

# Zusammenfassung Term Rewriting aAT

© Tim Baumann, <http://timbaumann.info/uni-spicker>

Dies ist eine übersetzte Zusammenfassung des Buches Term Rewriting and All That von Franz Baader und Tobias Nipkow.

## Abstrakte Reduktionssysteme

**Def.** Ein **abstraktes Reduktionssystem** ist ein Tupel  $(A, \rightarrow)$ , wobei  $\rightarrow \in A \times A$  eine Relation auf  $A$  ist.

**Def.**

$\overset{0}{\rightarrow} := \{(a, a) \mid a \in A\}$	Identität
$\overset{i+1}{\rightarrow} := \overset{i}{\rightarrow} \circ \rightarrow$	$(i+1)$ -fache Komposition, $i \geq 0$
$\leftarrow := \{(t, s) \mid (s, t) \in \rightarrow\}$	Inverse Relation
$\overset{\circ}{\rightarrow} := (\rightarrow) \cup (\overset{0}{\rightarrow})$	refl. Hülle
$\overset{*}{\rightarrow} := \bigcup_{i \geq 0} (\overset{i}{\rightarrow})$	refl. trans. Hülle
$\overset{+}{\rightarrow} := \bigcup_{i \geq 1} (\overset{i}{\rightarrow})$	refl. trans. Hülle
$\leftrightarrow := \rightarrow \cup \leftarrow$	symm. Hülle
$\overset{*}{\leftrightarrow} := (\overset{*}{\rightarrow})^*$	refl. trans. symm. Hülle

**Def.** Sei  $x \in A$  ein Term.

- Der Term  $x$  heißt **reduzibel**, falls ein  $y \in A$  mit  $x \rightarrow y$  existiert,
- **irreduzibel** (oder in **Normalform**) falls  $x$  nicht reduzibel ist.
- Ein Term  $y \in A$  heißt **Normalform** von  $x$ , falls  $x \overset{*}{\rightarrow} y$  und  $y$  irreduzibel ist.
- Eine Term  $y$  heißt **direkter Nachfolger** von  $x$ , falls  $x \rightarrow y$ .
- Eine Term  $y$  heißt **Nachfolger** von  $x$ , falls  $x \overset{+}{\rightarrow} y$ .
- $x$  und  $y$  heißen *joinable*, notiert  $x \downarrow y$ , falls  $\exists z : x \overset{*}{\rightarrow} z \leftarrow^* y$ .

**Def.** Eine Reduktion  $\rightarrow$  heißt

**Church-Rosser** :  $\iff x \overset{*}{\leftrightarrow} y \implies x \downarrow y$   
**konfluent** :  $\iff y_1 \leftarrow^* y \overset{*}{\rightarrow} y_2 \implies y_1 \downarrow y_2$   
**semi-konfluent** :  $\iff y_1 \leftarrow y \overset{*}{\rightarrow} y_2 \implies y_1 \downarrow y_2$   
**terminierend** :  $\iff$  es gibt keine unendlich absteigende Kette  $x_0 \rightarrow x_1 \rightarrow x_2 \rightarrow \dots$  (auch: *noethersch*)  
**normalisierend** :  $\iff$  jeder Term besitzt eine Normalform  
**konvergent** :  $\iff$  konfluent  $\wedge$  normalisierend

**Lem.** Für eine Reduktion  $\rightarrow$  sind äquivalent:

- $\rightarrow$  ist Church-Rosser
- $\rightarrow$  ist konfluent
- $\rightarrow$  ist semi-konfluent

**Lem.** Ist die Reduktion  $\rightarrow$  konfluent/terminierend/konvergent, so besitzt jeder Term höchstens/mindestens/genau eine Normalform.

**Notation.** Falls  $x$  eine NF  $y$  besitzt, so schreibe  $x := \downarrow y$ .

**Thm.** Ist  $\rightarrow$  konvergent, so gilt  $x \overset{*}{\leftrightarrow} y \iff x \downarrow = y \downarrow$ .

*Bem.* Dies liefert einen einfachen Algorithmus, um  $x \overset{*}{\leftrightarrow} y$  zu entscheiden: Reduziere die Terme  $x$  und  $y$  zu Normalformen  $x \downarrow$  bzw.  $y \downarrow$  und vergleiche diese.

## Terminierungsbeweise

**Lem.**  $\rightarrow$  ist terminierend  $\iff \rightarrow$  ist eine Wohlordnung

**Def.** Eine Relation  $\rightarrow$  heißt

- **endlich verzweigend**, falls jeder Term nur endlich viele direkte Nachfolger besitzt,
- **global endlich**, falls jeder Term nur endl. viele Nachfolger hat,
- **azyklisch**, falls kein Term  $a$  mit  $a \overset{+}{\rightarrow} a$  existiert.

**Lem.**

- Eine endlich verzweigende Relation ist global endlich, falls sie terminierend ist.
- Eine azykl. Relation ist terminierend, falls sie global endlich ist.

**Lem.** Sei  $(A, \rightarrow)$  ein Reduktionssystem und  $(B, >)$  eine wohlgeordnete Menge. Gibt es eine streng monotone Abbildung  $\varphi : A \rightarrow B$ , so ist  $A$  terminierend.

**Lem.** Ein endlich verzweigendes Reduktionssystem  $(A, \rightarrow)$  ist genau dann terminierend, falls es eine streng monotone Abbildung  $\varphi : (A, \rightarrow) \rightarrow (\mathbb{N}, >)$  gibt.

**Def.** Seien  $(A_i, >_i)_{i=1, \dots, n}$  geordnete Mengen. Die **lexikalische Ordnung**  $>_{\text{lex}}$  auf  $A_1 \times \dots \times A_n$  ist definiert durch

$(x_1, \dots, x_n) >_{\text{lex}} (y_1, \dots, y_n) : \iff \exists k \leq n : (\forall i < k : x_i = y_i) \wedge x_k <_k y_k$ .

