## Selected Decision Procedures and Techniques for SMT

- More on combination
- theories sharing sets
- convex theory
- Un-interpreted function symbols
(quantifier-free first-order logic)
- Ground terms (unification and dis-unification)
- Integers and bitvectors
- Quantifier instantiation


## SMT

## decidable

## quantifier-free combination

using $\wedge, \vee$, ᄀ
quantifier-free

## quantifier-free

## SAT <br> solver

linear programing solver
congruence closure implementation

## Satisfiability modulo theories (SMT) solver

# State of the art SMT solvers combine formulas with disjoint signatures (Nelson-Oppen approach) <br> $$
x<y+1 \wedge y<x+1 \wedge x^{\prime}=f(x) \wedge y^{\prime}=f(y) \wedge x^{\prime}=y^{\prime}+1
$$ 

linear programing solver

$$
\begin{aligned}
& x<y+1 \\
& y<x+1 \\
& x^{\prime}=y^{\prime}+1
\end{aligned}
$$

$$
0=1
$$

## SMT

congruence closure implementation
exchange equalities on demand

## Essence of such existing approach is reduction to equalities

$$
x<y+1 \wedge y<x+1 \wedge x^{\prime}=f(x) \wedge y^{\prime}=f(y) \wedge x^{\prime}=y^{\prime}+1
$$

reduction for SMT
reduction for congruence

$$
\begin{array}{ll}
x<y+1 & \\
y<x+1 & \exists(<)_{y}(+) \\
x^{\prime}=y^{\prime}+1 & x^{\prime}=f(x) \\
y^{\prime}=f(y)
\end{array}
$$

exchange equalities eagerly
unsatifiable propositional combination of equalities

## Generalize this reduction to sets of elements

## reduction for a logic quantified sets

$\forall x . x \in A \rightarrow x \in B$
$D=A \cup\{c\}$
quantifier elimination
$A \mu B$
$D=A \cup\{c\}$

$$
|\mathrm{D}| \leq|\mathrm{A}|
$$

$$
\{c\} \cap B=\varnothing
$$

unsatisfiable quantifier-free formula about sets

## Why the example is unsatisfiable


$A \mu B \quad|D| \leq|A|$
$D=A \cup\{c\}$
$\{c\} \cap B=\varnothing$
unsatisfiable quantifier-free formula about sets

## Soundness and Completeness by Definition

(3) symbols to extend are disjoint
across components
reduction for
...
prover for data structures
reduction for logic of set images
(1) $R$ is a consequence (in language of sets)
(2) models of R extend to models of original formula

$$
|\mathrm{D}| \leq|\mathrm{A}|
$$

$$
\{c\} \cap B=\varnothing
$$

## Essence of the reduction is simple

$$
\exists y . \exists z . \exists \mathrm{h} . \quad(\mathrm{P}(\mathrm{~h}, \mathrm{y}) \wedge \mathrm{Q}(\mathrm{y}, \mathrm{z}))
$$

is equivalent to

$$
\begin{aligned}
& \exists y \cdot((\exists h \cdot P(h, y)) \wedge(\exists z \cdot Q(y, z))) \\
& \exists y \cdot\left(\quad R_{P}(y) \wedge R_{Q}(y)\right)
\end{aligned}
$$

Reduction eliminates local symbols, h from P , gives formula $R_{P}(y)$ equivalent to $\exists \mathrm{h} . \mathrm{P}(\mathrm{h}, \mathrm{y})$
Quantifiers may be bounded and higher-order Applies to Nelson-Oppen and more generally

