TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Institute of Theoretical Computer Science Chair of Automata Theory

UNIFICATION MODULO BOOLEAN RINGS

Florian Starke

Dresden, 2015/2/3

Structure

Equational Unification

Boolean Rings

Unification modulo Boolean Rings

Unification Problem

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

Unification Problem

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

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

Unification Problem

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

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

Unification Classes

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?

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

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

Equational Unification

MGU?

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

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

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

Equational Unification

More General

$$\sigma \leq \sigma'$$

iff

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

More General

$\sigma \leq \sigma'$		$\sigma \lesssim^{X}_{E} \sigma'$
iff	$\Rightarrow$	iff
$\exists \delta : \delta\sigma = \sigma'$		$\exists \delta : \forall x \in X :$
		$\delta(\sigma(x)) \approx_{E} \sigma'(x)$

Minimal Complete Sets

Let S be an E-unification problem. A minimal complete set for 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 $\approx_{\mathrm{E}}$

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

Equational Unification

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.

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 $\approx_E$

- **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

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

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

Interpretation

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

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

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

Unification modulo Boolean Rings

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.

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

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

Unification modulo Boolean Rings

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

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

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

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

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

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

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

Transformation

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

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

Transformation

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

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

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

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

σ is a most general E-unifier of S

iff

$$\forall \tau \in \mathcal{U}_{\mathrm{E}}(\mathrm{S}) : \exists \theta : \forall \mathrm{x} \in \mathrm{X} :$$

$$\theta(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \tau(\mathrm{x})$$

Reproductive E-unifier

σ is a most general E-unifier 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: $\mathrm{xy} \overset{?}{\approx}_{\mathrm{B}} 0$

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

Löwenheim's Formula Example

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

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

Summary

Equational unification needs minimal complete sets of unifiers.

Elementary B-unification is unitary.

Finding an mgu is NP-complete.