Seminar Decision Procedures and Applications

Background Informations, Part 3

Viorica Sofronie-Stokkermans
University Koblenz-Landau

Preliminary form; to be presented on 19 June 2013
Topics for the talks:

- D. Basin & H. Ganzinger: “Automated complexity analysis based on ordered resolution”
- V. Kuncak & S. Jacobs: “Towards Complete Reasoning about Axiomatic Specifications”
- F. Baader & B. Morawska: “Unification in the description logic $\mathcal{EL}$
Overview

• Reasoning in standard theories
  last time

• Reasoning in complex theories
  – combinations of theories  last time: stably infinite; disjoint signatures
  – theory extensions  idea

• Examples of applications

Important: identify decidable/tractable fragments
Standard theories: Fragments

In order to obtain decidability results:

- Restrict the signature
- Enrich axioms
- Look at certain fragments \( \mathcal{L} \subseteq \text{Fma}(\Sigma) \)

**“Simpler” task:** Given \( \phi \) in \( \mathcal{L} \), is it the case that \( \mathcal{T} \models \phi \)?

Common restrictions on \( \mathcal{L} \)

<table>
<thead>
<tr>
<th>( \mathcal{L} )</th>
<th>( \text{Pred} = \emptyset )</th>
<th>( { \phi \in \mathcal{L} \mid \mathcal{T} \models \phi } )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( { \forall x A(x) \mid A \text{ atomic} } )</td>
<td>word problem</td>
<td></td>
</tr>
<tr>
<td>( { \forall x (A_1 \land \ldots \land A_n \rightarrow B) \mid A_i, B \text{ atomic} } )</td>
<td>uniform word problem</td>
<td>( \text{Th}_{\forall \text{Horn}} )</td>
</tr>
<tr>
<td>( { \forall x C(x) \mid C(x) \text{ clause} } )</td>
<td>clausal validity problem</td>
<td>( \text{Th}_{\forall, \text{cl}} )</td>
</tr>
<tr>
<td>( { \forall x \phi(x) \mid \phi(x) \text{ unquantified} } )</td>
<td>universal validity problem</td>
<td>( \text{Th}_{\forall} )</td>
</tr>
</tbody>
</table>
Standard theories: Fragments

In order to obtain decidability results:

• Restrict the signature
• Enrich axioms
• Look at certain fragments $\mathcal{L} \subseteq \text{Fma}(\Sigma)$

“Simpler” task: Given $\phi$ in $\mathcal{L}$, is it the case that $\mathcal{T} \models \phi$?

Common restrictions on $\mathcal{L}$

\[
\begin{align*}
\Pi &= \emptyset \\
\mathcal{L} &= \{ \exists x A_1 \land \ldots \land A_n \mid A_i \text{ atomic} \} \quad \text{unification problem} \\
\mathcal{L} &= \{ \forall x \exists x A_1 \land \ldots \land A_n \mid A_i \text{ atomic} \} \quad \text{unification with constants}
\end{align*}
\]
2. Unification

Common restrictions on $\mathcal{L}$

\[ \Pi = \emptyset \quad \{ \phi \in \mathcal{L} \mid \mathcal{T} \models \phi \} \]

$\mathcal{L} = \{ \exists x A_1 \land \ldots \land A_n \mid A_i \text{ atomic} \}$ unification problem $\text{Th}_\exists$

$\mathcal{L} = \{ \forall x \exists x A_1 \land \ldots \land A_n \mid A_i \text{ atomic} \}$ unification with constants $\text{Th}_\forall \exists$
Syntactic Unification

Let $S = \{s_1 \doteq t_1, \ldots, s_n \doteq t_n\}$ ($s_i, t_i$ terms or atoms) a multi-set of equality problems. $S$ is a unification problem.

A substitution $\sigma$ is called a unifier of $S$ if $s_i\sigma = t_i\sigma$ for all $1 \leq i \leq n$.

