

Decision Procedures for Logical Theories

Summary

Viorica Sofronie-Stokkermans

Overview

- **Theories**

- decidability for specific fragments

- **Extensions and combinations of theories**

- decidability and modularity for specific fragments

positive answers and limitations

- **Applications**

Overview

- **Theories**

- decidability for specific fragments

- **Extensions and combinations of theories**

- decidability and modularity results

positive answers and limitations

- **Applications**

Decidable theories

$\text{Th}(\mathbb{Z}_+)$ (Presburger arithmetic) dec.in 3EXPTIME [Presburger'29]

Idea

- decision procedure for the quantifier-free fragment
- method for quantifier elimination

Undecidable theories ...

... with decidable subfragments

- | | | |
|---|--|---|
| <ul style="list-style-type: none">• $\text{Th}(\Sigma\text{-alg})$• Theories of lists or arrays | | decision procedures known e.g.
for universal formulae or clauses |
|---|--|---|

Methods:

- Congruence closure (for $\text{Th}_{\forall}(\Sigma\text{-alg})$; also for theories of lists)
[Nelson, Oppen 1980], [Downey, Sethi, Tarjan, 1980]
- Superposition (refinement of resolution)
[Armando, Ranise, Rusinowitch 2001, 2003]

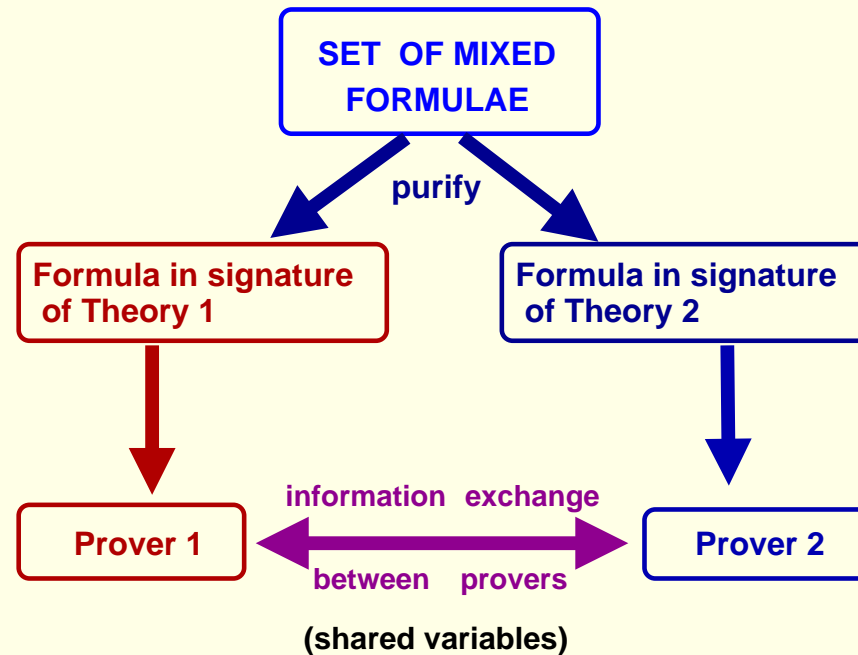
Overview

- **Theories** (syntactic vs. semantic view)
 - decidability for specific fragments
- **Combinations of theories**
 - decidability and modularity results
 - positive answers and limitations
- **Applications**

Nelson/Oppen procedure

- reasoning in combinations of theories over disjoint signatures
[Nelson, Oppen 1979], [Oppen 1980]

