

# Shostak's Method

talk by Arnaud Fietzke

Supervised by Uwe Waldmann

17th January 2006

# Outline

- 1 Introduction
  - Motivation
  - A Nelson-Oppen procedure
- 2 Shostak's method
  - Solvability
  - Examples of solvable theories
  - System S
  - Combinations of theories
- 3 Summary
  - Conclusion
  - Outlook

# Motivation

- The Nelson-Open procedure decides combinations of arbitrary numbers of (certain) theories.
- But: it needs to repeatedly test large sets of constraints for satisfiability.
- Shostak's method promises a **more efficient** procedure for certain classes of theories.

# Motivation

- The Nelson-Open procedure decides combinations of arbitrary numbers of (certain) theories.
- But: it needs to repeatedly test large sets of constraints for satisfiability.
- Shostak's method promises a **more efficient** procedure for certain classes of theories.

# Motivation

- The Nelson-Oppen procedure decides combinations of arbitrary numbers of (certain) theories.
- But: it needs to repeatedly test large sets of constraints for satisfiability.
- Shostak's method promises a **more efficient** procedure for certain classes of theories.

# Motivation

We will model Shostak's method as a refinement of a Nelson-Open procedure for the **combination of a convex theory together with free function symbols**. [Ganzinger '02]

# Definitions

- A  $\Sigma$ -theory  $\mathcal{T}$  is a class of  $\Sigma$ -models
  - we will consider only first-order signatures of function symbols (i.e. **without** predicates)
  - formal equality  $\approx$  is always assumed to be in the signature
- A theory  $\mathcal{T}$  is **convex** if  
whenever  $\mathcal{T} \models \forall X(\Gamma \rightarrow A_1 \vee \dots \vee A_n)$   
then  $\exists j : \mathcal{T} \models \forall X(\Gamma \rightarrow A_j)$   
for any finite set  $\Gamma$  of  $\Sigma$ -equations, and  $\Sigma$ -equations  $A_j$ .

# Definitions

- A  $\Sigma$ -theory  $\mathcal{T}$  is a class of  $\Sigma$ -models
  - we will consider only first-order signatures of function symbols (i.e. **without** predicates)
  - formal equality  $\approx$  is always assumed to be in the signature
- A theory  $\mathcal{T}$  is **convex** if  
whenever  $\mathcal{T} \models \forall X(\Gamma \rightarrow A_1 \vee \dots \vee A_n)$   
then  $\exists j : \mathcal{T} \models \forall X(\Gamma \rightarrow A_j)$   
for any finite set  $\Gamma$  of  $\Sigma$ -equations, and  $\Sigma$ -equations  $A_j$ .

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
- Suppose two disjoint signatures:
  - $\Delta$  of **defined** function symbols
  - $\Phi$  of **free** function symbols
- $\mathcal{T}$  is a  $\Delta$ -theory
- $\mathcal{T}^\Phi = \{ I \in (\Delta \cup \Phi)\text{-structures} \mid I|_\Delta \in \mathcal{T} \}$

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
- Suppose two disjoint signatures:
  - $\Delta$  of **defined** function symbols
  - $\Phi$  of **free** function symbols
- $\mathcal{T}$  is a  $\Delta$ -theory
- $\mathcal{T}^\Phi = \{ I \in (\Delta \cup \Phi)\text{-structures} \mid I|_\Delta \in \mathcal{T} \}$

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
- Suppose two disjoint signatures:
  - $\Delta$  of **defined** function symbols
  - $\Phi$  of **free** function symbols
- $\mathcal{T}$  is a  $\Delta$ -theory
- $\mathcal{T}^\Phi = \{ I \in (\Delta \cup \Phi)\text{-structures} \mid I_\Delta \in \mathcal{T} \}$

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
- Suppose two disjoint signatures:
  - $\Delta$  of **defined** function symbols
  - $\Phi$  of **free** function symbols
- $\mathcal{T}$  is a  $\Delta$ -theory
- $\mathcal{T}^\Phi = \{ I \in (\Delta \cup \Phi)\text{-structures} \mid I|_\Delta \in \mathcal{T} \}$

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
  - Assuming the clausal validity problem in  $\mathcal{T}$  is decidable, we want to **decide clausal validity in  $\mathcal{T}^\Phi$** .
- ⇒ we need a procedure that decides the **unsatisfiability** of a conjunction of equalities and disequalities over  $\Delta$ , and definitions of free function symbols.

