Theta: Abstraction Based Techniques for Verifying Concurrency (Competition Contribution)

*Levente Bajczi, **Csanád Telbisz**, Márk Somorjai, Zsófia Ádám, Mihály Dobos-Kovács, Dániel Szekeres, Milán Mondok, Vince Molnár*

MŰEGYETEM 1782

BME FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS

ftsrg Critical Systems Research Group

New algorithms

- Abstraction-based partial order reduction:
  - Variables untracked in the abstraction does not cause dependency
  - Static POR based on source sets

New algorithms

- Abstraction-based partial order reduction:
  - Variables untracked in the abstraction does not cause dependency
  - Static POR based on source sets

```
  Thread 1          |      Thread 2
1: y = 1;           | 2: x = 2;
                    | 3: y = 2;
                    | 4: assert(x == y);
```

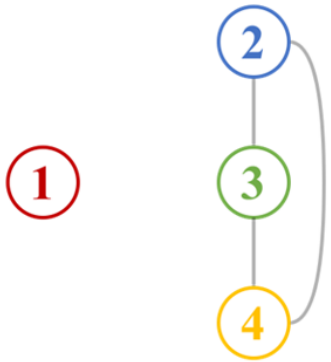
New algorithms

- Abstraction-based partial order reduction:
  - Variables untracked in the abstraction does not cause dependency
  - Static POR based on source sets

```
  Thread 1          |      Thread 2
1: y = 1;           | 2: x = 2;
                    | 3: y = 2;
                    | 4: assert(x == y);
```

Explicit-value abstraction

$\Pi = \{x\}$



New algorithms

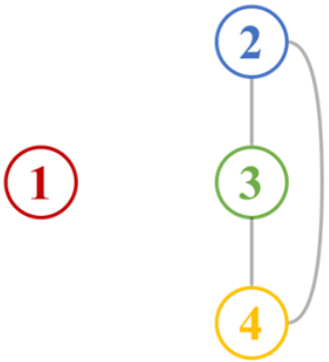
- Abstraction-based partial order reduction:
  - Variables untracked in the abstraction does not cause dependency
  - Static POR based on source sets

```
  Thread 1
1: y = 1;
```

```
     Thread 2
2: x = 2;
3: y = 2;
4: assert(x == y);
```

