensive operations
    - convex polytope, flow pipe
  - Hyper-rectangle
    - large approximation error
    - interval, face regions, ORH, orthogonal polyhedra, etc.
  - Zonotope
    - close under Minkowski sum, compact representation
    - order of zonotope increases
  - Others: ellipsoid, level set
- Reachability Techniques

Related Techniques

- System Model
- Specification
- Space Representation
- Reachability Techniques
  - Discretization
    - abstraction ignores analog characteristics
    - number of grids increases exponentially
  - Reachability analysis
    - constant ODE: mathematical solution
    - linear ODE: optimal control, Minkowski sum
    - nonlinear ODE: hybridization, interval, error analysis, level set, etc
  - Bisimulation
    - construct a finite-state transition system
  - Compositional reasoning
    - reduce system complexity

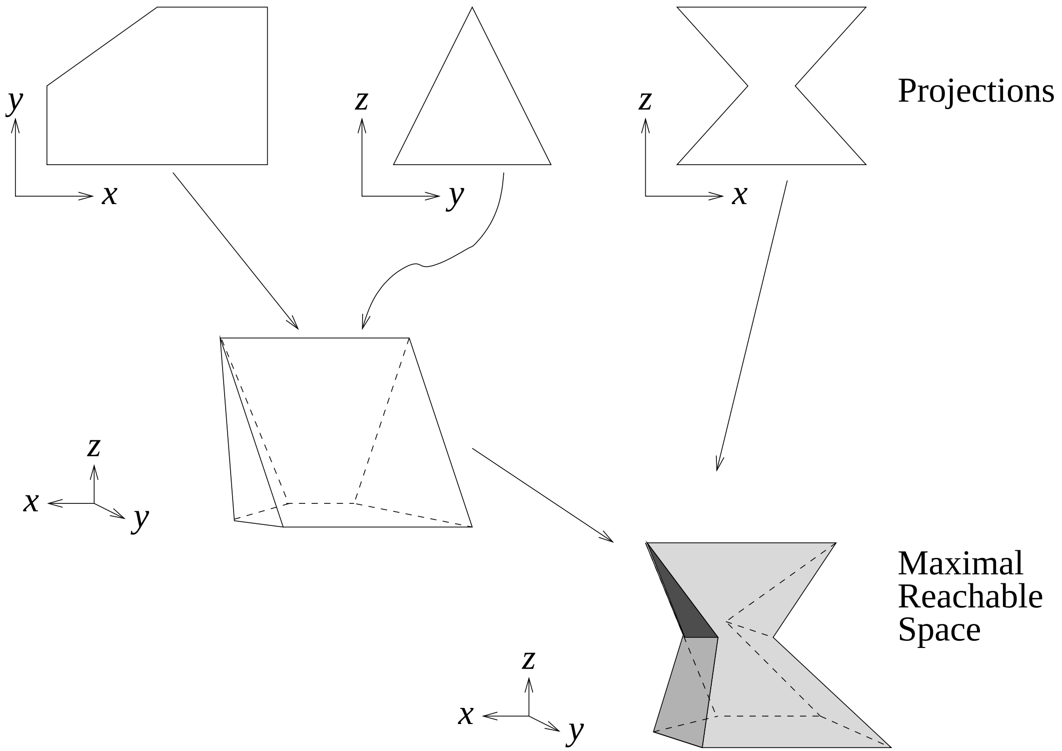
Applications

- Hybrid Systems
  - low dimensional or linear systems
- Circuits
  - tunnel-diode oscillator
  - voltage controlled oscillator
  - delta-sigma modulator
- Limitations
  - Small demo examples
  - Abstracted circuit models
  - Does not support circuits directly

COHO: A Reachability Analysis Tool

- Representing and manipulating high-dimensional space: projectagon
  - Provides a tractable representation.
  - Exploits extensive algorithms for 2D computational geometry.
- Solving dynamic systems: linear differential inclusions.
  - Approximate nonlinear ODE by $\dot{v} \in Av + b \pm u$, where u is an error term.
  - Solved by *Maximum Principle* without integration.
- All approximations overapproximate the reachable space:
  - COHO is sound for verifying safety properties.
  - False negatives are possible.
- Stability, performance and accuracy
  - COHO LP solver and projection algorithm
  - Interval closure
  - Guess-verify strategy

Projectagon



- COHO projects high-dimensional polyhedron onto two-dimensional subspaces.
- Projectagons are efficiently manipulated using two-dimensional geometry computation algorithms.
- Projectagon faces correspond to projection polygon edges.

