Symbolic Polytopes for Quantitative Interpolation and Verification

Klaus v. Gleissenthall, TU Munich
joint work with
Andrey Rybalchenko, Microsoft Research
and Boris Köpf, IMDEA

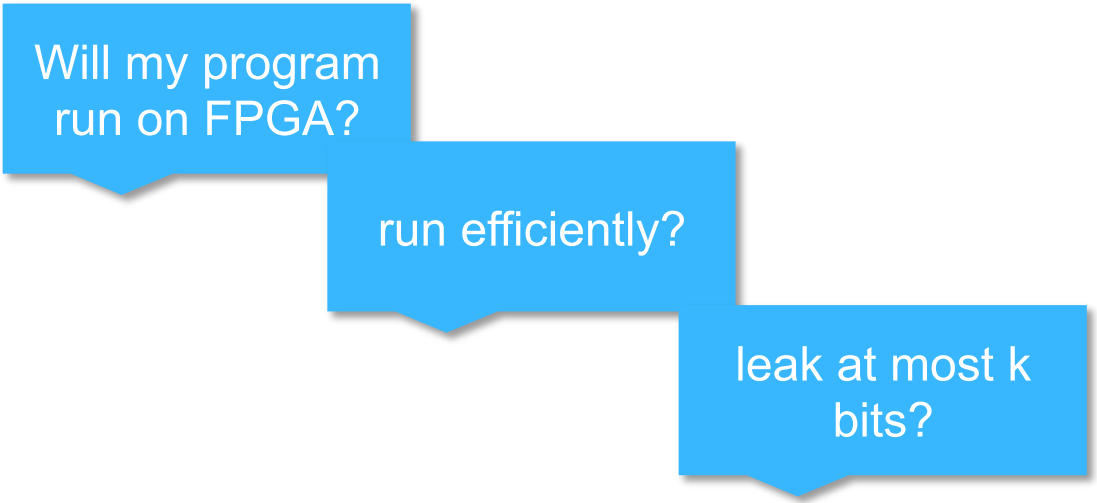
Verification

Will my program crash?

violate API usage rules?

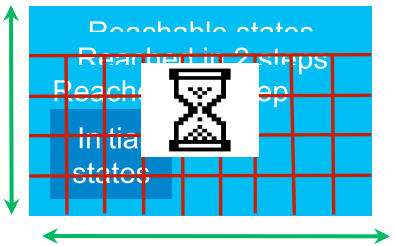
leak secrets?

Quantitative verification



Quantitative reachability property

To prove: at most k states are reachable

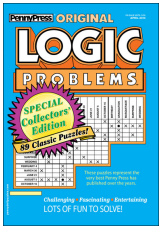


Observables, call-sites, memory locations

$$\text{size}(\text{Reachable states}) \leq k$$

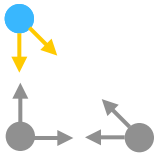
This talk

- Constraint solving problem



- Quantitative interpolation

- Symbolic polytopes and generating functions



$$P(x) = \frac{1}{1-x} + \cdots$$

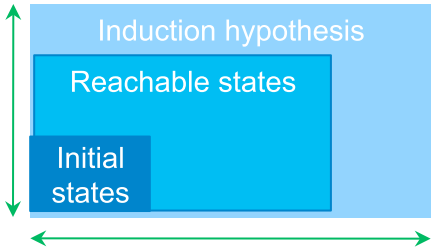
Program as formula

```
int v;

main(int k) {

  init(v,k);

  while (1) step(v);

}
```

$$init(v, k)$$

$$step(v, v')$$

Quantitative verification is a logic problem



Find h:

Base case

$$init(v, k) \rightarrow h(v, k)$$

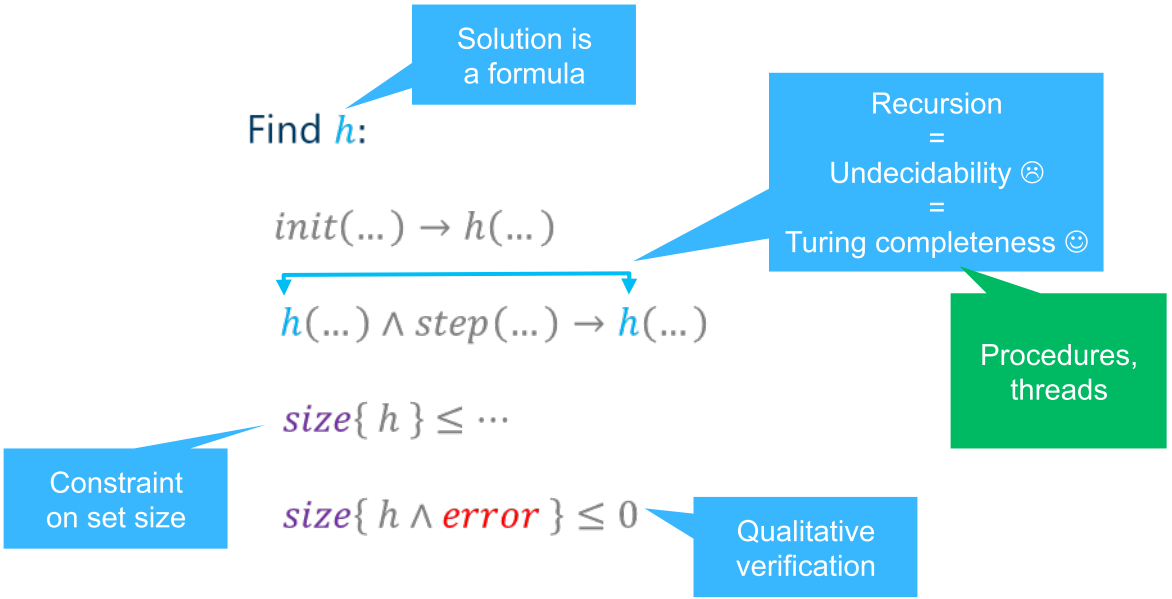
Induction step

$$h(v, k) \wedge step(v, v') \rightarrow h(v', k)$$

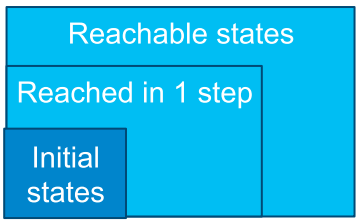
$$size\{\, v \mid h(v, k) \,\} \leq k$$

Sufficient strength

Simple yet expressive



Unfold, guess, and check



Find $h = h_0 \cup h_1$

Bounded problem

$init(\ldots) \rightarrow h_0(\ldots)$

$h_0(\ldots) \wedge step(\ldots) \rightarrow h_1(\ldots)$

$size\{h\} \leq k$

Recursion check

$h(\ldots) \wedge step(\ldots) \rightarrow h(\ldots)$

Solution to bounded problem

If implication fails, increase the bound

Bounded problem is interpolation

[Craig'57, McMillan'03]

Find h:

$low(\dots) \rightarrow h(\dots)$

$h(\dots) \rightarrow hi(\dots)$

Quantitative extension:

Find h:

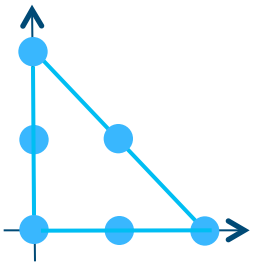
$low(\dots) \rightarrow h(\dots)$

$size\{\, h \,\} \leq k$

From size to set

Interpolants as polytopes

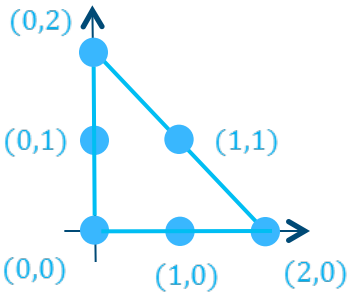
- Integer points represented by linear inequalities
- Model for numeric data types



$$0 \leq x \wedge 0 \leq y \wedge x + y \leq 2$$

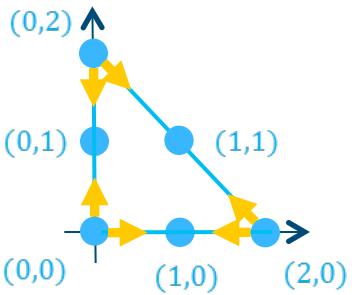
$$size\{\ (x, y) \mid \ldots\ \} = 6$$

Generating functions



- Generating function
  $P(i,j) = i^0 j^2 + i^0 j^1 + \cdots$
- One term per point,
  $P(1,1) = 6 =$ size

Decomposition [Brion'88, Barvinok'93]

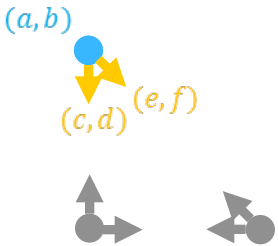


- Rational function

$$P(i,j) = \frac{i^0 j^2}{(1 - i^0 j^{-1})(1 - i^1 j^{-1})} + \cdots$$

- $P(1,1) = 6 =$ size
- One term per vertex

Quantitative interpolation w/o size



$$P(i,j) = \frac{i^a j^b}{(1 - i^c j^d)(1 - i^e j^f)} + \cdots$$

Find h given by a,b,c,d,e,f,... :

$$low(\ldots) \rightarrow h(\ldots)$$

$$P(1,1) \leq k$$

Evaluation

Program	Bound	Time
Dis1 [21]	$max(n - x_0, 0) + max(m - y_0, 0)$	0.19s
Dis2 [21]	$n - x_0 + m - z_0$	0.17s
SimpleSingle [21]	n	0.11s
SequentialSingle [21]	n	0.11s
NestedSingle [21]	$n + 1$	0.15s
SimpleSingle2 [21]	$max(n, m)$	0.13s
SimpleMultiple [21]	$n + m$	0.16s
NestedMultiple [21]	$max(n - x_0, 0) + max(m - y_0, 0)$	0.08s
SimpleMultipleDep [21]	$n \cdot (m + 1)$	0.15s
NestedMultipleDep [21]	$n \cdot (m + 1)$	0.09s
IsortList [23]	$n^2 \cdot m$	0.19s
LCS [23]	$n \cdot x$	0.15s
Example 1 [41]	n	0.15s
Sum [24]	$2n + 6$	0.15s
Flatten [24]	$8l + 8$	0.13s

Find h:

$init(\ldots) \rightarrow h(\ldots)$

$h(\ldots) \wedge step(\ldots) \rightarrow h(\ldots)$ 

$size\{\, h \,\} \leq k$

recursive

$low(\ldots) \rightarrow h(\ldots)$

$size\{\, h \,\} \leq k$ 

bounded

$P(1,1) \leq k$

generating functions