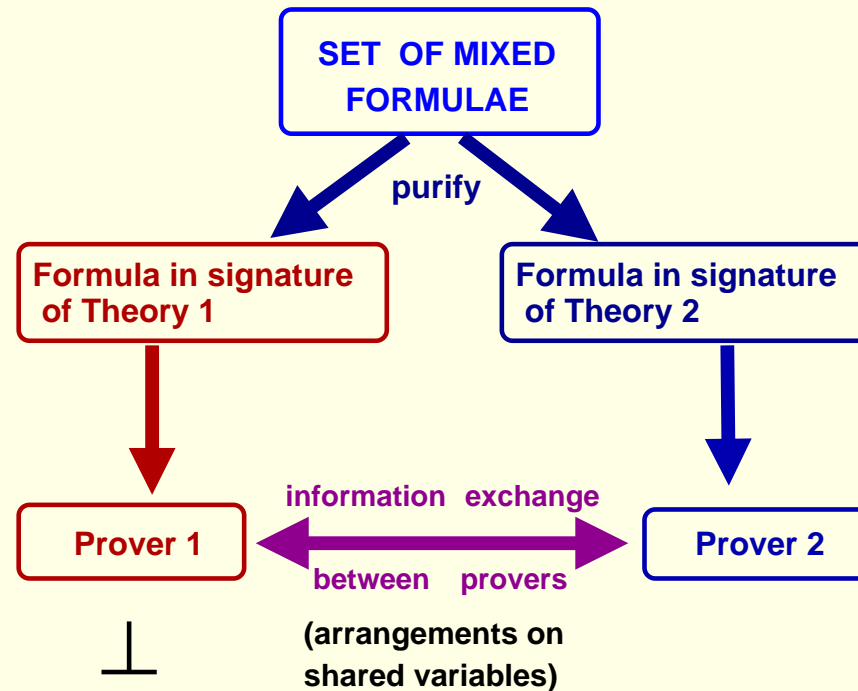
- general principle



Nelson/Oppen procedure

- reasoning in combinations of theories over disjoint signatures
[Nelson, Oppen 1979], [Oppen 1980]

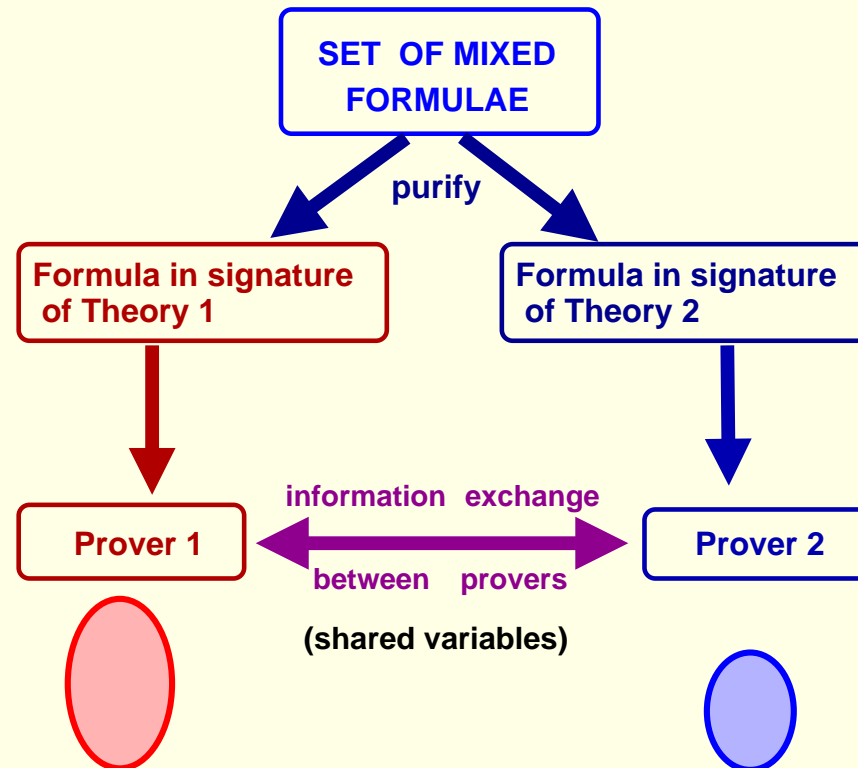
- general principle



Nelson/Oppen procedure

- reasoning in combinations of theories over disjoint signatures
[Nelson, Oppen 1979], [Oppen 1980]