**Lem.** Ist  $>$  eine strikte (Wohl-) Ordnung, so auch  $>_{\text{lex}}$ .

**Def.** Eine *Multimenge*  $M$  über einer Menge  $A$  ist eine Abbildung  $M : A \rightarrow \mathbb{N}$ . Sie ist endlich, falls  $\sum_{a \in A} M(a) < \infty$ .

**Notation.**  $\mathcal{M}(A) := \{ \text{Multimengen über } A \}$   
 $a \in M : \iff M(a) \geq 1$

**Def.** Die *Differenz* von Multimengen  $M, N \in \mathcal{M}(A)$  ist  $M - N \in \mathcal{M}(A)$  mit  $(M - N)(a) := \max\{0, M(a) - N(a)\}$ .

**Def.** Sei  $>$  eine strikte Ordnung auf  $A$ . Die **Multimengenordnung**  $>_{\text{mul}}$  auf  $\mathcal{M}(A)$  ist dann definiert durch

$M >_{\text{mul}} N : \iff M \neq N \wedge \forall n \in N - M : \exists m \in M - N : m > n$ .

**Lem.** Ist  $>$  eine strikte (Wohl-) Ordnung, so auch  $>_{\text{mul}}$ .

## Konfluenzbeweise

**Def.** Eine Relation  $\rightarrow$

- heißt **lokal konfluent**, falls  $y_1 \leftarrow y \rightarrow y_2 \implies y_1 \downarrow y_2$ .
- heißt **stark konfluent**, falls  $y_1 \leftarrow y \rightarrow y_2 \implies \exists z : y_1 \overset{*}{\rightarrow} z \overset{*}{\leftarrow} y_2$ .
- besitzt die **Diamant-Eigenschaft**, falls

$$y_1 \leftarrow y \rightarrow y_2 \implies \exists z : y_1 \rightarrow z \leftarrow y_2.$$

**Lem.** Falls  $\rightarrow_1 \leq \rightarrow_2 \leq \overset{*}{\rightarrow}_1$ , so gilt  $\overset{*}{\rightarrow}_1 = \overset{*}{\rightarrow}_2$ . Ist zusätzlich  $\rightarrow_2$  (stark) konfluent, so auch  $\rightarrow_1$ .

**Lem.**

- Stark konfluente Relationen sind konfluent.
- Eine terminierende Rel. ist konfluent, falls sie lokal konfluent ist.

**Def.** Zwei Relationen  $\rightarrow_1$  und  $\rightarrow_2$  auf  $A$

- **kommutieren**, falls  $y_1 \overset{*}{\leftarrow}_1 x \overset{*}{\rightarrow}_2 y_2 \implies \exists z : y_1 \overset{*}{\rightarrow}_2 z \overset{*}{\leftarrow}_1 y_2$ .
- **kommutieren stark**, falls

$$y_1 \leftarrow_1 x \rightarrow_2 y_2 \implies \exists z : y_1 \overset{=}{\rightarrow}_2 z \overset{*}{\leftarrow}_1 y_2.$$

- besitzen die **Kommutierender-Diamant-Eigenschaft**, falls

$$y_1 \leftarrow_1 x \rightarrow_2 y_2 \implies \exists z : y_1 \rightarrow_2 z \leftarrow_1 y_2.$$

**Lem.** Angenommen,  $\rightarrow_1$  und  $\rightarrow_2$  sind konfluent und kommutieren. Dann ist auch  $\rightarrow_1 \cup \rightarrow_2$  konfluent.

# Universelle Algebra

**Def.** Eine **Signatur**  $\Sigma$  ist eine Menge von *Funktionssymbolen* zusammen mit einer Aritätsabbildung  $\text{arity} : \Sigma \rightarrow \mathbb{N}$ .

**Notation.**  $\Sigma^{(n)} := \text{arity}^{-1}(n)$

**Def.** Sei  $\Sigma$  eine Signatur und  $X$  eine Menge von Variablen (d. h. es gilt  $X \cap \Sigma = \emptyset$ ). Die Menge  $T(\Sigma, X)$  der  **$\Sigma$ -Terme über  $X$**  ist induktiv definiert durch

- $X \subseteq T(\Sigma, X)$
- $\forall f \in \Sigma^{(n)}, t_1 \in T(\Sigma, X), \dots, t_n \in T(\Sigma, X) : f(t_1, \dots, t_n) \in T(\Sigma, X)$

*Bem.* Falls  $X \subseteq Y$ ,  $Y \cap \Sigma = \emptyset$ , so gilt  $T(\Sigma, X) \subseteq T(\Sigma, Y)$ .

**Def.** Terme  $t$  ohne freie Variablen (d. h.  $t \in T(\Sigma, \emptyset)$ ) heißen **Grundterme** oder **geschlossene Terme**.

**Def.** Die Menge der **Positionen**  $\text{Pos}(s)$  eines Terms  $s \in T(\Sigma, X)$  ist folgende Menge von Listen von natürlichen Zahlen

- Falls  $s = x \in X$ :  $\text{Pos}(s) := \{\epsilon\}$
- Falls  $s = f(s_1, \dots, s_n)$ :  $\text{Pos}(s) := \{\epsilon\} \cup \bigcup_{i=1}^n \{ip \mid p \in \text{Pos}(s_i)\}$

**Def.** Die **Größe** eines Terms  $s \in T(\Sigma, X)$  ist  $|s| := |\text{Pos}(s)|$ .

**Def.** Der **Subterm**  $s|_p$  an der Position  $p \in \text{Pos}(s)$  eines Terms  $s$  ist

$$s|_\epsilon := s, \quad f(s_1, \dots, s_n)|_{iq} := s_i|_q.$$

Die **Ersetzung**  $s[t]_p$  von  $s|_p$  durch einen Term  $t \in T(\Sigma, X)$  ist

$$s[t]_\epsilon := t, \quad f(s_1, \dots, s_n)[t]_{iq} := s_i[t]_q.$$

**Def.** Die **Menge der Variablen** in  $s \in T(\Sigma, X)$  ist

$$\text{Var}(s) := \{x \in X \mid \exists p \in \text{Pos}(s) : s|_p = x\}.$$

*Bem.* Für jeden Term  $t \in T(\Sigma, X)$  gilt  $t \in T(\Sigma, \text{Var}(t))$ .

