Short Accepting Lassos & Witnesses in ω-automata

Rüdiger Ehlers

Saarland University, Reactive Systems Group

LATA 2010 – May 27, 2010

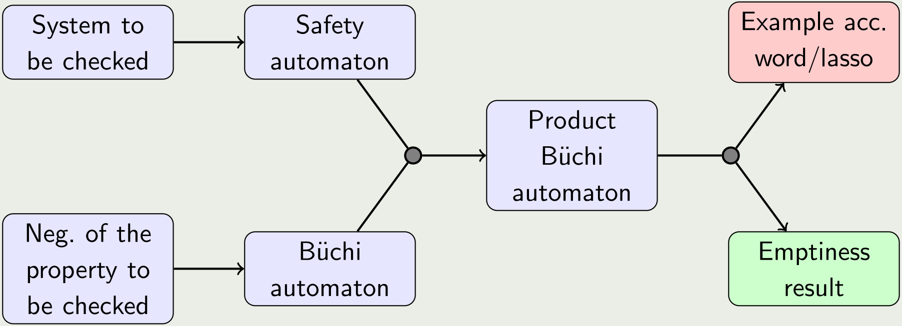
ω-automata

Basic properties

- Similar to ordinary finite automata
- Accept/reject infinite words $w \in \Sigma^{\omega}$
- Typical acceptance condition types: Safety, Büchi, Rabin, Streett, Muller, ...

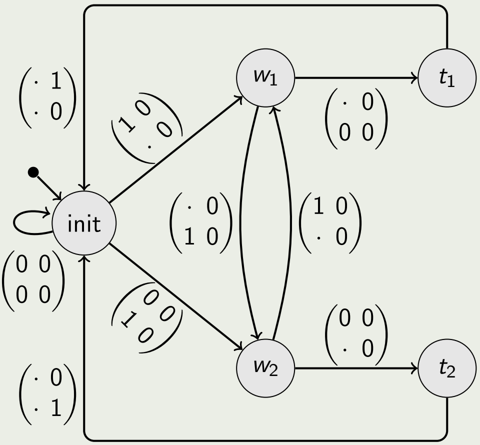
Automata theory & model checking

Overview

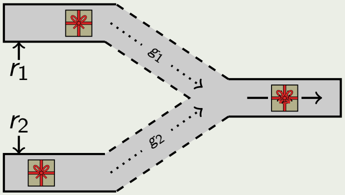


An example system

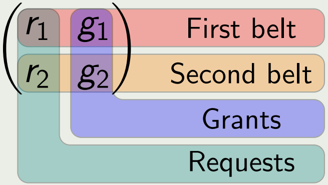
A conveyor belt merger controller



Setting



Alphabet semantics

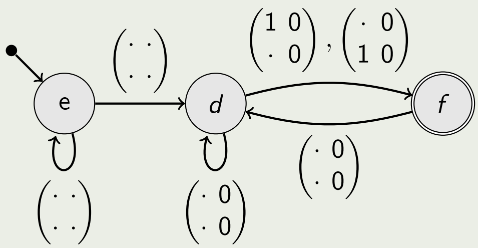


An example system

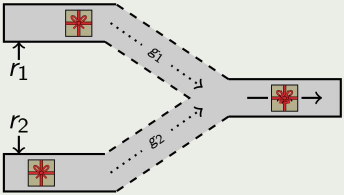
An example property

The system is starvation-free.