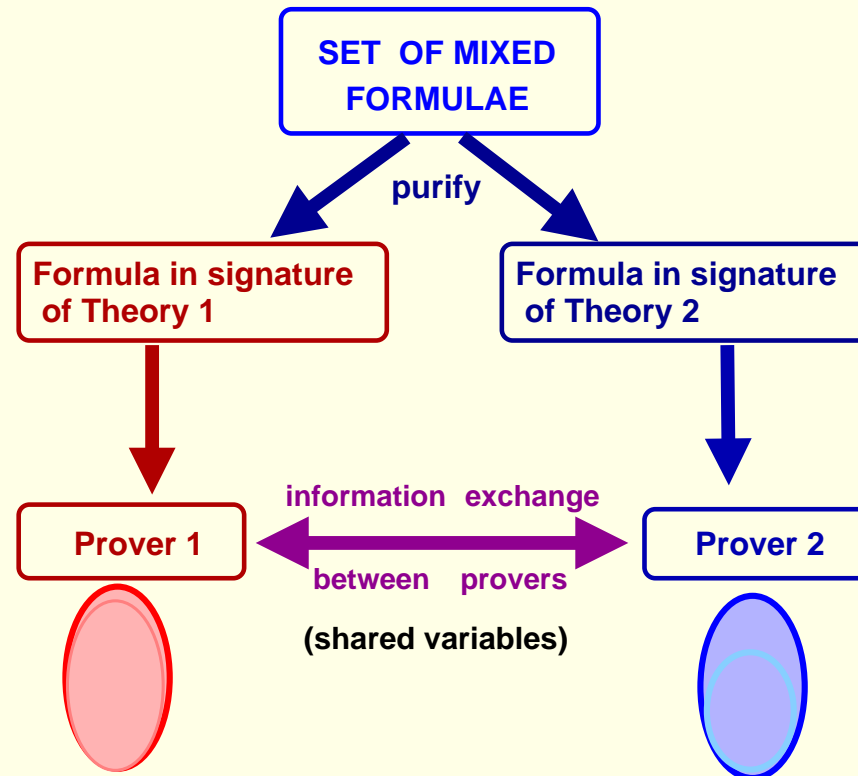
- general principle



Nelson/Oppen procedure

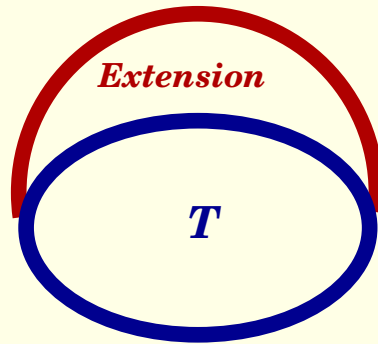
- reasoning in combinations of theories over disjoint signatures
[Nelson, Oppen 1979], [Oppen 1980]

