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

$$P_1 :: \begin{bmatrix} \ell_1 : \textbf{acquire}\ lck \\ \ell_2 : \textbf{critical} \\ \ell_3 : \textbf{release}\ lck \end{bmatrix} \quad \| \quad P_2 :: \begin{bmatrix} m_1 : \textbf{acquire}\ lck \\ m_2 : \textbf{critical} \\ m_3 : \textbf{release}\ lck \end{bmatrix}$$

acquire lck = <wait lck=false; lck:=true>
release lck = <lck:=false>

Where does the incompleteness come from?

Answer in M.,Podelski, Rybalchenko'06.

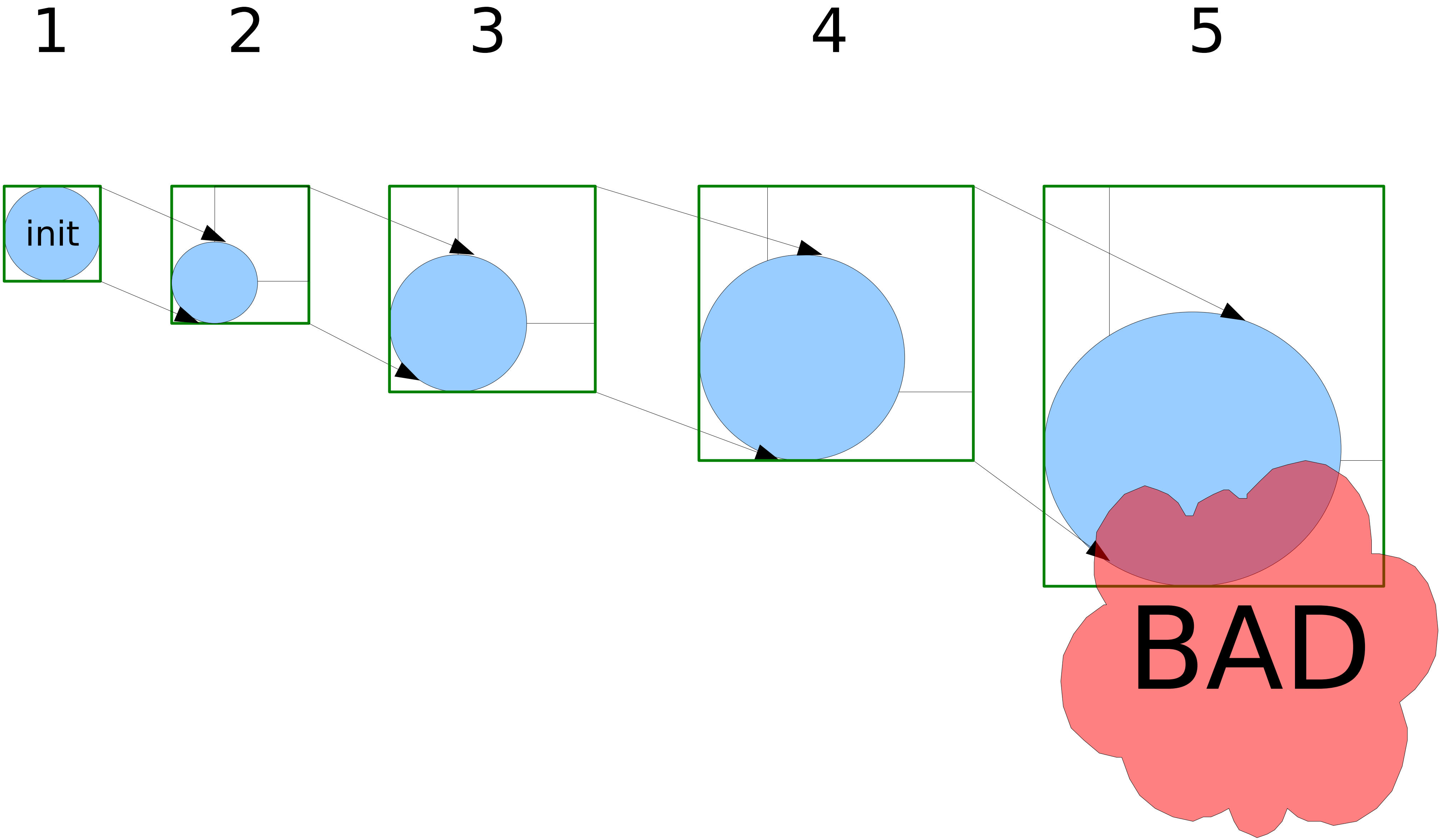
Thread-modularity = abstraction

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



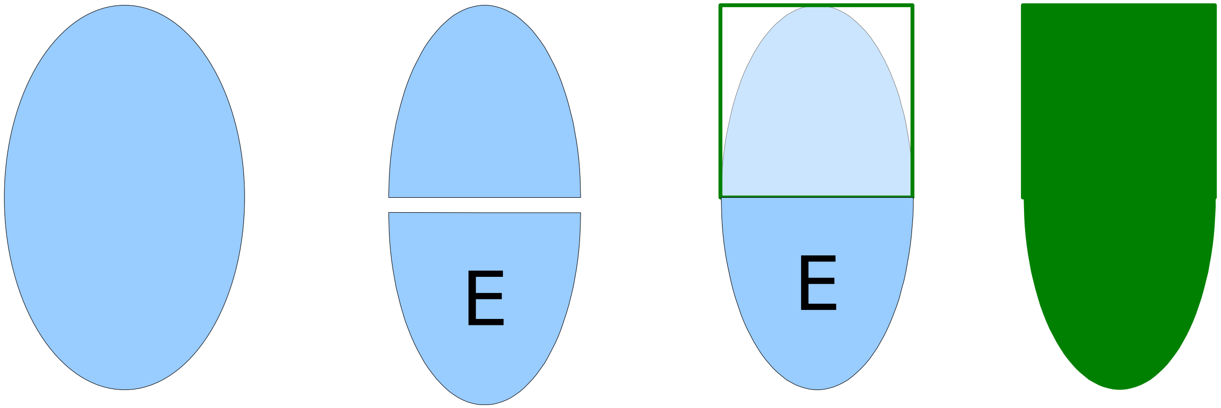
More precision?

- Can we fine-tune thread-modular verification?
- Can fine-tuned thread-modular verification still be polynomial?

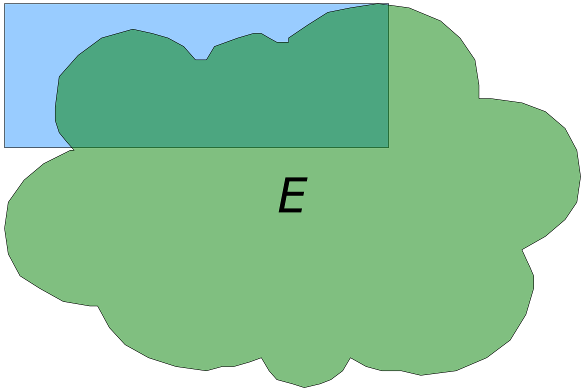
Fine-tuning via exceptions

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_1x...x$A_n \subset E$?

