Zusammenfassung Term Rewriting aAT

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 $(A, \to)$, wobei $\to \in A \times A$ eine Relation auf A ist.

Def.

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

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

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

Def. Eine Reduktion $\to$ heißt

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

Lem. Für eine Reduktion $\to$ sind äquivalent:

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

Lem. Ist die Reduktion $\to$ 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 $\to$ konvergent, so gilt $x \xleftrightarrow{*} y \iff x{\downarrow} = y{\downarrow}$.

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

Terminierungsbeweise

Lem. $\to$ ist terminierend $\iff$ $\to$ ist eine Wohlordnung

Def. Eine Relation $\to$ 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 $a \xrightarrow{+} a$ 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 $(A, \to)$ ein Reduktionssystem und $(B, >)$ eine wohlgeordnete Menge. Gibt es eine streng monotone Abbildung $\varphi : A \to B$, so ist A terminierend.

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

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

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

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

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

Notation. $\mathcal{M}(A) := \{$ 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 Ordung 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 $>_{mul}$.

Konfluenzbeweise

Def. Eine Relation $\to$

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

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

Bem. starke $\implies$ schwache/normale $\implies$ lokale Konfluenz

Lem. Falls $\to_1 \leq \to_2 \leq \xrightarrow{*}_1$, so gilt $\xrightarrow{*}_1 = \xrightarrow{*}_2$.
Ist zusätzlich $\to_2$ (stark) konfluent, so auch $\to_1$.

Lem (**Newman**)**.** Eine terminierende Relation ist genau dann konfluent, falls sie lokal konfluent ist.

Def. Zwei Relationen $\to_1$ und $\to_2$ auf A

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

$$y_1 \leftarrow_1 x \to_2 y_2 \implies \exists z : y_1 \xrightarrow{=}_2 z \xleftarrow{*}_1 y_2.$$

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

$$y_1 \leftarrow_1 x \to_2 y_2 \implies \exists z : y_1 \to_2 z \leftarrow_1 y_2.$$

Lem. Angenommen, $\to_1$ und $\to_2$ sind konfluent und kommutieren. Dann ist auch $\to_1 \cup \to_2$ konfluent.

Universelle Algebra

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

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

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

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

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** $\mathrm{Pos}(s)$ eines Terms $s \in T(\Sigma, X)$ ist folgende Menge von Listen von natürlichen Zahlen

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

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

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

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

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

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

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

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

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

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

$$\mathrm{Dom}(\sigma) := \{v \in V \,|\, \sigma(v) \neq v\}$$

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

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

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

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

Def. Die **Reduktionsrelation** $\to_E$ zu einer Menge E von Σ-Identitäten ist

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

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

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

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

- **kompatibel mit Σ-Operationen**, falls

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

- **kompatibel mit Σ-Kontexten**, falls

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

- **Umschreibungsrelation**, falls sie kompatibel mit Σ-Operationen und abgeschlossen unter Ersetzungen ist.

Lem. Es sind äquivalent:

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

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

- $\equiv$ ist abgeschlossen unter Σ-Operationen

Thm. Sei E eine Menge von Σ-Identitäten.

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

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

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

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

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

Def. • Eine **Σ-Subalgebra** von A ist eine Teilmenge $B \subset A$, sodass $f^{\mathcal{A}}(b_1, \ldots, b_n) \in B$ für alle $f \in \Sigma^{(n)}$ und $b_1, \ldots, b_n \in B$.

- Die von $X \subseteq A$ **erzeugte Σ-Subalgebra** ist die kleinste Σ-Subalgebra, die X enthält.

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

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

Bem. Damit bilden Σ-Algebren eine Kategorie.

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

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

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

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

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

Lem. Die Kategorie der Σ-Algebren enthält kleine Limiten.

Def. Eine Σ-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 $F : \mathbf{Set} \to \Sigma\text{-}\mathbf{Alg}$.

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

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

Def. • Eine Σ-Identität $s \approx t$ **gilt in einer Σ-Algebra** $\mathcal{A}$, falls für alle Homomorphismen $\phi : T(\Sigma, V) \to \mathcal{A}$ gilt: $\phi(s) = \phi(t)$.