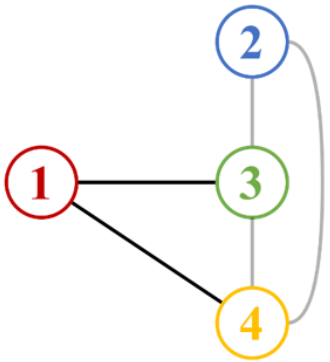
Explicit-value abstraction

$\Pi = \{x\}$



Explicit-value abstraction

$\Pi = \{x, y\}$

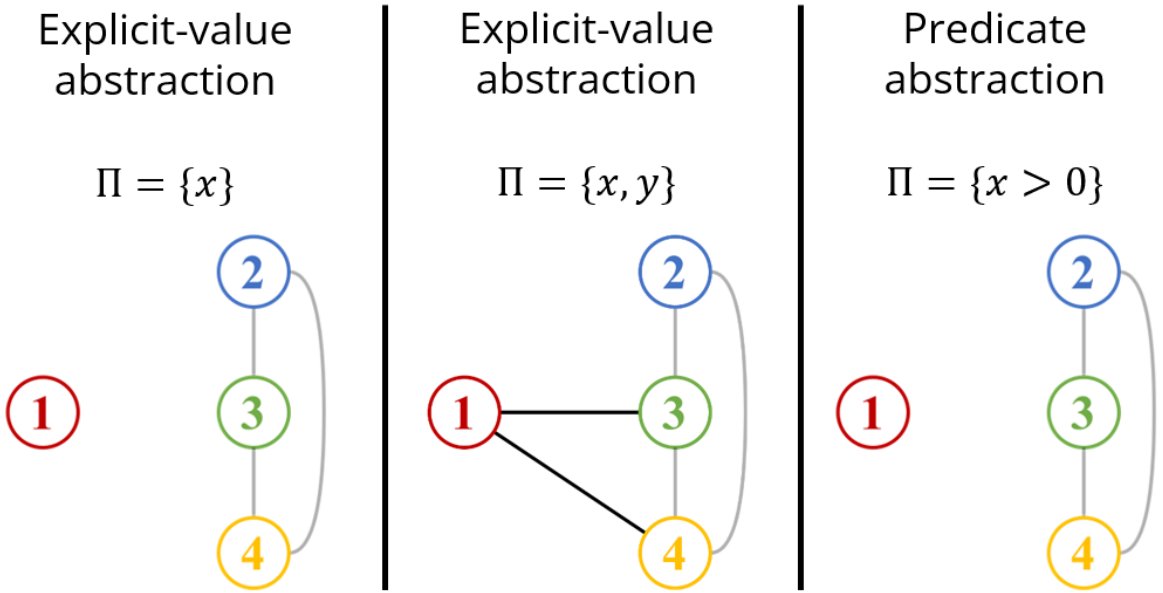


New algorithms

- Abstraction-based partial order reduction:
  - Variables untracked in the abstraction does not cause dependency
  - Static POR based on source sets

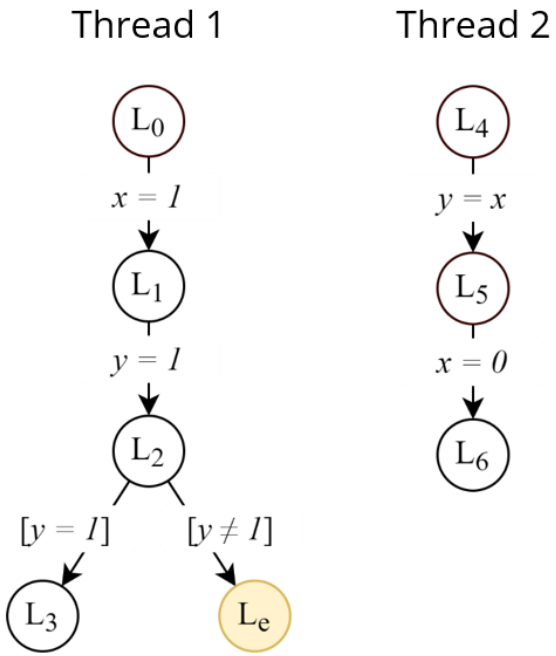
```
  Thread 1
1: y = 1;
```

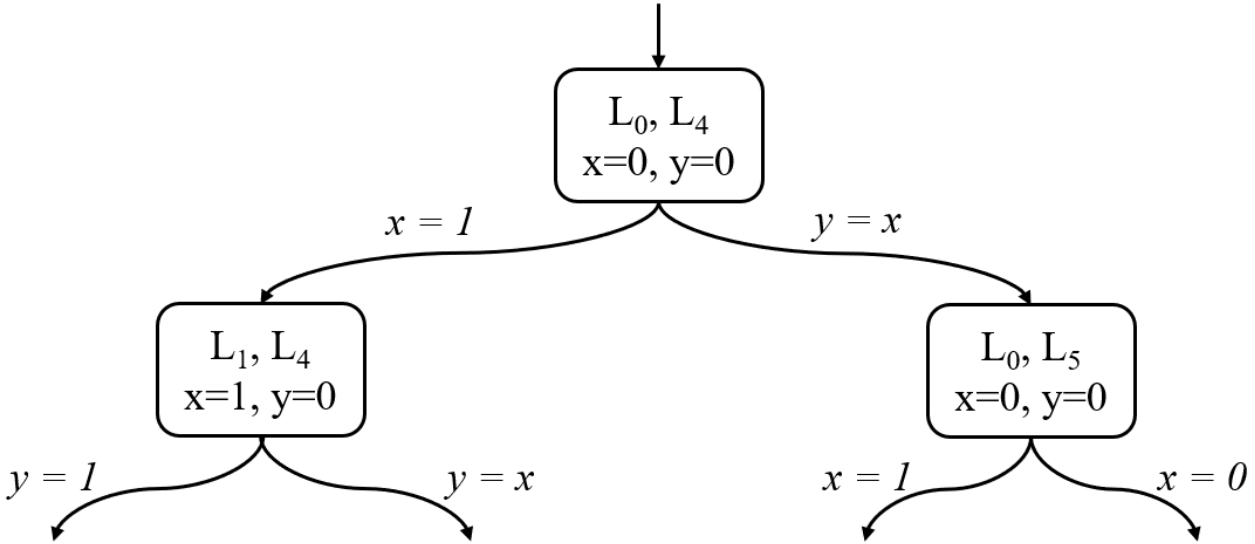
```
     Thread 2
2: x = 2;
3: y = 2;
4: assert(x == y);
```



