# First Order Theories - Combination Theories

K. Subramani[1]

[1]Lane Department of Computer Science and Electrical Engineering
West Virginia University

March 11 2013

# Outline

# Outline

# Introduction

# Introduction

## Main Ideas

# Introduction

## Main Ideas

In programming language verification, the formula whose validity (or satisfiability) needs to be checked typically does not belong to a single theory.

# Introduction

## Main Ideas

In programming language verification, the formula whose validity (or satisfiability) needs to be checked typically does not belong to a single theory. For instance, we may be interested in an assertion about an array of integers or an array of reals.

# Introduction

## Main Ideas

In programming language verification, the formula whose validity (or satisfiability) needs to be checked typically does not belong to a single theory. For instance, we may be interested in an assertion about an array of integers or an array of reals. Thus, single-theory decision procedures are essentially useless, unless they can be combined.

# Combination Theories

# Combination Theories

## Main points

# Combination Theories

## Main points

The theory $T$ defined by two theories $T_1$ and $T_2$ is said to be a combination theory, if $\Sigma_T = \Sigma_1 \cup \Sigma_2$ and $\mathcal{A}_T = \mathcal{A}_1 \cup \mathcal{A}_2$.

# Combination Theories

## Main points

The theory $T$ defined by two theories $T_1$ and $T_2$ is said to be a combination theory, if $\Sigma_T = \Sigma_1 \cup \Sigma_2$ and $\mathcal{A}_T = \mathcal{A}_1 \cup \mathcal{A}_2$. This definition can be applied inductively to account for more than two theories.

# Combination Theories

**Main points**

The theory $T$ defined by two theories $T_1$ and $T_2$ is said to be a combination theory, if $\Sigma_T = \Sigma_1 \cup \Sigma_2$ and $\mathcal{A}_T = \mathcal{A}_1 \cup \mathcal{A}_2$. This definition can be applied inductively to account for more than two theories. For instance, we could construct the theory of arrays of lists of reals.

# Nelson-Oppen framework

# Nelson-Oppen framework

## Main Points

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following:

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

1. Satisfiability in the quantifier-free fragment of $T_1$ is decidable,

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

1. Satisfiability in the quantifier-free fragment of $T_1$ is decidable,
2. Satisfiability in the quantifier-free fragment of $T_2$ is decidable,

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

1. Satisfiability in the quantifier-free fragment of $T_1$ is decidable,
2. Satisfiability in the quantifier-free fragment of $T_2$ is decidable,
3. certain technical requirements are met,

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

1. Satisfiability in the quantifier-free fragment of $T_1$ is decidable,
2. Satisfiability in the quantifier-free fragment of $T_2$ is decidable,
3. certain technical requirements are met,

satisfiability in the quantifier-free fragment of the combination theory $T = T_1 \cup T_2$ is decidable.

# Nelson-Oppen framework

## Main Points

Nelson and Oppen proved the following: Given two theories $T_1$ and $T_2$, with $\Sigma_1 \cap \Sigma_2 = \{=\}$, such that

1. Satisfiability in the quantifier-free fragment of $T_1$ is decidable,
2. Satisfiability in the quantifier-free fragment of $T_2$ is decidable,
3. certain technical requirements are met,

satisfiability in the quantifier-free fragment of the combination theory $T = T_1 \cup T_2$ is decidable. Furthermore, if the decision procedures for $T_1$ and $T_2$ are in **P**, then so is the combined decision procedure for $T_1 \cup T_2$.

# Examples

# Examples

## Example

# Examples

## Example

1. Consider the formula

# Examples

## Example

1. Consider the formula $F\ :\ (a = b) \rightarrow a[i] \geq b[i]$.

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid?

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid?

# Examples

## Example

1. Consider the formula $F \ : \ (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^= \cup T_{\mathbb{Z}}$-valid?

# Examples

## Example

1. Consider the formula $F\ :\ (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^{=} \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula

# Examples

## Example

1. Consider the formula $F \ : \ (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^= \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G \ : \ 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^= \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid?

# Examples

## Example

1. Consider the formula $F\ :\ (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^{=} \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G\ :\ 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable?

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^{=} \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Z}}$?

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^{=} \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G : 1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Z}}$? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Q}}$?

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^= \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Z}}$? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Q}}$?
3. Consider the formula

# Examples

## Example

1. Consider the formula $F : (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^= \cup T_\mathbb{Z}$-valid?
2. Consider the formula $G : 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable? Is $G$ satisfiable in $T_E \cup T_\mathbb{Z}$? Is $G$ satisfiable in $T_E \cup T_\mathbb{Q}$?
3. Consider the formula $H : f(f(x) - f(y)) \neq f(z) \wedge x \leq y \wedge (y + z) \leq x \wedge 0 \leq z$.

# Examples

## Example

1. Consider the formula $F\ :\ (a = b) \rightarrow a[i] \geq b[i]$.
   Is it valid? Is it $T_A$-valid? Is it $T_A^{=} \cup T_{\mathbb{Z}}$-valid?
2. Consider the formula $G\ :\ 1 \leq x \wedge x \leq 2 \wedge f(x) \neq f(1) \wedge f(x) \neq f(2)$.
   Is $G$ valid? Is $G$ satisfiable? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Z}}$? Is $G$ satisfiable in $T_E \cup T_{\mathbb{Q}}$?
3. Consider the formula $H\ :\ f(f(x) - f(y)) \neq f(z) \wedge x \leq y \wedge (y + z) \leq x \wedge 0 \leq z$.
   Is $H$ $(T_E \cup T_{\mathbb{Q}})$-satisfiable?