- $\mathcal{A}$ ist ein **Modell** einer Menge E von Σ-Algebren (notiert $\mathcal{A} \models E$), falls jede Identität aus E in $\mathcal{A}$ gilt.
- Die Subkategorie von Σ-**Alg** der Modelle von E heißt *durch E definierte* **Σ-Varietät** $\mathcal{V}(E)$.

Def. • 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.

- $\approx_E := \{(s, t) \,|\, E \models s \approx t\}$ 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. $\phi : T(\Sigma, V) \to T(\Sigma, V)$.

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 ≤ 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

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

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 Σ-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 σ mit $\sigma(s) \approx_E \sigma(t)$ gibt.

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

Thm. Ist E endlich und $\to_E$ 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 $\mathrm{Var}(l) \supseteq \mathrm{Var}(r)$.
- 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** $\mathrm{CC}(E)$ von $E \subseteq T(\Sigma, V) \times T(\Sigma, V)$ ist die kleinste Kongruenzrelation, die $\equiv$ enthält.

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

$$\frac{}{(t,t) \in \mathrm{CC}(E)} \qquad \frac{(t,s) \in \mathrm{CC}(E)}{(s,t) \in \mathrm{CC}(E)} \qquad \frac{(r,s) \in \mathrm{CC}(E) \quad (s,t) \in \mathrm{CC}(E)}{(r,t) \in \mathrm{CC}(E)}$$

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

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

Notation. Sei G im Folgenden eine Menge von Grundidentitäten.

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

Def. Die Menge der **Unterterme** ist

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

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

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

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

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

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

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

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 $i = 1, \dots, \mathrm{arity}(f)$ nummeriert sind.
- Wir repräsentieren Identifikationen von Knoten im Graph über Zeiger wie in der Union-Find-Datenstruktur. Wir definieren $u \sim v \;:\iff\; \textsc{find}(u) = \textsc{find}(v)$ für Knoten u und v.

function $\textsc{merge}(u, v)$
  if $u \not\sim v$ **then**
    $P := \textsc{pred}(u)$, $Q := \textsc{pred}(v)$
    $\textsc{union}(u, v)$
    for $(p, q) \in P \times Q$ **do**
      if $p \not\sim q \land \textsc{congruent}(p, q)$ **then**
        $\textsc{merge}(p, q)$
function $\textsc{congruent}(p = f(p_1, \dots, p_n),\ q = g(q_1, \dots, q_m))$
  if $f \neq g \in \Sigma$ **then return** false
  for $i = 1, \dots, n$ **do**
    if $p_i \not\sim q_i$ **then return** false
  return true

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

Syntaktische Unifikation

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

Lem. $\lesssim$ ist eine Quasiordnung

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

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

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 σ mit $\hat\sigma(s_i) = \hat\sigma(t_i)$ 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 ($\textsc{unify}(S)$)**.** 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 $x \in \mathrm{Var}(S) \setminus \mathrm{Var}(t)$

Wenn keine Tranformationsregel mehr angewandt werden kann, so

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

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

Thm. $\textsc{unify}(S)$ ist korrekt:

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

Bem. Folgende Regeln bewirken einen frühen Abbruch:

Clash	$\{f(\vec{s}) \stackrel{?}{=} g(\vec{t})\} \sqcup S$	$\rightsquigarrow$	$\bot$	falls $f \neq g$
Occurs-Check	$\{x \stackrel{?}{=} t\} \sqcup S$	$\rightsquigarrow$	$\bot$	falls $x \in \mathrm{Var}(t)$ 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 das Halteproblem für Turingmaschinen unentscheidbar ist.

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

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

- R ist *nicht* terminierend
- Es gibt eine Regel $(l \to r) \in R$ 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 $\to_R$) auf der Menge der Terme durch, beginnend bei der Wurzelmenge $\{r \mid (l \to r) \in R\}$. 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 Σ-Operationen* ist, d. h. aus $s > t$ folgt
$$f(s_1, \ldots, s_{i-1}, s, s_{i+1}, \ldots, s_n) > f(s_1, \ldots, s_{i-1}, t, s_{i+1}, \ldots, s_n)$$
- 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 $(l \to r) \in R$.