**Def.** Sei  $\Sigma$  eine Signatur und  $V$  eine abzählbar unendliche Menge von Variablen. Eine  $T(\Sigma, V)$ -**Ersetzung** ist eine Abbildung  $\sigma : V \rightarrow T(\Sigma, V)$ , für die gilt:

$$\text{Dom}(\sigma) := \{v \in V \mid \sigma(v) \neq v\}$$

ist endlich. Die Menge der  $T(\Sigma, V)$ -Ersetzungen ist  $\text{Sub}(T(\Sigma, V))$ . Wir können  $\sigma$  ausdehnen zu einer Abb.  $\hat{\sigma} : T(\Sigma, V) \rightarrow T(\Sigma, V)$  durch

$$\hat{\sigma}(v) := \sigma(v), \quad \hat{\sigma}(f(s_1, \dots, s_n)) := f(\hat{\sigma}(s_1), \dots, \hat{\sigma}(s_n)).$$

Die **Komposition** zweier Ersetzungen  $\sigma$  und  $\tau$  ist  $\sigma \circ \tau := \hat{\sigma} \circ \tau$ .

**Def.** Eine  **$\Sigma$ -Identität** ist ein Paar  $(s, t) \in T(\Sigma, V) \times T(\Sigma, V)$ , auch geschrieben  $s \approx t$ .

**Def.** Die **Reduktionsrelation**  $\rightarrow_E$  zu einer Menge  $E$  von  $\Sigma$ -Identitäten ist

$$s \rightarrow_E t : \iff \exists (l \approx r) \in E, p \in \text{Pos}(s), \sigma \in \text{Sub}(T(\Sigma, V)) : \\ s|_p = \sigma(l) \wedge t = s[\sigma(r)]_p.$$

**Def.** Eine Relation  $\equiv$  auf  $T(\Sigma, V)$  heißt

- **abgeschlossen unter Ersetzungen**, falls  $s = t \implies \sigma(s) = \sigma(t)$
- **abgeschlossen unter  $\Sigma$ -Operationen**, falls

$$s_1 \equiv t_1, \dots, s_n \equiv t_n \implies f(s_1, \dots, s_n) \equiv f(t_1, \dots, t_n)$$

- **kompatibel mit  $\Sigma$ -Operationen**, falls

$$s \equiv t \implies \begin{aligned} f(s_1, \dots, s_{i-1}, s, s_{i+1}, \dots, s_n) \\ \equiv f(s_1, \dots, s_{i-1}, t, s_{i+1}, \dots, s_n) \end{aligned}$$

- **kompatibel mit  $\Sigma$ -Kontexten**, falls

$$s \equiv s' \implies t[s]_p \equiv t[s']_p$$

- **Umschreibungsrelation**, falls sie kompatibel mit  $\Sigma$ -Operationen und abgeschlossen unter Ersetzungen ist.

**Lem.** Es sind äquivalent:

- $\equiv$  ist kompatibel mit  $\Sigma$ -Operationen
- $\equiv$  ist kompatibel mit  $\Sigma$ -Kontexten

Ist  $\equiv$  reflexiv und transitiv, so ist außerdem äquivalent:

- $\equiv$  ist abgeschlossen unter  $\Sigma$ -Operationen

**Thm.** Sei  $E$  eine Menge von  $\Sigma$ -Identitäten.

- $\rightarrow_E$ ,  $\xrightarrow{+}_E$  und  $\xrightarrow{*}_E$  sind Umschreibungsrelationen.
- Die Relation  $\xleftrightarrow{*}_E$  ist die kleinste Äquivalenzrelation, die  $E$  enthält und abg. ist unter Ersetzungen und  $\Sigma$ -Operationen.

**Def.** Eine  **$\Sigma$ -Algebra**  $\mathcal{A}$  besteht aus

- einer *Trägermenge*  $A$  und
- einer Abbildung  $f^{\mathcal{A}} : A^n \rightarrow A$  für alle  $f \in \Sigma^{(n)}$ .

**Bsp.**  $T(\Sigma, V)$  ist eine  $\Sigma$ -Algebra mit

$$f^{T(\Sigma, V)} : T(\Sigma, V)^n \rightarrow T(\Sigma, V), \quad (t_1, \dots, t_n) \mapsto f(t_1, \dots, t_n).$$

- Eine  **$\Sigma$ -Subalgebra** von  $A$  ist eine Teilmenge  $B \subset A$ , sodass  $f^{\mathcal{A}}(b_1, \dots, b_n) \in B$  für alle  $f \in \Sigma^{(n)}$  und  $b_1, \dots, b_n \in B$ .
- Die von  $X \subseteq A$  **erzeugte  $\Sigma$ -Subalgebra** ist die kleinste  $\Sigma$ -Subalgebra, die  $X$  enthält.

**Def.** Ein *Homomorphismus*  $\phi$  zwischen  $\Sigma$ -Algebren  $\mathcal{A}$  und  $\mathcal{B}$  (mit Trägermengen  $A$  bzw.  $B$ ) ist eine Abbildung  $\phi : A \rightarrow B$ , sodass

$$\phi(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(\phi(a_1), \dots, \phi(a_n)).$$

*Bem.* Damit bilden  $\Sigma$ -Algebren eine Kategorie.