# Definitions

- We want to combine a convex theory  $\mathcal{T}$  with the theory of free function symbols.
  - Assuming the clausal validity problem in  $\mathcal{T}$  is decidable, we want to **decide clausal validity in  $\mathcal{T}^\Phi$** .
- ⇒ we need a procedure that decides the **unsatisfiability** of a conjunction of equalities and disequalities over  $\Delta$ , and definitions of free function symbols.

# Inference system $\mathcal{NO}$

- $\mathcal{NO}$  works on **configurations** of the form  $E \parallel D$  where
  - $E$ : set of equations and disequations over  $\mathcal{T}$  (**constraints**)
  - $D$ : set of function definitions  $F \approx u$   
 $F = f(s_1, \dots, s_n)$ ,  $f \in \Phi$ ,  $s_i, u$  are  $\Delta$ -terms
- $E \parallel D$  means:  $\exists X(E \wedge D)$  satisfiable in  $\mathcal{T}^\Phi$

# Inference system $\mathcal{NO}$

- $\mathcal{NO}$  works on **configurations** of the form  $E \parallel D$  where
  - $E$ : set of equations and disequations over  $\mathcal{T}$  (**constraints**)
  - $D$ : set of function definitions  $F \approx u$   
 $F = f(s_1, \dots, s_n)$ ,  $f \in \Phi$ ,  $s_i, u$  are  $\Delta$ -terms
- $E \parallel D$  means:  $\exists X(E \wedge D)$  satisfiable in  $\mathcal{T}^\Phi$

# Inference system $\mathcal{NO}$

$$E = \{s_1 \approx t_1, \dots, s_n \approx t_n, w_1 \not\approx v_1, \dots, w_m \not\approx v_m\}$$

$$D = \{F_1 \approx u_1, F_2 \approx u_2, \dots\}$$

## CONTRADICTION

$$\frac{E \cup D}{\perp}$$

if  $\mathcal{T} \models \forall X(E \rightarrow \perp)$

# Inference system $\mathcal{NO}$

$$E = \{s_1 \approx t_1, \dots, s_n \approx t_n, w_1 \not\approx v_1, \dots, w_m \not\approx v_m\}$$

$$D = \{F_1 \approx u_1, F_2 \approx u_2, \dots\}$$

## CONTRADICTION

$$\frac{E \sqcup D}{\perp}$$

if  $\mathcal{T} \models \forall X(E \rightarrow \perp)$

## COMPOSE

$$\frac{E \sqcup D \cup \{f(s_1, \dots, s_n) \approx s, f(s'_1, \dots, s'_n) \approx s'\}}{E \cup \{s \approx s'\} \sqcup D \cup \{f(s_1, \dots, s_n) \approx s\}}$$

if  $\mathcal{T} \models \forall X(E \rightarrow s_i \approx s'_i)$ , for  $1 \leq i \leq n$

# Inference system $\mathcal{NO}$

$\mathcal{NO}$  is

- **sound**, i.e.

if  $E \upharpoonright D \vdash E' \upharpoonright D'$ , then  $\mathcal{T}^\Phi \models \forall X (E \wedge D \leftrightarrow E' \wedge D')$   
 and if  $E \upharpoonright D \vdash \perp$ , then  $E \cup D$  **unsatisfiable** in  $\mathcal{T}^\Phi$ .

- **complete** if  $\mathcal{T}$  is convex

i.e.  $E \wedge D$  unsatisfiable in  $\mathcal{T}^\Phi \Rightarrow E \upharpoonright D \vdash \perp$

i.e.  $\mathcal{NO}$  terminates with  $E \upharpoonright D \Rightarrow E \wedge D$  satisfiable in  $\mathcal{T}^\Phi$

Proof

# Inference system $\mathcal{NO}$

$\mathcal{NO}$  is

- **sound**, i.e.

if  $E \parallel D \vdash E' \parallel D'$ , then  $\mathcal{T}^\Phi \models \forall X (E \wedge D \leftrightarrow E' \wedge D')$   
and if  $E \parallel D \vdash \perp$ , then  $E \cup D$  **unsatisfiable** in  $\mathcal{T}^\Phi$ .

