Combining Decision Procedures

Ashish Tiwari

tiwari@csl.sri.com

http://www.csl.sri.com/.

Computer Science Laboratory

SRI International

333 Ravenswood

Menlo Park, CA 94025

Outline

- Preliminaries/Notation
- Nelson-Oppen Combination (NO)
  - The Non-Deterministic Version
  - Determinizing the Combination Procedure
  - Equational Theory Version
- Applications
  - Pure Theory of Equality
  - Commutative Semigroups
  - Polynomial Ideals
  - Combination
- Summary

Language: Signatures

A *signature*, Σ, is a finite set of

$$\begin{array}{lcl} \text{Function Symbols} & : & \Sigma_F = \{f, g, \ldots\} \\ \text{Predicate Symbols} & : & \Sigma_P = \{P, Q, \ldots\} \end{array}$$

along with an arity function $arity : \Sigma \mapsto \mathbb{N}$.

Function symbols with arity 0 are called *constants* and denoted by $a, b, \ldots$, with possible subscripts.

A countable set $\mathcal{V}$ of *variables* is assumed disjoint of Σ.

Language: Terms

The set $\mathcal{T}(\Sigma, \mathcal{V})$ of *terms* is the smallest set s.t.

- $\mathcal{V} \subset \mathcal{T}(\Sigma, \mathcal{V})$, and
- $f(t_1, \ldots, t_n) \in \mathcal{T}(\Sigma, \mathcal{V})$ whenever $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$ and $arity(f) = n$.

The set of *ground* terms is defined as $\mathcal{T}(\Sigma, \emptyset)$.

Language: Atomic Formulas

An *atomic formula* is an expression of the form

$$P(t_1, \ldots, t_n)$$

where P is a predicate in Σ s.t. $arity(P) = n$ and $t_1, \ldots, t_n \in \mathcal{T}(\Sigma, \mathcal{V})$.

If $t_1, \ldots, t_n$ are ground terms, then $P(t_1, \ldots, t_n)$ is called a ground (atomic) formula.

Mostly, we assume a special binary predicate $=$ to be present in Σ.

Language: Logical Symbols

The set of *quantifier-free formula* (over Σ), $QFF(\Sigma, \mathcal{V})$, is the smallest set s.t.

- Every atomic formula is in $QFF(\Sigma, \mathcal{V})$,
- If $\phi \in QFF(\Sigma, \mathcal{V})$, then $\neg\phi \in QFF(\Sigma, \mathcal{V})$,
- If $\phi_1, \phi_2 \in QFF(\Sigma, \mathcal{V})$, then

$$\begin{array}{ccccc} \phi_1 & \wedge & \phi_2 & \in & QFF(\Sigma, \mathcal{V}) \\ \phi_1 & \vee & \phi_2 & \in & QFF(\Sigma, \mathcal{V}) \\ \phi_1 & \Rightarrow & \phi_2 & \in & QFF(\Sigma, \mathcal{V}) \\ \phi_1 & \Leftrightarrow & \phi_2 & \in & QFF(\Sigma, \mathcal{V}). \end{array}$$

An atomic formula or its negation is a *literal*.

Language: Sentence, Theory

The closure of $QFF(\Sigma, \mathcal{V})$ under existential ($\exists$) and universal ($\forall$) quantification defines the set of *(first-order) formulas*.

A *sentence* is a FO formula with no free variables.

A *(first-order) theory* $\mathcal{T}$ (over a signature Σ) is a set of (deductively closed) set of sentences (over Σ and $\mathcal{V}$).

A theory $\mathcal{T}$ is consistent if *false* $\notin \mathcal{T}$.

Due to completeness of first-order logic, we can identify a a FO theory $\mathcal{T}$ with the class of all models of $\mathcal{T}$.

Semantic Characterization

A model $\mathbb{A}$ is defined by a

- Domain A: set of elements
- Interpretation $f^{\mathbb{A}} : A^n \mapsto A$ for each $f \in \Sigma_F$ with $arity(f) = n$
- Interpretation $P^{\mathbb{A}} \subseteq A^n$ for each $P \in \Sigma_P$ with $arity(P) = n$
- Assignment $x^{\mathbb{A}} \in A$ for each variable $x \in \mathcal{V}$

A formula ϕ is true in a model $\mathbb{A}$ if it evaluates to true under the given interpretations over the domain A.

If all sentences in a $\mathcal{T}$ are true in a model $\mathbb{A}$, then $\mathbb{A}$ is a model for the theory $\mathcal{T}$.

Satisfiability and Validity

A formula $\phi(\vec{x})$ is *satisfiable* in a theory $\mathcal{T}$ if there is a model of $\mathcal{T} \cup \{\exists \vec{x}.\phi(\vec{x})\}$, i.e., there exists a model $\mathbb{M}$ for $\mathcal{T}$ in which ϕ evaluates to true, denoted by,

$$\mathbb{M} \models_{\mathcal{T}} \phi$$

A formula $\phi(\vec{x})$ is *valid* in a theory $\mathcal{T}$ if $\forall \vec{x}.\phi(\vec{x}) \in \mathcal{T}$, i.e., ϕ evaluates to true in every model $\mathbb{M}$ of $\mathcal{T}$. $\mathcal{T}$-validity is denoted by $\models_{\mathcal{T}} \phi$.

ϕ is $\mathcal{T}$-unsatisfiable if it is not the case that $\models_{\mathcal{T}} \phi$.

Decision Procedure

Given

- $\mathcal{T}$: Some FO-theory
- ϕ: A QFF in $\mathcal{T}$

Decide if ϕ is satisfiable in $\mathcal{T}$.

Algorithm which always

- Terminates
- Produces correct answer

Wlog ϕ is a conjunction of literals

Example: Theory of Equality

- $\Sigma_0 = \{a, b, c\}$
  $\phi_0 : a = b \ \wedge \ b = c \ \wedge \ a \neq c$
- $\Sigma_1 = \Sigma_0 \cup \{f^{(1)}\}$
  $\phi_1 : a = f f f a \ \wedge \ f f f f f a = a \ \wedge \ a \neq f a$

Combination of Theories

$$
\begin{array}{lcl}
\Sigma & = & \Sigma_1 \cup \Sigma_2 \\
\mathcal{T}_1, \mathcal{T}_2 & : & \text{Theories over } \Sigma_1 \text{ and } \Sigma_2 \\
\mathcal{T} & = & \text{Deductive closure of } \mathcal{T}_1 \cup \mathcal{T}_2
\end{array}
$$

Problem1. Is $\mathcal{T}$ consistent?

Problem2. Given satisfiability procedures for (quantifier-free) conjunction of literals in $\mathcal{T}_1$ and $\mathcal{T}_2$, how to decide satisfiability in $\mathcal{T}$?

Problem3. What is the complexity of the combination procedure?

Stably-Infinite Theories

A theory is *stably-infinite* if every satisfiable QFF is satisfiable in an infinite model.

Example. Theories with only finite models are not stably infinite. Thus, theory induced by the axiom $\forall x, y, z.(x = y \vee y = z \vee z = x)$ is not stably-infinite.

Proposition. If E is an equational theory, then $E \cup \{\exists x, y. x \neq y\}$ is stably-infinite.
Proof. If M is a model, then $M \times M$ is a model as well. Hence, by compactness, there is an infinite model.

Proposition. The union of two consistent, disjoint, stably-infinite theories is consistent.
Proof. Later!

Convexity

A theory is *convex* if whenever a conjunction of literals implies a disjunction of atomic formulas, it also implies one of the disjuncts.

Example. The theory of integers over a signature containing $<$ is not convex. The formula $1 < x \ \wedge \ x < 4$ implies $x = 2 \ \vee \ x = 3$, but it does not imply either $x = 2$ or $x = 3$ independently.

Example. The theory of rationals over the signature $\{+, <\}$ is convex.

Example. Equational theories are convex, but need not be stably-infinite.

Convexity: Observation

Proposition. A convex theory $\mathcal{T}$ with no trivial models is stably-infinite.
Proof. If not, then for some QFF ϕ, $\mathcal{T} \cup \phi$ has only finite models. Thus, ϕ implies a disjunction $\vee_{i,j} x_i = x_j$, without implying any disjunct.

