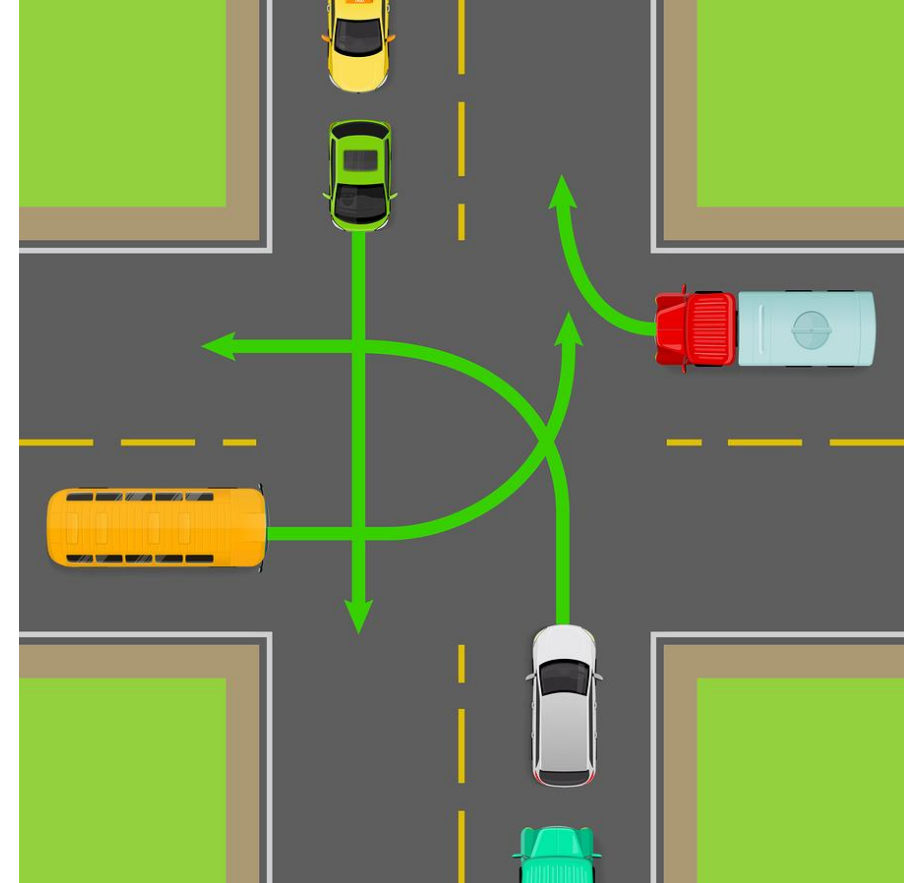


Verified Quadratic Virtual Substitution for Real Arithmetic

Matias Scharager, Katherine Cordwell, Stefan Mitsch, André Platzer

Motivation: Real World Example

- Suppose cars are moving in a 2D grid
- Position: multivariate polynomials
- Many unknown variables
 - Time
 - Gas in car
 - etc.
- How to ensure cars don't crash?
 - There never exists a time t when two cars have the same x and y coordinates



Quantifier Elimination

$$\exists x. \forall y. x * y \leq 0 \quad \longrightarrow \quad 0 * 5 \leq 0 \quad \longrightarrow \quad \textit{true}$$

$$\exists b. ((b < 5c + 10) \wedge (5a^2 + ab + 2 \neq 0)) \\ \longrightarrow (c > -2) \vee (a = 0) \vee \dots$$

- Tarski–Seidenberg theorem:

- In First Order Logic of Real Arithmetic...
- It is possible to write an equivalent formula with no quantifiers!