**Def.** Eine Äquivalenzrelation  $\equiv$  auf  $A$  heißt **Kongruenz** auf  $\mathcal{A}$ , falls

$$a_1 \equiv b_1, \dots, a_n \equiv b_n \implies f^{\mathcal{A}}(a_1, \dots, a_n) \equiv f^{\mathcal{A}}(b_1, \dots, b_n).$$

**Lem/Def.** Ist  $\equiv$  eine Äquivalenz, so wird  $A/\equiv$  mit

$$f^{A/\equiv}([a_1], \dots, [a_n]) := [f^{\mathcal{A}}(a_1, \dots, a_n)]$$

eine  $\Sigma$ -Algebra, die **Quotientenalgebra**  $\mathcal{A}/\equiv$ .

**Lem.** Die Kategorie der  $\Sigma$ -Algebren enthält kleine Limiten.

**Def.** Eine  $\Sigma$ -Algebra heißt **frei**, falls sie isomorph ist zu  $F(X) := T(\Sigma, X)$  für eine Menge  $X$  von Variablen.

*Bem.* Diese Setzung definiert einen Funktor  $F : \mathbf{Set} \rightarrow \Sigma\text{-}\mathbf{Alg}$ .

**Lem.**  $F \dashv U$ , wobei  $U : \mathbf{Set} \rightarrow \Sigma\text{-}\mathbf{Alg}$  der Vergissfunctor ist.

**Kor.**  $F(\emptyset) = T(\Sigma, \emptyset)$  ist das initiale Objekt in  $\Sigma\text{-}\mathbf{Alg}$ .

- Eine  $\Sigma$ -Identität  $s \approx t$  **gilt in einer  $\Sigma$ -Algebra  $\mathcal{A}$** , falls für alle Homomorphismen  $\phi : T(\Sigma, V) \rightarrow \mathcal{A}$  gilt:  $\phi(s) = \phi(t)$ .
- $\mathcal{A}$  ist ein **Modell** einer Menge  $E$  von  $\Sigma$ -Algebren (notiert  $\mathcal{A} \models E$ ), falls jede Identität aus  $E$  in  $\mathcal{A}$  gilt.
- Die Subkategorie von  $\Sigma\text{-}\mathbf{Alg}$  der Modelle von  $E$  heißt *durch  $E$  definierte  $\Sigma$ -Varietät*  $\mathcal{V}(E)$ .

- Die Identität  $s \approx t$  ist eine **semantische Konsequenz** von  $E$  (notiert  $E \models s \approx t$ ), falls  $s \approx t$  in allen  $\mathcal{A} \in \mathcal{V}(E)$  gilt.
- $\approx_E := \{(s, t) \mid E \models s \approx t\}$  heißt von  $E$  **induzierte Theorie**.

**Def.** Eine Relation  $\equiv$  auf  $T(\Sigma, V)$  heißt **voll invariant**, falls  $s \equiv t \implies \phi(s) \equiv \phi(t)$  für alle Mor.  $\phi : T(\Sigma, V) \rightarrow T(\Sigma, V)$ .

**Lem.**  $\approx_E$  ist eine voll invariante Kongruenz.

**Lem/Def.** Es sind äquivalent:

- $E$  heißt **trivial**
- $\approx_E = T(\Sigma, V) \times T(\Sigma, V)$
- $x \approx_E y$  gilt für Variablen  $x, y \in V$ ,  $x \neq y$
- $\mathcal{V}(E)$  besteht aus Algebren der Kardinalität  $\leq 1$ .

**Thm.** Sei  $V$  eine abzählbar unendliche Menge von Variablen.

- $T(\Sigma, V)/\approx_E$  ist eine freie Algebra in  $\mathcal{V}(E)$  mit erz. Menge  $V/\approx_E$ . Falls  $E$  nicht trivial ist, so ist  $V/\approx_E$  abzählbar unendlich.
- $T(\Sigma, V)/\approx_E \models s \approx t \iff s \approx_E t$

**Def.** Die durch  $E$  **induzierte induktive Theorie** ist

$$\approx_E^I := \{(s, t) \mid T(\Sigma, \emptyset) \models s \approx t\} \subseteq T(\Sigma, V) \times T(\Sigma, V).$$

*Bem.*  $\approx_E \subseteq \approx_E^I$

*Umformulierung.* Die Relation  $\xleftrightarrow{*}_E$  ist die kleinste voll invariante Kongruenz auf  $T(\Sigma, V)$ , die  $E$  enthält.

**Lem.** Für eine voll invariante Kongruenz  $\equiv$  auf  $T(\Sigma, V)$  gilt:

$$E \subseteq \equiv \implies \approx_E \subseteq \equiv.$$

**Kor (Birkhoffs Lemma).**  $\xleftrightarrow{*}_E = \approx_E$

**Thm.** Für eine Klasse  $\mathcal{K}$  von  $\Sigma$ -Algebren sind äquivalent:

- $\mathcal{K}$  ist eine Varietät, d. h.  $\mathcal{K} = \mathcal{V}(E)$  für eine Menge  $E$  von Identitäten.
- $\mathcal{K}$  ist abgeschlossen unter dem Bilden von Unteralgebren, Bildalgebren und direkten Produkten.

# Gleichheitsprobleme

**Def.** Sei  $E$  eine Menge von Identitäten. Eine Gleichheit  $s \approx t$  heißt

- **gültig** in  $E$ , falls  $s \approx_E t$ ,
- **erfüllbar** in  $E$ , falls es eine Ersetzung  $\sigma$  mit  $\sigma(s) \approx_E \sigma(t)$  gibt.

**Problem (matching problem).** Gegeben Terme  $s$  und  $l$ , gibt es eine Ersetzung  $\sigma$ , sodass  $\sigma(s) = l$ ?

