Cartesian Abstraction Refinement

*Alexander Malkis*    *Andreas Podelski*    *Andrey Rybalchenko*

University of Freiburg
Germany

MPI-SWS, Saarbrücken
Germany
State explosion: the curse of concurrency

- Research in model-checking: try to optimize an exponential-cost algorithm.
- Alternative:
  - Start with a polynomial-cost algorithm.
  - Add fine-tuning.
  - Make fine-tuning automatic.
Thread-Modular Verification

• successor states for each thread locally.
• stores thread-local states only.
• fast (polynomial in number of threads)
• sometimes incomplete (e.g. for mutual exclusion protocol).
Example: Mutual Exclusion

\[ P_1 ::= \left[ \ell_1 : \text{acquire } lck \right] \quad \ell_2 : \text{critical} \quad \ell_3 : \text{release } lck \quad \parallel \quad P_2 ::= \left[ m_1 : \text{acquire } lck \right] \quad m_2 : \text{critical} \quad m_3 : \text{release } lck \]

\begin{align*}
\text{acquire } lck &= \langle \text{wait } lck=\text{false}; lck:=\text{true} \rangle \\
\text{release } lck &= \langle lck:=\text{false} \rangle
\end{align*}
Where does the incompleteness come from?

Answer in M., Podelski, Rybalchenko'06.
Thread-modularity = abstraction

Thread-modular verification algorithm = attribute-independent program analysis for concurrent programs (attributes = local states)

= abstract interpretation with Cartesian abstraction

Idea: approximate set of tuples by Cartesian product
Cartesian abstraction

1  2  3  4  5

init  BAD
More precision?

• Can we fine-tune thread-modular verification?
• Can fine-tuned thread-modular verification still be polynomial?
Fine-tuning via exceptions

New abstraction in 3 steps:
1. Remove some states ("exception states").
2. Apply Cartesian Abstraction.
3. Add exception states back.
Reduce To

Fix $E$.
Is $A_1 \times \ldots \times A_n \subseteq E$ ?

Precompute a data structure for $E$ so that inclusion is poly-time.
No state explosion

• Thread-modular verification with exception sets is still polynomial.
• ... and practical?
• 100 threads, 9 critical sections per thread: 7328 s.
Find exception sets automatically?
Exception sets for Cartesian bad regions?

Find dimension \( i \) with \( \pi_i(C) \cap \pi_i(F) = \emptyset \).

Here \( i = 2 \).

Maximal \( E \subseteq B \) s.t. \( \pi_2(E) = \pi_2(B) \cap \pi_2(F) \)
Exception sets for unions of Cartesian bad regions?

Take union of exception sets for $F_1$ and $F_2$. 
Next round

1 2 3 4 5

BAD
Experiments

\[
P_1 :: \begin{cases} \ell_1^1 : \text{acquire lck} \\ \ell_2^1 : \text{critical} \\ \ell_3^1 : \text{release lck} \end{cases} \quad || \quad \cdots \quad || \quad P_n :: \begin{cases} \ell_1^m : \text{acquire lck} \\ \ell_2^m : \text{critical} \\ \ell_3^m : \text{release lck} \end{cases}
\]

Runtime(threads, critical sections) in seconds.
Related Work

- C. Flanagan, S. Qadeer. Thread-modular model-checking. SPIN'03.
- R. Manevich, M. Sagiv. Partially disjunctive shape analysis. AHA'07
- A. Cohen, K. Namjoshi. Local Proofs for Global Safety Properties. CAV'07
- Tons of work on compositional reasoning.
Thank you for your attention