If a unifier of $S$ exists, then $S$ is called unifiable.
(1) \[ t \doteq t, E \Rightarrow_{MM} E \]

(2) \[ f(s_1, \ldots, s_n) \doteq f(t_1, \ldots, t_n), E \Rightarrow_{MM} s_1 \doteq t_1, \ldots, s_n \doteq t_n, E \]

(3) \[ f(\ldots) \doteq g(\ldots), E \Rightarrow_{MM} \perp \]

(4) \[ x \doteq t, E \Rightarrow_{MM} x \doteq t, E[t/x] \]
\[ \text{if } x \in \text{var}(E), x \not\in \text{var}(t) \]

(5) \[ x \doteq t, E \Rightarrow_{MM} \perp \]
\[ \text{if } x \neq t, x \in \text{var}(t) \]

(6) \[ t \doteq x, E \Rightarrow_{MM} x \doteq t, E \]
\[ \text{if } t \not\in X \]
Unification

A substitution $\sigma$ is called more general than a substitution $\tau$ (denoted by $\sigma \leq \tau$), if there exists a substitution $\rho$ such that

$$\rho \circ \sigma = \tau$$

where $(\rho \circ \sigma)(x) := (x\sigma)\rho$ is the composition of $\sigma$ and $\rho$ as mappings.

(Note that $\rho \circ \sigma$ has a finite domain as required for a substitution.)
MM: Main Properties

If \( S = \{ x_1 \doteq u_1, \ldots, x_k \doteq u_k \} \), with \( x_i \) pairwise distinct, \( x_i \not\in \text{var}(u_j) \), then \( S \) is called an (unification problem in) **solved form** representing the solution \( \sigma_S = [x_1 \mapsto u_1, \ldots, x_k \mapsto u_k] \).

**Theorem:**

1. If \( S \Rightarrow_{MM} S' \) then \( \sigma \) is a unifier of \( S \) iff \( \sigma \) is a unifier of \( S' \)
2. If \( S \Rightarrow^*_{MM} \bot \) then \( S \) is not unifiable.
3. If \( S \Rightarrow^*_{MM} S' \) with \( S' \) in solved form, then \( \sigma_{S'} \) is an mgu of \( S \).
Main Unification Theorem

Theorem 2.30:
$S$ is unifiable if and only if there is a most general unifier $\sigma$ of $S$, such that $\sigma$ is idempotent and $\text{dom}(\sigma) \cup \text{codom}(\sigma) \subseteq \text{var}(S)$.

Proof: See e.g. Baader & Nipkow: Term rewriting and all that.

Problem: exponential growth of terms possible

Example:
$S = \{x_1 \doteq f(x_0, x_0), x_2 \approx f(x_1, x_1), \ldots, x_n \approx f(x_{n-1}, x_{n-1})\}$
m.g.u. $[x_1 \mapsto f(x_0, x_0), x_2 \mapsto f(f(x_0, x_0), f(x_0, x_0)), ...]$
$x_i \mapsto \text{complete binart tree of heigth } i$

Solution: Use acyclic term graphs; union/find algorithms
Like syntactical unification, equational unification is concerned with the problem of making terms equal by applying a suitable substitution.

The only difference is that syntactic equality is replaced by equality modulo an equational theory.
Like syntactical unification, equational unification is concerned with the problem of making terms equal by applying a suitable substitution. The only difference is that syntactic equality is replaced by equality modulo an equational theory.

**Motivation:**

- Automated reasoning in algebra
- Resolution “modulo” a theory
- Description logics: Concept term unification
$E$-Unification

$E$ equational theory; signature $\Sigma$; $\Sigma \subseteq \Delta$

$E$-unification problem over $\Delta$

$S : \{s_1 \doteq t_1, \ldots, s_k \doteq t_k\} \quad s_i, t_i \in T_\Delta(Y)$

- **elementary:** $\Delta \subseteq \Sigma$
- **with (free) constants:** $C = \Delta \setminus \Sigma$ constants
- **linear constant restrictions (l.c.r.):** $< \text{lin. ord. on } Y \cup C$

Unification with free constants

$S$ has a solution iff $\exists \sigma : Y \rightarrow T_\Delta(Y)$ s.t.

$E \models \sigma(s_i) \approx \sigma(t_i), \ i = 1, \ldots, k$

l.c.r. $<$ $y < c$: $c$ does not occur in $\sigma(y)$
$E$-Unification with free constants

Theorem [cf. Bockmayr92]

$S$ has a solution iff

$$\exists h : Y \rightarrow F^E_{\Sigma}(C) \text{ s.t.}$$

$$\overline{h}(s_i) = \overline{h}(t_i), \forall i,$$

where $\overline{h}(c) = [c]$ for all $c \in C$. 

If $E = \emptyset$ we know that every unification problem has a most general unifier.