Example. If E is an equational theory, then $E \cup \{\exists x, y . x \neq y\}$ has no trivial models, and hence it is stably-infinite.

Nelson-Oppen Combination Result

Theorem 1 *Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be consistent, stably-infinite theories over disjoint (countable) signatures. Assume satisfiability of (quantifier-free) conjunction of literals can be decided in $O(T_1(n))$ and $O(T_2(n))$ time respectively. Then,*

1. *The combined theory $\mathcal{T}$ is consistent and stably infinite.*
2. *Satisfiability of (quantifier-free) conjunction of literals in $\mathcal{T}$ can be decided in $O(2^{n^2} * (T_1(n) + T_2(n)))$ time.*
3. *If $\mathcal{T}_1$ and $\mathcal{T}_2$ are convex, then so is $\mathcal{T}$ and satisfiability in $\mathcal{T}$ is in $O(n^4 * (T_1(n) + T_2(n)))$ time.*

Proof. Later.

Examples

Convexity is important for point (3) above.

	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_1 \cup \mathcal{T}_2$
Signature	Σ_F	$\{\mathbb{Z}, <\}$	$\{\mathbb{Z}, <\} \cup \Sigma_F$
Satisfiability	$O(n \log(n))$	$O(n^2)$	NP-complete!

Note that $\mathcal{T}_2$ is not convex.

We can allow a "add constant" operator in signature of $\mathcal{T}_2$. Atomic formulae are of the form $x - y < c$, for some constant c, and satisfiability can be tested by searching for negative cycles in a "difference graph".

For NP-completeness of the union theory, see [Pratt77].

Nelson-Oppen Result: Correctness

Recall the theorem. The combination procedure:

Initial State : ϕ is a conjunction of literals over $\Sigma_1 \cup \Sigma_2$.

Purification : Preserving satisfiability, transform ϕ to $\phi_1 \wedge \phi_2$, s.t. ϕ_i is over Σ_i.

Interaction : Guess a partition of $\mathcal{V}(\phi_1) \cap \mathcal{V}(\phi_2)$ into disjoint subsets.
Express it as a conjunction of literals ψ.
Example. The partition $\{x_1\}, \{x_2, x_3\}$ is represented as $x_2 = x_3 \ \wedge \ x_1 \neq x_2 \ \wedge \ x_1 \neq x_3$.

Component Procedures : Use individual procedures to decide if $\phi_i \ \wedge \ \psi$ is satisfiable.

Return : If both answer yes, return yes. No, otherwise.

Separating Concerns: Purification

Purification: $$\frac{\phi \;\wedge\; P(\ldots, s[t], \ldots)}{\phi \;\wedge\; P(\ldots, s[x], \ldots) \;\wedge\; t = x}$$ if $s[t]$ is not a variable.

Proposition. Purification is satisfiability preserving: if ϕ' is obtained from ϕ by purification, then ϕ is satisfiable in the union theory iff ϕ' is satisfiable in the union theory.

Proposition. Purification is terminating.

Proposition. Exhaustive application results in conjunction where each conjunct is over exactly one signature.

Purification: Illustration

$$f(\underbrace{x-1}_{u_1})-1 \;=\; x+1,\; f(y)+1 \;=\; y-1,\; y+1 \;=\; x$$

Purification: Illustration

$$\frac{f(\underbrace{x-1}_{u_1}) - 1 = x+1,\ f(y)+1 = y-1,\ y+1 = x}{\underbrace{f(u_1)}_{u_2} - 1 = x+1,\ f(y)+1 = y-1,\ y+1 = x}$$

$x - 1 = u_1$

Purification: Illustration

$$\frac{\frac{f(\underbrace{x-1}_{u_1}) - 1 \;=\; x+1,\; f(y)+1 \;=\; y-1,\; y+1 \;=\; x}{\underbrace{f(u_1)}_{u_2} - 1 \;=\; x+1,\; f(y)+1 \;=\; y-1,\; y+1 \;=\; x}}{u_2 - 1 \;=\; x+1,\; \underbrace{f(y)}_{u_3}+1 \;=\; y-1,\; y+1 \;=\; x}$$

$x - 1 = u_1$,$f(u_1) = u_2$

Purification: Illustration

$$f(\underbrace{x-1}_{u_1}) - 1 \;=\; x+1,\; f(y)+1 \;=\; y-1,\; y+1 \;=\; x$$

$$\underbrace{f(u_1)}_{u_2} - 1 \;=\; x+1,\; f(y)+1 \;=\; y-1,\; y+1 \;=\; x$$

$$u_2 - 1 \;=\; x+1,\; \underbrace{f(y)}_{u_3}+1 \;=\; y-1,\; y+1 \;=\; x$$

$$u_2 - 1 \;=\; x+1,\; u_3+1 \;=\; y-1,\; y+1 \;=\; x$$

$$x-1=u_1\;, f(u_1)=u_2\;, f(y)=u_3$$

NO Procedure Soundness

Each step is satisfiability preserving.
Say ϕ is satisfiable (in the combination).

NO Procedure Soundness

Each step is satisfiability preserving.
Say ϕ is satisfiable (in the combination).

1. *Purification:* $\therefore\ \phi_1 \ \wedge\ \phi_2$ is satisfiable.

NO Procedure Soundness

Each step is satisfiability preserving.
Say ϕ is satisfiable (in the combination).

1. *Purification:* $\therefore \phi_1 \ \wedge \ \phi_2$ is satisfiable.
2. *Interaction:* $\therefore$ for some partition ψ, $\phi_1 \ \wedge \ \phi_2 \ \wedge \ \psi$ is satisfiable.

NO Procedure Soundness

Each step is satisfiability preserving.
Say ϕ is satisfiable (in the combination).

1. *Purification:* $\therefore \phi_1 \wedge \phi_2$ is satisfiable.
2. *Interaction:* $\therefore$ for some partition ψ, $\phi_1 \wedge \phi_2 \wedge \psi$ is satisfiable.
3. *Components Procedures:* $\therefore$, $\phi_1 \wedge \psi$ and $\phi_2 \wedge \psi$ are both satisfiable in component theories.

Therefore, if the procedure returns unsatisfiable, then the formula ϕ is indeed unsatisfiable.

NO Procedure Correctness

Suppose the procedure returns satisfiable.

NO Procedure Correctness

Suppose the procedure returns satisfiable.

- Let ψ be the partition and $\mathbb{A}$ and $\mathbb{B}$ be models of $\mathcal{T}_1 \ \wedge \ \phi_1 \ \wedge \ \psi$ and $\mathcal{T}_2 \ \wedge \ \phi_2 \ \wedge \ \psi$.

NO Procedure Correctness

Suppose the procedure returns satisfiable.

- Let ψ be the partition and $\mathbb{A}$ and $\mathbb{B}$ be models of $\mathcal{T}_1 \ \wedge \ \phi_1 \ \wedge \ \psi$ and $\mathcal{T}_2 \ \wedge \ \phi_2 \ \wedge \ \psi$.
- Component theories are stably-infinite, $\therefore$ assume models are infinite (of same cardinality).
- Let h be a bijection between A and B s.t. $h(x^{\mathbb{A}}) = x^{\mathbb{B}}$ for each shared variable x. We can do this $\because$ of ψ.

NO Procedure Correctness

Suppose the procedure returns satisfiable.