Solving dynamic systems

- Given a region represented by

$$Px \leq q$$

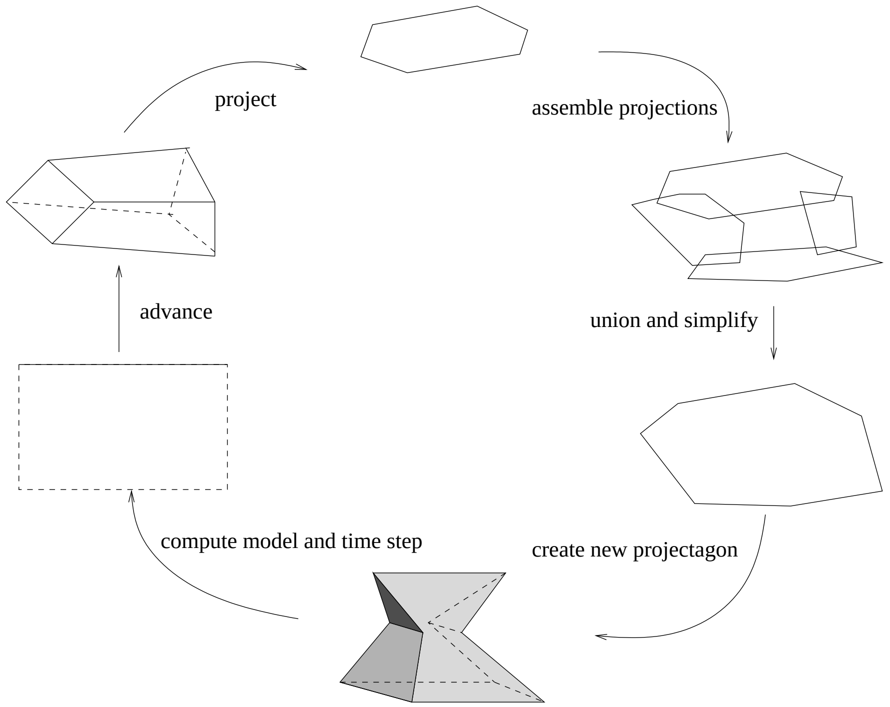
- Approximate non-linear ODE in the region by

$$\dot{x} \in Ax + b \pm u$$

- Compute foward reachable region using *Maximum Principle* as

$$\begin{aligned} PEx &\leq \hat{q} \\ E &= e^{-At} \\ \hat{q} &= q + P(I-E)A^{-1}q + P(I-E)A^{-1}q \cdot *sign(P)u \end{aligned}$$

Basic Step of COHO



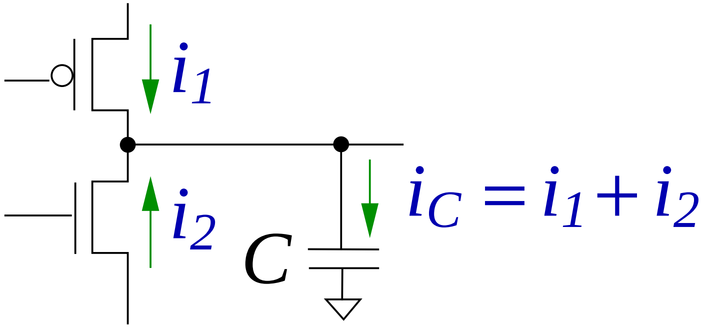
- Extremal trajectories original from projectagon faces.
- A bounding projectagon is obtained by moving each face forward in time.
- The advanced face is projected onto two-dimensional subspaces to maintain the structure of projectagon.