Die Interpretationsmethode

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

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

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

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

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

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

Lem/Def. Sei $\mathcal{A}$ eine polynomielle Interpretation $\mathcal{A}$, deren Polynome P_f alle strikt monoton sind. Dann ist die von $\mathcal{A}$ induziert 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:

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

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

$$\frac{x \in X}{x \trianglerighteq_{\mathrm{emb}} x} \qquad \frac{s_1 \trianglerighteq_{\mathrm{emb}} t_1 \quad \cdots \quad s_n \trianglerighteq_{\mathrm{emb}} t_n}{f(s_1, \ldots, s_n) \trianglerighteq_{\mathrm{emb}} f(t_1, \ldots, t_n)} \qquad \frac{s_j \trianglerighteq_{\mathrm{emb}} t \;\; (1 \leq j \leq n)}{f(s_1, \ldots, s_n) \trianglerighteq_{\mathrm{emb}} t}$$

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

$$R \coloneqq \{f(x_1, \ldots, x_n) \to x_i \mid n \in \mathbb{N}, f \in \Sigma^{(n)}, 1 \leq i \leq n\}$$

Da R terminiert ist $\trianglerighteq_{\mathrm{emb}}$ wohlfundiert. Für Σ, X endlich gilt sogar:

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

Bem. Wohlpartialordnungen sind wohlfundiert.

Thm (**Kruskal**). Sei Σ eine endliche Signatur und X eine endliche Variablenmenge. Dann ist $>_{\mathrm{emb}}$ eine Wohlpartialord. auf $T(\Sigma, X)$.

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

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

Thm. Sei Σ 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 Σ ist eine Σ-Algebra $\mathcal{A}$ mit

- nichtleerer Trägermenge $A \subseteq \mathbb{R}$ und
- $f^{\mathcal{A}}(a_1, \ldots, a_n) = P_f(a_1, \ldots, a_n)$ mit einem Polynom $P_f \in \mathbb{R}[X_1, \ldots, X_n]$ 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 $a, b, a_1, \ldots, a_n \in A$ mit $a > b$ gilt
$$P_f(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n) > P_f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n).$$
- Für alle $n \in \mathbb{N}$, $f \in \Sigma^{(n)}$ und $a_1, \ldots, a_n \in A$ gilt
$$P_f(a_1, \ldots, a_n) > \max\{a_1, \ldots, a_n\}.$$

Beob. Sei Σ 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 Σ induzierte **lexikographische Pfadordnung** $>_{\mathrm{lpo}}$ ist def. durch $s >_{\mathrm{lpo}} t \;:\Longleftrightarrow$

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

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

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

Bemn.
- Ersetzt man $(\star)$ in der Def. der lex. Pfadordnung durch
$$\{s_1, \ldots, s_m\} >_{\mathrm{mpo}}^{\mathrm{mul}} \{t_1, \ldots, t_n\},$$
wobei $>_{\mathrm{mpo}}^{\mathrm{mul}}$ die von $>_{\mathrm{mpo}}$ induzierte Multimengenordnung ist, so erhält man die **Multimengenpfadordnung** $>_{\mathrm{mpo}}$.
- Man kann auch „gemischte“ Pfadordnungen bilden, bei denen je nach Signatur $f = g \in \Sigma$ die lexikographische oder die Multimengenordnung für die Subterme $s_1, \ldots, s_m, t_1, \ldots, t_n$ verwendet wird.

Def. Sei Σ endlich, $w : \Sigma \cup V \to \mathbb{R}_{\geq 0}$ eine **Gewichtsfunktion** und $>$ eine strikte Ordnung auf Σ. Es gelte:

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

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

- $\forall\, x \in V \,:\, |s|_x \geq |t|_x$ 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*
  - $s = f(\cdots)$, $t = g(\cdots)$ und $f > g$ *oder*
  - $s = f(s_1, \ldots, s_n)$, $t = f(t_1, \ldots, t_n)$ und
    $\exists\, i \,:\, s_1 = t_1 \wedge \ldots \wedge s_{i-1} = t_{i-1} \wedge s_i >_{\mathrm{kbo}} t_i$

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

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

Konfluenz

Problem (**Konfluenz**). Gegeben ein TUS R. Frage: Ist R konfluent?

Satz. Das Konfluenz-Problem ist unentscheidbar.