Want algorithms that are

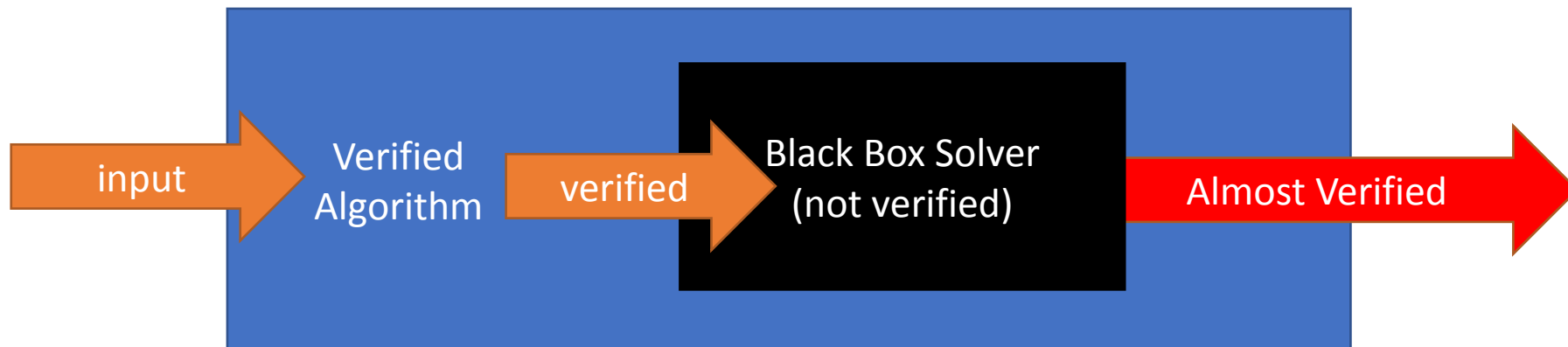
- Correct!
 - Preserve formula equivalence
 - Verified in a theorem prover
- Efficient!
 - Runtime – Fast enough to eliminate all quantifiers
 - Result – Smallest possible equivalent formula
- It's difficult to have both efficient and correct algorithms

100



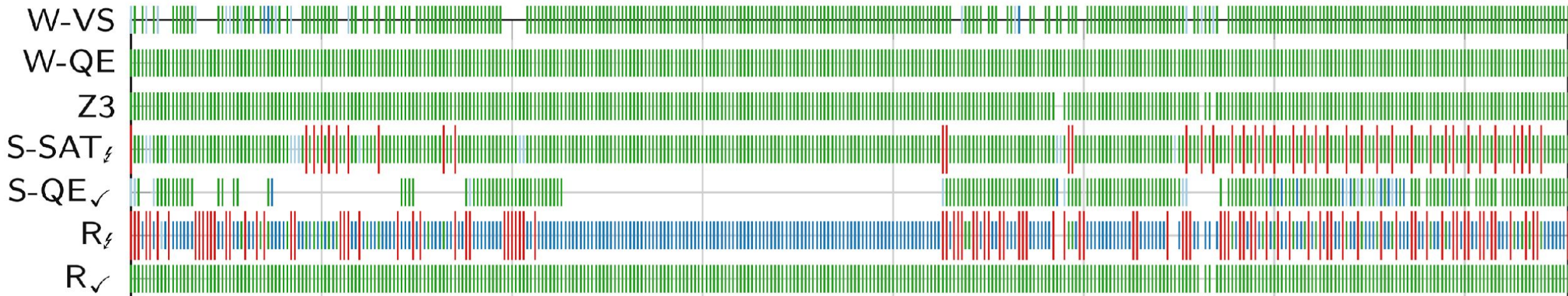
Black Box Algorithms

- Export QE to another software which is not computationally verified

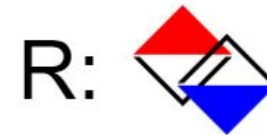


Can We Trust Them?

- Test for “A” and “¬A”
 - Both passed: “A” is true, “¬A” is false
 - Only one passed
 - Contradiction: “A” is true, “¬A” is true – Can’t both be true!