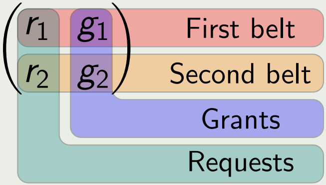
The corresponding neg. automaton



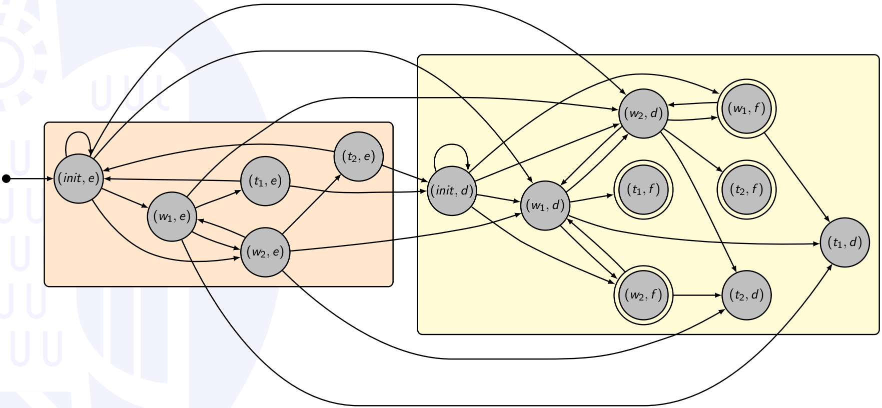
Setting



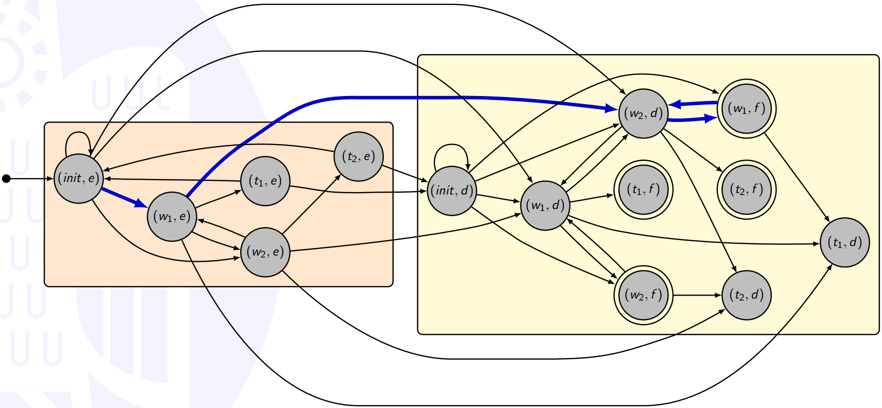
Alphabet semantics



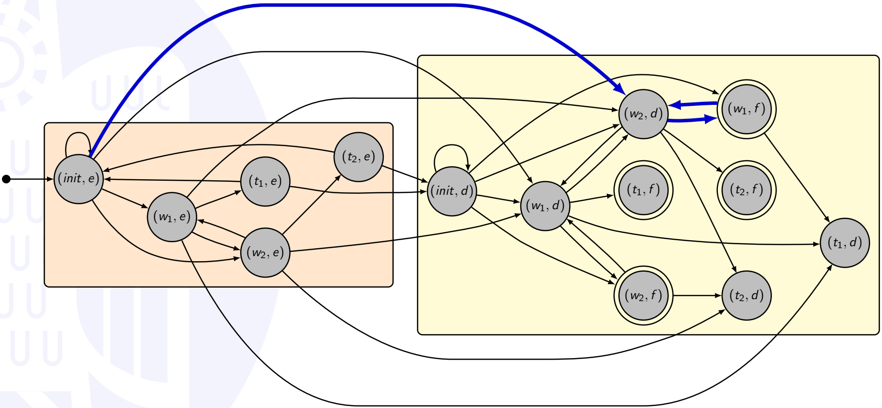
The product



Short lassos: an example



Short lassos: an example



An alternative point of view – short witnesses

A different kind of counter-examples

- Often, it is enough for the designer to know one erroneous example trace of the system.
- Such a trace can often be represented in a much shorter way.

An example

The conveyor belt merger behaves incorrectly with the following input/output:

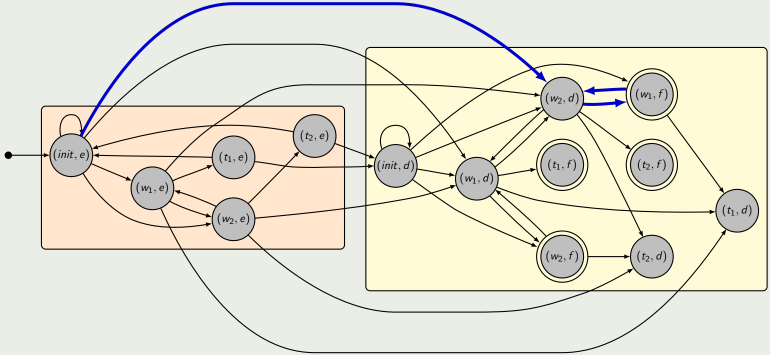
$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}^{\omega}$$

Conclusion

A "witness" is often much simpler to understand by the system designer.

Defining the size of a counter-example

Lassos



This lasso is of size **3**.

Witnesses

For uw^{ω} being the witness for $u, w \in \Sigma^*$, we define the size to be $|u| + |w|$.

Applications of short lassos & witnesses

Some examples:

- Model checking
- Certificates for the satisfiability of a formula in logics such as S1S
- Sanity checks of specification automata
- ...

Consequences

It makes sense to consider this problem for all commonly used types of acceptance conditions. **The main question we ask here is: what is the complexity of this problem?**

Previously known results

Direct results on the complexity of these problems previously known

Acc. cond. type	Short lassos	Short witnesses
Safety		
Büchi	$O(\|Q\|^2)$ [SE05]	NP-complete [KSF06]
co-Büchi		
Parity		
Rabin		
Gen. Büchi	NP-complete [CGMZ95]	
Streett		
Muller		

Previously known results

Implicit results on the complexity of these problems previously known

Acc. cond. type	Short lassos	Short witnesses
Safety	$O(\|Q\|^2)$	
Büchi	$O(\|Q\|^2)$	NP-complete
co-Büchi	in PTIME	
Parity	in PTIME	NP-complete
Rabin	in PTIME	NP-complete
Gen. Büchi	NP-complete	NP-complete
Streett	NP-complete	NP-complete
Muller		

Our completion of the landscape

All results now known

Acc. cond. type	Short lassos	Short witnesses
Safety	in PTIME	NP-complete
Büchi		
co-Büchi		
Parity		
Rabin		
Gen. Büchi	NP-complete	
Streett		
Muller		

On approximating shortest witnesses & lassos

In practice

For practical application, approximate shortest witnesses and lassos would usually suffice!

