Symbolic vs. Bounded Synthesis for Petri Games

Bernd Finkbeiner\textsuperscript{1}, Manuel Gieseking\textsuperscript{2},
Jesco Hecking-Harbusch\textsuperscript{1}, Ernst-Rüdiger Olderog\textsuperscript{2}

\textsuperscript{1}Universität des Saarlandes
\textsuperscript{2}Carl von Ossietzky Universität Oldenburg

SYNT, July 22, 2017
Synthesis
Synthesis

System

Global controller

R1
R2
R3
R4
R5
R6

Environment
Distributed Synthesis
Local Information

System

R1 -- R2

R3

R5 -- R4

R6

Environment
Distributed Synthesis with Petri Games
[Finkbeiner, Olderog, ’14]

Existing tool:
- **Adam** is used to synthesize Petri games *symbolically*.

New tool:
- Prototype implementation of *bounded synthesis*.

We compare experimental results of the two approaches.
Distributed Alarm Systems

**Diagram**

- **ECa** to **SysA** via **tA**
- **Env** to **SysA**
- **SysB** to **ECh** via **tB**
- **infoB** to **infoA**
- **Comm.**
- **ACa** to **ACh**
- **BCa** to **BCh**
- **Burglary**
- **Alarm**
Petri Games are based on Petri Nets
Two System Players

- Env
- SysA
- SysB
- Burglary
- info_A
- info_B
- Comm.
- ACa
- ACh
- BCa
- BCh

Diagram showing interactions between the systems and the environment.
One Environment Player

Env

ECa

SysA

tA

SysB

tB

ECh

Burglary

infoB

infoA

Comm.

ACa

ACg

Alarm

BCa

BCh
Intrusion at Location A

- ECa
- SysA
- Env
- SysB
- ECh
- Burglary
- infoA
- infoB
- Comm.
- ACa
- ACh
- Alarm
- BCa
- BCh
Detection of Intrusion via Synchronization

Environmental Context

System

Event

Alarm

Info

Communication

Detection of Intrusion via Synchronization

Environment

System A

System B

Burglary

Alarm

ACa

ACh

BCa

BCh
Exchange of Information via Synchronization
Setting-Off an Alarm

Env

Burglary

Comm.

ACa

ACh

Alarm

BCa

BCh
Setting-Off the Second Alarm

Diagram showing the relationship between various components and systems, including:
- ECa
- SysA
- Env
- SysB
- ECh
- Burglary
- tA
- tB
- infoA
- infoB
- Comm.

Additional elements include:
- ACa
- ACh
- BCa
- BCh

The diagram illustrates the flow of information and events related to setting off the second alarm.
System Players can Refuse to Fire Transitions...
...Based on their Causal Memory
Unfolding of Distributed Alarm System

Diagram showing the interaction between different components such as ECa, Env, SysA, SysB, ECh, and the Burglary and Alarm systems. The diagram includes nodes labeled with information (infoA, infoB) and timestamp (tA, tB) to illustrate the flow of data and time in the system.
Winning Strategy of Distributed Alarm System

[Diagram and text related to the strategy of a distributed alarm system]
Local controllers for Distributed Alarm System
For a single environment token and a bounded number of system tokens, deciding the existence of a safety strategy for the system players is EXPTIME-complete [Finkbeiner, Olderog, ’14].
For a single environment token and a bounded number of system tokens, deciding the existence of a safety strategy for the system players is EXPTIME-complete [Finkbeiner, Olderog, ’14].

Underlying reduction to a Büchi game implemented in Adam symbolically [Finkbeiner, Gieseking, Olderog, ’15].
Bounded Synthesis for Petri Games

- Petri game
- Bound $b$
- Bounded unfolding
- QBF-encoding of existence of a bounded winning strategy
- Bounded winning strategy

- Increase bound
QBF-Encoding of Existence of Bounded Winning Strategy

$\exists V_S \cdot \forall V_{M,n} \cdot \phi_n$

Variables encoding choices of the strategy.

Variables encoding all possible sequences of markings.

Boolean formula encoding whether the strategy is winning.
QBF-Encoding of Existence of Bounded Winning Strategy

$$\exists V_S. \forall V_{M,n} \cdot \phi_n$$

- Variables encoding choices of the strategy.
- Variables encoding all possible sequences of markings.
QBF-Encoding of Existence of Bounded Winning Strategy

\[ \exists V_S \cdot \forall V_{M,n} \cdot \phi_n \]

- Variables encoding choices of the *strategy*.
- Boolean formula encoding whether the strategy is *winning*.
- Variables encoding all possible sequences of *markings*. 
The environment can intrude one of $n$ locations.

All $n$ locations have to indicate where the intrusion occurred.

Scalable in $n$
Runtime – Distributed Alarm System

- winning strategy of symbolic approach,
- winning strategy of bounded approach
Benchmark – Concurrent Machines

- $k$ orders to manufacture goods are processed by $n$ distributed machines.
- The environment can destroy one machine.
- The orders have to avoid the defective machines and each machine can process at most one order.
- Scalable in $n$ and $k$
Runtime – Concurrent Machines

- winning strategy of symbolic approach,
- ■ winning strategy of bounded approach
Benchmark – Document Workflow simple

- $n$ clerks should endorse a document.
- The environment decides which clerk gets the document first.
- Scalable in $n$
• winning strategy of symbolic approach,
• winning strategy of bounded approach
Benchmark – Document Workflow

- $n$ clerks have to make a unanimous decision to endorse or reject the document.
- The environment decides which clerk has to start.
- scalable in $n$
Runtime – Document Workflow

- winning strategy of symbolic approach,
- winning strategy of bounded approach
Results for Comparison of Runtime

- The symbolic approach has better runtime for benchmarks with numerous transitions to bad places.
- The bounded approach synthesizes distributed systems with up to 75 processes.
input Petri game
• winning strategy of symbolic approach
■ bounded winning strategy
The bounded unfolding allows succinct representation of situations where the same decision suffices for different causal pasts.
Conclusions

- Petri games are the first scalable framework for distributed synthesis of systems with up to 75 distributed components.
- Winning strategies of the bounded approach are by order of magnitude smaller than winning strategies of the symbolic approach.
- Bounded synthesis solves games with more than one environment player which we plan to realize for the symbolic approach in future work (including further benchmarks).