Z3: 



Verified QE Algorithms

- Cohen-Hormander
 - McLaughlin/Harrison, 2005
- Tarski's QE
 - Cohen/Mahboubi, 2012
- Univariate case of CAD
 - Li/Passmore/Paulson, 2018
 - Narkawicz/Munoz/Dutle, 2018

100



Virtual Substitution (VS)

- **Efficient** algorithm for special cases of QE that involve **low degree** polynomials
- Two flavors of VS
 - Equality
 - General

Related Work

- Quadratic Equality Case of Virtual Substitution (Chaieb) (2008)
- Linear Quantifier Elimination (Nipkow) (2010)

We formalize **Equality** and **General** for Linear and Quadratic Virtual Substitution In Isabelle/HOL

Archive of Formal Proofs Entry:

https://www.isa-afp.org/entries/Virtual_Substitution.html

Equality Virtual Substitution

$$\exists x. (y^2 x^2 = 2 \wedge w(x^2 + 1) = 0)$$

$$\exists x. \left(x = \pm \sqrt{\frac{2}{y^2}} \wedge w(x^2 + 1) = 0 \wedge y \neq 0 \right)$$

$$w\left(\left(\frac{2}{y^2}\right) + 1\right) = 0 \wedge y \neq 0$$

$$w(2 + y^2) = 0 \wedge y \neq 0$$

General Virtual Substitution

$$\exists x. (x^2 - 5 < 0 \wedge -x^2 + 2 < 0)$$

Plugging in roots 

General Virtual Substitution

$$\exists x. (x^2 - 5 < 0 \wedge -x^2 + 2 < 0)$$

Plugging in roots



Plugging in ranges



Use continuity of polynomials


General Virtual Substitution

$$\exists x. (x^2 - 5 < 0 \wedge -x^2 + 2 < 0)$$

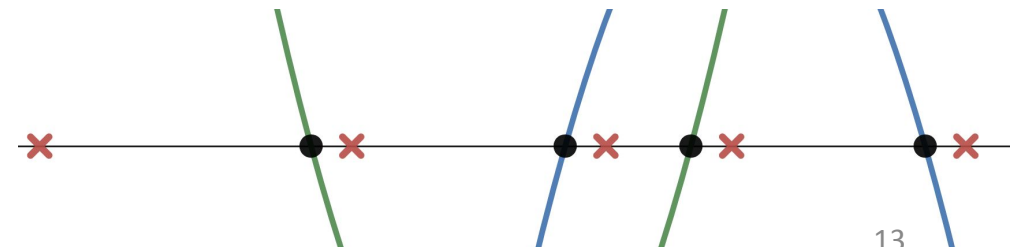
Plugging in roots 

Plugging in ranges 

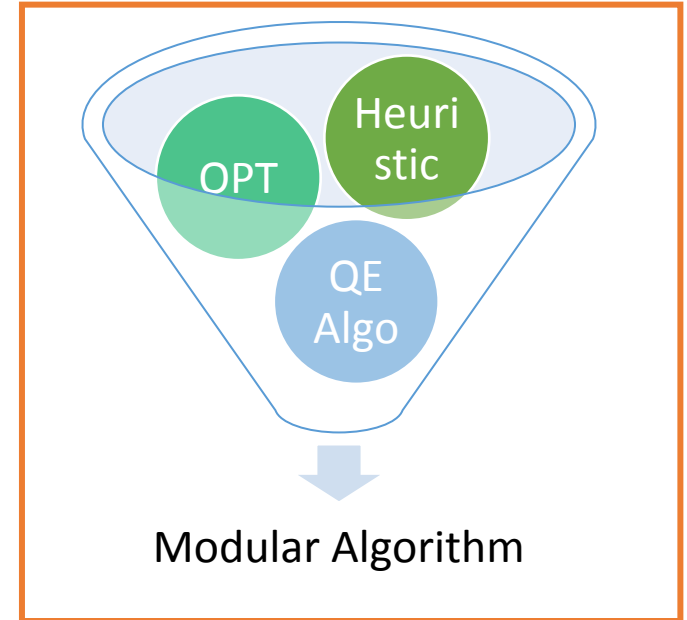
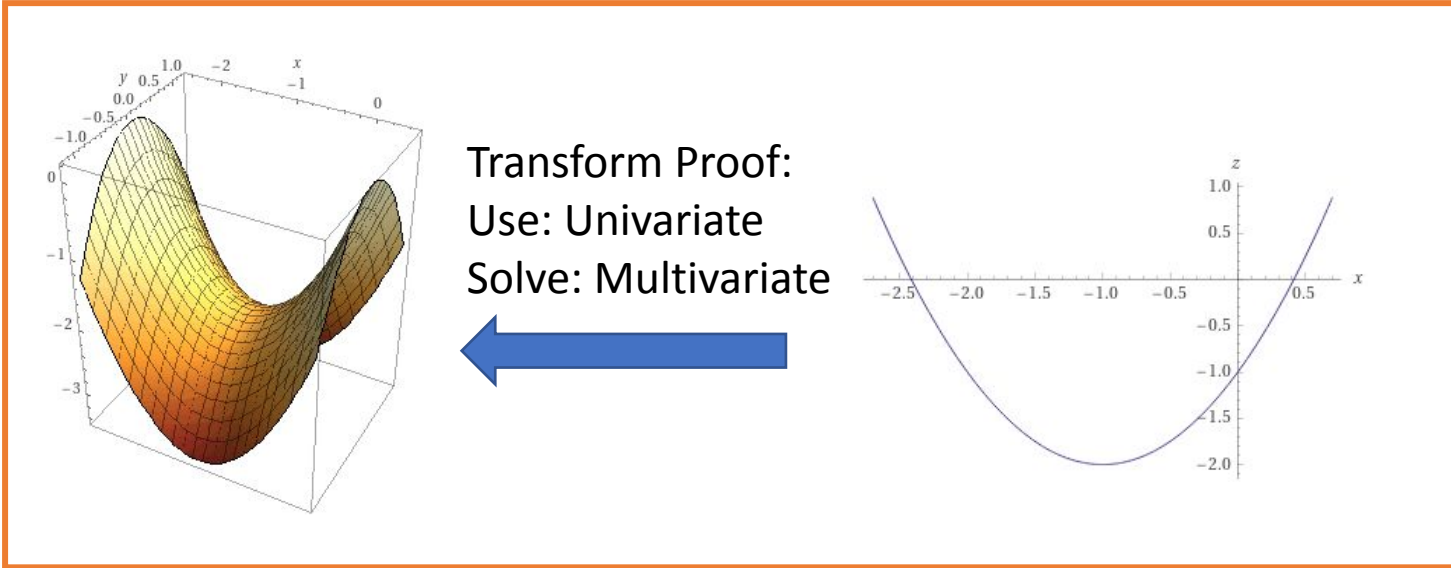
Use continuity of polynomials