Verification of AMS Circuits

- Support AMS circuit verification directly
  - Modeling circuits as ODE systems
  - Abstracting signals by Brockett's annulus
- Integration with COHO
  - Simulation and Verification
  - Linear differential inclusion
    - Least square method
    - Quadratic interpolataion method
  - Error and Performance
    - Multiple models
    - Partitioning state space
    - Assume-guarantee strategy
    - Decompose complex circuits

Circuit Model

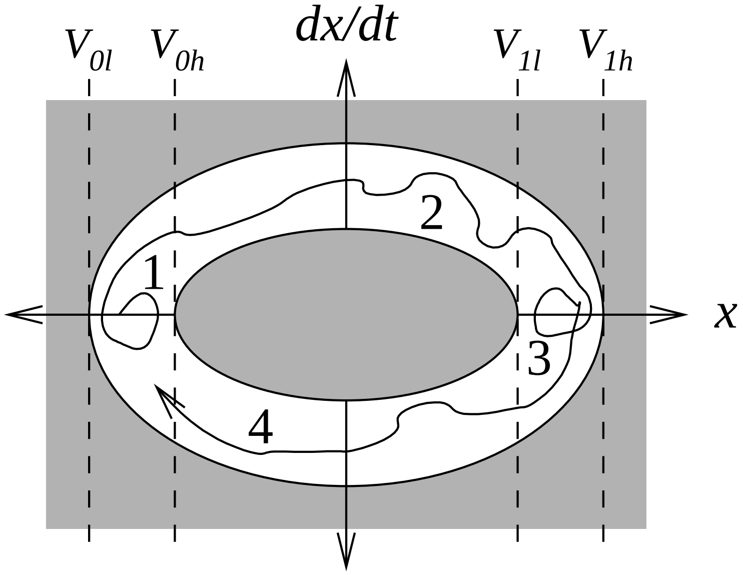
- Transistors modeled as voltage controlled current sources.
- The I_{ds} function is obtained by tabulated data from HSPICE simulations.



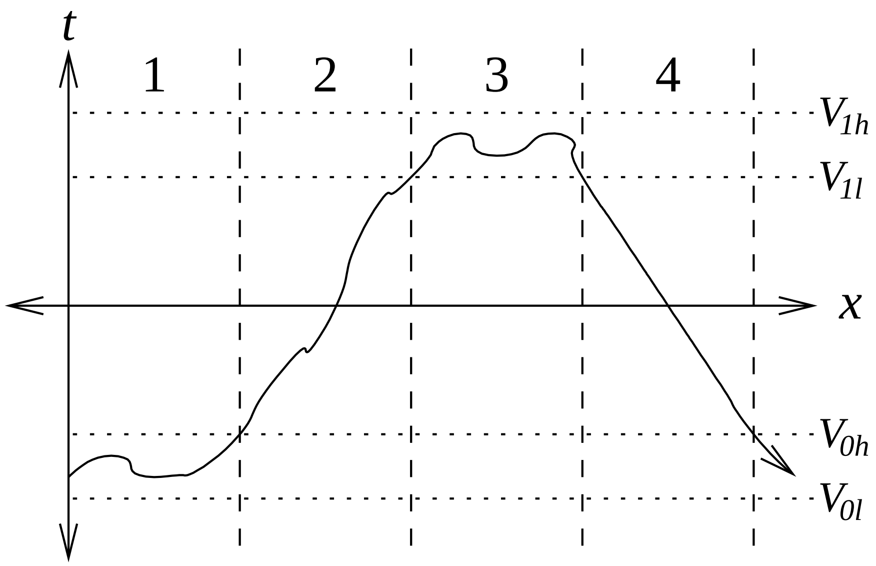
- Construct system ODEs automatically
  - computes a model of the form $i_1 = A_1 v + b_1 \pm u_1$. Likewise for i_2.
  - bounds $i_c = (A_2 + A_2)v + (b_1 + b_2) \pm (u_1 + u_2)$.
  - $\dot{V} = C^{-1} \cdot I$
- Approximate the ODEs by *linear differential inclusions*:

$$A \begin{bmatrix} v \\ in \end{bmatrix} + b - u \leq \dot{v} \leq A \begin{bmatrix} v \\ in \end{bmatrix} + b + u$$

