Synthesizing Robust Systems

Roderick Bloem, Karin Greimel, Thomas A. Henzinger and Barbara Jobstmann
TU Graz, EPFL, IST Austria

Motivation

Tower controls ≤ 100 airplanes

What happens with the 101st plane?

1) System shut down.
2) Ignore 101st plane.
3) Control 101 planes, accepting a system slow down.

A. M. Davis. *Software Requirements — Analysis and Specification.* Prentice Hall, 1990.

Contributions

– Robust System

– Ratio Games

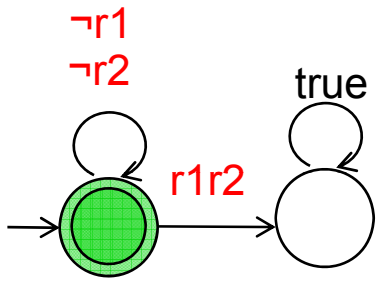
Specification of Arbiter

r1, r2 …requests, input signals

g1, g2 …grants, output signals

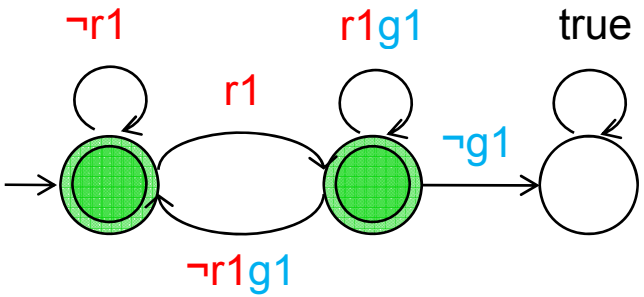
$A \rightarrow G1 \wedge G2 \wedge G3$

$A = G \neg (r1 \wedge r2)$

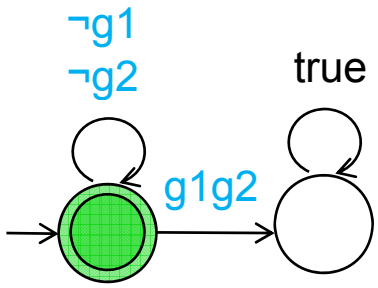


$G1 = G(r1 \rightarrow Xg1)$

$G2 = G(r2 \rightarrow Xg2)$



$G3 = G \neg (g1 \wedge g2)$



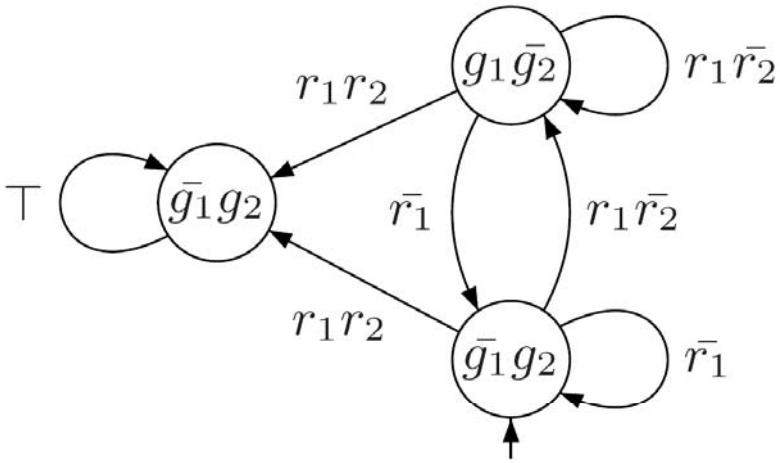
Specification

Words satisfying $A \rightarrow G1 \wedge G2 \wedge G3$

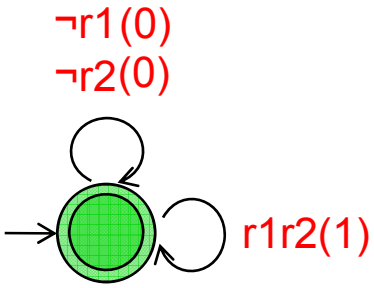
g1	0 0 1 1 1 1 …	g1	0 0 0 0 0 0 …
g2	1 1 0 0 0 0 …	g2	1 1 1 1 1 1 …
r1	0 1 1 1 1 1 ...	r1	0 1 1 1 1 1 ...
r2	0 0 0 0 0 0 ...	r2	0 1 0 0 0 0 ...