**Thm.** Ist  $E$  endlich und  $\rightarrow_E$  konvergent, so ist  $\approx_E$  entscheidbar.

**Algorithmus.** Seien  $x$  und  $y$  gegeben. Wegen der Endlichkeit von  $E$  sind  $x \downarrow$  und  $y \downarrow$  berechenbar. Es gilt  $x \approx_E y \iff x \downarrow = y \downarrow$ .

**Def.** • **Wortproblem:** Gegeben  $x, y \in T(\Sigma, V)$ , gilt  $x \approx_E y$ ?  
• **Grundwortproblem:** Gegeben  $x, y \in T(\Sigma, \emptyset)$ , gilt  $x \approx_E y$ ?

**Bem.** Das Wortproblem ist im Allgemeinen unentscheidbar, denn:

- Man kann den turingvollständigen SKI-Kalkül als Reduktionssystem durch Angabe einer Menge von Gleichheiten spezifizieren.
- Gleichheit von Programmen ist unentscheidbar.

**Def.** • Eine **Umschreibungsregel** ist eine Identität  $l \approx r$  bei der  $s$  keine Variable ist und  $\text{Var}(l) \supseteq \text{Var}(r)$ .  
• Ein **Termumschreibungssystem** (TUS) ist eine Menge von Umschreibungsregeln.

**Bem.** Die zwei Bedingungen für Umschreibungsregeln sind notwendig (aber nicht hinreichend) dafür, dass Termumschreibungssysteme terminierend sind.

## Die kongruente Hülle

**Def.** Die **kongruente Hülle**  $\text{CC}(E)$  von  $E \subseteq T(\Sigma, V) \times T(\Sigma, V)$  ist die kleinste Kongruenzrelation, die  $\equiv$  enthält.

**Bem.**  $(s, t) \in \text{CC}(E)$  gilt genau dann, wenn die Aussage aus folgenden Inferenzregeln herleitbar ist:

$$\frac{}{(t, t) \in \text{CC}(E)} \quad \frac{(t, s) \in \text{CC}(E)}{(s, t) \in \text{CC}(E)} \quad \frac{(r, s) \in \text{CC}(E) \quad (s, t) \in \text{CC}(E)}{(r, t) \in \text{CC}(E)} \\ \frac{(s, t) \in E \quad f \in \Sigma^{(n)} \quad (s_1, t_1) \in \text{CC}(E), \dots, (s_n, t_n) \in \text{CC}(E)}{(s, t) \in \text{CC}(E)} \quad \frac{(f(s_1, \dots, s_n), f(t_1, \dots, t_n)) \in \text{CC}(E)}{(s, t) \in \text{CC}(E)}$$

**Def.** Eine Id.  $l \approx r$  heißt **Grundidentität**, falls  $\text{Var}(l) = \text{Var}(r) = \emptyset$ .

**Notation.** Sei  $G$  im Folgenden eine Menge von Grundidentitäten.

**Lem.**  $\text{CC}(G) = \approx_G$

**Def.** Die Menge der **Unterterme** ist

$$\text{Subterms}(t) := \{t|_p \mid p \in \text{Pos}(t)\} \quad \text{für } t \in T(\Sigma, V) \text{ bzw.} \\ \text{Subterms}(G) := \bigcup_{l \approx r} \text{Subterms}(l) \cup \text{Subterms}(r).$$

**Thm.** Fixiere zwei Terme  $s, t \in T(\Sigma, V)$ . Setze

$$S := \text{Subterms}(s) \cup \text{Subterms}(t) \cup \text{Subterms}(G).$$

Es gilt  $G \subseteq S \times S$ . Es sei  $\text{CC}_S(G)$  die kongruente Hülle von  $G$  innerhalb von  $S \times S$ . Dann gilt:

$$\text{CC}_S(G) = \approx_G \cap (S \times S).$$

**Kor.** Das Wortproblem ist für endliche Mengen  $G$  von Grundidentitäten entscheidbar.

**Beweisidee.** Seien  $s$  und  $t$  gegeben. Berechne die endliche Menge  $\text{CC}_S(G)$ . Es gilt dann:  $s \approx_G t \iff (s, t) \in \text{CC}_S(G)$ .

**Bem.** Dies liefert einen Entscheidungsalgorithmus mit polynomieller Laufzeit in  $G$ ,  $s$  und  $t$ .

**Algorithmus.** Effiziente Realisierung:

- Repräsentiere die Termmenge  $S$  als gerichteter Graph, wobei jeder Knoten  $v$  mit einem Symbol  $f \in \Sigma$  beschriftet ist und dessen Auskanten mit  $i = 1, \dots, \text{arity}(f)$  nummeriert sind.
- Wir repräsentieren Identifikationen von Knoten im Graph über Zeiger wie in der Union-Find-Datenstruktur. Wir definieren  $u \sim v : \iff \text{FIND}(u) = \text{FIND}(v)$  für Knoten  $u$  und  $v$ .

```

1: function MERGE( $u, v$ )
2:   if  $u \not\sim v$  then
3:      $P := \text{PRED}(u)$ ,  $Q := \text{PRED}(v)$ 
4:     UNION( $u, v$ )
5:     for  $(p, q) \in P \times Q$  do
6:       if  $p \not\sim q \wedge \text{CONGRUENT}(p, q)$  then
7:         MERGE( $p, q$ )
8: function CONGRUENT( $p = f(p_1, \dots, p_n)$ ,  $q = g(q_1, \dots, q_m)$ )
9:   if  $f \neq g \in \Sigma$  then return false
10:  for  $i = 1, \dots, n$  do
11:    if  $p_i \not\sim q_i$  then return false
    return true

```

- Rufe zu Beginn des Algorithmus  $\text{MERGE}(l, r)$  für alle Grundidentitäten  $(l \approx r) \in G$  auf.
- Das Ergebnis ist nun  $s \sim t$ .

## Syntaktische Unifikation

**Def.** Eine Substitution  $\sigma$  heißt **allgemeiner** (notiert  $\sigma \lesssim \sigma'$ ) als  $\sigma'$ , falls eine Substitution  $\delta$  mit  $\sigma' = \delta\sigma$  existiert.