- Let ψ be the partition and $\mathbb{A}$ and $\mathbb{B}$ be models of $\mathcal{T}_1 \;\wedge\; \phi_1 \;\wedge\; \psi$ and $\mathcal{T}_2 \;\wedge\; \phi_2 \;\wedge\; \psi$.
- Component theories are stably-infinite, $\therefore$ assume models are infinite (of same cardinality).
- Let h be a bijection between A and B s.t. $h(x^{\mathbb{A}}) = x^{\mathbb{B}}$ for each shared variable x. We can do this $\because$ of ψ.
- Extend $\mathbb{B}$ to $\overline{\mathbb{B}}$ by interpretations of symbols in Σ_1:

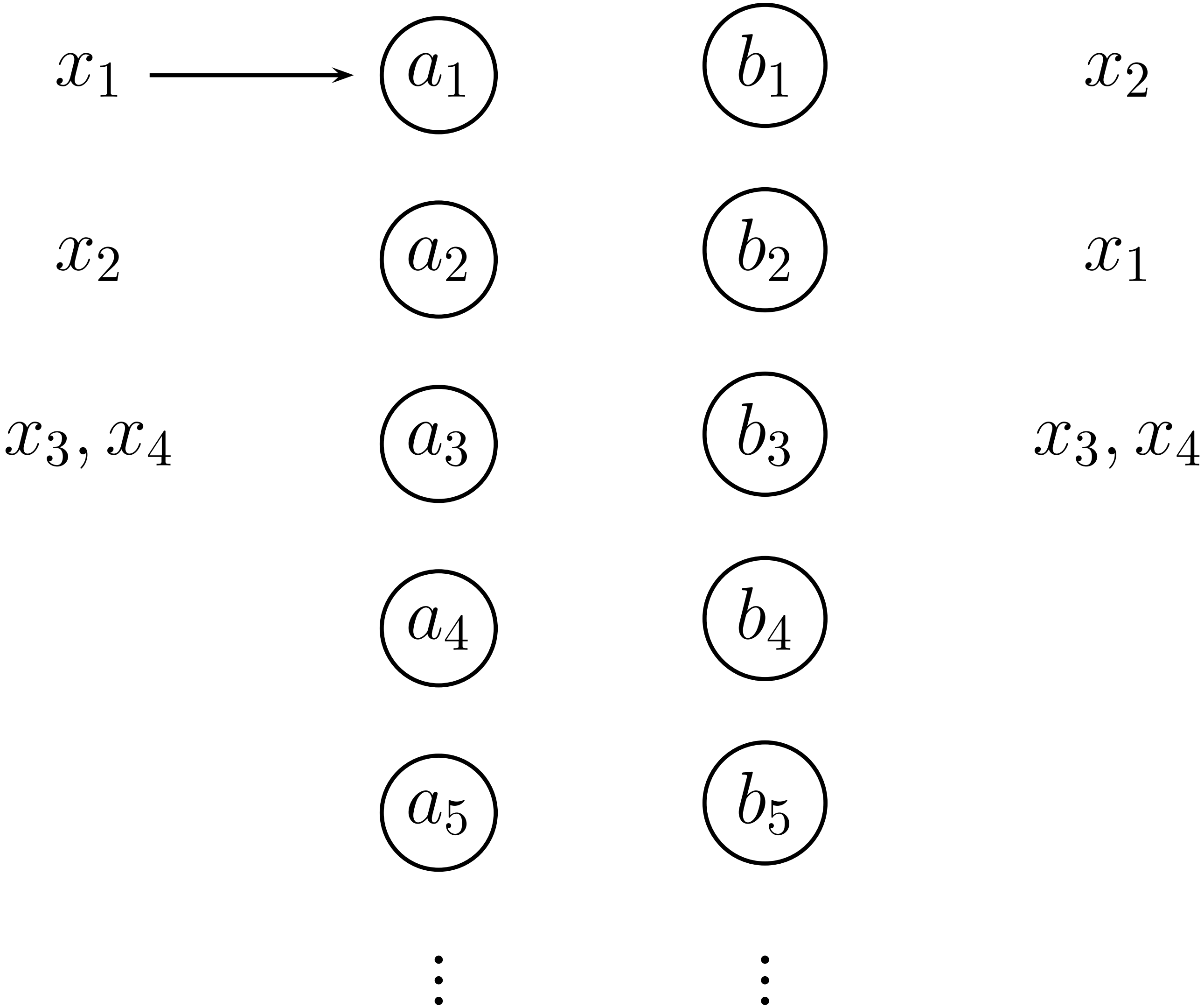
$$f^{\overline{\mathbb{B}}}(b_1, \ldots, b_k) = h(f^{\mathbb{A}}(h^{-1}(b_1), \ldots, h^{-1}(b_k)))$$

Such an extended $\overline{\mathbb{B}}$ is a model of

$$\mathcal{T}_1 \;\wedge\; \mathcal{T}_2 \;\wedge \phi_1 \;\wedge\; \phi_2 \;\wedge\; \psi$$

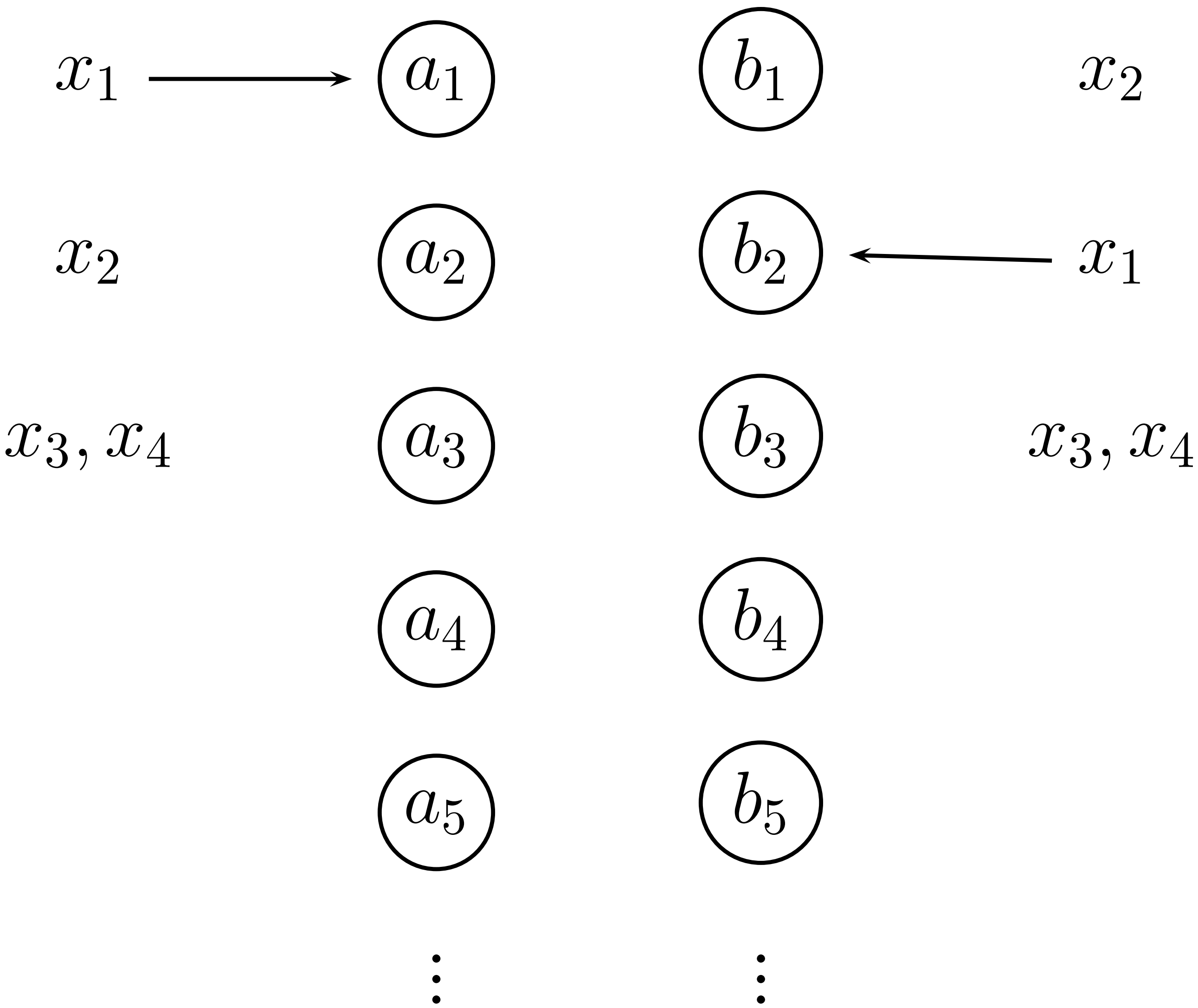
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