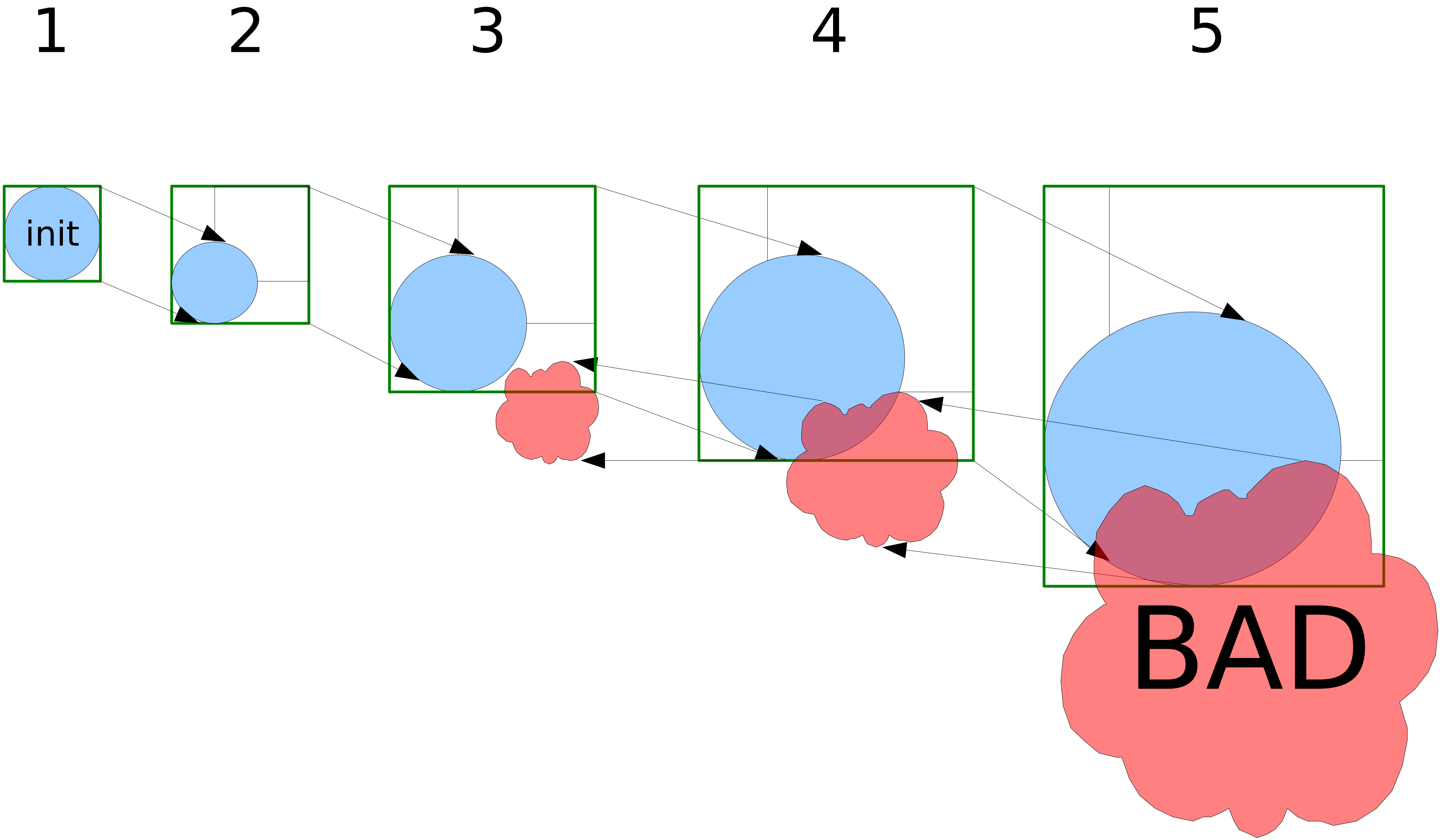
Precompute a data structure for *E*
so that inclusion is poly-time.

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?