- **complete** if  $\mathcal{T}$  is convex

i.e.  $E \wedge D$  unsatisfiable in  $\mathcal{T}^\Phi \Rightarrow E \parallel D \vdash \perp$

i.e.  $\mathcal{NO}$  terminates with  $E \parallel D \Rightarrow E \wedge D$  satisfiable in  $\mathcal{T}^\Phi$

Proof

# $NO$ can be inefficient

Assume  $E$  and  $D$  are large and  $E$  is consistent, e.g.

$$E = \{ [4x + y + 7z \approx 30], [2x + 3y \approx 19], [x \approx 2z + 1], \dots \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18], [f(4y + 1) \approx z], \dots \}$$

- CONTRADICTION cannot be applied
- COMPOSE has to check  
 $\mathcal{T} \models \forall X(E \rightarrow s_i \approx s'_i)$  for every pair  $f(s_i) \approx u, f'(s'_i) \approx u'$  in  $D$
- How about **solving and simplifying constraints** instead?

# $NO$ can be inefficient

Assume  $E$  and  $D$  are large and  $E$  is consistent, e.g.

$$E = \{ [4x + y + 7z \approx 30], [2x + 3y \approx 19], [x \approx 2z + 1], \dots \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18], [f(4y + 1) \approx z], \dots \}$$

- CONTRADICTION cannot be applied
- COMPOSE has to check  
 $\mathcal{T} \models \forall X(E \rightarrow s_i \approx s'_i)$  for every pair  $f(s_i) \approx u, f'(s'_i) \approx u'$  in  $D$
- How about solving and simplifying constraints instead?

# *NO* can be inefficient

Assume  $E$  and  $D$  are large and  $E$  is consistent, e.g.

$$E = \{ [4x + y + 7z \approx 30], [2x + 3y \approx 19], [x \approx 2z + 1], \dots \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18], [f(4y + 1) \approx z], \dots \}$$

- CONTRADICTION cannot be applied
- COMPOSE has to check  
 $\mathcal{T} \models \forall X(E \rightarrow s_i \approx s'_i)$  for every pair  $f(s_i) \approx u, f'(s'_i) \approx u'$  in  $D$
- How about **solving and simplifying constraints** instead?

# Solvability

- a **solver** is a computable function that takes a  $\mathcal{T}$ -equation  $s \approx t$  and returns:
  - $\perp$  iff  $s \approx t$  is **unsatisfiable**
  - $\sigma = \{x_1 \Rightarrow u_1, \dots, x_n \Rightarrow u_n\}$  iff  $s \approx t$  is **satisfiable**
- $\sigma$  finite set of rewrite rules over  $\Delta$  such that
  - the  $x_i$  are pairwise different variables occurring in  $s \approx t$ ;
  - the  $x_i$  do not occur in any  $u_j$ ; and
  - $\mathcal{T} \models \forall X[(s \approx t) \leftrightarrow \exists Y(x_1 \approx u_1 \wedge \dots \wedge x_n \approx u_n)]$
- $\sigma = \emptyset$  iff  $s \approx t$  is **valid**

# Solvability

- a **solver** is a computable function that takes a  $\mathcal{T}$ -equation  $s \approx t$  and returns:
  - $\perp$  iff  $s \approx t$  is **unsatisfiable**
  - $\sigma = \{x_1 \Rightarrow u_1, \dots, x_n \Rightarrow u_n\}$  iff  $s \approx t$  is **satisfiable**
- $\sigma$  finite set of rewrite rules over  $\Delta$  such that
  - the  $x_i$  are pairwise different variables occurring in  $s \approx t$ ;
  - the  $x_i$  do not occur in any  $u_j$ ; and
  - $\mathcal{T} \models \forall X[(s \approx t) \leftrightarrow \exists Y(x_1 \approx u_1 \wedge \dots \wedge x_n \approx u_n)]$
- $\sigma = \emptyset$  iff  $s \approx t$  is **valid**