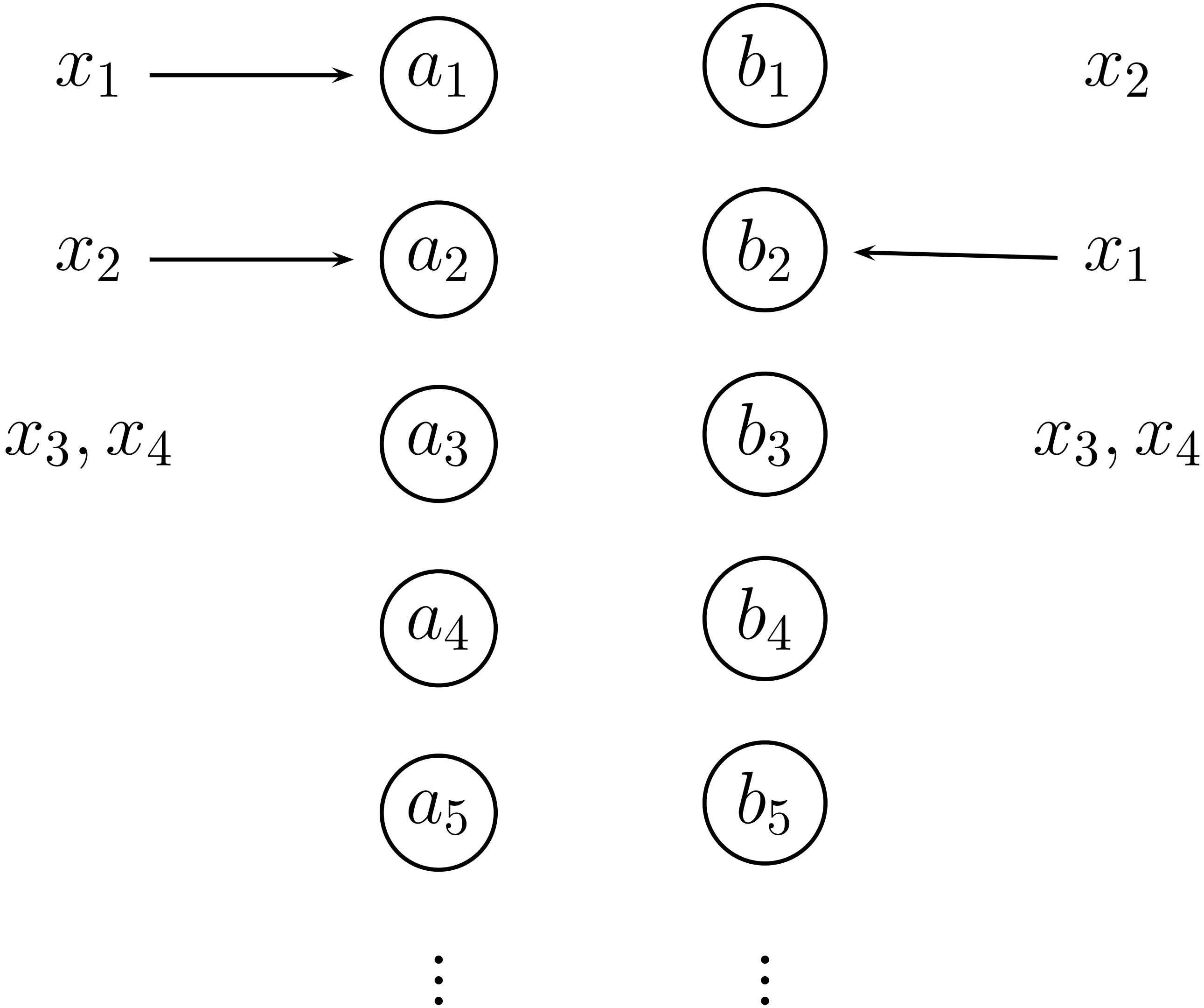
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



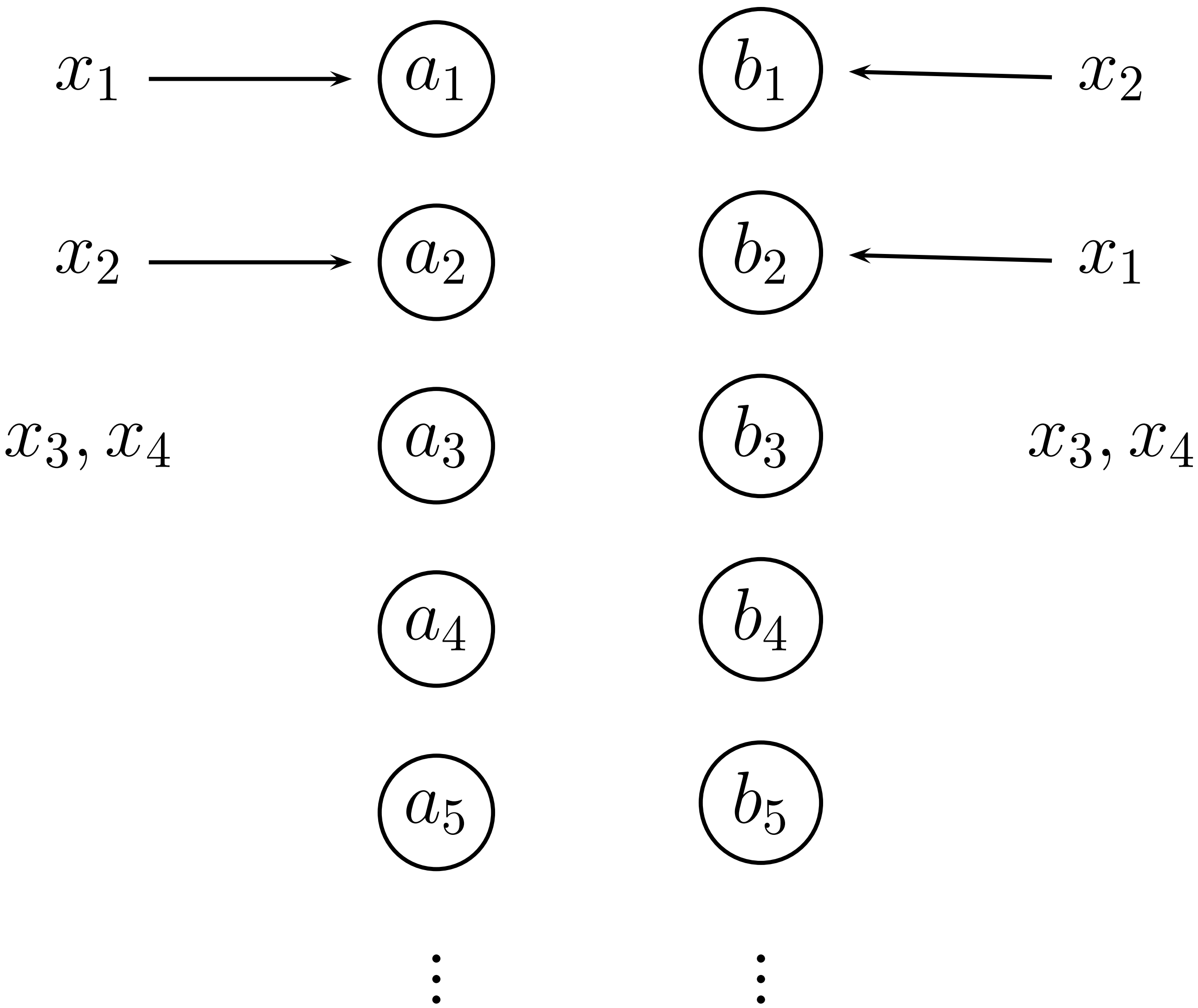
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



