TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Institute of Theoretical Computer Science Chair of Automata Theory

UNIFICATION MODULO BOOLEAN RINGS

Florian Starke

Dresden, 2015/1/25

Structure

Equational Unification

Boolean Rings

Unification modulo Boolean Rings

Unification Problem

$$S := \left\{ f(a, x) \stackrel{?}{\approx} x \right\}$$

Equational Unification

Unification Problem

$\mathrm{I} := \{\mathrm{f}(\mathrm{x}, \mathrm{x}) \approx \mathrm{x}\}$

$$\mathrm{S} := \left\{\mathrm{f}(\mathrm{a}, \mathrm{x}) \overset{?}{\approx} \mathrm{x}\right\}$$

Unification Problem

$\mathrm{I} := \{\mathrm{f}(\mathrm{x}, \mathrm{x}) \approx \mathrm{x}\}$

$$\mathrm{S} := \left\{\mathrm{f}(\mathrm{a}, \mathrm{x}) \overset{?}{\approx} \mathrm{x}\right\} \qquad \Rightarrow \qquad \mathrm{S} := \left\{\mathrm{f}(\mathrm{a}, \mathrm{x}) \overset{?}{\approx}_{\mathrm{I}} \mathrm{x}\right\}$$

Let S be an I-unification problem . . .

elementary: $S := \left\{ f(y, x) \overset{?}{\approx}_{I} x \right\}$

with constants: $S := \left\{ f(a, x) \overset{?}{\approx}_{I} x \right\}$

general: $S := \left\{ f(g(a), x) \overset{?}{\approx}_{I} x \right\}$

Equational Unification
MGU?

$C := \{f(x, y) \approx f(y, x)\}$

$$S := \left\{ f(x, y) \overset{?}{\approx}_C f(a, b) \right\}$$

Equational Unification
MGU?

$\mathrm{C} := \{\mathrm{f}(\mathrm{x},\mathrm{y}) \approx \mathrm{f}(\mathrm{y},\mathrm{x})\}$

$$\mathrm{S} := \left\{\mathrm{f}(\mathrm{x},\mathrm{y}) \overset{?}{\approx}_{\mathrm{C}} \mathrm{f}(\mathrm{a},\mathrm{b})\right\}$$

$$\sigma_1 := \{\mathrm{x} \mapsto \mathrm{a}, \mathrm{y} \mapsto \mathrm{b}\} \qquad \sigma_2 := \{\mathrm{x} \mapsto \mathrm{b}, \mathrm{y} \mapsto \mathrm{a}\}$$

More General

$$\sigma < \sigma'$$

iff

$$\exists \delta : \delta(\sigma) = \sigma'$$

Equational Unification

More General

$$\sigma < \sigma' \quad \text{iff} \quad \exists \delta : \delta(\sigma) = \sigma'$$

$$\Rightarrow$$

$$\sigma \lesssim_{\mathrm{E}}^{\mathrm{X}} \sigma' \quad \text{iff} \quad \exists \delta : \forall \mathrm{x} \in \mathrm{X} : \delta(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \sigma'(\mathrm{x})$$

Minimal Complete Sets

Let S be an E-unification problem. A minimal complete set of S is a set of substitutions $\mathcal{M}$ that satisfy the following properties:

- each $\sigma \in \mathcal{M}$ is an E-unifier of S
- for all $\theta \in \mathcal{U}_{\mathrm{E}}(\mathrm{S})$ there exists a $\sigma \in \mathcal{M}$ such that $\sigma \lesssim_{\mathrm{E}}^{\mathrm{X}} \theta$
- for all $\sigma, \sigma' \in \mathcal{M},\ \sigma \lesssim_{\mathrm{E}}^{\mathrm{X}} \sigma'$ implies $\sigma = \sigma'$.

Unification Type of $\approx_E$

unitary iff for all E-unification problems S there exists a minimal complete set of cardinality ≤ 1.

Unification Type of $\approx_{\mathrm{E}}$

unitary iff for all E-unification problems S there exists a minimal complete set of cardinality ≤ 1.

finitary iff for all E-unification problems S there exists a minimal complete set with finite cardinality.

Unification Type of $\approx_E$

unitary	iff for all E-unification problems S there exists a minimal complete set of cardinality ≤ 1.
finitary	iff for all E-unification problems S there exists a minimal complete set with finite cardinality.
infinitary	iff for all E-unification problems S there exists a minimal complete set, and there exists an E-unification problem for which this set is infinite.

Unification Type of $\approx_{\mathrm{E}}$

unitary	iff for all E-unification problems S there exists a minimal complete set of cardinality ≤ 1.
finitary	iff for all E-unification problems S there exists a minimal complete set with finite cardinality.
infinitary	iff for all E-unification problems S there exists a minimal complete set, and there exists an E-unification problem for which this set is infinite.
zero	iff there exists an E-unification problem that does not have a minimal complete set.