Beweisskizze. Sei E eine Gleichungsmenge mit $\mathrm{Var}(l) = \mathrm{Var}(r)$ für alle $l \approx r \in E$ und unentscheidbarem Grundwortproblem über E. Für Terme $t, s \in T(\Sigma, \emptyset)$ betrachte das TUS

$$R_{st} \coloneqq E \cup E^{-1} \cup \{a \to s, a \to t\}.$$

Dann gilt: R_{st} ist konfluent $\iff$ $t \approx_E s$

Kritische Paare

Situation. Angenommen, der Term s wird für $i = 1, 2$ mittels $l_i \to r_i \in R$ zu t_i umgeschrieben, d. h. es gibt je eine Position p_i und eine Ersetzung σ_i mit

$$s|_{p_i} = \sigma_i l_i \text{ und } t_i = s[\sigma_i r_i]_{p_i}.$$

Um lokale Konfluenz nachzuweisen, müssen wir zeigen, dass $t_1 \downarrow t_2$. Wir können drei Fälle unterscheiden:

1. $s|_{p_1}$ und $s|_{p_2}$ sind zwei disjunkte Subterme von s, d. h. weder p_1 ist ein Präfix von p_2, noch umgekehrt
2. $s|_{p_2}$ ist ein Subterm von $s|_{p_1}$ (bzw. umgekehrt), d. h. $p_2 = p_1 p$ für ein möglicherweise leeres $p \in \mathbb{N}^*$
   (a) **Nichkritischer Überlapp**: $s|_{p_2}$ ist Subterm einer ersetzten Variable in l_1, d. h. $p = q_1 q_2$, wobei $l_i|_{q_1} \in V$.
   (b) **Kritischer Überlapp**: l_1 und l_2 überlappen, d. h. $p \in \mathrm{Pos}(l_1)$ und $l_1|_p \notin V$.

Lem.
- In den Fällen 1 und 2a gilt $t_1 \downarrow t_2$.
- Im Fall 2b gilt $t_1 \downarrow t_2$, falls $t_1|_{p_1} = \sigma_1 r_1 \downarrow t_2|_{p_1} = (s|_{p_1})[\sigma_2 r_2]_p$.

Def. Seien $l_1 \to r_1, l_2 \to r_2 \in E$ Regeln mit so umbenannten Variablen, dass $(\mathrm{Var}(l_1) \cup \mathrm{Var}(r_1)) \cap (\mathrm{Var}(l_2) \cup \mathrm{Var}(r_2)) = \emptyset$. Sei $p \in \mathrm{Pos}(l_1)$ mit $l_1|_p \notin V$ und θ eine allgemeinste Lösung von $l_1|_p =^? l_2$. Dann heißt $(\theta r_1, (\theta l_1)[\theta r_2]_p)$ ein **kritisches Paar**.

Achtung. Bei den beiden Regeln $l_1 \to r_1$ und $l_2 \to r_2$ kann es sich auch um Kopien derselben Regel handeln!

Beob. Im Fall 2b gibt es ein kritisches Paar (k_1, k_2) (konstruiert aus den beiden gegebenen Gleichungen zusammen mit p wie oben) und eine Ersetzung τ mit $t_1|_{p_1} = \tau k_1$ und $t_2|_{p_1} = \tau k_2$.

Satz. Ein TUS ist genau dann lokal konfluent, falls für alle kritischen Paare (k_1, k_2) gilt, dass $k_1 \downarrow k_2$.

Da für terminierende TUS Konfluenz und lokale Konfluenz übereinstimmen, folgt:

Kor. Die Konfluenz eines endlichen, terminierenden TUS ist entscheidbar.

Beweisskizze. Es gibt nur endlich viele kritische Paare (k_1, k_2) bis auf α-Äquivalenz. Prüfe für jedes solche Paar, ob $k_1{\downarrow} = k_2{\downarrow}$.

- Falls ja: Dann gilt $k_1 \downarrow k_2$.
- Falls nein: Dann ist das TUS nicht konfluent, denn es gilt: $(k_1{\downarrow}) \xleftarrow{*} k_1 \leftarrow l_1 \to k_2 \xrightarrow{*} (k_2{\downarrow})$ aber nicht $(k_1{\downarrow}) \downarrow (k_2{\downarrow})$.