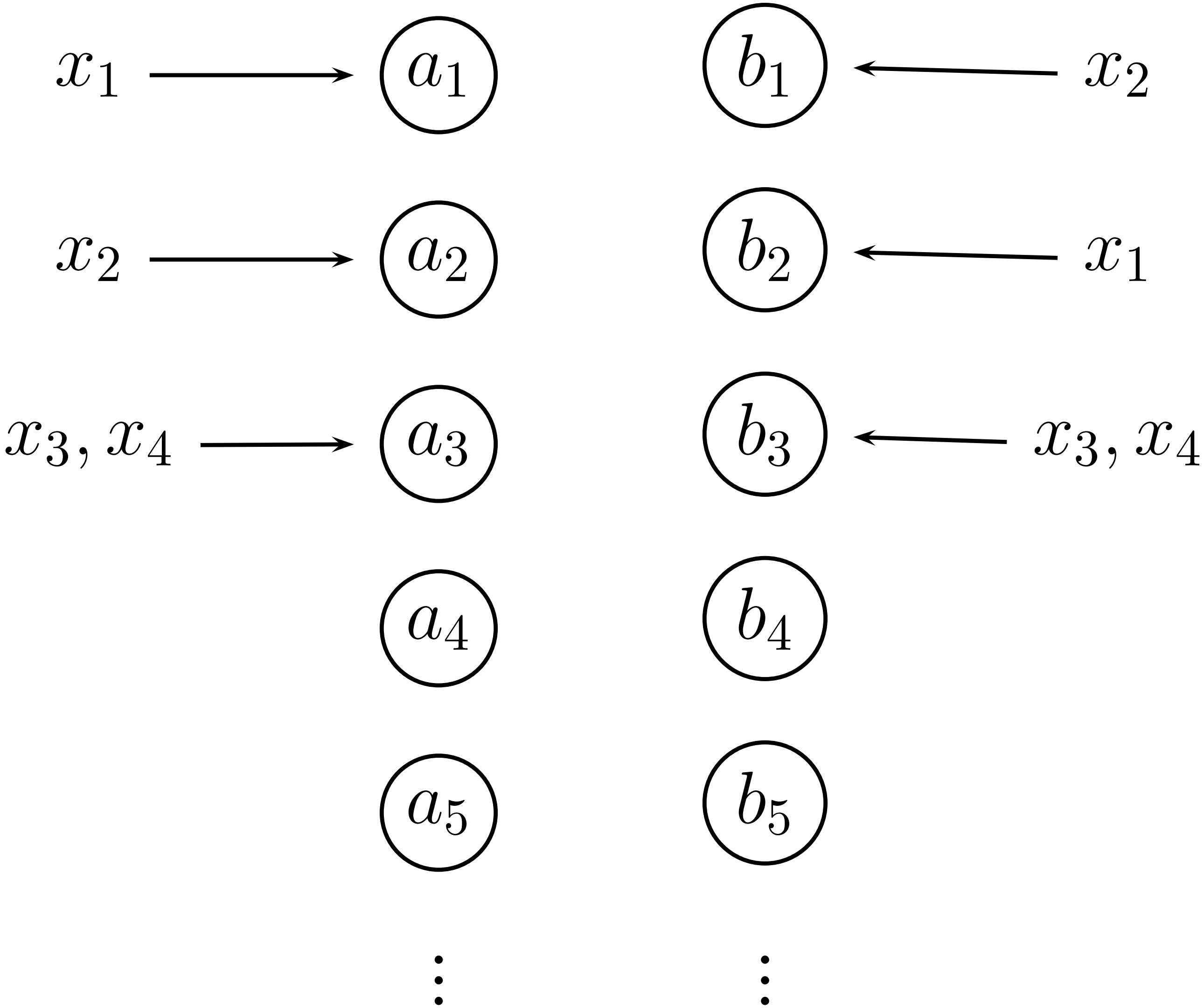
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



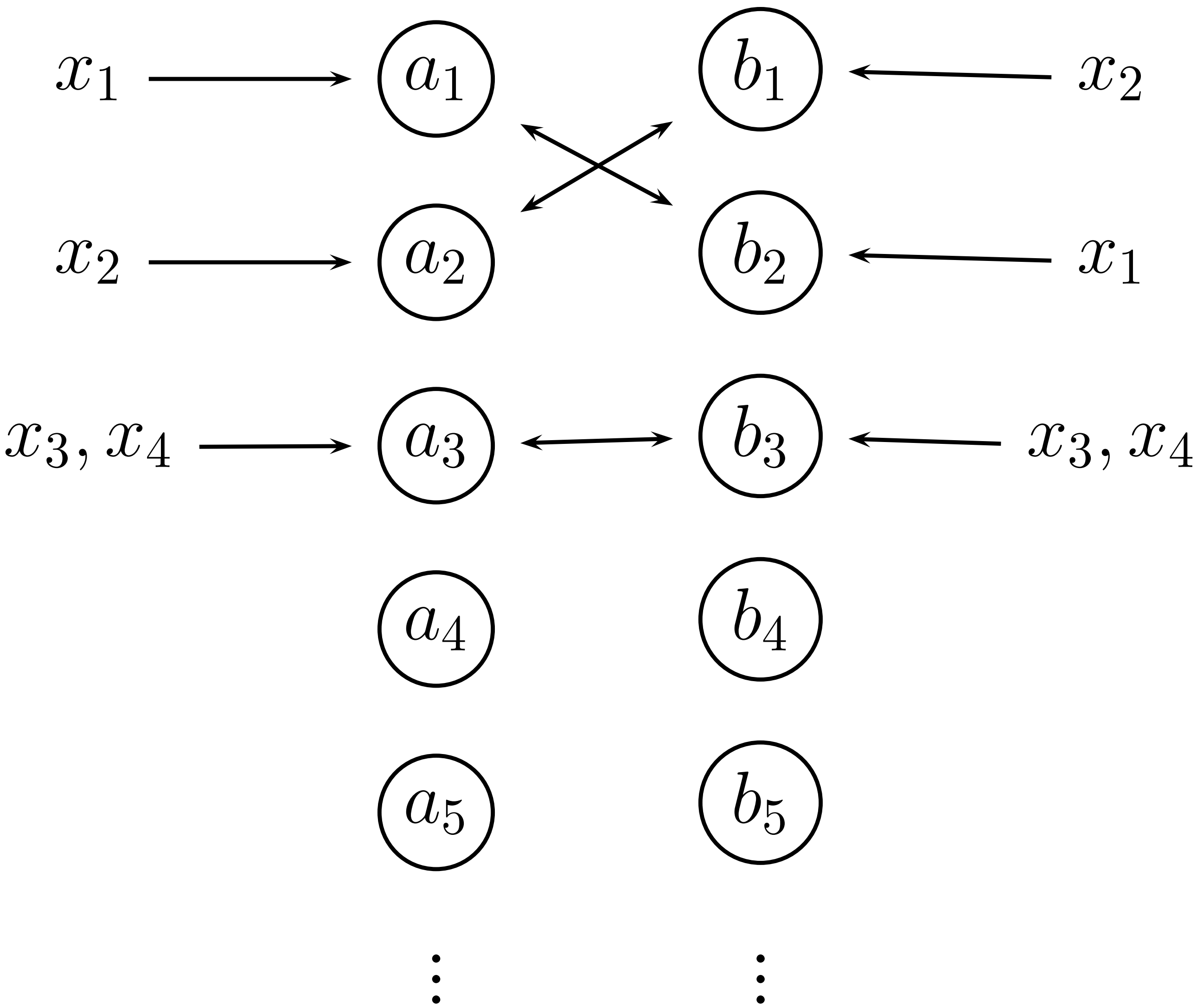
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