Boolean Rings

$$B := \left\{ \begin{array}{cc} x + y \approx y + x, & x * y \approx y * x, \\ (x + y) + z \approx x + (y + z), & (x * y) * z \approx x * (y * z), \\ x + x \approx 0, & x * x \approx x, \\ 0 + x \approx x, & 0 * x \approx 0, \\ x * (y + z) \approx (x * y) + (x * z), & 1 * x \approx x \end{array} \right\}$$

Interpretation

$$\mathcal{B}_2 := (\Delta^{\mathcal{B}_2}, \cdot^{\mathcal{B}_2})$$

$$\Delta^{\mathcal{B}_2} := \{\bot, \top\}$$

Boolean Rings

Interpretation

$\mathcal{B}_2 := (\Delta^{\mathcal{B}_2}, \cdot^{\mathcal{B}_2})$

$\Delta^{\mathcal{B}_2} := \{\bot, \top\}$

$$
\begin{aligned}
(\mathrm{x} + \mathrm{y})^{\mathcal{B}_2} &:= \left(\mathrm{x}^{\mathcal{B}_2} \wedge \neg \mathrm{y}^{\mathcal{B}_2}\right) \vee \left(\neg \mathrm{x}^{\mathcal{B}_2} \wedge \mathrm{y}^{\mathcal{B}_2}\right) \\
(\mathrm{x} * \mathrm{y})^{\mathcal{B}_2} &:= \mathrm{x}^{\mathcal{B}_2} \wedge \mathrm{y}^{\mathcal{B}_2} \\
0^{\mathcal{B}_2} &:= \bot \\
1^{\mathcal{B}_2} &:= \top
\end{aligned}
$$

Example

$$
\begin{aligned}
(1+0)^{\mathcal{B}_2} &= \left(1^{\mathcal{B}_2} \wedge \neg 0^{\mathcal{B}_2}\right) \vee \left(\neg 1^{\mathcal{B}_2} \wedge 0^{\mathcal{B}_2}\right) \\
&= (\top \wedge \neg \bot) \vee (\neg \top \wedge \bot) \\
&= \top \vee \bot \\
&= \top
\end{aligned}
$$

In the following we will only consider elementary B-unification.

We will see:

- how to find a B-unifier.
- how to turn this B-unifier into an mgu.
- that elementary B-unification is unitary.

Unification modulo Boolean Rings

Solution in $\mathcal{B}_2 \Rightarrow$ B-unifier

$$\mathrm{S} := \mathrm{x} + \mathrm{y} + \mathrm{z} \overset{?}{\approx}_{\mathrm{B}} \mathrm{z} + 1$$

Unification modulo Boolean Rings

Solution in $\mathcal{B}_2 \Rightarrow$ B-unifier

$S := x + y + z \overset{?}{\approx}_B z + 1$

$$\varphi(w) := \begin{cases} \bot & \text{if } w = x \\ \top & \text{if } w \neq x \end{cases}$$

Unification modulo Boolean Rings

Solution in $\mathcal{B}_2 \Rightarrow$ B-unifier

$\mathrm{S} := \mathrm{x} + \mathrm{y} + \mathrm{z} \overset{?}{\approx}_{\mathrm{B}} \mathrm{z} + 1$

$$\varphi(\mathrm{w}) := \begin{cases} \bot & \text{if } \mathrm{w} = \mathrm{x} \\ \top & \text{if } \mathrm{w} \neq \mathrm{x} \end{cases} \qquad \Rightarrow \qquad \sigma' := \{\mathrm{x} \mapsto 0, \mathrm{y} \mapsto 1, \mathrm{z} \mapsto 1\}$$

Transformation

$$S = \left\{ s_1 \overset{?}{\approx}_B t_1, \ldots, s_n \overset{?}{\approx}_B t_n \right\}$$

Unification modulo Boolean Rings

Transformation

$$
\begin{aligned}
& S = \left\{ s_1 \overset{?}{\approx}_B t_1, \ldots, s_n \overset{?}{\approx}_B t_n \right\} \\
\Rightarrow \quad & S = \left\{ s_1 + t_1 \overset{?}{\approx}_B 0, \ldots, s_n + t_n \overset{?}{\approx}_B 0 \right\}
\end{aligned}
$$

