# Verification of ***Open*** Interactive Markov Chains

Tomáš Brázdil[1]
Holger Hermanns[2]
Jan Krčál[1,2]
*Jan Křetínský*[1,3,4]
Vojtěch Řehák[1]

[1] Faculty of Informatics, Masaryk University, Brno, Czech Republic
[2] Saarland University – Computer Science, Saarbrücken, Germany
[3] Institut für Informatik, Technische Universität München, Germany
[4] IST Austria

Highlights, Paris
September 19, 2013

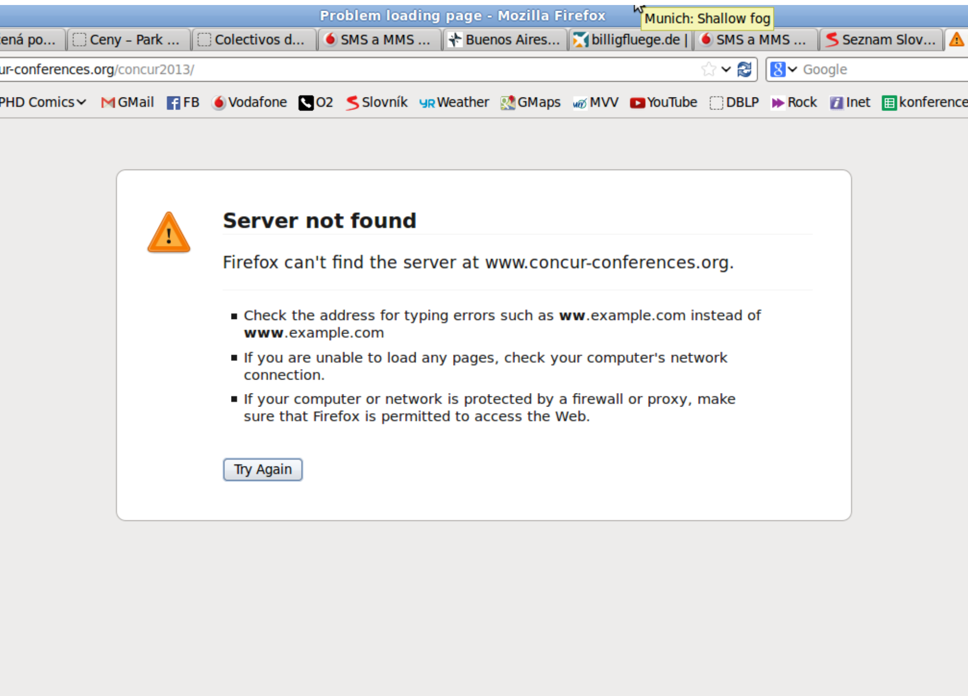
# Our contribution

The first assume-guarantee reasoning
for systems with stochastic continuous time

# Our contribution

The first assume-guarantee reasoning
for systems with stochastic continuous time

- given a system $S$,
  we compute guarantees on $S \parallel ?$
- we give a specification formalism to express assumptions
- given a system $S$ and assumptions $\varphi$ on its environment,
  we compute guarantees on $S \parallel \varphi$



## Server not found

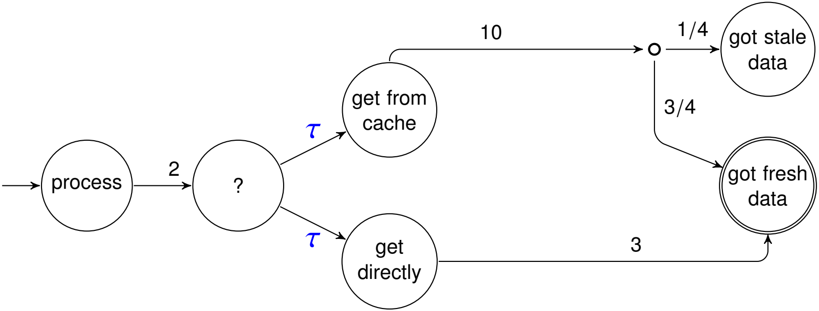
Firefox can't find the server at www.concur-conferences.org.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

# Guarantees in continuous-time stochastic systems

Synthesize optimal scheduler $\sigma$ of system $S$

$$\sup_{\sigma} \quad Pr_S^{\sigma} \quad [Reach \leq 1.5] = ?$$



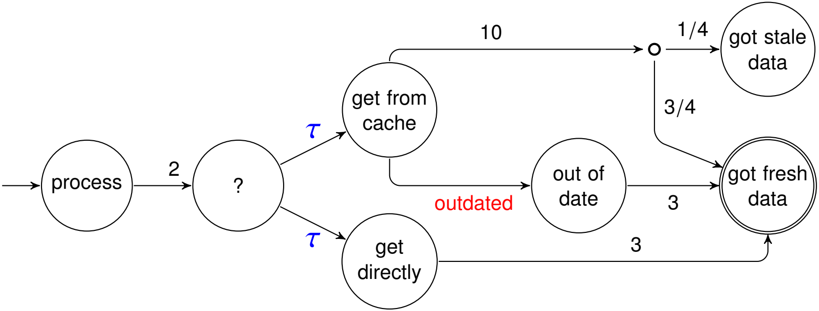
Interactive Markov chains

- similar to continuous-time Markov decision processes
- *compositional* process-algebraic framework

