Property Synthesis

Barbara Jobstmann
Graz University of Technology, Austria
Advisor: Roderick Bloem

HDL from Specification

Background:

- Automatic construction of correct functional HDL design from spec
- Specification given as properties in linear logic (e.g., LTL, PSL, SVA)
- LTL synthesis well studied but considered too hard: no implementations thus far

Contributions:

- First implementation of a synthesis algorithm for full LTL (see below)
- Application of synthesis techniques to repair problem (see box on the right)

Application: Repair

Problem:

- Faulty finite-state system (program or circuit),
- Formal specification in LTL

Aim:

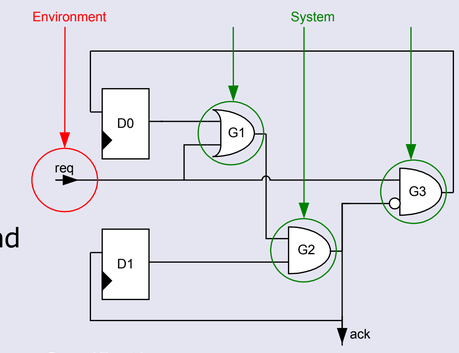
- Correct system
- Simple repairs

Idea:

- Remove potentially faulty parts and synthesize them again [JGB05]

Solution:

- Modify system to infinite game
- Then find right choices (similar to controller synthesis)



Specification:
G(req →(ack ∨ X(ack)) ∧ (ack→¬X(ack)))
Fault: fails on two consecutive requests
G2 should be G1 ∧ ¬D1

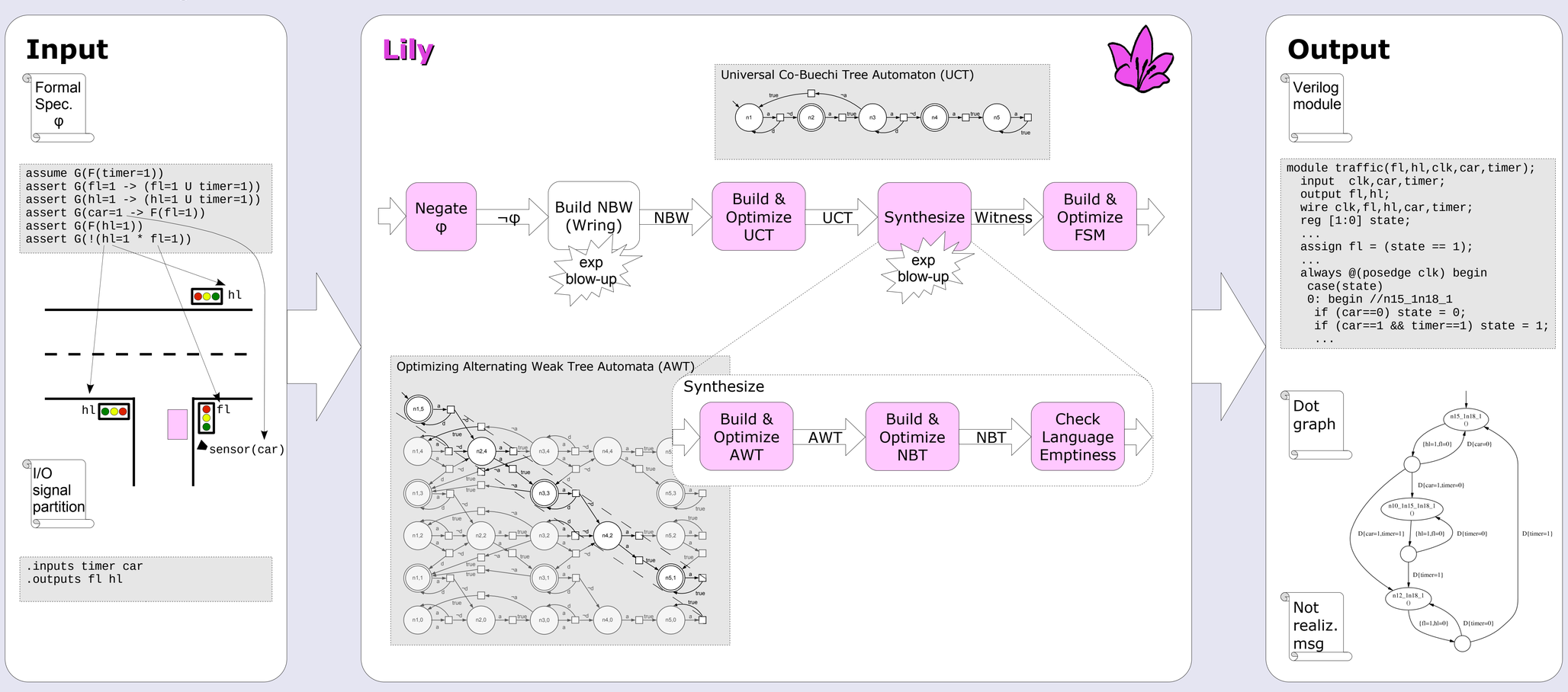
Optimizations for LTL Synthesis

Lily (LInear Logic sYnthesizer):

- First tool to offer synthesis for full LTL
- Based on a translation through universal co-Buechi tree automata and alternating weak tree automata proposed by Kupferman and Vardi [KV05], which avoids Safra's determinization construction
- Carefully optimizes all intermediate automata [JB06]. Optimizations are the enabling factor. See box below.

Applications:

- Property debugging (simulation, satisfiability vs. realizability)
- Working environment
- Prototyping (on block level)



List of Optimizations

- Game-based approximation for language emptiness of tree automata
- Extensive use of simulation relation for word and tree automata
- Exploit equivalence classes and simulation relation during Miyano-Hayashi's (MH) construction
- Incremental MH construction with language emptiness check
- Merge Edges (simplifies 'release' function)
- Stay in odd ranks (simplifies 'release' function)
- Increase rank incrementally and reuse the results

This work was supported in part by the European Union under contract 507219 (PROSYD).

Some References

[KV05] O. Kupferman and M. Vardi. Safraless Decision Procedures. In Proc. of the Symposium on Foundations of Computer Science (FOCS'05), 2005.
[JGB05] B. Jobstmann, A. Griesmayer, and R. Bloem. Program Repair as a Game. In Proc. of the Conference on Computer Aided Verification (CAV'05), 2005.
[SJB05] S. Staber, B. Jobstmann, and R. Bloem. Finding and Fixing Faults. In Proc. of the Conf. on Correct Hardware Design and Verification (CHARME'05), 2005.
[JB06] B. Jobstmann and R. Bloem. Optimizations for LTL Synthesis. In Proc. of the Conf. on Formal Methods in Computer-Aided Design (FMCAD'06), to appear.