New algorithms

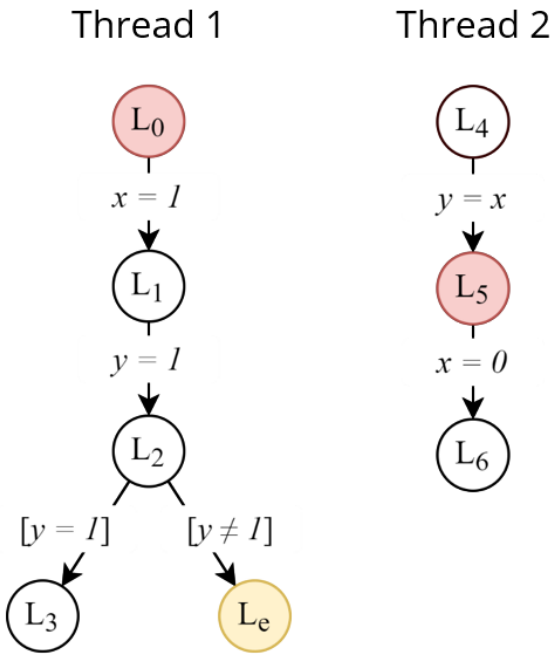
- Statement reduction based on current thread context

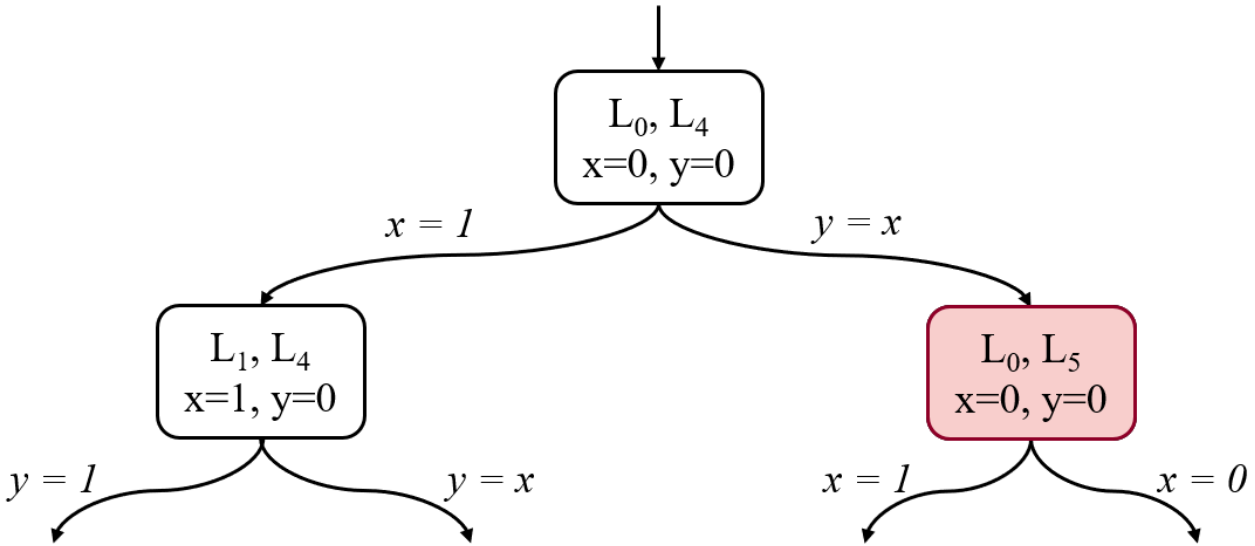




New algorithms

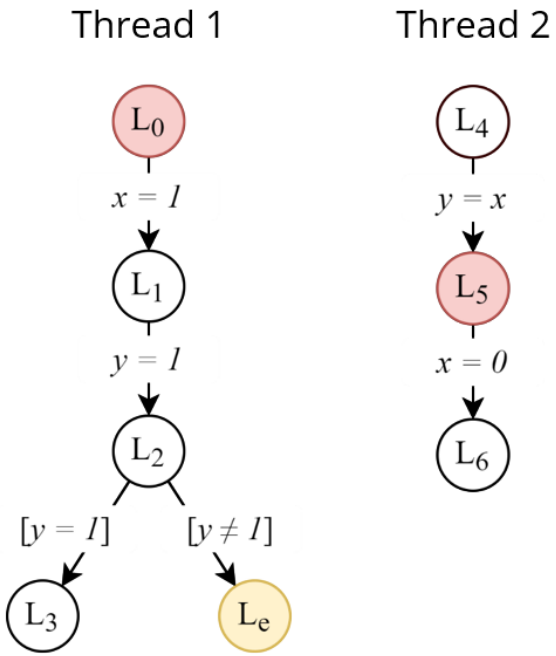
- Statement reduction based on current thread context



