raSAT – an SMT for Polynomial Constraints

What are Polynomial Constraints?

Q: Find the real values of x, y such that:

$$y^2 + y - x^2y + 1 < 0 \text{ and } x^2 + y^2 - 4 < 0$$

A: x = 0.687783209694, y = 1.875

$$f > 0 \text{ is } \begin{cases} satisfiable\ (SAT)\ if\ there\ exist\ values\ for\ variables\ x,y,.. \\ unsatisfiable\ (UNSAT) otherwise \end{cases}$$

Many applications in Software Verification

- Automatic termination proving.
- Round-off and overflow errors analysis.
- Invariant generation.
- Test case generation.

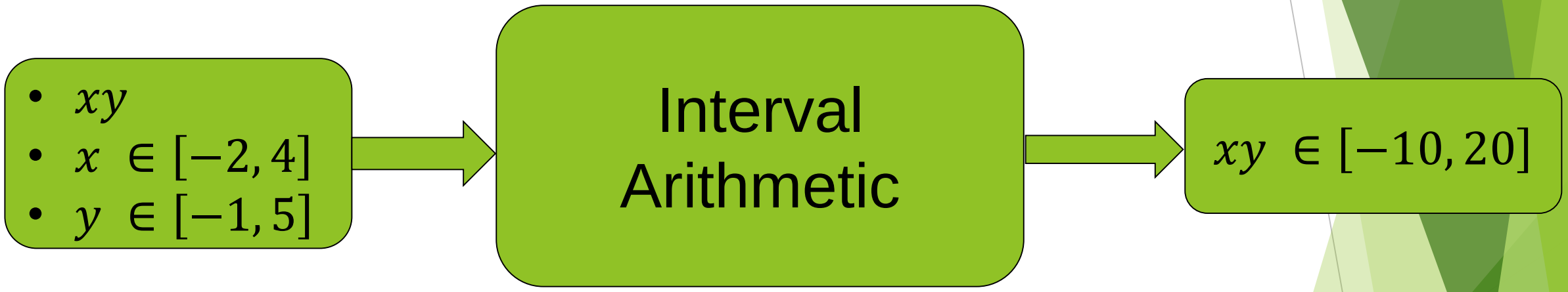
Approaches for Polynomial Constraints

- QE-CAD: complete but DEXPTIME complexity.
- Bit-blasting: suffers with high number of variables or high degree of polynomials.
- Linearization: suffers with high degree of polynomials.
- Virtual substitution: needs root formulas of polynomial
- ➔ degree <= 4
- ICP: uses Interval arithmetic (IA) and suffers with touching cases.

raSAT = ICP + testing

Interval Arithmetic

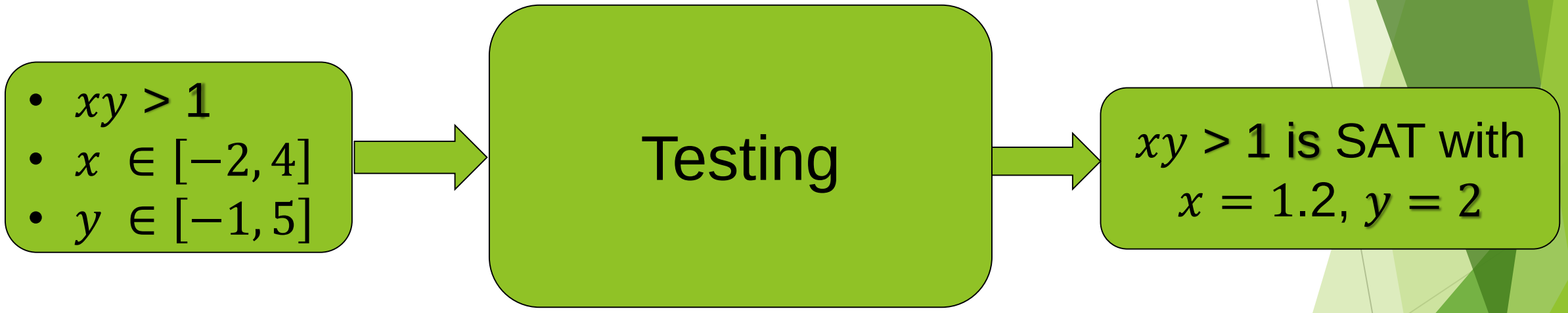
estimate ranges of polynomials



- e.g., $f \in [1, 10] \rightarrow f > 0$ is IA-VALID $\Longrightarrow$ SAT
- e.g., $f \in [-10, -1] \rightarrow f > 0$ is IA-UNSAT $\Longrightarrow$ UNSAT
- e.g., $f \in [-12, 10] \rightarrow f > 0$ is IA-SAT $\Longrightarrow$ UNKNOWN