# Solvability

- a **solver** is a computable function that takes a  $\mathcal{T}$ -equation  $s \approx t$  and returns:
  - $\perp$  iff  $s \approx t$  is **unsatisfiable**
  - $\sigma = \{x_1 \Rightarrow u_1, \dots, x_n \Rightarrow u_n\}$  iff  $s \approx t$  is **satisfiable**
- $\sigma$  finite set of rewrite rules over  $\Delta$  such that
  - the  $x_i$  are pairwise different variables occurring in  $s \approx t$ ;
  - the  $x_i$  do not occur in any  $u_j$ ; and
  - $\mathcal{T} \models \forall X[(s \approx t) \leftrightarrow \exists Y(x_1 \approx u_1 \wedge \dots \wedge x_n \approx u_n)]$
- $\sigma = \emptyset$  iff  $s \approx t$  is **valid**

# Solvability

- a **solver** is a computable function that takes a  $\mathcal{T}$ -equation  $s \approx t$  and returns:
  - $\perp$  iff  $s \approx t$  is **unsatisfiable**
  - $\sigma = \{x_1 \Rightarrow u_1, \dots, x_n \Rightarrow u_n\}$  iff  $s \approx t$  is **satisfiable**
- A theory is **solvable** if it has a solver.

# Convex theory of *cons*, *car*, *cdr*

[Shostak '84]

axiomatized by:

$$A_1 \quad \text{car}(\text{cons}(x, y)) = x$$

$$A_2 \quad \text{cdr}(\text{cons}(x, y)) = y$$

$$A_3 \quad \text{cons}(\text{car}(x), \text{cdr}(x)) = x$$

$$\text{cdr}(\text{car}(y)) = \text{cdr}(x)$$

$$\rightarrow_{A_2} \text{car}(y) = \text{cons}(b, \text{cdr}(x)), \quad b \text{ fresh variable}$$

$$\rightarrow_{A_1} y = \text{cons}(\text{cons}(b, \text{cdr}(x)), c), \quad c \text{ fresh variable}$$

$$\sigma = \{y \Rightarrow \text{cons}(\text{cons}(b, \text{cdr}(x)), c)\}$$

# Convex theory of *cons*, *car*, *cdr*

[Shostak '84]

axiomatized by:

$$A_1 \quad \text{car}(\text{cons}(x, y)) = x$$

$$A_2 \quad \text{cdr}(\text{cons}(x, y)) = y$$

$$A_3 \quad \text{cons}(\text{car}(x), \text{cdr}(x)) = x$$

$$\text{cdr}(\text{car}(y)) = \text{cdr}(x)$$

$$\rightarrow_{A_2} \text{car}(y) = \text{cons}(b, \text{cdr}(x)), \quad b \text{ fresh variable}$$

$$\rightarrow_{A_1} y = \text{cons}(\text{cons}(b, \text{cdr}(x)), c), \quad c \text{ fresh variable}$$

$$\sigma = \{y \Rightarrow \text{cons}(\text{cons}(b, \text{cdr}(x)), c)\}$$

# Convex theory of *cons*, *car*, *cdr*

[Shostak '84]

axiomatized by:

$$A_1 \quad \text{car}(\text{cons}(x, y)) = x$$

$$A_2 \quad \text{cdr}(\text{cons}(x, y)) = y$$

$$A_3 \quad \text{cons}(\text{car}(x), \text{cdr}(x)) = x$$

$$\text{cdr}(\text{car}(y)) = \text{cdr}(x)$$

$$\rightarrow_{A_2} \text{car}(y) = \text{cons}(b, \text{cdr}(x)), \quad b \text{ fresh variable}$$

$$\rightarrow_{A_1} y = \text{cons}(\text{cons}(b, \text{cdr}(x)), c), \quad c \text{ fresh variable}$$

$$\sigma = \{y \Rightarrow \text{cons}(\text{cons}(b, \text{cdr}(x)), c)\}$$

# Convex theory of *cons*, *car*, *cdr*

[Shostak '84]

axiomatized by:

$$A_1 \quad \text{car}(\text{cons}(x, y)) = x$$

$$A_2 \quad \text{cdr}(\text{cons}(x, y)) = y$$

$$A_3 \quad \text{cons}(\text{car}(x), \text{cdr}(x)) = x$$

$$\text{cdr}(\text{car}(y)) = \text{cdr}(x)$$

$$\rightarrow_{A_2} \text{car}(y) = \text{cons}(b, \text{cdr}(x)), \quad b \text{ fresh variable}$$

$$\rightarrow_{A_1} y = \text{cons}(\text{cons}(b, \text{cdr}(x)), c), \quad c \text{ fresh variable}$$

$$\sigma = \{y \Rightarrow \text{cons}(\text{cons}(b, \text{cdr}(x)), c)\}$$

# Real linear arithmetic

[Shostak '84]