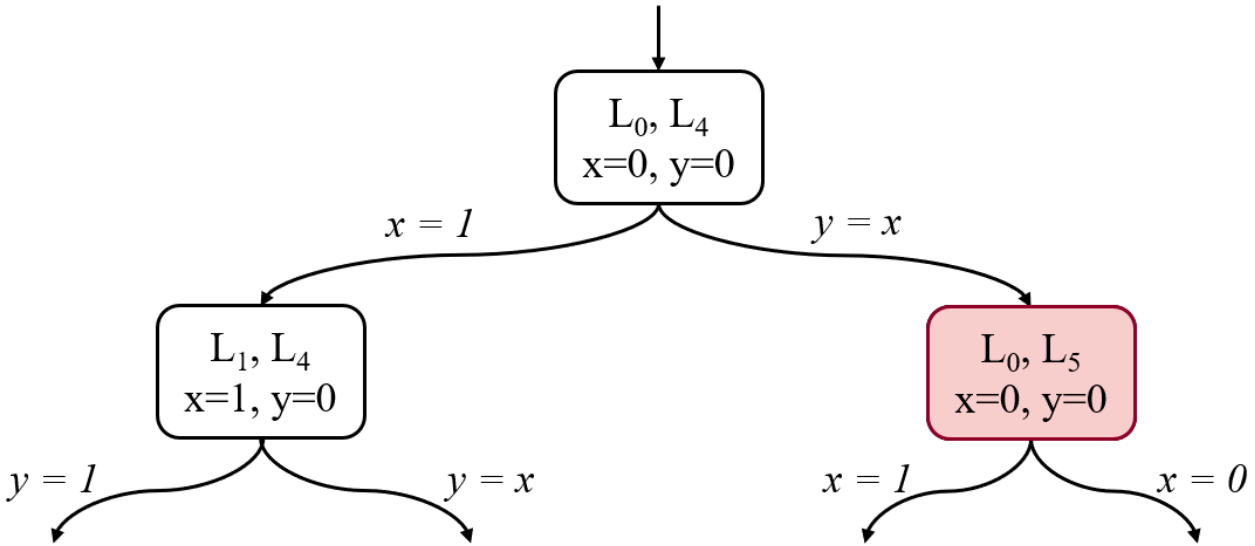


New algorithms

- Statement reduction based on current thread context

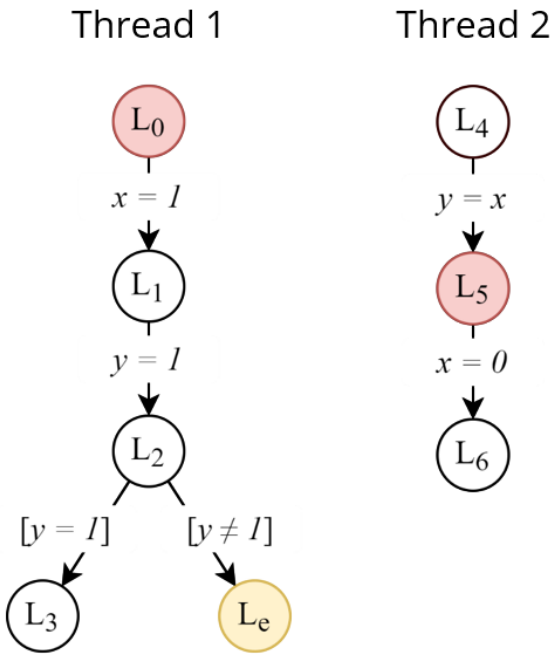


The value of x is not used after this state!