Brockett’s Annulus



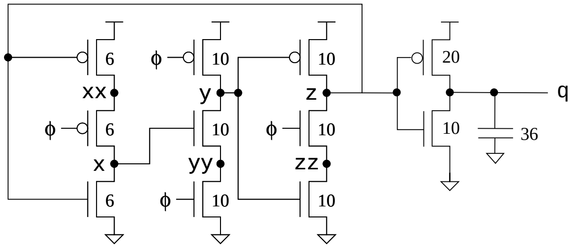
The Annulus



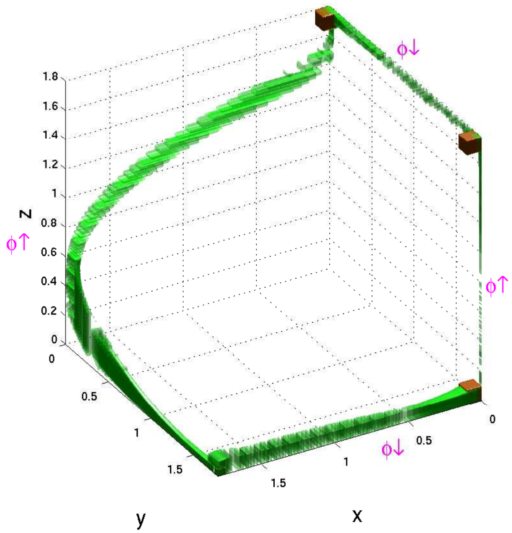
A "typical" trajectory

- Region 1 represents a logical low signal. The signal may wander in a small interval.
- Region 2 represents a monotonically rising signal.
- Region 3 represents a logical high signal.
- Region 4 represents a monotonically falling signal.
- Brockett’s annulus allows entire families of signals to be specified.

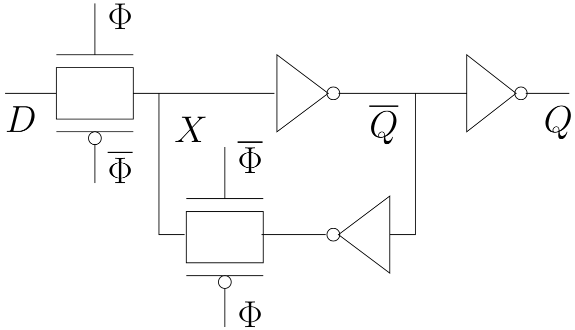
Examples: Toggle Circuit

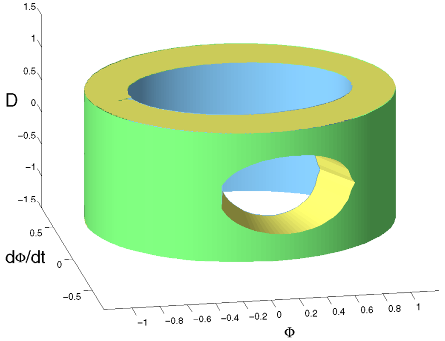


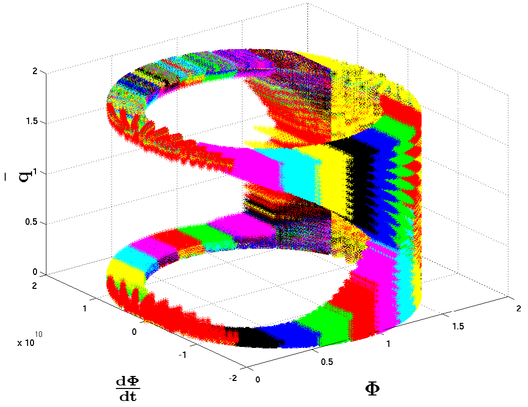
- Challenge
  - Seven dimensional system
  - Circuit-level model
- Solution
  - Divide reachability computation into phases
  - Partition state space
  - Add keeper circuit
- Result
  - The period of output is twice that of the clock
  - The output satisfies the same brockett annulus of the clock ⇒ a ripper counter



