

# Z3 Logic Engines as a Service

Leonardo de Moura and Nikolaj Bjørner  
Microsoft Research

# Satisfiability

Solution/Model

$$x^2 + y^2 < 1 \text{ and } xy > 0.1$$



$$\text{sat, } x = \frac{1}{8}, y = \frac{7}{8}$$

$$x^2 + y^2 < 1 \text{ and } xy > 1$$



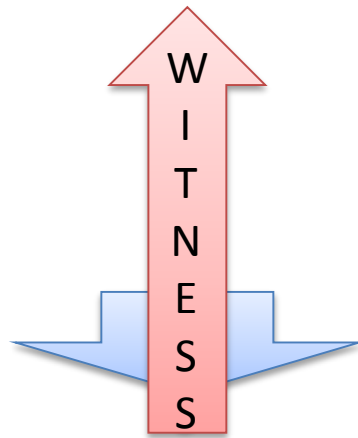
unsat, Proof

Is execution path  $P$  feasible?



**SAGE**

Is assertion  $X$  violated?



Is Formula  $F$  Satisfiable?

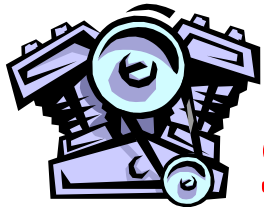
# Z3 Theorem Prover

DPLL

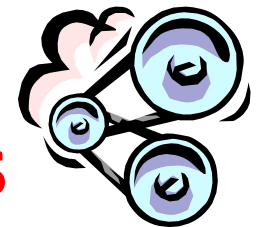
Simplex

Rewriting

Superposition



Z3 is a collection of  
**Symbolic Reasoning Engines**



Congruence  
Closure

Groebner  
Basis

$\forall\exists$   
elimination

Euclidean  
Solver

# Symbolic Reasoning Engine

Test Case Generation

Verifying Compilers

Invariant Generation

Model Based Testing

Type Checking

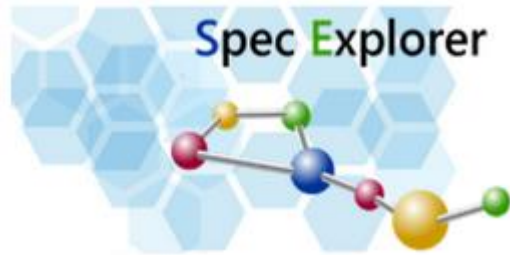
Model Checking

# Some Applications at Microsoft

SAGE



HAVOC



TERMINATOR

Vigilante



# Impact

Used by many research groups

TACAS paper (> 1500 citations)

More than 35k downloads

Ships with many popular systems

Isabelle, Pex, SLAM/SDV, ...

Solved more than 5 Billion constraints created by SAGE when checking Win8 and Office.

# Results and Contributions

Algorithms

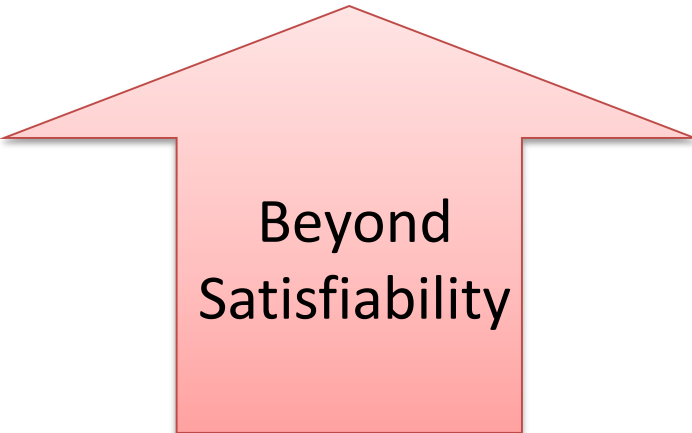
Decidable Fragments

Data structures

Heuristics

# Recent Progress

1. Interpolants
2. Fixed Points



Beyond  
Satisfiability



**Z3**

Arithmetic, Bit-Vectors,  
Booleans, Arrays,  
Datatypes, Quantifiers



New Engines

3. Strings
4. Nonlinear arith.



# SMT solvers are popular

MathSAT 5



Yices2



Barcelologic



SMTInterpol

*veriT* solver

Boolector

# Future

Z3 with objective functions (Bjørner)

Leverage progress in MaxSAT for SMT

Stochastic Local Search in Z3 (Wintersteiger)

For hard feasibility problems from symbolic execution, floating points

*Lean*: new theorem prover (de Moura)

Powerful Dependent Type system, Higher-Order