**Lem.**  $\lesssim$  ist eine Quasiordnung

**Def.** Eine **Umbenennung** ist eine Ersetzung  $\rho$  mit  $\text{im}(\rho) \subseteq V$  ( $\implies \text{im}(\rho) = V$ ).

**Lem.**  $\sigma \lesssim \sigma' \wedge \sigma' \lesssim \sigma \iff \exists \text{ Umbenennung } \rho : \sigma = \rho\sigma'$

**Def.** Ein **Unifikationsproblem** ist gegeben durch eine endliche Menge von Gleichungen

$$S = \{s_1 \stackrel{?}{=} t_1, \dots, s_n \stackrel{?}{=} t_n\}.$$

Eine *Lösung* von  $S$  ist eine Ersetzung  $\sigma$  mit  $\sigma(s_i) = \sigma(t_i)$  für  $i = 1, \dots, n$ . Notation:  $\mathcal{U}(S) := \{ \text{Lösungen von } S \}$

**Gesucht.** Eine **allgemeinste Lösung** von  $S$ , das ist ein bezüglich  $\lesssim$  kleinstes Element in  $\mathcal{U}(S)$ .

**Thm.** Hat ein Unifikationsproblem eine Lösung, so hat es auch eine idempotente, allgemeinste Lösung.

**Def.** Ein Unifikationsproblem  $S = \{x_1 \stackrel{?}{=} t_1, \dots, x_n \stackrel{?}{=} t_n\}$  ist in **gelöster Form**, falls  $x_1, \dots, x_n$  paarweise verschieden Variablen sind, die nicht in den Termen  $t_1, \dots, t_n$  auftreten. In diesem Fall ist

$$\vec{S} := \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}.$$

**Lem.** Sei  $S$  in gelöster Form. Dann gilt:

- $\forall \sigma \in \mathcal{U}(S) : \sigma = \sigma\vec{S}$
- $\vec{S}$  ist eine idempotente, allgemeinste Lösung von  $S$ .

**Algorithmus** (UNIFY( $S$ )). Wende wiederholt folgende Transformationsregeln (in beliebiger Reihenfolge) auf  $S$  an:

Delete	$\{t \stackrel{?}{=} t\} \sqcup S$	$\rightsquigarrow$	$S$
Decompose	$\{f(\vec{s}) \stackrel{?}{=} f(\vec{t})\}$	$\rightsquigarrow$	$\{s_1 \stackrel{?}{=} t_1, \dots, s_n \stackrel{?}{=} t_n\} \cup S$
Orient	$\{t = x\} \sqcup S$	$\rightsquigarrow$	$\{x = t\} \cup S$ falls $t \notin V$
Eliminate	$\{x \stackrel{?}{=} t\} \sqcup S$	$\rightsquigarrow$	$\{x \stackrel{?}{=} t\} \cup [t/x]S$ falls $x \in \text{Var}(S) \setminus \text{Var}(t)$

Wenn keine Transformationsregel mehr angewandt werden kann, so

- gib  $\vec{T}$  zurück, falls die nach Anwendung aller Transformationen erhaltene Gleichungsmenge  $T$  in gelöster Form ist,
- ansonsten gib  $\perp$  zurück.

**Lem.** Falls  $S \rightsquigarrow T$ , so gilt  $\mathcal{U}(S) = \mathcal{U}(T)$ .

**Thm.** UNIFY( $S$ ) ist korrekt:

- Der Algorithmus terminiert für alle Eingaben.
- Die Ausgabe ist eine idempotente, allgemeinste Lösung von  $S$  oder  $\perp$ , falls  $S$  keine Lösung besitzt.

**Bem.** Folgende Regeln bewirken einen frühen Abbruch:

Clash	$\{f(\vec{s}) \stackrel{?}{=} g(\vec{t})\} \sqcup S$	$\rightsquigarrow$	$\perp$	falls $f \neq g$
Occurs-Check	$\{x \stackrel{?}{=} t\} \sqcup S$	$\rightsquigarrow$	$\perp$	falls $x \in \text{Var}(t)$ und $x \neq t$

**Bem.** Naive Implementierungen von Unifikation benötigen exponentielle Zeit. Es gibt einen Algorithmus auf Termgraphen, der nur (fast) lineare Zeit benötigt.

## Terminierung

**Problem.** Gegeben ein Termumschreibungssystem  $R$ , gibt es einen Algorithmus, der entscheidet, ob  $R$  terminierend ist oder nicht?

**Thm.** Dieses Problem ist im Allgemeinen unentscheidbar.

*Beweisidee.* Man kann Turingmaschinen als Termumschreibungssysteme kodieren. Die Aussage folgt daraus, dass das Halteproblem für Turingmaschinen unentscheidbar ist.

**Def.** Ein TUS  $R$  heißt **rechtsseitig geschlossen**, falls für alle  $(l \rightarrow r) \in R$  der rechte Term  $r$  geschlossen ist (d. h.  $\text{Var}(r) = \emptyset$ ).

**Lem.** Sei  $R$  ein endliches, rechtsseitig geschlossenes Termumschreibungssystem. Dann sind äquivalent:

- $R$  ist *nicht* terminierend
- Es gibt eine Regel  $(l \rightarrow r) \in R$  und einen Term  $t$ , sodass  $r \xrightarrow{+}_R t$  und  $t$  den Subterm  $r$  besitzt.

**Thm.** Für endliche, rechtsseitig geschlossene TUSe ist das Terminierungsproblem entscheidbar.

*Beweisidee.* Führe Breitensuche (gemäß  $\rightarrow_R$ ) auf der Menge der Terme durch, beginnend bei der Wurzelmenge  $\{r \mid (l \rightarrow r) \in R\}$ . Falls  $R$  terminiert, so endet diese Suche. Ansonsten findet man bei der Suche in endlicher Zeit eine Verletzung von Punkt zwei aus dem vorherigen Lemma.

