TECHNISCHE
UNIVERSITÄT
DRESDEN

DRESDEN
concept

Institute of Theoretical Computer Science Chair of Automata Theory

UNIFICATION MODULO BOOLEAN RINGS

Florian Starke

Structure

Equational Unification

Boolean Rings

Unification modulo Boolean Rings

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

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

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

Equational Unification
Unification Problem

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

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

Equational Unification
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: $S := \left\{ f(g(a), x) \overset{?}{\approx}_I x \right\}$

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

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

MGU?

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

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

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

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

$$\sigma \leq \sigma' \qquad\qquad\qquad \sigma \lesssim_{\mathrm{E}}^{\mathrm{X}} \sigma'$$

$$\text{iff} \qquad\qquad \Rightarrow \qquad\qquad \text{iff}$$

$$\exists \delta : \delta(\sigma) = \sigma' \qquad\qquad \exists \delta : \forall \mathrm{x} \in \mathrm{X} :$$

$$\delta(\sigma(\mathrm{x})) \approx_{\mathrm{E}} \sigma'(\mathrm{x})$$

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 $\sigma = \sigma'$.

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

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.

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

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

Boolean Rings
Interpretation

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

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

Boolean Rings
Interpretation

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

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

$$(x + y)^{\mathcal{B}_2} := \left(x^{\mathcal{B}_2} \wedge \neg y^{\mathcal{B}_2}\right) \vee \left(\neg x^{\mathcal{B}_2} \wedge y^{\mathcal{B}_2}\right)$$

$$(x * y)^{\mathcal{B}_2} := x^{\mathcal{B}_2} \wedge y^{\mathcal{B}_2}$$

$$0^{\mathcal{B}_2} := \bot$$

$$1^{\mathcal{B}_2} := \top$$

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

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

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

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

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

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

Transformation

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

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

Unification modulo Boolean Rings
Transformation

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

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

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

Transformation

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

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

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

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

Unification modulo Boolean Rings
Reproductive E-unifier

σ is a most general E-unifier of S

iff

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

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

Unification modulo Boolean Rings
Reproductive E-unifier

σ is a most general E-unifier of S

iff $\Rightarrow$

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

$\theta(\sigma(x)) \approx_E \tau(x)$

σ is a reproductive E-unifier of S

iff

$\forall \tau \in \mathcal{U}_E(S) : \forall x :$

$\tau(\sigma(x)) \approx_E \tau(x)$

Löwenheim's Formula

Let τ be a B-unifier of $t \overset{?}{\approx}_B 0$. 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 $t \overset{?}{\approx}_B 0$.

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: $xy \overset{?}{\approx}_B 0$

$x = 0, y = 0 :$ $\sigma_1(x) = (xy + 1) * x + xy * 0 \approx_B xy + x$
                     $\sigma_1(y) = (xy + 1) * y + xy * 0 \approx_B xy + y$

$x = 0, y = 1 :$

$x = 1, y = 0 :$

Unification modulo Boolean Rings
Löwenheim's Formula Example

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

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

Summary

Equational unification needs minimal complete sets of unifiers.

Elementary B-unification is unitary.

Finding an mgu is NP-complete.