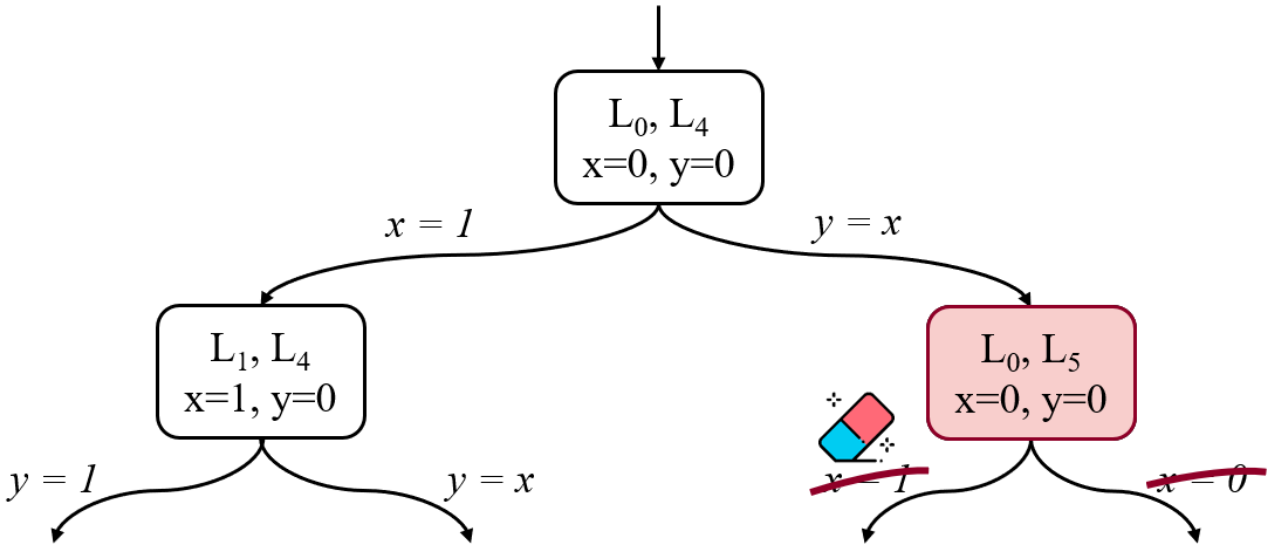


New algorithms

- Statement reduction based on current thread context

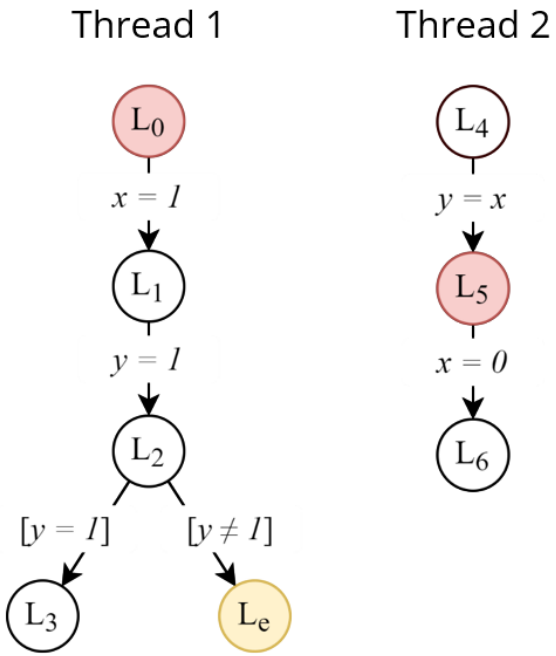


The value of x is not used after this state!