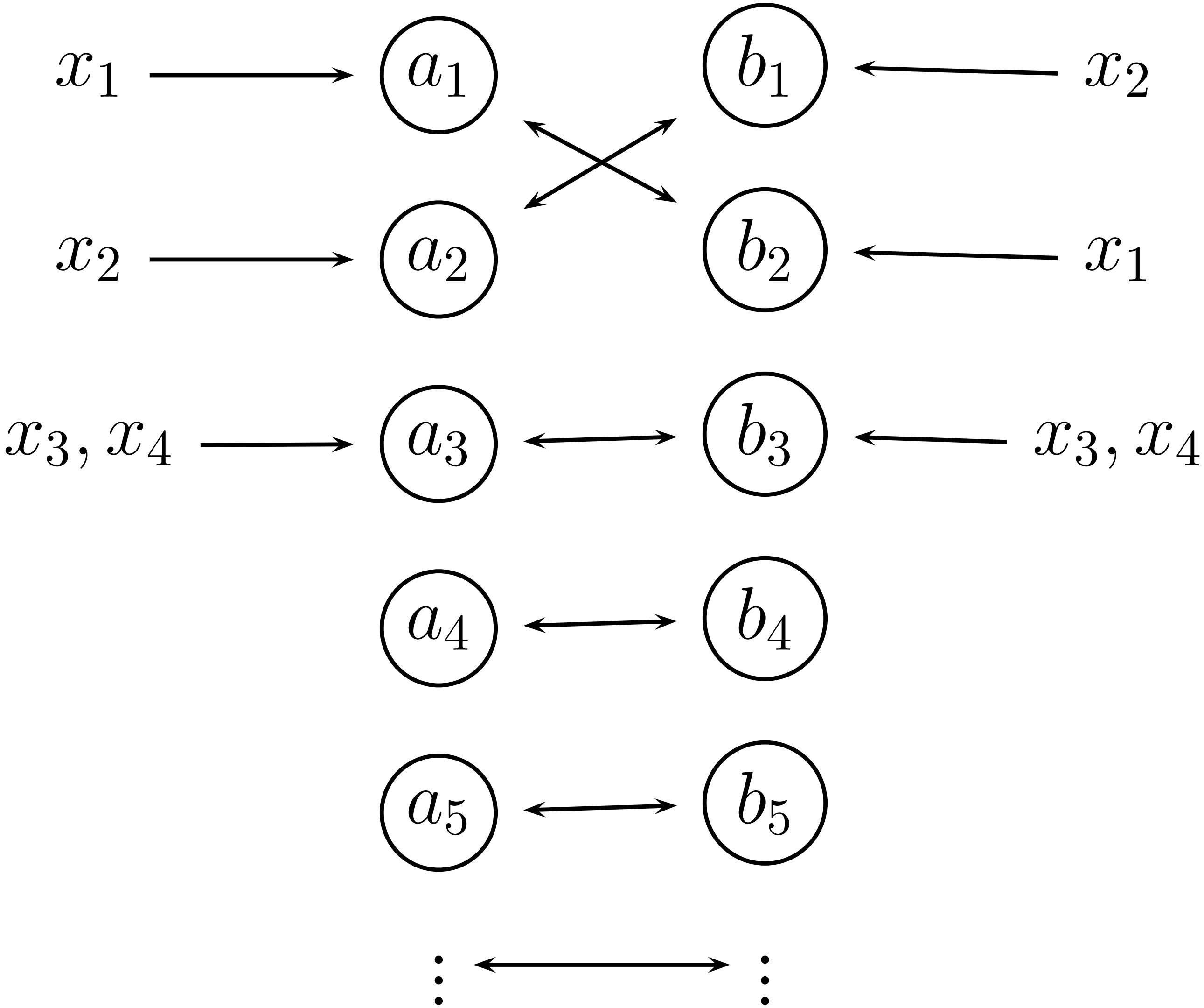
Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



Model Construction Picture

Consider $\mathcal{T}_i$-models $\mathbb{A}$ and $\mathbb{B}$ of $\phi_i \wedge \psi$:



Alternate Correctness Proof

Say $\mathcal{T}_1 \ \wedge \ \mathcal{T}_2 \ \wedge \ \phi$ is unsatisfiable.

- *Purification*: $(\mathcal{T}_1 \wedge \phi_1) \wedge (\mathcal{T}_2 \wedge \phi_2)$ is unsatisfiable
- *Compactness*: $(T_1 \wedge \phi_1) \wedge (T_2 \wedge \phi_2)$ is unsatisfiable
- *Logically*: $(T_1 \wedge \phi_1) \Rightarrow \neg(T_2 \wedge \phi_2)$
- *Craig's Interpolation Lemma*: There exists a formula ψ s.t.

$$\begin{array}{rcl} (T_1 \wedge \phi_1) & \Rightarrow & \psi \\ \psi & \Rightarrow & \neg(T_2 \wedge \phi_2) \end{array}$$

Each nonlogical free symbol in ψ is free in the other two.

Alternate Proof Contd

- *Craig's Interpolation Lemma*:

$$\begin{aligned} (T_1 \wedge \phi_1) &\Rightarrow \psi \\ (T_2 \wedge \phi_2) &\Rightarrow \neg\psi \end{aligned}$$

- ψ: quantified formula, atomic formulas are equations between variables
- If $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably-infinite, then ψ is equivalent to a quantifier-free formula, call it ψ.
- For any partition ψ_0 of variables, either ψ or $\neg\psi$ evaluates to false.
- For no partition ψ_0 are both $\mathcal{T}_1 \wedge \phi_1 \wedge \psi_0$ and $\mathcal{T}_2 \wedge \phi_2 \wedge \psi_0$ satisfiable.

NO Procedure Complexity

Proposition. The non-deterministic procedure can be determinised to give a $O(2^{n^2} * (T_1(n) + T_2(n)))$-time algorithm.

Proof.

NO Procedure Complexity

Proposition. The non-deterministic procedure can be determinised to give a $O(2^{n^2} * (T_1(n) + T_2(n)))$-time algorithm.

Proof.

1. Number of purification steps $< n$ and size of resulting $\phi_1 \ \wedge \ \phi_2$ is $O(n)$.

NO Procedure Complexity

Proposition. The non-deterministic procedure can be determinised to give a $O(2^{n^2} * (T_1(n) + T_2(n)))$-time algorithm.

Proof.

1. Number of purification steps $< n$ and size of resulting $\phi_1 \ \wedge \ \phi_2$ is $O(n)$.
2. Number of partition of a set with n variables: $B(n) < 2^{n^2}$.

NO Procedure Complexity

Proposition. The non-deterministic procedure can be determinised to give a $O(2^{n^2} * (T_1(n) + T_2(n)))$-time algorithm.

Proof.

1. Number of purification steps $< n$ and size of resulting $\phi_1 \ \wedge \ \phi_2$ is $O(n)$.
2. Number of partition of a set with n variables: $B(n) < 2^{n^2}$.
3. For each $B(n)$ choices, the component procedures take $T_1(n)$ and $T_2(n)$-time respectively.

NO Deterministic Procedure

Instead of guessing, we can deduce the equalities to be shared. The new combination procedure:

Purification : As before.

Interaction : Deduce an equality $x = y$:

$$\mathcal{T}_1 \vdash (\phi_1 \Rightarrow x = y)$$

Update $\phi_2 := \phi_2 \wedge x = y$. And vice-versa. Repeat until no further changes to get ϕ_{i_∞}.

Component Procedures : Use individual procedures to decide if ϕ_{i_∞} is satisfiable.

Note, $\mathcal{T}_i \vdash (\phi_i \Rightarrow x = y)$ iff $\phi_1 \wedge x = y$ is not satisfiable in $\mathcal{T}_i$.

Deterministic Version: Correctness

Each step is satisfiability preserving, $\therefore$ soundness follows.

Deterministic Version: Correctness

Each step is satisfiability preserving, $\therefore$ soundness follows.

Assume that the theories are convex.

- Let ϕ_{i_∞} be satisfiable.

Deterministic Version: Correctness

Each step is satisfiability preserving, $\therefore$ soundness follows.

Assume that the theories are convex.

- Let ϕ_{i_∞} be satisfiable.
- If $\{x_1, \ldots, x_m\}$ is the set of variables not yet identified, $\mathcal{T}_i \not\models \phi_{i_\infty} \Rightarrow (x_j = x_k)$.

Deterministic Version: Correctness

Each step is satisfiability preserving, $\therefore$ soundness follows.

Assume that the theories are convex.

- Let ϕ_{i_∞} be satisfiable.
- If $\{x_1, \ldots, x_m\}$ is the set of variables not yet identified, $\mathcal{T}_i \not\models \phi_{i_\infty} \Rightarrow (x_j = x_k)$.
- By convexity, $\mathcal{T}_i \not\models \phi_{i_\infty} \Rightarrow \bigvee_{j \neq k}(x_j = x_k)$.

Deterministic Version: Correctness

Each step is satisfiability preserving, $\therefore$ soundness follows.

Assume that the theories are convex.