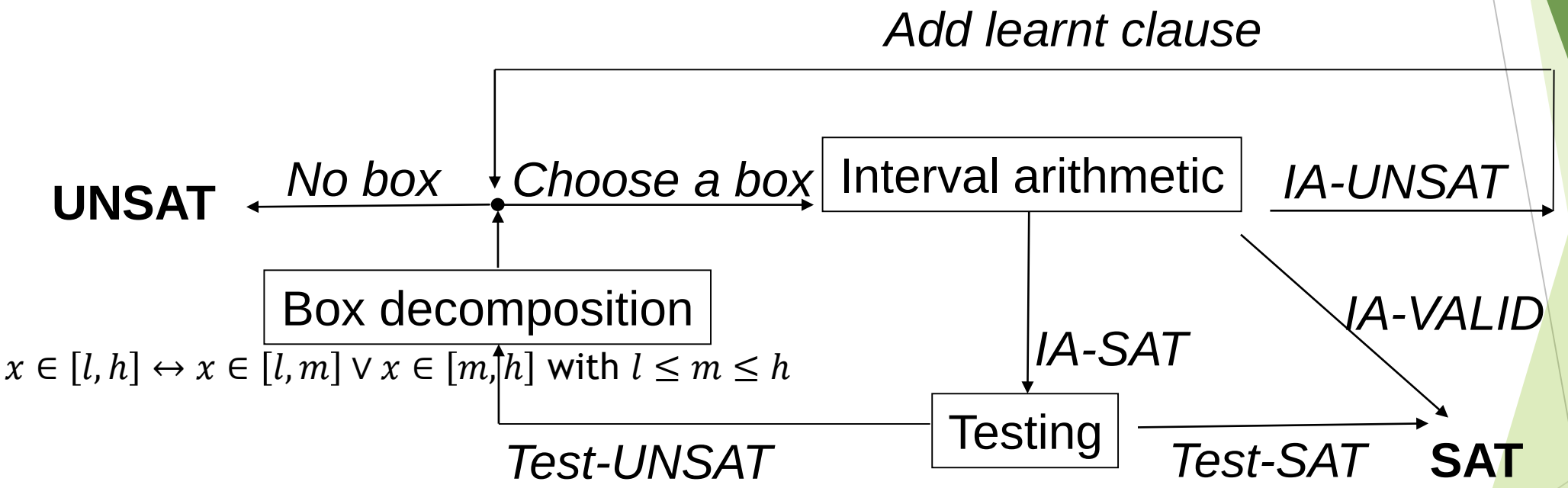
Testing

find values for variables that satisfy the constraint



Randomly generated with the guide of IA results

raSAT loop


Add learnt clause
UNSAT
No box
Choose a box
Interval arithmetic
IA-UNSAT
Box decomposition
IA-VALID
$x \in [l,h] \leftrightarrow x \in [l,m] \vee x \in [m,h]$ with $l \leq m \leq h$
IA-SAT
Testing
Test-UNSAT
Test-SAT
SAT

raSAT Performance

- iSAT3, dREAL: ICP-based solvers

Benchmarks	raSAT		iSAT3 with bounds [-1000, 100]		dREAL	
	Solved No.	Time(s)	Solved No.	Time(s)	Solved No.	Time(s)
Matrix-1(SAT)	**25**	**414.99**	11	4.68	46*	3573.43
Matrix-1(UNSAT)	2	0.01	3	0.00	0	0.00
Matrix-25(SAT)	**11**	**1264.77**	3	196.40	19*	2708.89
Matrix-25(UNSAT)	8	0.38	12	8.06	0	0.00
Meti-Tarski(SAT)	**3473**	**419.25**	2916	811.53	3523*	441.35
Meti-Tarski(UNSAT)	1052	821.85	1225	73.83	1197	55.39

* means $\delta - SAT$ and $\delta - SAT \nrightarrow SAT$

raSAT Performance

Participated in SMT competition 2015.

- 3rd among 6 in QF_NRA – category for reals
- 2nd among 7 in QF_NIA – category for integers
- Overall, ranked 8th among 19 solvers.
- http://smtcomp.sourceforge.net/2015/results-competition-main.shtml?v=1436156934