**Def.** Eine strikte Ordnung  $>$  auf  $T(\Sigma, V)$  heißt **Umschreibungsordnung** (UO), falls sie

- *kompatibel mit  $\Sigma$ -Operationen* ist, d. h. aus  $s > t$  folgt

$$f(s_1, \dots, s_{i-1}, s, s_{i+1}, \dots, s_n) > f(s_1, \dots, s_{i-1}, t, s_{i+1}, \dots, s_n)$$

- und *abgeschlossen unter Ersetzungen* ist, d. h.

$$s_1 > s_2 \implies \sigma(s_1) > \sigma(s_2).$$

Eine **Reduktionsordnung** ist eine wohlfundierte Umschreibungsordnung.

**Thm.** Für eine Termumschreibungssystem  $R$  sind äquivalent:

- $R$  terminiert.
- Es gibt eine Reduktionsordnung  $>$  mit  $l > r$  für alle  $(l \rightarrow r) \in R$ .

## Die Interpretationsmethode

**Lem/Def.** Sei  $\mathcal{A}$  eine nichtleere  $\Sigma$ -Algebra und  $>$  eine wohlfundierte Ordnung auf deren Trägermenge  $A$ . Angenommen,  $f^{\mathcal{A}} : A^n \rightarrow A$  ist in jedem Argument streng monoton für alle  $n \in \mathbb{N}$ ,  $f \in \Sigma^{(n)}$ . Dann definiert

$$s >_{\mathcal{A}} t : \iff \pi(s) > \pi(t) \text{ für alle Mor. } \pi : T(\Sigma, V) \rightarrow \mathcal{A}$$

eine Reduktionsordnung auf  $T(\Sigma, V)$ .

**Def.** Eine **polynomielle Interpretation** von  $\Sigma$  ist eine  $\Sigma$ -Algebra  $\mathcal{A}$  mit

- Trägermenge  $A \subseteq \mathbb{N} \setminus \{0\}$
- Es gilt  $f^{\mathcal{A}}(a_1, \dots, a_n) = P_f(a_1, \dots, a_n)$  mit einem Polynom  $P_f \in \mathbb{N}[X_1, \dots, X_n]$  für alle  $n \in \mathbb{N}$ ,  $f \in \Sigma^{(n)}$ .

**Def.** Ein Polynom  $P \in \mathbb{N}[X_1, \dots, X_n]$  heißt **strikt monoton**, falls  $P \notin \mathbb{N}[X_1, \dots, \widehat{X}_i, \dots, X_n]$  für  $i = 1, \dots, n$ .

**Lem/Def.** Sei  $\mathcal{A}$  eine polynomielle Interpretation  $\mathcal{A}$ , deren Polynome  $P_f$  alle strikt monoton sind. Dann ist die von  $\mathcal{A}$  induzierte Ordnung  $>_{\mathcal{A}}$  eine Reduktionsordnung. Solche Ordnungen auf  $T(\Sigma, V)$  heißen **Polynomordnungen**.

**Prop.** Angenommen, die Terminierung eines TUS  $R$  kann mit einer Polynomordnung gezeigt werden. Dann gibt es eine Konstante  $C > 0$ , sodass für alle Terme  $t$  gilt, dass jede Reduktionssequenz ausgehend von  $t$  eine Länge  $\leq 2^{2^{C|t|}}$  hat.

## Vereinfachungsordnungen

**Def.** Eine Umschreibungsordnung  $>$  auf  $T(\Sigma, V)$  heißt **Vereinfachungsordnung**, falls sie die **Subtermeigenschaft** erfüllt:

$$\forall t \in T(\Sigma, V) : \forall p \in \text{Pos}(t) \setminus \{\epsilon\} : t > t|_p$$

**Def.** Die **homöomorphe Einbettung**  $\succeq_{\text{emb}} \subseteq T(\Sigma, X) \times T(\Sigma, X)$  ist definiert durch die Schlussregeln

$$\frac{x \in X}{x \succeq_{\text{emb}} x} \quad \frac{s_1 \succeq_{\text{emb}} t_1 \quad \dots \quad s_n \succeq_{\text{emb}} t_n}{f(s_1, \dots, s_n) \succeq_{\text{emb}} f(t_1, \dots, t_n)} \quad \frac{s_j \succeq_{\text{emb}} t \quad (1 \leq j \leq n)}{f(s_1, \dots, s_n) \succeq_{\text{emb}} t}$$

*Bem.* Es gilt  $\succeq_{\text{emb}} = \xrightarrow{*}_R$  mit dem Termumschreibungssystem

$$R := \{f(x_1, \dots, x_n) \rightarrow x_i \mid n \in \mathbb{N}, f \in \Sigma^{(n)}, 1 \leq i \leq n\}$$

Da  $R$  terminiert ist  $\succeq_{\text{emb}}$  wohlfundiert. Für  $\Sigma, X$  endlich gilt sogar:

**Lem.** Eine **Wohlpartialordnung** ist eine Partialordnung  $\geq$  mit der Eigenschaft, dass es in jeder unendlichen Folge  $x_1, x_2, \dots$  Indizes  $i < j$  mit  $x_i \leq x_j$  gibt.

*Bem.* Wohlpartialordnungen sind wohlfundiert.

**Thm (Kruskal).** Sei  $\Sigma$  eine endliche Signatur und  $X$  eine endliche Menge von Variablen. Dann ist  $\succeq_{\text{emb}}$  eine Wohlordnung auf  $T(\Sigma, X)$ .