First round

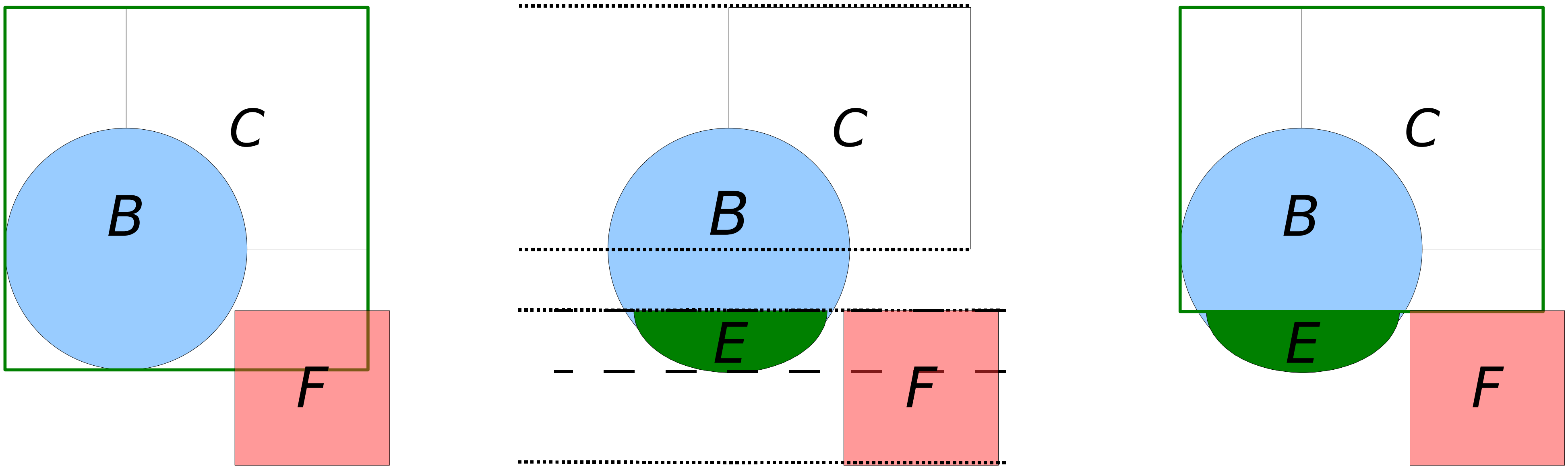


Exception sets for Cartesian bad regions?

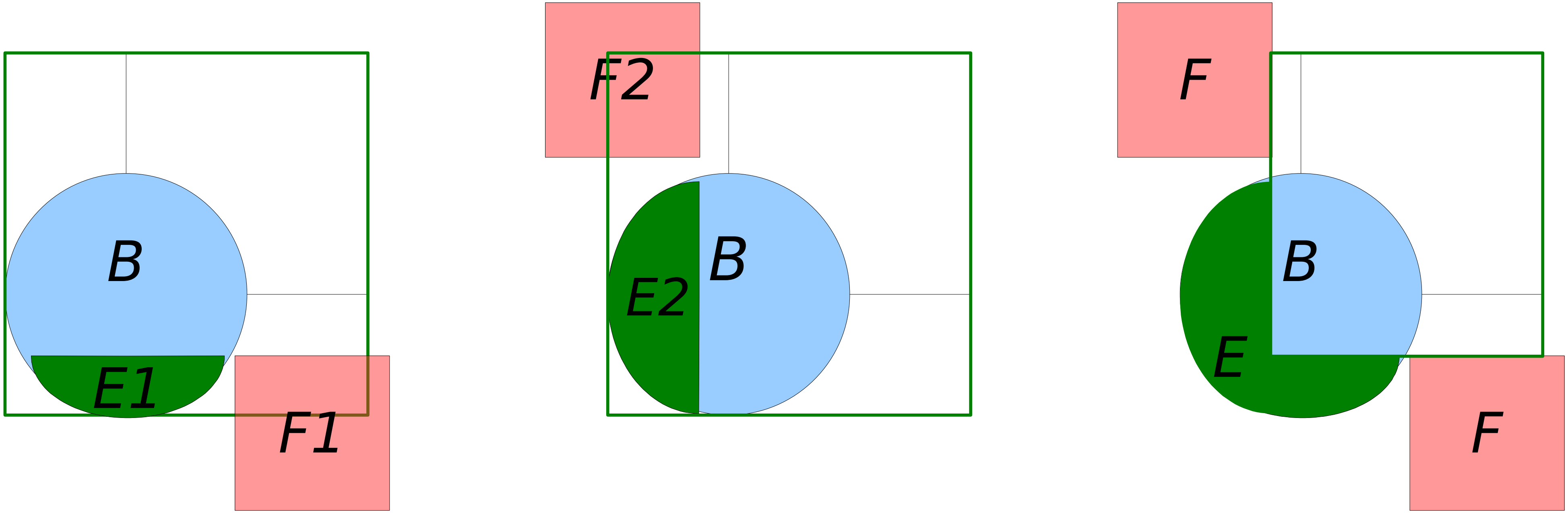
Find dimension i with $\pi_i(C)\cap\pi_i(F)=\emptyset$.

Here $i=2$.