Latch Circuit

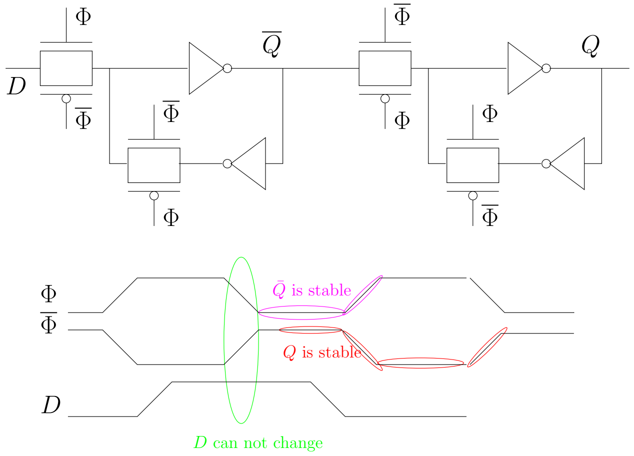






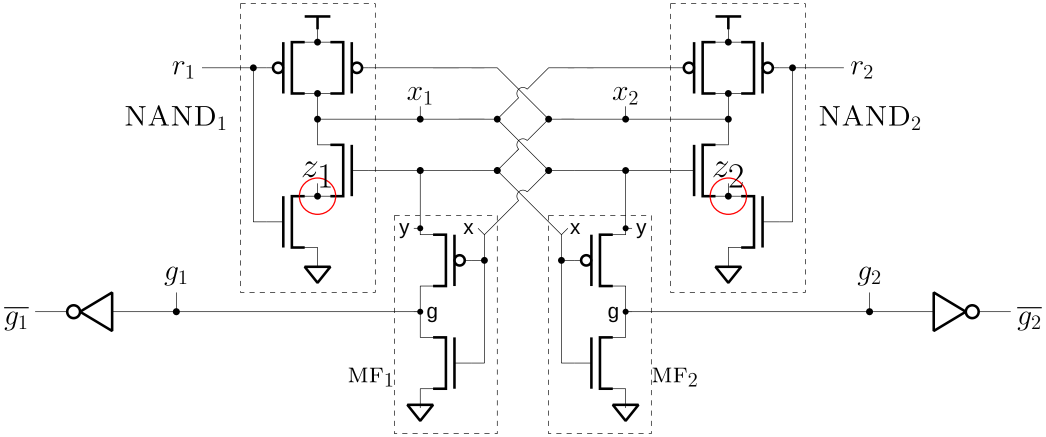
- Challenge
  - One input and one clock signal
- Solution
  - Partition state space
- Result
  - Input Specification: input signal can not change when the clock falls
  - Output Specification: output signal is stable when the clock is clear low or rising

Latch Circuit



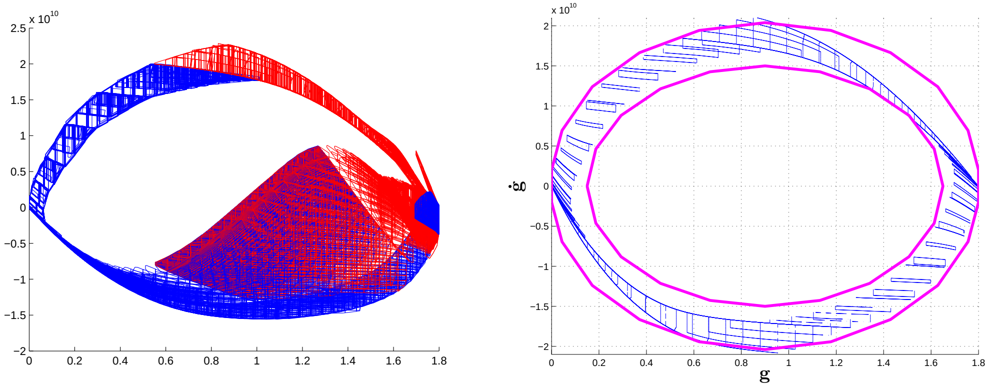
- Challenge
  - One input and one clock signal
- Solution
  - Partition state space
- Result
  - The upper bound of clock-to-q delay is 200ps
  - Clock frequency is up to 1.3GHz

Arbiter



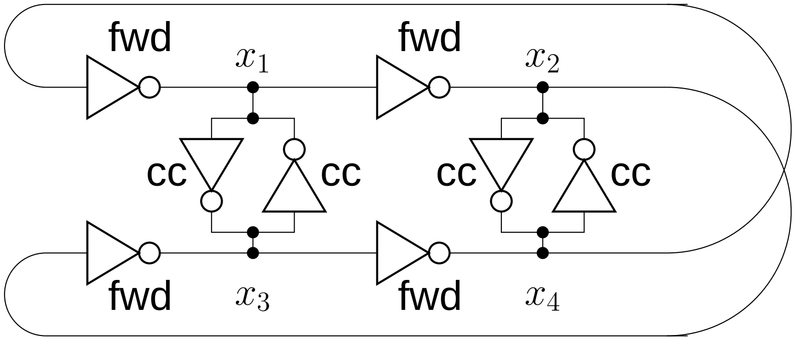
- Challenge
  - Asynchronous inputs
  - Stiffness
  - Metastability
- Solution
  - Changing variables, pre-computed constraints
  - Almost surely verification
- Result