- Let ϕ_{i_∞} be satisfiable.
- If $\{x_1, \ldots, x_m\}$ is the set of variables not yet identified, $\mathcal{T}_i \not\models \phi_{i_\infty} \Rightarrow (x_j = x_k)$.
- By convexity, $\mathcal{T}_i \not\models \phi_{i_\infty} \Rightarrow \bigvee_{j \neq k}(x_j = x_k)$.
- $\therefore \phi_{i_\infty} \wedge \bigwedge_{j \neq k}(x_j \neq x_k)$ is satisfiable.
- The proof is now identical to the previous case.

Deterministic Version: Complexity

For convex theories, the combination procedure runs in $O(n^4 * (T_1(n) + T_2(n)))$ time:

1. Identifying if an equality $x = y$ is implied by ϕ_i takes $O(n^2 * T_i(n))$ time.
2. Since there are $O(n^2)$ possible equalities between variables, fixpoint is reached in $O(n^2)$ iterations.

Modularity of convexity: Unsatisfiability is signaled when any one procedures signals unsatisfiable.

NO: Equational Theory Version

Equational Theory: Axiomatized by universally quantified equations.
Examples: Semi-groups, Groups, Rings, etc.

1. Equational theories are always consistent.
2. If $E \cup \{\exists x, y. x \neq y\}$ is consistent, then this theory is also stably-infinite.
3. Equational theories are convex. (If $E \vdash \phi \Rightarrow (l_1 \vee l_2)$, then consider the initial algebra induced by $E \cup \phi$ over an extended signature.)
4. Therefore, satisfiability procedures can be combined with only a polynomial time overhead.

Equational Decision Procedures

- Equations can either be oriented or not

$$\begin{aligned} 0 + x &= x \\ x + y &= y + x \end{aligned}$$

- Oriented equations are handled using Superposition:

$$\frac{s[u] = t \qquad v = w}{s\sigma[w\sigma] = t\sigma}$$

  if $u\sigma \equiv v\sigma$, $s[u] \succ t$, $v \succ w$.

- Non-orientable equations are handled in $\equiv$

Equational Decision Procedures

- Two kinds of equations:
  - axioms of theory $\mathcal{T}$
  - literals in (purified) ϕ: These are "ground"
- Superposition modulo unorientable equations:
  - axiom–axiom: Assume saturated
  - axiom/groundLiteral–groundLiteral: Need to apply rule
- Termination?: ??
- Correctness?: Yes

Outline

- Preliminaries/Notation
- Nelson-Oppen Combination (NO)
  - The Non-Deterministic Version
  - Determinizing the Combination Procedure
  - Equational Theory Version
- Applications
  - Pure Theory of Equality
  - Commutative Semigroups
  - Polynomial Ideals
  - Combination
- Summary

A Simple Theory of Equality

$$\begin{array}{lcl} \Sigma & = & \Sigma_F = \{f\} \text{ (uninterpreted)} \\ \mathcal{T} & = & \text{Deductive closure of axioms of equality} \end{array}$$

- Axioms = $\emptyset$
- "Ground" equations over $\{f\}$ can be oriented: $f(u_1, \ldots, u_k) = u$
- Deduction rules:

$$\frac{f(u_1, \ldots, u_k) = u \qquad f(u_1, \ldots, u_k) = u'}{u = u'}$$

$$\frac{f(u_1, \ldots, u_k) = u \qquad u_1 = u'}{f(u', \ldots, u_k) = u}$$

Application: Theory of Equality

$$\begin{array}{lcl} \Sigma & = & \Sigma_F = \{f\} \cup \{g\} \cup \cdots \\ \mathcal{T} & = & \text{Deductive closure of axioms of equality} \end{array}$$

- $\mathcal{T}$ is a stably-infinite equational theory.
- Above "congruence closure" procedure decides satisfiability of QFF over Σ_i.
- $\therefore$ congruence closure for disjoint Σ_i can be combined in polynomial time.
- This way we get an "abstract congruence closure" for the combined signature.

Commutative Semigroup

$$\begin{array}{rcl} \Sigma & = & \{f\} \\ \mathcal{T} & = & \text{Axioms of equality + AC axioms for } f. \end{array}$$

- Treat f as variable arity

$$\begin{array}{rcll} f(\ldots, f(\ldots), \ldots) & = & f(\ldots, \ldots, \ldots) & (F) \\ f(\ldots, x, y, \ldots) & = & f(\ldots, y, x, \ldots) & (P) \end{array}$$

- Flatten all equations and do completion modulo P

$$\frac{f(c_1, c_1, x) = f(c_1, x) \qquad f(c_1, c_2, x) = f(c_2, c_2, x)}{f(c_1, c_2, y) = f(c_1, c_2, c_2, y)}$$

Commutative Semigroup

- All rules are of the form $f(\ldots) \to f(\ldots)$.
- Collapse guarantees termination of completion via Dickson's lemma.

$$\frac{f(c_1, c_1, c_2) = c_1 \qquad f(c_1, c_2) = c_1}{f(c_1, c_1, c_2) = c_1}$$

- Using an appropriate ordering on multisets, we get a algorithm to construct convergent systems (and decide satisfiability of QFF).

Example: Commutative Semigroup

If $E_0 = \{c_1^2 c_2 = c_3,\ c_1 c_2^2 = c_1 c_2\}$, we can use orientation, superposition (modulo AC), collapse to get a convergent (modulo AC) rewrite system

$$c_1^2 c_2 \longrightarrow c_3,\ c_1 c_2^2 \longrightarrow c_1 c_2$$

$$c_2 c_3 = c_1^2 c_2$$

$$c_1^2 c_2 \longrightarrow c_2 c_3$$

$$c_3 = c_2 c_3$$

$$c_2 c_3 \longrightarrow c_3$$

$$c_1^2 c_3 \longrightarrow c_3^2$$

Application: Ground AC-theories

$$\begin{array}{rcl}\Sigma & = & \Sigma_F \cup \Sigma_{AC} \\ \mathcal{T} & = & \text{Axioms of equality + AC axioms for each } f \in \Sigma_{AC}.\end{array}$$

- Use purification
- Use abstract congruence closure on $\Sigma - \Sigma_{AC}$
- Use completion modulo AC on each $\{f\}$, $f \in \Sigma_{AC}$
- Combine by sharing equations between constants

Time Complexity: $O(n^2 * (T_{AC}(n) + n\log(n)))$.

Similarly, ACU-symbols can be added.

Gröbner Bases

$$\begin{array}{rcl} \Sigma & = & \{0, 1, +, \cdot, X_1, \ldots, X_n\} \cup \mathbb{Q} \\ \mathcal{T} & = & \text{Polynomial ring } \mathbb{K}[X_1, \ldots, X_n] \text{ over field } \mathbb{K} \end{array}$$

- Given a finite set of polynomial equations, new equations (between variables) can be deduced using Gröbner basis construction.
- Main inference rule is superposition. For e.g.,

$$\frac{c_1^2 c_2 = 0 \qquad c_1 c_2^2 = 1}{c_2 \cdot 0 = c_1 \cdot 1}$$

The equations are simplified and oriented s.t. the maximal monomial occurs on LHS, for e.g., $c_1 = 0$.

Gröbner Bases: Contd

- Collapse simplifies LHS of rewrite rules.

$$\frac{c_1 \rightarrow 0 \qquad c_1 c_2^2 \rightarrow 1}{0 \cdot c_2^2 = 1}$$

  which simplifies to $0 = 1$, a contradiction.

- Using suitable ordering on monomials and sums of monomials, a convergent rewrite system (modulo AC axioms), called a Gröbner basis, can be constructed in finite steps.
  Eg. $GB(\{c_1^2 = 0, c_1 c_2^2 = 1\}) = \{1 = 0\}$.
- Termination is established using Dickson's lemma as before.

Application: Gröbner Bases Plus . . .

$$\begin{aligned} \Sigma &= \Sigma_F \cup \Sigma_{AC} \cup \Sigma_{ACU} \cup \Sigma_{GB} \\ \mathcal{T} &= \text{Union of the respective theories} \end{aligned}$$

Use NO combination, with the following decision procedures to deduce equalities:

- Use abstract congruence closure on $\Sigma - \Sigma_{AC}$
- Use completion modulo AC on each $\{f\}$, $f \in \Sigma_{AC}$
- Use completion modulo ACU on each $\{f\}$, $f \in \Sigma_{ACU}$
- Use Gröbner basis algorithm on equations over Σ_{GB}

Since each theory is convex and stably-infinite, we get a polynomial time combination over the individual theories.