This is not always true for $E$-unifiability: there may exist $E$-unifiable terms which do not have a most general $E$-unifier.
Let $S : \{s_1 \equiv t_1, \ldots, s_k \equiv t_k\}$ be an unification problem.

An $E$-unifier of $S$ is a substitution $\sigma$ such that

$$E \models \sigma(s_i) = \sigma(t_i) \text{ for all } i = 1, \ldots, n.$$ 

The set of all unifiers of $S$ is denoted by $\mathcal{U}_E(S)$.

$S$ is $E$-unifiable iff $\mathcal{U}_E(S) \neq 0$. 

Example 1

Let $E_C = \{ f(x, y) = f(y, x) \}$

$S : \{ f(a, x) \doteq f(b, y) \}$

- not syntactically unifiable
- $E_C$-unifier: $[x \mapsto b, y \mapsto a]$. 
Example 2

\[ E_A = \{ f(x, f(y, z)) = f(f(x, y), z) \} \]  

associativity

\[ S : \{ f(a, x) \doteq f(y, b) \} \]

\[ \mathcal{U}_{E_A}(S) \text{ contains} \]

- \[ [x \mapsto b, y \mapsto a], \]

- but also additional unifiers, e.g. \[ [x \mapsto f(z, b), y \mapsto f(a, z)]. \]
$E$-Unification

The instantiation ordering on substitutions is adapted to equational unification as follows:

A substitution $\sigma$ is more general modulo $E$ on $X$ than a substitution $\tau$, (Notation: $\sigma \leq^X_E \tau$) if there exists a substitution $\rho$ such that for all $x \in X$:

$$E \models \rho \circ \sigma(x) = \tau(x),$$

where $(\rho \circ \sigma)(x) := (x\sigma)\rho$ is the composition of $\sigma$ and $\rho$ as mappings. (Note that $\rho \circ \sigma$ has a finite domain as required for a substitution.)

$\leq^X_E$ is a quasi-ordering (reflexive and transitive).

When comparing $E$-unifiers of a unification problem $S$, the set $X$ is the set of all variables occurring in $S$. 

Unlike the case of syntactic unification, unifiable $E$-unification problems do not need to have a most general unifier.

**Example:**

$E_C = \{ f(x, y) = f(y, x) \}$

$S : \{ f(x, y) \equiv f(a, b) \}$

$S$ has two $E$-unifiers:

- $\sigma_1 := [x \mapsto a, y \mapsto b]$
- $\sigma_2 := [x \mapsto b, y \mapsto a]$

but they are not comparable.
**E-Unification**

**Definition.** A complete set of *E*-unifiers of $S$ is a set $C$ of substitutions s.t.:

- $C \subseteq \mathcal{U}_E(S)$
- for each $\theta \in \mathcal{U}_E(S)$ there exists $\sigma \in C$ such that $\sigma \leq_E^X \theta$.

**Definition.** $C$ is a minimal complete set of *E*-unifiers of $S$ iff it is complete and any two distinct elements of $C$ are incomparable w.r.t. $\leq_E^X$.

**Definition.** The substitution $\sigma$ is a most general *E*-unifier of $S$ if $\{\sigma\}$ is a (minimal) complete set of *E*-unifiers of $S$.

**Remark:** Minimal complete sets of unifiers need not always exist, and even if they do, they may be infinite; but it can be shown that they are unique up to $\equiv_E^X$ (equivalence associated with $\leq_E^X$).
Unification type

Definition:

Let \( E \) be an equational theory and let \( S \) be an \( E \)-unification problem.

\( S \) has:

- **unitary unification type** iff it has a minimal complete sets of unifiers of size 1
- **finitary unification type** iff it has a minimal complete sets of unifiers of finite cardinality
- **infinitary unification type** iff it has a minimal complete sets of unifiers of infinite cardinality

If \( S \) does not have a minimal complete sets of unifiers, then it is of type 0.
Examples

- **Unitary**: Syntactic unification
- **Finitary**: $E_C = \{ f(x, y) = f(y, x) \}$
- **Infinitary**: $E_A = \{ f(x, f(y, z)) = f(f(x, y), z) \}$

\[ S = \{ f(a, x) = f(x, a) \} \]

has an infinite minimal complete set of $E$-unifiers:

\[ \sigma_n := [x \mapsto f(a, f(a, \ldots f(a, a) \ldots))] \] (n occurrences of $a$).

- **Type zero**: The theory of idempotent semigroups

  (Fages and Huet 1983, 1986).