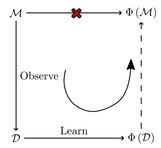
Model-based Specification Reconstruction

A. Porter (UMD PI & Director), M. Lindvall (Fraunhofer PI), S. Huang, M. Diep, J. Kristjansson, A. Kyei, R. Cleaveland, NSF CNS 1446583
aporter@cs.umd.edu, mikli@fc-md.umd.edu, srhuang@cs.umd.edu, MDiep@fc-md.umd.edu,
JKristjansson@fc-md.umd.edu, akyei@fc-md.umd.edu, rance@cs.umd.edu

Specification Reconstruction

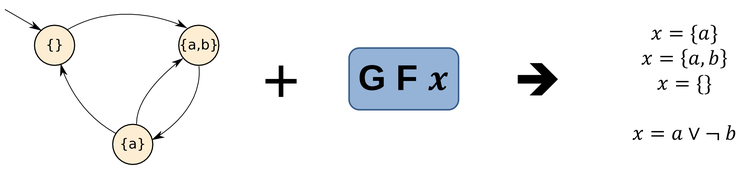
- Given: a system model M
- Goal: identify properties of behavior of M
- Two approaches:
  - Query checking of model
  - Data mining from system executions



Query Checking

- Using formula templates such as
  $\phi[x]$:= "Condition x always holds"
  find solution for x such that $\phi[x]$ is satisfied by M
- Many solutions can exist, determine extremal (strongest or weakest) solutions
- Hard in general case, finding some solutions is not so bad!

Model M **Template $\phi[x]$** **Solutions**



Invariant Reconstruction of Heart Models

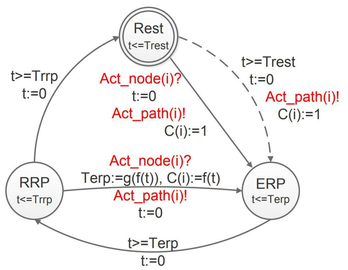
- Cyberphysical systems are represented in multiple forms while developed:

Possible development cycle

- Transitioning between forms → incongruencies!

Design requirement — Model invariant

- Clarification between invariant sets is needed!



Portion of an automaton model for a heart

Q: Does a model such as the one to the left exhibit certain properties we need?

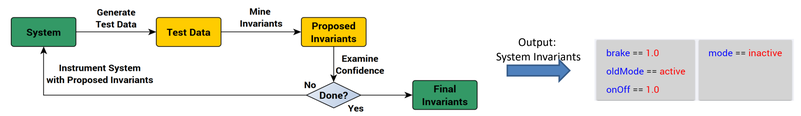
```
prevTRRP_cur == One ->
  Active == NotActive

inActive == NotActive & prevState ==
ERPState & prevTRRP_cur == Zero ->
  State == RestState
```

Invariants inferred from the automaton

Automatic Invariant Inference of Models

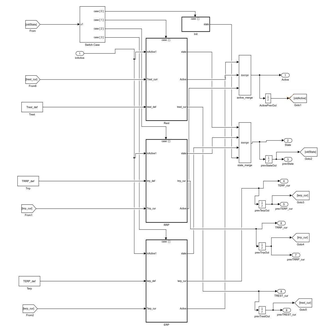
- Given: A CPS system as a model M
- Goal: Automatic inference of invariants from M
- Can help to identify problems in design pipeline
- Current methodology – Specstractor
  - Iterative approach based on test case generation and data mining



- Invariants take the form of horn clauses:
  - `Prop_a && prop_b .. && prop_n → consequent`

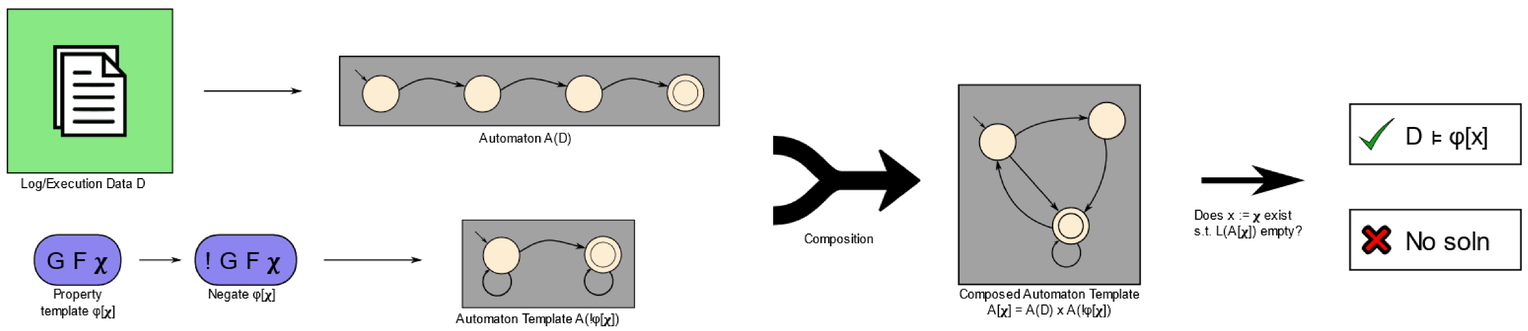
Empirical Work

- Investigating models of heart and pacemakers
  - Heart Models: Can we verify properties? (tachycardia, bradycardia, etc)
  - Pacemakers: Can we discover properties? (bugs, unexpected behavior)
- Currently using MATLAB/Simulink models from literature
- Evaluating mined invariants against known properties of the heart
- Goal: identify invariants that are ultimately useful to an expert/researcher



Portion of a Heart Model in MATLAB/Simulink

Query Checking of System Executions



- Execution data is converted into an automaton accepting finite length inputs
- Use "Finite Linear Temporal Logic" to represent properties
  - Works naturally over finite streams
  - Constructed to have strong similarities to standard LTL
- Determining a solution x is done using graph theoretic analysis coupled with data mining.
- Pilot study done using web server log data with known properties
- Investigating applications to heart data as well (eg. Diagnostic output of pacemakers)

References

- Huang S., Cleaveland R. (2017) Query Checking for Linear Temporal Logic. In: Petrucci L., Seceleanu C., Cavalcanti A. (eds) Critical Systems: Formal Methods and Automated Verification. FMICS 2017, AVoCS 2017. Lecture Notes in Computer Science, vol 10471. Springer, Cham
- Christoph Schulze and Rance Cleaveland. 2017. Improving Invariant Mining via Static Analysis. ACM Trans. Embed. Comput. Syst. 16, 5s, Article 167 (September 2017), 20 pages. DOI: https://doi.org/10.1145/3126504