# Guarantees in continuous-time stochastic systems

Synthesize optimal scheduler $\sigma$ of system $S$

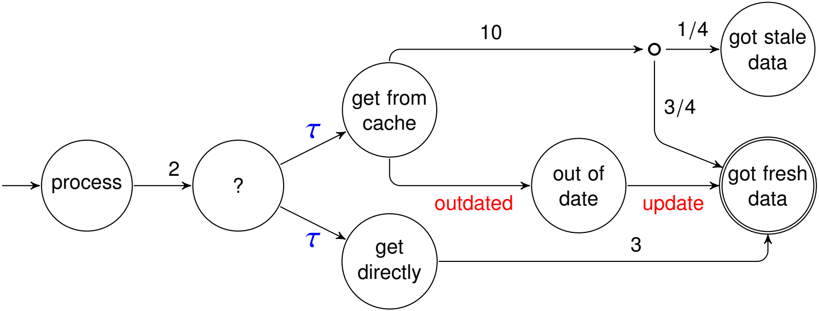
$$\sup_{\sigma} \inf_{E} Pr^{\sigma}_{S\|E}\,[Reach \leq 1.5] = ?$$



# Guarantees in continuous-time stochastic systems

Synthesize optimal scheduler $\sigma$ of system $S$

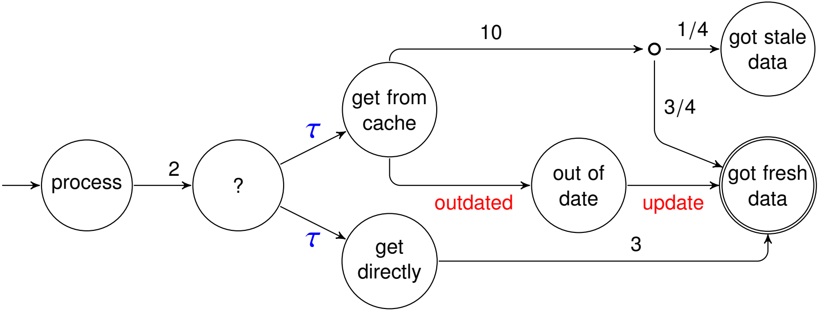
$$\sup_{\sigma} \inf_{E} Pr^{\sigma}_{S\|E} [Reach \leq 1.5] = ?$$



# Guarantees in continuous-time stochastic systems

Synthesize optimal scheduler $\sigma$ of system $S$

$$\sup_{\sigma} \inf_{E \models \varphi} Pr^{\sigma}_{S \| E}\,[Reach \leq 1.5] = ?$$

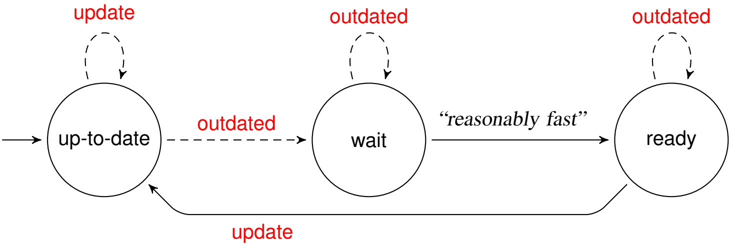


# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]

**Example:** after each outdated an update is ready *reasonably fast*



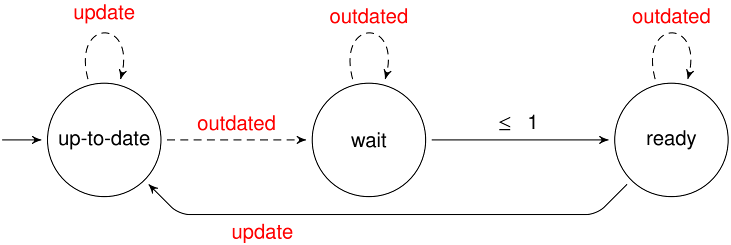
# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]

  extending timed automata [Alur,Courcoubetis&Dill'91]