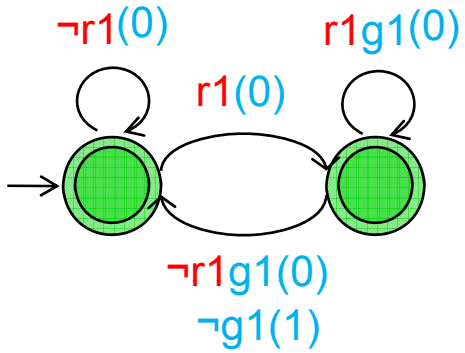
g1	0 0 1 1 1 1 …	
g2	1 1 0 0 0 0 …	
r1	0 1 1 1 1 1 ...	
r2	0 1 0 0 0 0 ...	

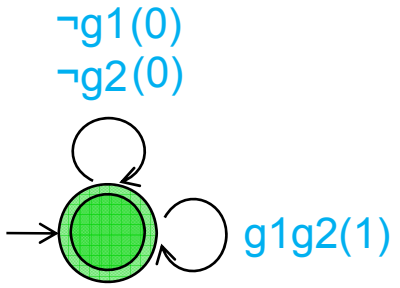
Automatically synthesized Moore machine for $A \rightarrow G1 \wedge G2 \wedge G3$



Error specification







The *error* of a word is the sum of its costs:

g1	0	0	1	1	1	1	…
g2	1	1	0	0	0	0	…
r1	0	1	1	1	1	1	...
r2	0	0	0	0	0	0	...

System error: 0
Environment error: 0

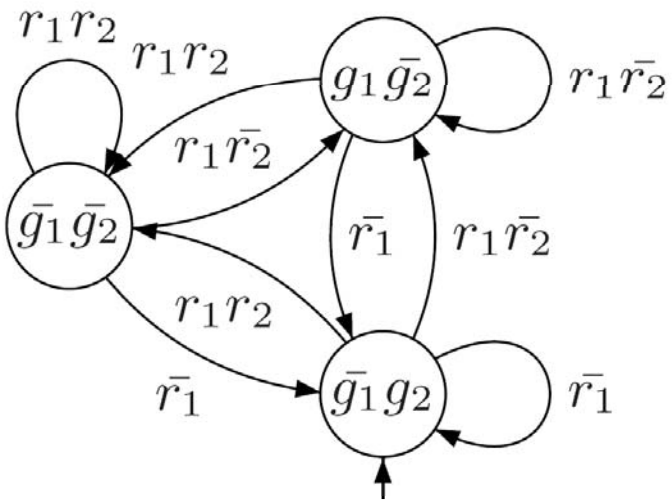
g1	0	0	0	0	0	0	…
g2	1	1	1	1	1	1	…
r1	0	1	1	1	1	1	...
r2	0	1	0	0	0	0	...

System error: ∞
Environment error: 1

An error specification is a double cost automaton.

Robustness

Definition: A Moore machine is *robust* if for all words w:
environment error is finite → system error is finite.



g1	0	0	0	1	1	1	…
g2	1	1	0	0	0	0	…
r1	0	1	1	1	1	1	...
r2	0	1	0	0	0	0	...