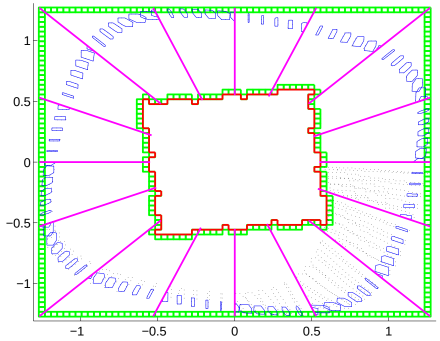
Arbiter



- Challenge
- Solution
- Result
  - Safety Properties
    - Mutual exclusion,
    - Handshake protocol,
    - Brockett annulus specification
  - Liveness Properties
    - Initialization, Uncontested Requests, Contested Request
    - Reset, Fairness

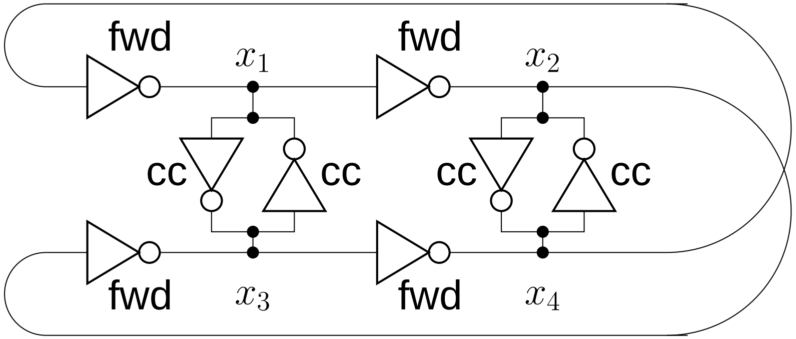
Rambus Oscillator

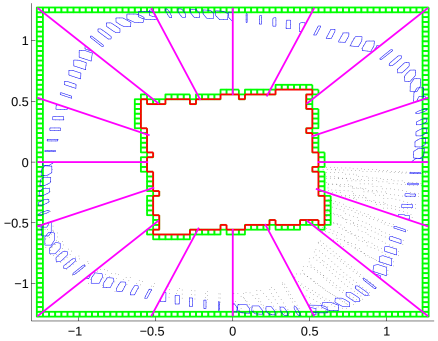




- Challenge
  - Analog circuit
  - Failures have been observed for real chips
  - All possible initial conditions
- Solution
  - Differential Operation: coordinate transformation, space reduction
  - Metastable Region: Almost-surely verification?
  - Reachability Analysis: 4D → 2D

Rambus Oscillator





- Problems to be solved
  - A general solution for high-dimensional metastability problem
    - current condition is not correct
    - sufficient condition is too conservative
  - Extend the method to n-stage Rambus oscillator
    - much more expensive computation
    - harmonic behaviors
  - Verifying other ring oscillators
    - similar structure
    - shifting equilibrium points

Contributions

- A robust and efficient implementation of COHO tool.
  - A projection based representation of high dimensional, non-convex regions
  - Reachability algorithms for linear differential inclusion
  - Interval computation and arbitrary precision rational arithmetic
- A framework of modeling and verifying circuits
  - Model a circuit as a system of non-linear ODEs
  - Use Brockett's annulus to represent a family of signals
  - Techniques to reduce approximation error and improve performance
- Examples of practical circuit verification
  - Synchronous circuits: toggle circuit, latch and flip-flop
  - Asynchronous circuit: arbiter circuit
  - Analog circuit: Rambus ring oscillator

Projectagon based reachability analysis can formally verify digital and analog circuits using nonlinear, ordinary differential equation models.

Research Plan and Time line

- Research plan
  - Release COHO to public research community
  - Solve the metastability problem in the Rambus oscillator's verification
  - Extend the Rambus oscillator verification to other oscillators
  - Apply to other hybrid systems or analog circuits
- Timeline
  - Jun. 2: proposal defense
  - Oct. 1: thesis to committee
  - Nov. 1: thesis to FOGS
  - Feb. 1, 2011: defend

Conclusions

- Formal methods are extended to circuit-level verification
  - Implemented an efficient and robust reachability analysis tool
  - Developed a verification flow for circuit
  - Verified synchronous, asynchronous and analog circuits
- Graduation plan
  - Research is 90% done
  - Clean up the code and fix the problem of oscillator verification
  - Plan to graduate in early 2011