Off-roots: $r + \epsilon$ 

Also $-\infty$

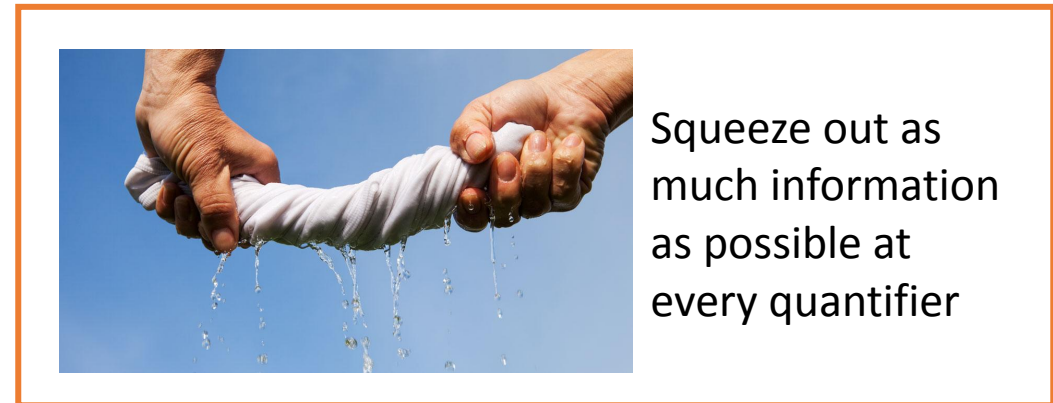


Implementation Highlights

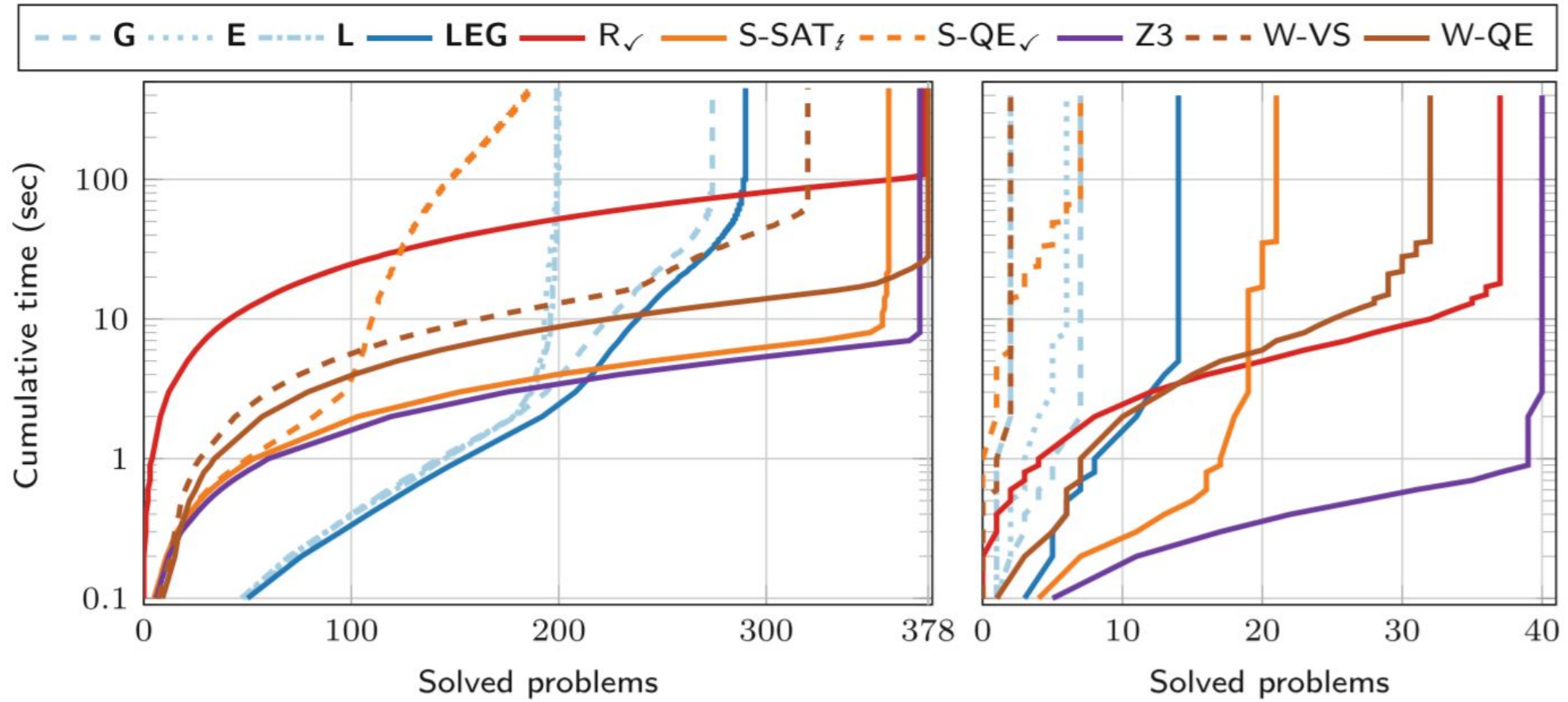


Block Quantifiers:
Run heuristic to pick first to eliminate

$$\exists x_1. \exists x_2. \exists x_3. \exists x_4. \exists x_5. F$$



Benchmark Testing



(a) CADE09 (378 examples)

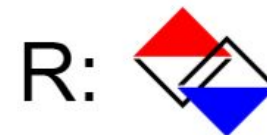
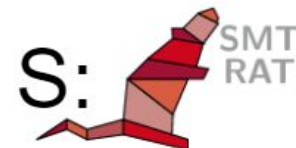
(b) Economics (45 examples)

Results

- Test for “A” and “¬A”
 - Both passed: “A” is true, “¬A” is false
 - Only one passed
 - Contradiction: “A” is true, “¬A” is true – Can’t both be true!