Transformation

$$S = \left\{ s_1 \overset{?}{\approx}_B t_1, \ldots, s_n \overset{?}{\approx}_B t_n \right\}$$

$$\Rightarrow \qquad S = \left\{ s_1 + t_1 \overset{?}{\approx}_B 0, \ldots, s_n + t_n \overset{?}{\approx}_B 0 \right\}$$

$$\Rightarrow \qquad S = \left\{ (s_1 + t_1 + 1) * \cdots * (s_n + t_n + 1) \overset{?}{\approx}_B 1 \right\}$$

Transformation

$$S = \left\{ s_1 \overset{?}{\approx}_B t_1, \ldots, s_n \overset{?}{\approx}_B t_n \right\}$$

$$\Rightarrow \qquad S = \left\{ s_1 + t_1 \overset{?}{\approx}_B 0, \ldots, s_n + t_n \overset{?}{\approx}_B 0 \right\}$$

$$\Rightarrow \qquad S = \left\{ (s_1 + t_1 + 1) * \cdots * (s_n + t_n + 1) \overset{?}{\approx}_B 1 \right\}$$

$$\Rightarrow \qquad S = \left\{ (s_1 + t_1 + 1) * \cdots * (s_n + t_n + 1) + 1 \overset{?}{\approx}_B 0 \right\}$$

Reproductive E-unifier

$$
\begin{gathered}
\sigma \text{ is an mgu of S} \\
\text{iff} \\
\forall \tau \in \mathcal{U}_{\mathrm{E}}(\mathrm{S}) : \exists \theta : \forall \mathrm{x} \in \mathrm{X} : \\
\theta(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \tau(\mathrm{x})
\end{gathered}
$$

Reproductive E-unifier

σ is an mgu of S		σ is a reproductive E-unifier of S
iff	$\Rightarrow$	iff
$\forall \tau \in \mathcal{U}_{\mathrm{E}}(\mathrm{S}) : \exists \theta : \forall \mathrm{x} \in \mathrm{X} :$		$\forall \tau \in \mathcal{U}_{\mathrm{E}}(\mathrm{S}) : \forall \mathrm{x} :$
$\theta(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \tau(\mathrm{x})$		$\tau(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \tau(\mathrm{x})$

Löwenheim's Formula

Let τ be a B-unifier of $t \stackrel{?}{\approx}_B 0$. The substitution σ defined by

$$\sigma(x) := \begin{cases} (t+1) * x + t * \tau(x) & \text{if } x \in \mathcal{V}ar(t) \\ x & \text{if } x \notin \mathcal{V}ar(t) \end{cases}$$

is a reproductive B-unifier of $t \stackrel{?}{\approx}_B 0$.

Löwenheim's Formula

Why is σ reproductive?

Let τ' be an arbitrary B-unifier of S.

$$\begin{aligned}
\tau'(\sigma(\mathrm{x})) &= \ \tau'((\mathrm{t}+1)*\mathrm{x}+\mathrm{t}*\tau(\mathrm{x})) \\
&= \ (\tau'(\mathrm{t})+1)*\tau'(\mathrm{x})+\tau'(\mathrm{t})*\tau'(\tau(\mathrm{x})) \\
&\approx_{\mathrm{B}} (0+1)*\tau'(\mathrm{x})+0*\tau'(\tau(\mathrm{x})) \\
&\approx_{\mathrm{B}} \tau'(\mathrm{x})
\end{aligned}$$

Löwenheim's Formula Example

B-unification problem: $xy \overset{?}{\approx}_B 0$

$x = 0, y = 0 :$

$x = 0, y = 1 :$

$x = 1, y = 0 :$

Löwenheim's Formula Example

B-unification problem: $xy \overset{?}{\approx}_B 0$

$$
\begin{aligned}
x = 0, y = 0: \quad & \sigma_1(x) = (xy + 1) * x + xy * 0 \approx_B xy + x \\
& \sigma_1(y) = (xy + 1) * y + xy * 0 \approx_B xy + y \\
x = 0, y = 1: \quad & \\
& \\
x = 1, y = 0: \quad &
\end{aligned}
$$

Löwenheim's Formula Example

B-unification problem: $xy \overset{?}{\approx}_B 0$

$$
\begin{aligned}
x = 0, y = 0: \quad & \sigma_1(x) = (xy + 1) * x + xy * 0 \approx_B xy + x \\
& \sigma_1(y) = (xy + 1) * y + xy * 0 \approx_B xy + y \\
x = 0, y = 1: \quad & \sigma_2(x) = (xy + 1) * x + xy * 0 \approx_B xy + x \\
& \sigma_2(y) = (xy + 1) * y + xy * 1 \approx_B y \\
x = 1, y = 0: \quad & \text{similar to } x = 0, y = 1.
\end{aligned}
$$

Summary

Equational unification needs minimal complete sets of unifiers.

Elementary B-unification is unitary.

Finding an mgu is NP-complete.