- general principle



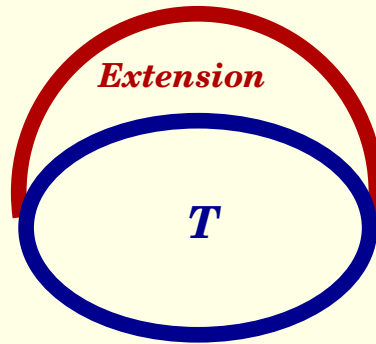
- additional condition: stable infinity

Theory extensions



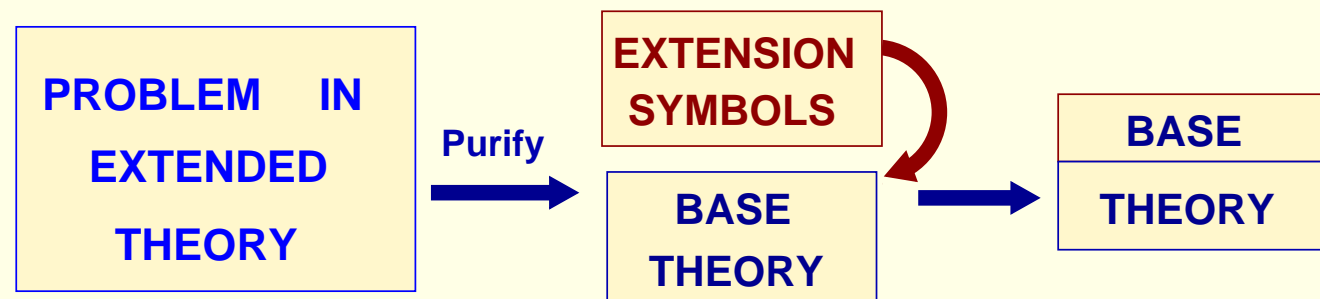
- Shostak's method reasoning in extensions with free functions
[Shostak 1984], [Ganzinger 2002]
NO + built-in simplification w.r.t. base theory
use canonizer/solver for the base theory

Theory extensions

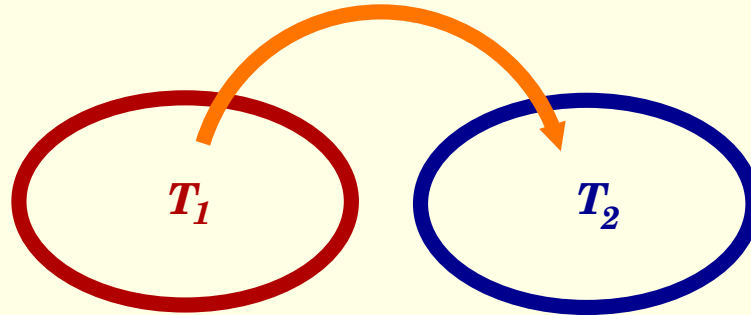


Hierarchic reasoning: e.g. for local theory extensions [Sofronie 2005]

Idea:

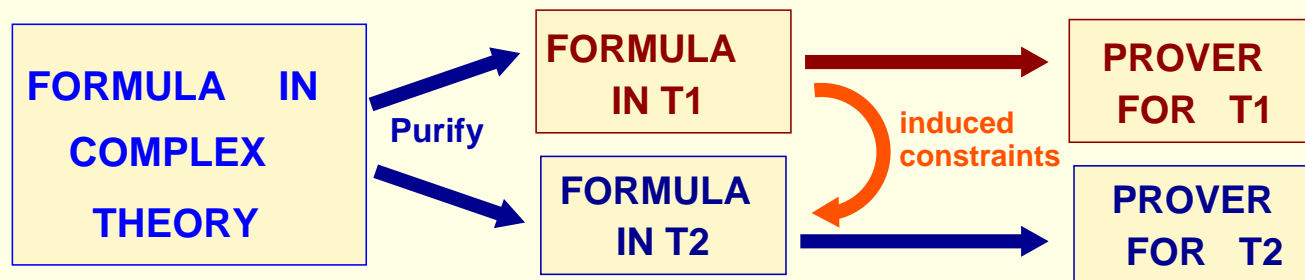


More general combinations: bridging functions



Example: Recursive datatypes + length: [Zhang, Sipma, Manna 2004]

Idea:



Beyond the universal fragment: quantifier elimination

Efficient theory reasoning

- Combine SAT-based reasoning with theory reasoning
[Ganzinger, Hagen, Nieuwenhuis, Oliveras, Tinelli 2002]
 - $DPLL(\mathcal{T})$
 - useful especially for large inputs, because it helps to rule out obvious cases of inconsistency at propositional level.

Applications

Discussed:

- Translation validation

use decision procedures as black-boxes.

Many application domains

- Distributed databases
- Program verification
- Verification of complex systems
- Mathematics

Conclusions

- Very dynamic field, many results are very recent
- Especial interests at the moment
 - relax condition of stable infinity in Nelson/Oppen procedure
 - combinations of theories over non-disjoint signatures
 - modularity in theorem proving
 - beyond the universal fragment