- Equations and inequations between linear polynomials over real variables
- Can be trivially enriched with free function symbols
- Example:

$$3x + 2y = 2x + 4$$

$$\rightarrow x = -2y + 4$$

$$\sigma = \{x \Rightarrow -2y + 4\}$$

# Real linear arithmetic

[Shostak '84]

- Equations and inequations between linear polynomials over real variables
- Can be trivially enriched with free function symbols
- Example:

$$3x + 2y = 2x + 4$$

$$\rightarrow x = -2y + 4$$

$$\sigma = \{x \Rightarrow -2y + 4\}$$

# Integer linear arithmetic

[Shostak '84]

- Also works since new variables may be introduced
- Example:

$$17x - 49y = 30$$

→  $x = 49z - 4$ ,  $y = 17z - 2$ ,  $z$  fresh variable

$$\sigma = \{x \mapsto 49z - 4, y \mapsto 17z - 2\}$$

# Integer linear arithmetic

[Shostak '84]

- Also works since new variables may be introduced
- Example:

$$17x - 49y = 30$$

→  $x = 49z - 4$ ,  $y = 17z - 2$ ,  $z$  fresh variable

$$\sigma = \{x \Rightarrow 49z - 4, y \Rightarrow 17z - 2\}$$

# Shostak's method

- We will model Shostak's method as a refinement of  $\mathcal{NO}$ , assuming  $\mathcal{T}$  is solvable. [Ganzinger '02]
- System  $S$  works on configurations of the form  $U, R \parallel D$  where
  - $U$  set of disequations and "unsolved" equations
  - $R$  set of "solved" equations
  - $U, R \parallel D$  corresponds to  $U \cup R \parallel D$  in  $\mathcal{NO}$
  - Initial configurations are of the form  $U, \emptyset \parallel D$

# Shostak's method

- We will model Shostak's method as a refinement of  $\mathcal{NO}$ , assuming  $\mathcal{T}$  is solvable. [Ganzinger '02]
- System  $\mathcal{S}$  works on configurations of the form  $U, R \parallel D$  where
  - $U$  set of disequations and "unsolved" equations
  - $R$  set of "solved" equations
  - $U, R \parallel D$  corresponds to  $U \cup R \parallel D$  in  $\mathcal{NO}$
  - Initial configurations are of the form  $U, \emptyset \parallel D$

# Inference system $\mathcal{S}$ (1/4)

## CONTRADICTION in $\mathcal{NO}$

$$\frac{E \sqcup D}{\perp} \quad \text{if } \mathcal{T} \models \forall X(E \rightarrow \perp)$$

## CONTRADICTION

$$\frac{U \cup \{s \approx t\}, R \sqcup D}{\perp} \quad \text{if } \text{solve}(s \approx t) = \perp$$

$$\frac{U \cup \{s \not\approx t\}, R \sqcup D}{\perp} \quad \text{if } \text{solve}(s \approx t) = \emptyset$$

Inference system  $\mathcal{S}$  (2/4)COMPOSE in  $\mathcal{NO}$ 

$$\frac{E \parallel DU\{f(s_1, \dots, s_n) \approx s, f(s'_1, \dots, s'_n) \approx s'\}}{EU\{s \approx s'\} \parallel DU\{f(s_1, \dots, s_n) \approx s\}}$$

if  $\mathcal{T} \models \forall X(E \rightarrow s_i \approx s'_i)$ , for  $1 \leq i \leq n$