System error: 2
Environment error: 1

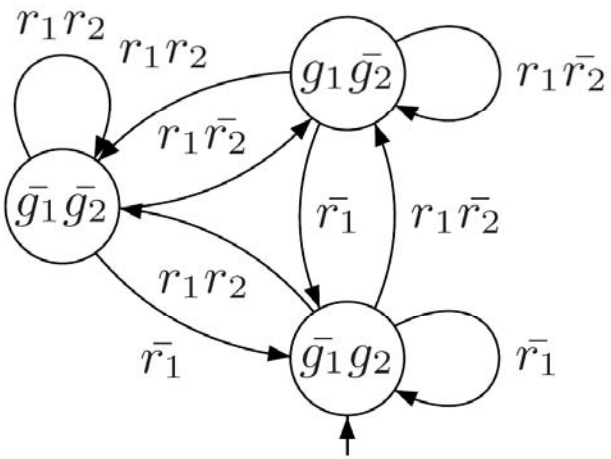
Synthesizing a robust system

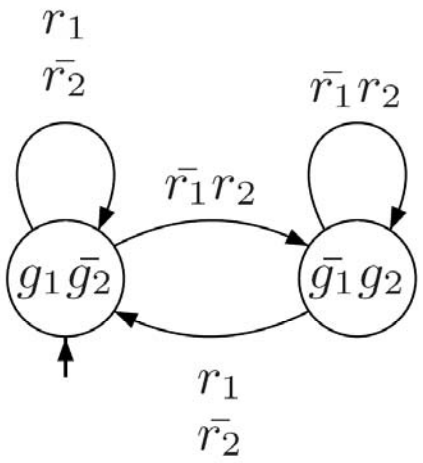
- Translate the error specification into a Streett game with one pair, the winning condition is

  GF sys_cost → GF env_cost.

- A winning strategy for the Streett game corresponds to a robust Moore machine.
- Streett games can be solved in quadratic time.

k-robustness





g1	0	0	0	0	0	0	0	0	…
g2	1	0	0	0	0	0	0	0	…
r1	0	1	0	0	0	1	0	0	...
r2	0	1	0	0	0	1	0	0	...

System error = **2** · Environment error

g1	1	1	1	1	1	1	1	1	…
g2	0	0	0	0	0	0	0	0	…
r1	0	1	0	0	0	1	0	0	...
r2	0	1	0	0	0	1	0	0	...

System error = **1** · Environment error

k-robustness

Definition: A Moore machine is *k-robust,* if for all finite prefixes of all w: system error ≤ k · environment error + d, for some finite d.

Formally:

$$\sum_{i=0}^{n} c_s(s_i, s_{i+1}) \leq k \cdot \sum_{i=0}^{n} c_e(s_i, s_{i+1}) + d$$

where $s_0\ s_1\ \ldots\ s_n$ is the run of a prefix of w on the error specification with system and environment costs c_s and c_e.

$$\lim_{m\to\infty} \limsup_{n\to\infty} \frac{\sum_{i=m}^{n} c_s(s_i, s_{i+1})}{1 + \sum_{i=m}^{n} c_e(s_i, s_{i+1})} \leq k$$

Ratio games

Definition: A *ratio game* consists of a game graph (S,s_0,E) and two weight functions c_s, c_e: $E \to \mathbb{N}$. The value function for a play $\rho = s_0\, s_1 \ldots$ in S^ω is

$$v(\rho) = \lim_{m\to\infty} \operatorname{limsup}_{n\to\infty} \frac{\sum_{i=m}^{n} c_s(s_i, s_{i+1})}{1 + \sum_{i=m}^{n} c_e(s_i, s_{i+1})}$$

- Player 1 (System) = min, Player 2 (Environment) = max.
- If $c_e(s_i,s_{i+1}) = 1$ for all (s_i,s_{i+1}) in E, then the ratio game is a *mean payoff game*

$$v'(\rho) = \operatorname{limsup}_{n\to\infty} \frac{\sum_{i=0}^{n} c(s_i, s_{i+1})}{n}.$$

Ratio games

- Ratio games have optimal positional strategies.
- Possible values of a state are 0, 1/|S|·C, ..., |S|·C/1, ∞, where C is the maximal value of c_s and c_e.
- We reduce the decision if v(s) ≤ a/b to the decision if the mean payoff value v'(s) ≤ 0 (NP ∩ co-NP):

  If the weight function in the mean payoff game is

  $c(s_i,s_{i+1}) = b \cdot c_s(s_i,s_{i+1}) - a \cdot c_e(s_i,s_{i+1})$, then

$$\lim_{m\to\infty} \limsup_{n\to\infty} \frac{\sum_{i=m}^{n} c_s(s_i,s_{i+1})}{1+\sum_{i=m}^{n} c_e(s_i,s_{i+1})} \le \frac{a}{b} \Leftrightarrow \limsup_{n\to\infty} \frac{\sum_{i=0}^{n} c(s_i,s_{i+1})}{n} \le 0$$

Summary

- Novel definition of Robustness
  - graceful degradation
  - error specifications

- Novel games: Ratio games
  - positional
  - reduction to mean payoff games
  - pseudopolynomial algorithm