Important question: For those problems that are not in PTIME (assuming NP$\neq$PTIME), can they be approximated well in polynomial time?

On finding approximate short lassos

Overview

Acc. cond. type	Short lassos
Safety	in PTIME
Büchi	
co-Büchi	
Parity	
Rabin	
Gen. Büchi	This case
Streett	
Muller	

Generalised Büchi & Streett

Not approximable within any constant in polynomial time (unless P=NP).

Proof idea

Reduction to the Ek-Vertex-Cover problem

On finding approximate short lassos

Overview

Acc. cond. type	Short lassos
Safety	in PTIME
Büchi	
co-Büchi	
Parity	
Rabin	
Gen. Büchi	
Streett	
Muller	This case

The Muller case

Not approximable within $\frac{321}{320} - \epsilon$ (unless P=NP), **approximable within** $\lceil \log_2 |Q| \rceil$ in polynomial time.

Proof idea

Using the connection to the **asymmetric metric travelling salesman problem**.

On finding approximate short witnesses

Overview

Acc. cond. type	**Short witnesses**
Safety	NP-complete
Büchi	
co-Büchi	
Parity	
Rabin	
Gen. Büchi	
Streett	
Muller	

The safety case

Not approximable within any polynomial function in polynomial time (unless P=NP).

Proof idea

Reduction from the **satisfiability** problem using the **gap** technique.

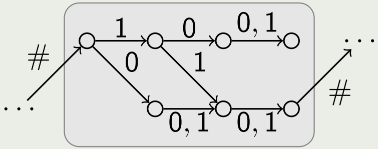
Proof idea for the shortest witness case

Reduction from the SAT-problem

Idea:

- Encode potential solutions to a SAT problem as words over $\{0, 1, \#\}$
- For every clause in the SAT problem, build a block requiring that a part of the word "satisfies" the clause.
- For every clause, put k of these blocks in a line (for some $k \in \mathbb{N}$) and plug together the lines for all clauses.

Example block for the clause $\neg v_1 \vee v_2$

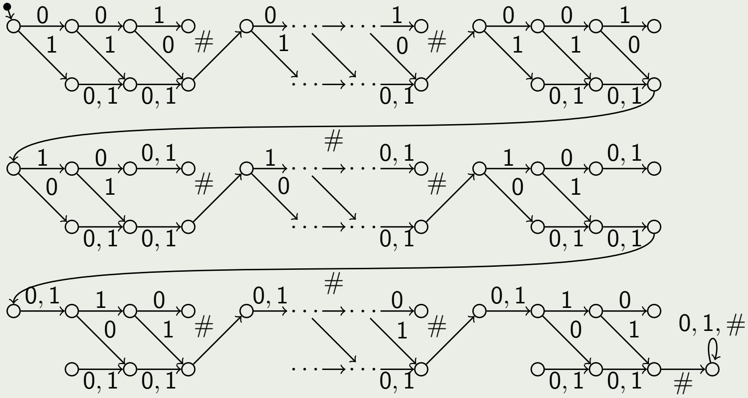


Shortest witness case - An example

SAT instance

$(v_1 \vee v_2 \vee \neg v_3) \wedge (\neg v_1 \vee v_2) \wedge (\neg v_2 \vee v_3)$

Safety automaton



Implications for practice

Counter-example generation for model checking

We can either:

- stick to the shortest lasso case (when applicable)
- try to use potentially slow techniques
- develop & use suitable heuristics

Outlook

Implications for **synthesis of open systems**

- Finding a small implementation satisfying a specification is a hard problem, even for safety games!

References

[CGMZ95] Edmund M. Clarke, Orna Grumberg, Kenneth L. McMillan, and Xudong Zhao. Efficient generation of counterexamples and witnesses in symbolic model checking. In *DAC*, pages 427–432, 1995.

[KSF06] Orna Kupferman and Sarai Sheinvald-Faragy. Finding shortest witnesses to the nonemptiness of automata on infinite words. In Christel Baier and Holger Hermanns, editors, *CONCUR*, volume 4137 of *LNCS*, pages 492–508. Springer, 2006.

[SE05] Stefan Schwoon and Javier Esparza. A note on on-the-fly verification algorithms. In Nicolas Halbwachs and Lenore D. Zuck, editors, *TACAS*, volume 3440 of *LNCS*, pages 174–190, 2005.