**Lem.** Sei  $>$  eine Vereinfachungsordnung auf  $T(\Sigma, V)$ . Dann gilt

$$s \succeq_{\text{emb}} t \implies s \geq t \quad \text{für alle } s, t \in T(\Sigma, V).$$

**Thm.** Sei  $\Sigma$  endlich. Jede Vereinfachungsordnung  $>$  auf  $T(\Sigma, V)$  ist wohlfundiert, also eine Reduktionsordnung.

**Prop.** Sei  $>$  eine Reduktionsord. auf  $T(\Sigma, V)$ , deren Einschränkung auf  $T(\Sigma, \emptyset)$  total ist. Dann erfüllt  $>$  die Subtermeig. für  $t \in T(\Sigma, \emptyset)$ .

**Def.** Eine **polynomielle Interpretation über  $\mathbb{R}$**  von  $\Sigma$  ist eine  $\Sigma$ -Algebra  $\mathcal{A}$  mit

- nichtleerer Trägermenge  $A \subseteq \mathbb{R}$  und

- $f^{\mathcal{A}}(a_1, \dots, a_n) = P_f(a_1, \dots, a_n)$  mit einem Polynom  $P_f \in \mathbb{R}[X_1, \dots, X_n]$  für alle  $n \in \mathbb{N}$ ,  $f \in \Sigma^{(n)}$

sodass folgende Eigenschaften erfüllt sind:

- Für alle  $n \in \mathbb{N}$ ,  $f \in \Sigma^{(n)}$  und  $a, b, a_1, \dots, a_n \in A$  mit  $a > b$  gilt  $P_f(a_1, \dots, a_{i-1}, a, a_{i+1}, \dots, a_n) > P_f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n)$ .
- Für alle  $n \in \mathbb{N}$ ,  $f \in \Sigma^{(n)}$  und  $a_1, \dots, a_n \in A$  gilt  $P_f(a_1, \dots, a_n) > \max\{a_1, \dots, a_n\}$ .

**Beob.** Sei  $\Sigma$  endlich. Dann ist die von  $A$  induzierte **polynomielle Vereinfachungsordnung**  $>_{\mathcal{A}}$  eine Reduktionsordnung.

*Bem.* Ist  $A$  in der Theorie der reellen Zahlen in Prädikatenlogik erster Stufe beschrieben, so sind die beiden Eigenschaften aus der Definition sowie  $>_{\mathcal{A}}$  entscheidbar.

**Def.** Die durch eine strikte Ordnung  $>$  auf  $\Sigma$  induzierte **lexikographische Pfadordnung**  $>_{\text{lpo}}$  ist def. durch  $s >_{\text{lpo}} t : \iff$

- $t \in \text{Var}(s)$  und  $s \neq t$  oder
- $s = f(s_1, \dots, s_m)$ ,  $t = g(t_1, \dots, t_n)$  und
  - $\exists i : s_i \geq_{\text{lpo}} t$  oder
  - $f > g$  und  $\forall j : s >_{\text{lpo}} t_j$  oder
  - $f = g$  und  $\forall j : s >_{\text{lpo}} t_j$  und
- (\*)  $\exists i : s_1 = t_1 \wedge \dots \wedge s_{i-1} = t_{i-1} \wedge s_i >_{\text{lpo}} t_i$

**Thm.** Sei  $\Sigma$  endlich. Die lexikographische Pfadordnung  $\geq_{\text{lpo}}$  ist eine Vereinfachungsordnung auf  $T(\Sigma, V)$ .

**Prop.**  $s \geq_{\text{lpo}} t$  ist in polynomieller Zeit (in  $s$  und  $t$ ) entscheidbar.

*Bemn.* • Ersetzt man (\*) in der Def. der lex. Pfadordnung durch

$$\{s_1, \dots, s_m\} >_{\text{mpo}}^{\text{mul}} \{t_1, \dots, t_n\},$$

wobei  $>_{\text{mpo}}^{\text{mul}}$  die von  $>_{\text{mpo}}$  induzierte Multimengenordnung ist, so erhält man die **Multimengenpfadordnung**  $>_{\text{mpo}}$ .

- Man kann auch „gemischte“ Pfadordnungen bilden, bei denen je nach Signatur  $f = g \in \Sigma$  die lexikographische oder die Multimengenordnung für die Subterme  $s_1, \dots, s_m, t_1, \dots, t_n$  verwendet wird.

**Def.** Sei  $\Sigma$  endlich,  $w : \Sigma \cup V \rightarrow \mathbb{R}_{>0}$  eine **Gewichtsfunktion** und  $>$  eine strikte Ordnung auf  $\Sigma$ . Die Gewichtsfunktion heißt **zulässig**, falls

- $\exists w_0 > 0 : \forall v \in V : w(v) = w_0 \wedge \forall c \in \Sigma^{(0)} : w(c) \geq w_0$
- $\forall f \in \Sigma^{(1)} : w(f) = 0 \implies f \geq g$

Die **Knuth-Bendix-Ordnung**  $>_{\text{kbo}}$  induziert durch  $>$  und  $w$  ist definiert durch:  $s >_{\text{kbo}} t : \iff$

- $\forall x \in V : |s|_x \geq |t|_x$  und  $w(s) > w(t)$  oder
- $\forall x \in V : |s|_x \geq |t|_x$  und  $w(s) = w(t)$  und
  - $\exists f \in \Sigma^{(1)} : \exists n \in \mathbb{N}_{>0} : s = f^n(t)$  und  $t \in X$  oder
  - $s = f(\dots), t = g(\dots)$  und  $f > g$  oder
  - $s = f(s_1, \dots, s_n), t = f(t_1, \dots, t_n)$  und  $\exists i : s_1 = t_1 \wedge \dots \wedge s_{i-1} = t_{i-1} \wedge s_i >_{\text{kbo}} t_i$

**Thm.**  $>_{\text{kbo}}$  ist eine Vereinfachungsordnung.

**Prop.**  $s >_{\text{kbo}} t$  ist in polynomieller Zeit (in  $s$  und  $t$ ) entscheidbar.