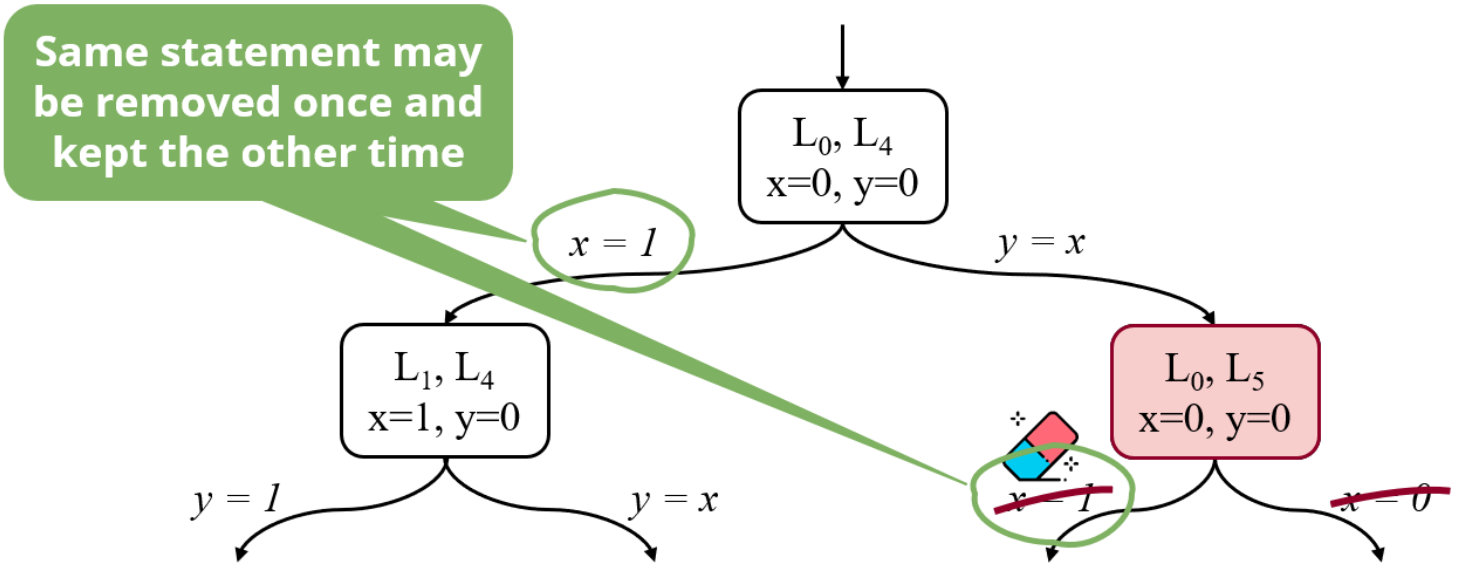


New algorithms

- Statement reduction based on current thread context

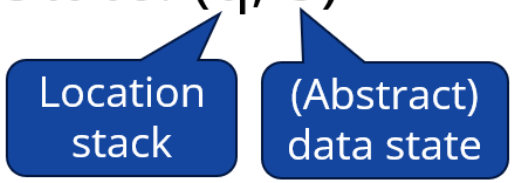


The value of x is not used after this state!