**Example:** after each outdated an update is ready *reasonably fast*



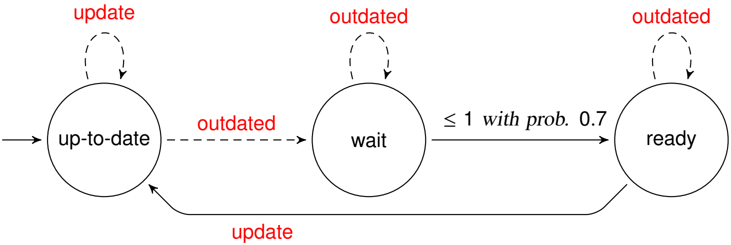
# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]

  extending timed automata [Alur,Courcoubetis&Dill'91]

**Example:** after each outdated an update is ready *reasonably fast*



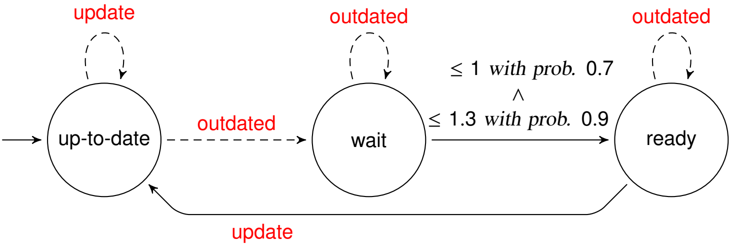
# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]

  extending timed automata [Alur,Courcoubetis&Dill'91]

**Example:** after each outdated an update is ready *reasonably fast*



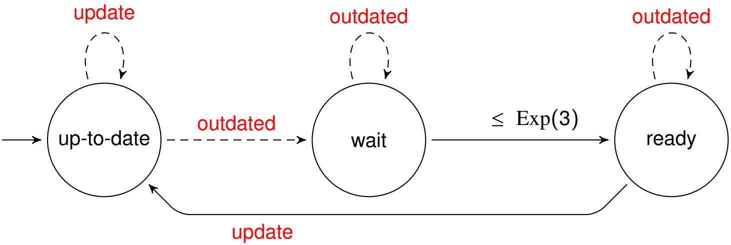
# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]

  extending timed automata [Alur,Courcoubetis&Dill'91]

**Example:** after each outdated an update is ready within time ~Exp(3)

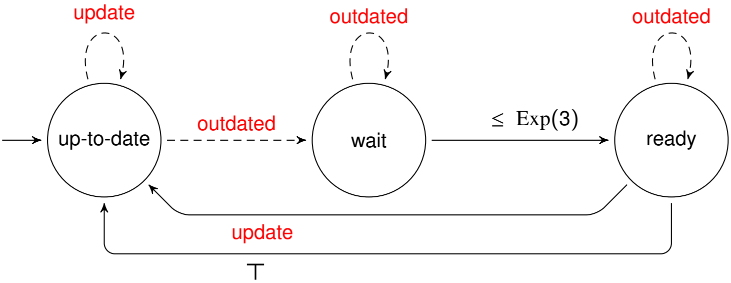


# Specification formalism

We introduce modal continuous-time automata (MCA)

- may/must transitions as in modal transition systems [Larsen&Thomsen'88]
- continuous time constraints extending timed automata [Alur,Courcoubetis&Dill'91]

**Example:** after each outdated an update is ready within time ∼Exp(3)



# Main results

**Theorem**

*For IMC $S$ without internal and external edges enabled at once, the guarantee $\sup_{\sigma} \inf_{E} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in polynomial time.*

**Theorem**

*For IMC $S$ and a modal continuous-time automaton $\varphi$, the guarantee $\sup_{\sigma} \inf_{E \models \varphi} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in exponential time.*

# Main results

**Theorem**

*For IMC $S$ without internal and external edges enabled at once, the guarantee $\sup_{\sigma} \inf_{E} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in polynomial time.*

**Idea:** games with stochastic and non-deterministic time

*more on Saturday 16:45 (the very last talk!)*

**Theorem**

*For IMC $S$ and a modal continuous-time automaton $\varphi$, the guarantee $\sup_{\sigma} \inf_{E \models \varphi} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in exponential time.*

**Idea:** reduce to $\sup_{\sigma} \inf_{E} Pr^{\sigma}_{(S\times\varphi)\|E}[Reach \leq T]$

games with partial information

# Summary and conclusions

- The first assume-guarantee reasoning on stochastic continuous-time systems
- Specification language **modal continuous-time automata** with *continuous time constraints*

For IMC $S$ without internal and external edges enabled at once, the guarantee $\sup_{\sigma} \inf_{E} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in polynomial time.

For IMC $S$ and a modal continuous-time automaton $\varphi$, the guarantee $\sup_{\sigma} \inf_{E \models \varphi} Pr^{\sigma}_{S\|E}[Reach \leq T]$ can be $\varepsilon$-approximated in exponential time.

Future work

- lowering the theoretical/practical complexity
- logical specification language