Maximal $E \subseteq B$ s.t. $\pi_2(E)=\pi_2(B)\cap\pi_2(F)$

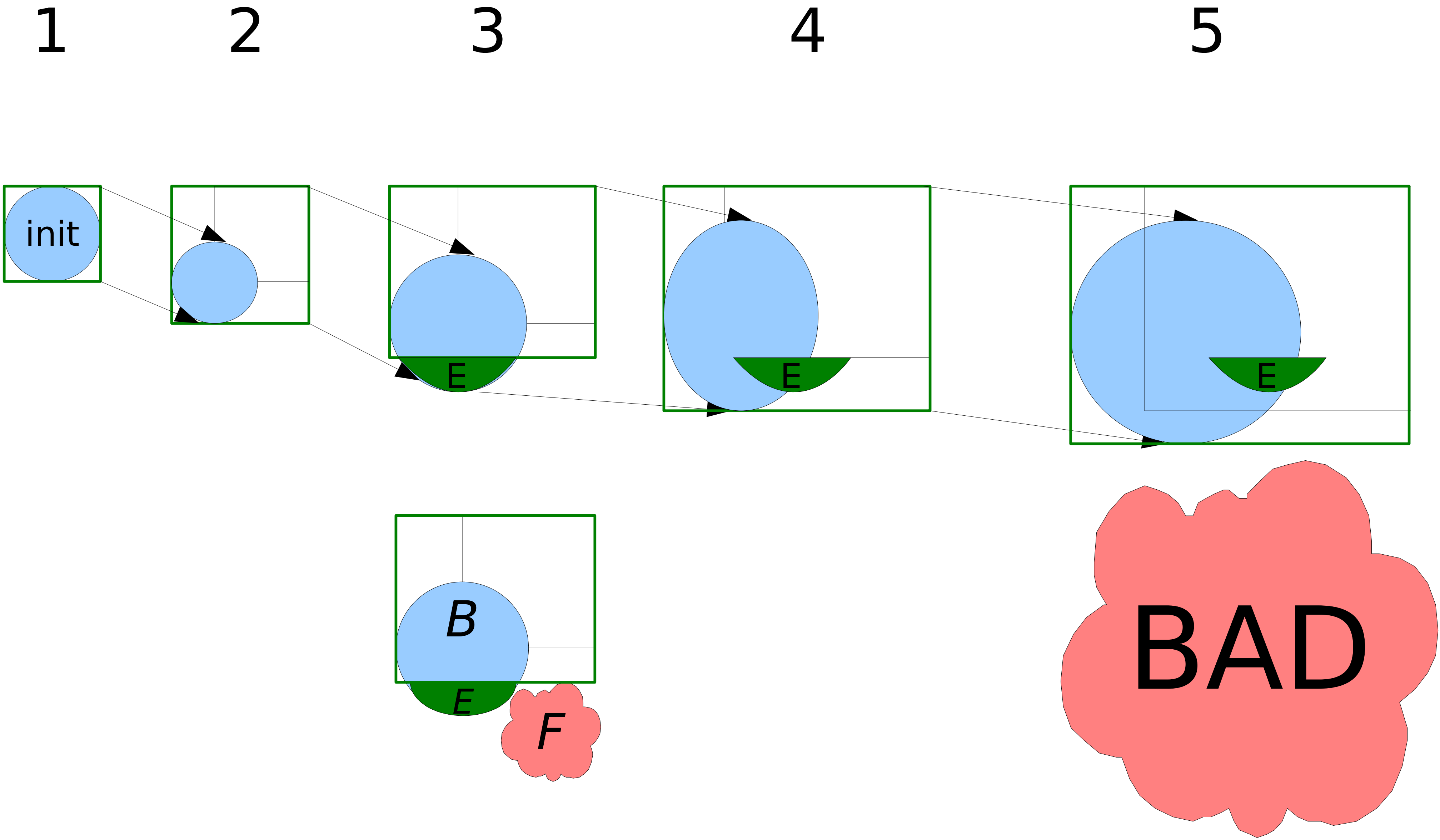


Exception sets for unions of Cartesian bad regions?



Take union of exception sets for *F1* and *F2*.