New algorithms

- Interprocedural analysis, stack abstraction for recursion
  State: (q, S)



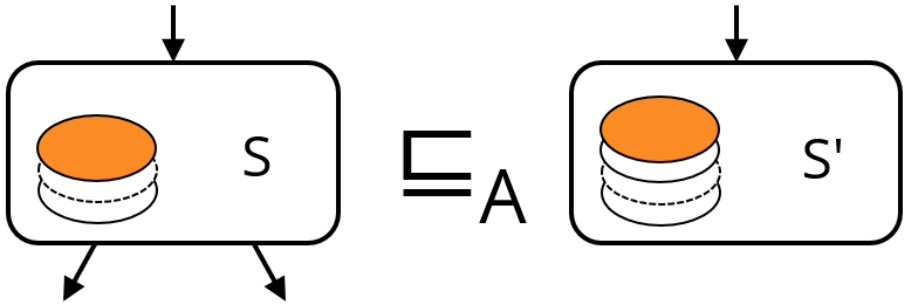
New algorithms

- Interprocedural analysis, stack abstraction for recursion
  State: (q, S)

Location stack

(Abstract) data state

$$(q, S) \sqsubseteq_A (q', S') \iff top(q) = top(q') \wedge S \sqsubseteq S'$$



New algorithms

- Interprocedural analysis, stack abstraction for recursion
  State: (q, S)

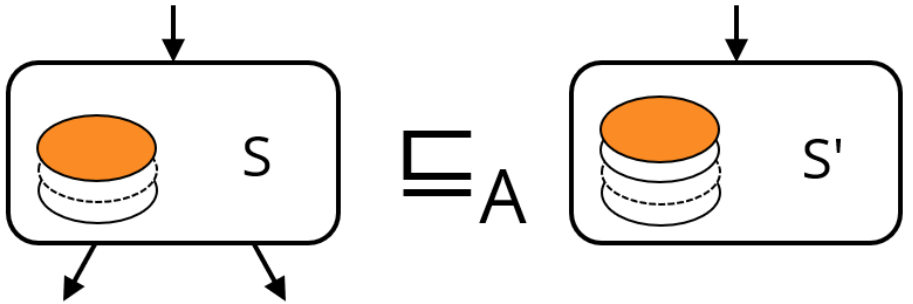
Location stack

(Abstract) data state

$$(q, S) \sqsubseteq_A (q', S') \iff top(q) = top(q') \wedge S \sqsubseteq S'$$

If $(q, S) \sqsubseteq_A (q', S')$ found:

- pop top location of q'
- continue exploration



New algorithms

- Interprocedural analysis, stack abstraction for recursion
  State: (q, S)

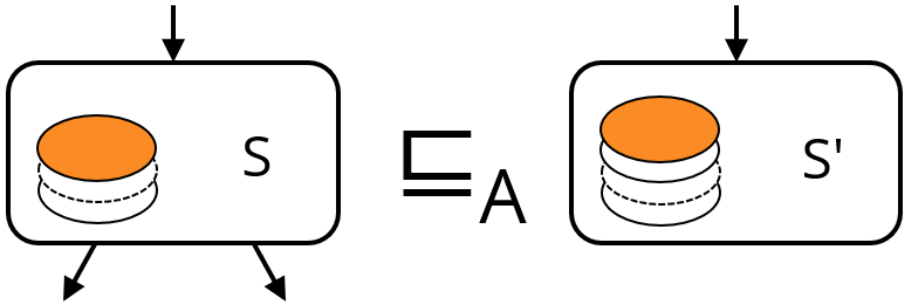
Location stack

(Abstract) data state

$$(q, S) \sqsubseteq_A (q', S') \iff top(q) = top(q') \wedge S \sqsubseteq S'$$

If $(q, S) \sqsubseteq_A (q', S')$ found:

- pop top location of q'
- continue exploration



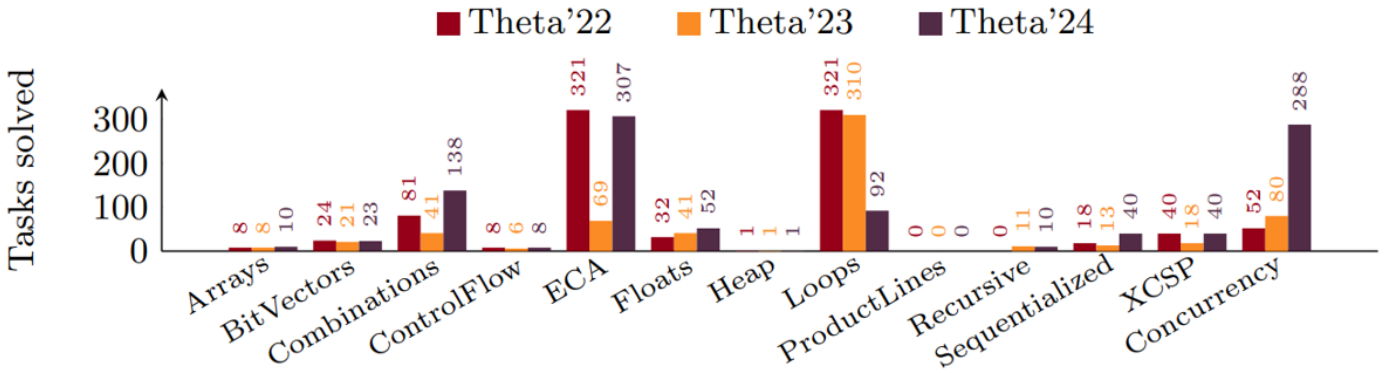
Advantages:

- **Reduced abstract state-space**
- **Can solve infinitely recursive tasks**

Results, Future Directions

Results, Future Directions

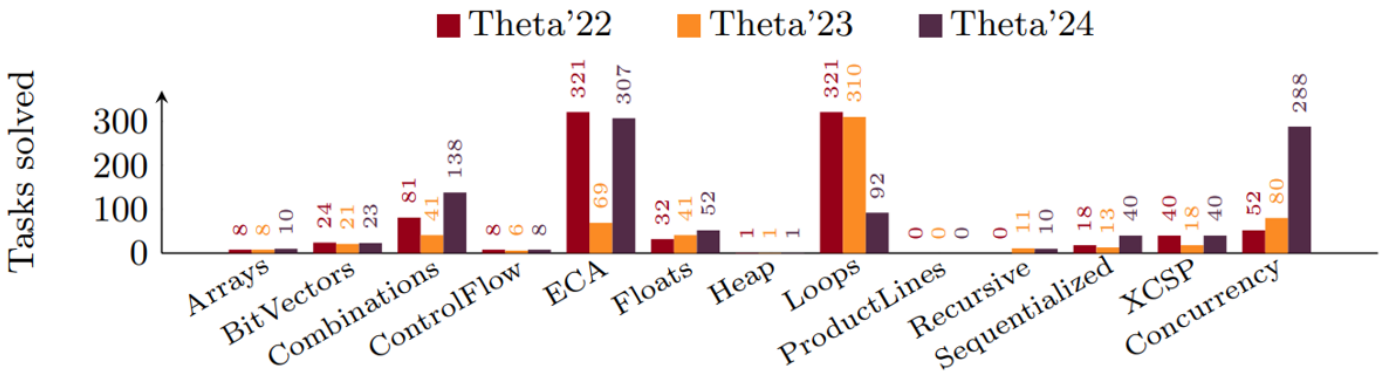
- This year's focus:
  - Concurrency (reachability): 3.5 times more tasks solved
  - Striving for correctness: 0 incorrect tasks for reachability properties (only 2 other tools managed this)



Successful reachability tasks of THETA per year

Results, Future Directions

- This year's focus:
  - Concurrency (reachability): 3.5 times more tasks solved
  - Striving for correctness: 0 incorrect tasks for reachability properties (only 2 other tools managed this)



Successful reachability tasks of THETA per year

- Next steps:
  - frontend development: support for more C language constructs
  - analysis of worse-than-expected results