Z3: 



Virtual Substitution is

- Correct!
 - Preserve formula equivalence
 - Verified in Isabelle/HOL

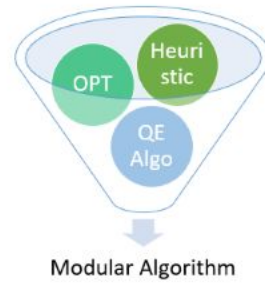
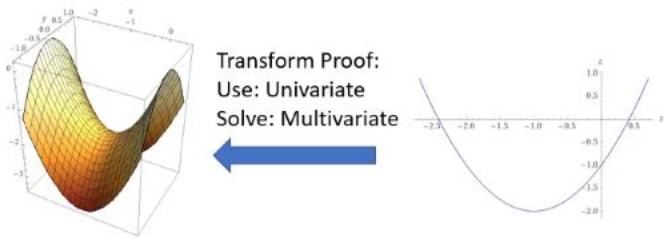
100

- Efficient!
 - Promising
 - Experimentally tested



Questions?

Implementation Highlights



Block Quantifiers:
Run heuristic to pick first to eliminate

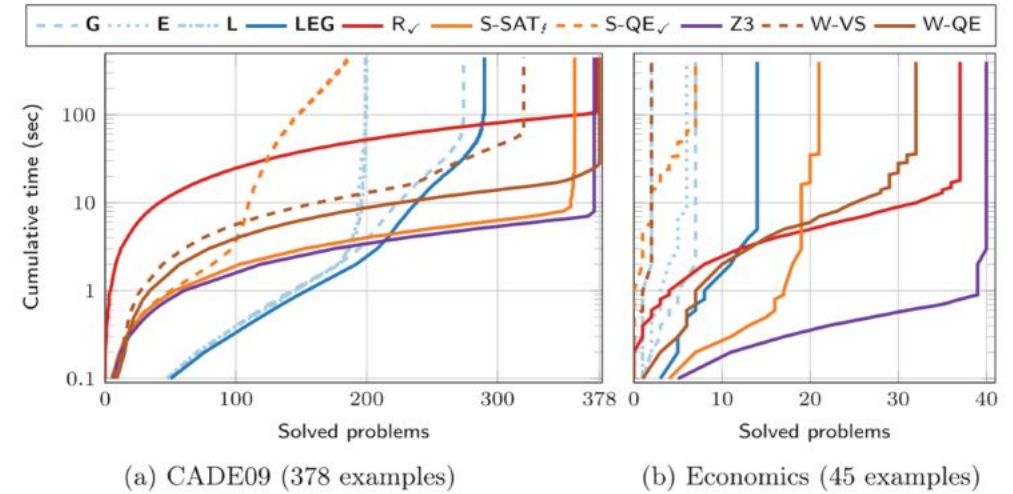
$$\exists x_1. \exists x_2. \exists x_3. \exists x_4. \exists x_5. F$$



Squeeze out as much information as possible at every quantifier

15

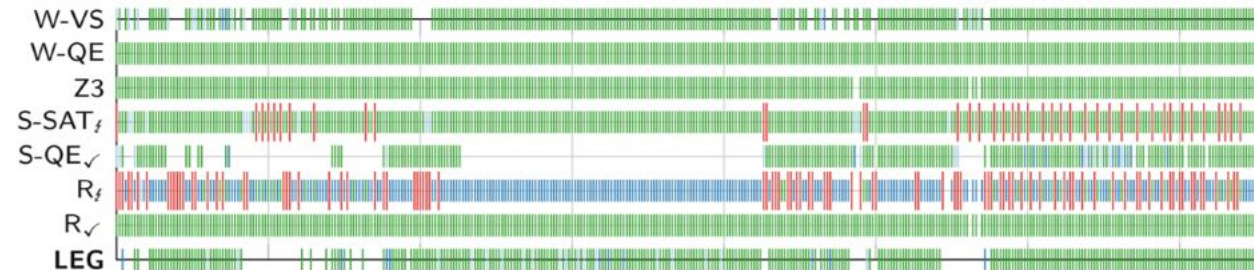
Benchmark Testing



15

Results

- Test for “A” and “¬A”
 - Both passed: “A” is true, “¬A” is false
 - Only one passed
 - Contradiction: “A” is true, “¬A” is true – Can’t both be true!



17