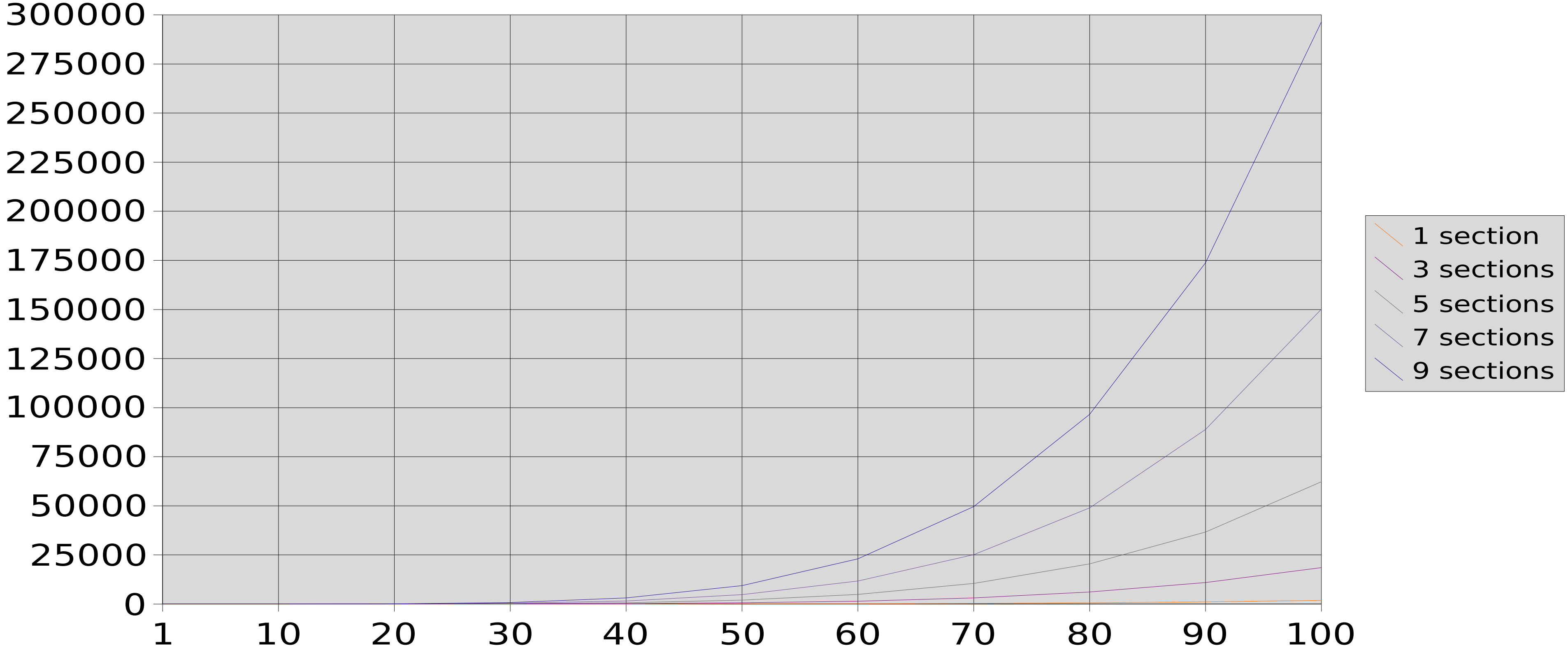
Next round



Experiments

$$P_1 :: \begin{bmatrix} \ell_1^1 : \textbf{acquire}\ lck \\ \ell_2^1 : \textbf{critical} \\ \ell_3^1 : \textbf{release}\ lck \\ \vdots \\ \ell_1^m : \textbf{acquire}\ lck \\ \ell_2^m : \textbf{critical} \\ \ell_3^m : \textbf{release}\ lck \end{bmatrix} \quad \| \quad \cdots \quad \| \quad P_n :: \begin{bmatrix} \ell_1^1 : \textbf{acquire}\ lck \\ \ell_2^1 : \textbf{critical} \\ \ell_3^1 : \textbf{release}\ lck \\ \vdots \\ \ell_1^m : \textbf{acquire}\ lck \\ \ell_2^m : \textbf{critical} \\ \ell_3^m : \textbf{release}\ lck \end{bmatrix}$$

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