Summary

The Nelson-Oppen theorem combines satisfiability procedures for conjunctions of literals in disjoint and stably-infinite theories.

- This is equivalent to deciding the validity of clauses: $\mathcal{T} \vdash \forall \vec{x}.(\phi_1 \Rightarrow \phi_2)$ where ϕ_1/ϕ_2 are AND/OR of atomic formulas.
- Using Purification, it is easy to see that we can restrict ϕ_2 to contain atomic formulae over variables.
- By definition, if $\mathcal{T}$ is convex and $=$ is the only predicate symbol, then validity above is equivalent to horn validity: $\mathcal{T} \vdash \forall \vec{x}.(\phi_1 \Rightarrow x_1 = x_2)$. This motivates the definition of convexity.

Summary

- Convexity allows optimization.
  - Convexity is also necessary for completeness of deterministic version of the NO procedure.
  - Additional assumptions, usually grouped under the name Shostak theories, allow for further optimized implementations of the deterministic NO procedure.
- Stably-infiniteness is required for completeness, i.e., if the component procedures return satisfiable, it allows construction of the fusion model.

Special Case: Theory with UIFs

Theorem 1 *Let $\mathcal{T}_1$ be a theory over a signature Σ. Let Σ_F be a disjoint set of function symbols with pure theory $\mathcal{T}_2$ of equality over it. If satisfiability of (quantifier-free) conjunction of literals can be decided in $O(T_1(n))$ time in $\mathcal{T}_1$, then,*

1. *The combined theory $\mathcal{T}$ is consistent.*
2. *Satisfiability of (quantifier-free) conjunction of literals in $\mathcal{T}$ can be decided in $O(2^{n^2} * (T_1(n) + n\log(n)))$ time.*
3. *If $\mathcal{T}_1$ and $\mathcal{T}_2$ are convex, then so is $\mathcal{T}$ and satisfiability in $\mathcal{T}$ is in $O(n^4 * (T_1(n) + n\log(n)))$ time.*

Single Theory with UIFs

- We modify the deterministic and non-deterministic procedures as follows:
  - purification is applied until all disequations over terms in Σ_2 are reduced to disequations between variables
  - all variables introduced by purification are considered shared between the two theories
  - rest is identical to the NO procedure
- Stably-infiniteness was required to get a bijection between the two models. Since there exist models of any cardinality, above a minimum which is communicated to $\mathcal{T}_1$, in $\mathcal{T}_2$, completeness holds.

Combination for the Word Problem

The word problem concerns with validity of an atomic formula.

- NO result can be modified to give a modularity result for this case.
- NO result can not be used as such, because the generated satisfiability checks may not be equivalent to word problems.
- If E_1 and E_2 are non-trivial equational theories over disjoint signatures with decidable word problems, then the word problem for $E_1 \cup E_2$ is decidable with a polynomial time overhead.

Non-Disjoint Signatures

Word problem in the union may not be decidable

$$\begin{array}{lll} E & : & \text{semigroup presentation with undecidable word problem} \\ E_1 & : & \text{Theory induced by } E\text{, with } \cdot \text{ uninterpreted} \\ & & \text{(decided by congruence closure).} \\ E_2 & : & \text{Theory of semigroups} \\ & & \text{(decided by flattening).} \end{array}$$

Satisfiability in the union may not be decidable

$$\begin{array}{lll} E_1 & : & \{f(x, f(y, z)) = g(x, y, z)\} \\ E_2 & : & \{f(f(x, y), z) = g(x, y, z)\} \\ E & : & \text{Theory of semi-groups} \end{array}$$

Non-Disjoint Signatures

- If $\mathbb{A}$ is a model for theory $\mathcal{T}_1 \cup \mathcal{T}_2$, then $\mathbb{A}^{\Sigma_1}$ and $\mathbb{A}^{\Sigma_2}$ is a model for $\mathcal{T}_1$ and $\mathcal{T}_2$ respectively.
- Define fusion of models $\mathbb{A}_1$ and $\mathbb{A}_2$ s.t. converse hold as well.
- Define a bijection between A_1 and A_2 and give interpretations accordingly.
- Generalize "stably-infiniteness": Identify conditions under which two models can be fused.
- Kinds of assumptions:
  - $\mathcal{T}_1^{\Sigma_1 \cap \Sigma_2}$ is identical to $\mathcal{T}_2^{\Sigma_1 \cap \Sigma_2}$
  - $\Sigma_1 \cap \Sigma_2$, or a subset thereof, generates both A_2 and A_2
  - Examples. Theories which admit constructors

Bibliography

- Armando, A., Ranise, S., and Rusinowitch, M., "*A rewriting approach to satisfiability procedure*", IC'02.
  deriving decision procedures
- Baader, F. and Tinelli, C., "*Deciding the word problem in the union of equational theories*", IC'02.
  theories sharing constructors
- Bachmair, L., Tiwari, A., and Vigneron, L., "*Abstract congruence closure*", JAR'02.
  Abstract CC, specializations, complexity
- Barrett, C. W., Dill, D. L., and Stump, A., "*A generalization of Shostak's method for combining decision procedures*", FroCoS'02.
  Shostak in NO procedure, convexity and stably-infiniteness

Bibliography

- Bjorner, N. S., "*Integrating decision procedures for temporal verification*", PhD Thesis'98.
  general results plus proedures for individual theories
- Cyrluk, D., Lincoln, P., and Shankar, N., "*On Shostak's decision procedure for combination of theories*", CADE'96.
  Shostak's CC, Single theory with UIF
- Downey, P. J., Sethi, R., and Tarjan, R. E., "*Variations on the common subexpression problem*", JACM'80.
  CC + linear variant
- Ganzinger, H., "*Shostak Light*", CADE 2002.
  Th + UIFs, convexity also necessary, stably-infiniteness not required, sigma-models indistinguishable

Bibliography

- Halpern, J. Y., "*Presburger arithmetic with unary predicates is Π^1_1-complete*", JSC'91.
  undecidability by adding predicates
- Kapur, D., "*Shostak's congruence closure as completion*", RTA'97.
  CC algorithm
- Kapur, D., "*A rewrite rule based framework for combining decision procedures*", FroCoS'02.
  Shostak combination
- Lynch, C. and Morawska, B., "*Automatic decidability*", LICS'02.
  deriving decision procedures and complexity

Bibliography

- Nelson, G. and Oppen, D., "*Simplification by cooperating decision procedures*", ACM TOPLAS'79.
  Combination result, specific theories
- Nelson, G. and Oppen, D., "*Fast decision procedures based on congruence closure*", JACM'80.
  CC, theory of lists
- Oppen, D. C., "*Complexity, convexity, and combination of theories*", TCS'80.
  NO main theorem, complexity, special theories
- Pratt, V. R., "Two easy theories whose combination is hard", MIT TR'77.
  validity hard for a combination of non-convex PTIME theories

Bibliography

- Rueß, H. and Shankar, N.,“*Deconstructing Shostak*”, LICS’01.
  Shostak theory + UIF–the Shostak way
- Shankar, N. and Rueß, H., “*Combining Shostak theories*”, RTA’02.
  Multiple Shostak theory combination
- Shostak, R. E., “*An efficient decision procedure for arithmetic with function symbols*”, SRI TR’77.
  arithmetic + UIFs
- Shostak, R. E., “*Deciding combinations of theories*”, JACM’84.
  Shostak theory + UIF

Bibliography

- Stump, A., Dill, D., Barrett, C., and Levitt, J., "*A decision procedure for extensional theory of arrays*", LICS'01.
  theory of arrays
- Tinelli, C. and Ringeissen, C., "*Unions of non-disjoint theories and combinations of satisfiability procedures*", Elveiser Science'01.
  New advances for non-disjoint combinations
- Tiwari, A., "*Decision procedures in automated deduction*", PhD Thesis'00.
  Shostak theories in NO framework