## COMPOSE

$$\frac{U, R \parallel DU\{f(s_1, \dots, s_n) \approx s, f(s'_1, \dots, s'_n) \approx s'\}}{UU\{s \approx s'\}, R \parallel DU\{f(s_1, \dots, s_n) \approx s\}}$$

if  $\text{solve}(s_i \approx s'_i) = \emptyset$ , for  $1 \leq i \leq n$

# Inference system $\mathcal{S}$ (3/4)

## SOLVE

$$\frac{U \cup \{s \approx t\}, R \parallel D}{U, R \cup \mathcal{S} \parallel D}$$

where

- $\mathcal{S} = \text{solve}(s \approx t) \neq \perp$
- $s$  and  $t$  irreducible by  $R$

# Inference system $\mathcal{S}$ (4/4)

## REDUCE

$$\frac{U, R \cup \{x \Rightarrow t\} \parallel D \cup \{F[x] \approx s\}}{U, R \cup \{x \Rightarrow t\} \parallel D \cup \{F[t] \approx s\}}$$

$$\frac{U \cup \{L[x]\}, R \cup \{x \Rightarrow t\} \parallel D}{U \cup \{L[t]\}, R \cup \{x \Rightarrow t\} \parallel D}$$

# Inference system $\mathcal{S}$

$\mathcal{S}$  is

- **sound**  
(Follows from the soundness of `solve`)
- **complete** if  $\mathcal{T}$  is convex **and solvable**  
(Follows from the completeness of  $\mathcal{NO}$ )

# Example

$$U = \{ [2x + 3y \approx 19], [4y \approx 12] \}$$

$$R = \emptyset$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \{ [2x + 3y \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \{ [2x + 9 \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

# Example

$$U = \{ [2x + 3y \approx 19], [4y \approx 12] \}$$

$$R = \emptyset$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \{ [2x + 3y \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \{ [2x + 9 \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

# Example

$$U = \{ [2x + 3y \approx 19], [4y \approx 12] \}$$

$$R = \emptyset$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \{ [2x + 3y \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(7y) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \{ [2x + 9 \approx 19] \}$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

## Example (cont'd)

$$U = \{ [2x + 9 \approx 19] \}$$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 15], [f(21) \approx 18] \}$$

->  $\perp$  follows by COMPOSE and CONTRADICTION.

## Example (cont'd)

$$U = \{ [2x + 9 \approx 19] \}$$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 15], [f(21) \approx 18] \}$$

->  $\perp$  follows by COMPOSE and CONTRADICTION.

## Example (cont'd)

$$U = \{ [2x + 9 \approx 19] \}$$

$$R = \{ y \Rightarrow 3 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

SOLVE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 3x], [f(4x + 1) \approx 18] \}$$

REDUCE->  $U = \emptyset$

$$R = \{ y \Rightarrow 3, x \Rightarrow 5 \}$$

$$D = \{ [f(21) \approx 15], [f(21) \approx 18] \}$$

->  $\perp$  follows by COMPOSE and CONTRADICTION.

# Combinations of theories

- So far, we combined **one** solvable theory with the theory of free function symbols.
- Shostak claims that the disjoint union of two solvable theories is again a solvable theory [Shostak '84]
- In this way, **any** number of solvable theories could be combined.

# Combinations of theories

- In [Shostak '84] a procedure for combining solvers is presented.
- However, there were errors in the procedure.
- [Krstić&Conchon '03] proved that **in general solvers of different theories cannot be combined into a solver for the combined theory.**

# Conclusion

- Shostak's method is an efficient procedure for deciding a solvable theory with additional free function symbols.
- It is complete for any solvable convex theory, but
- in general solvers of different theories cannot be combined  
[Krstic&Conchon '03]

# Outlook

- Shostak's method can be extended to work on non-convex theories [[Ganzinger '02](#)]
- There might exist ways to combine solvers under certain conditions [[Krstic&Conchon '03](#)]
- Combining decision procedures for multisorted theories seems to be a promising approach.

# Thank you!

# For Further Reading I



Robert E. Shostak

Deciding Combinations of Theories

*In Journal of the ACM, Vol 31, No 1, January 1984, pp 1-12*



Harald Ganzinger

Shostak Light

2002



Sava Krstić, Sylvain Conchon

Canonization for Disjoint Unions of Theories

2003