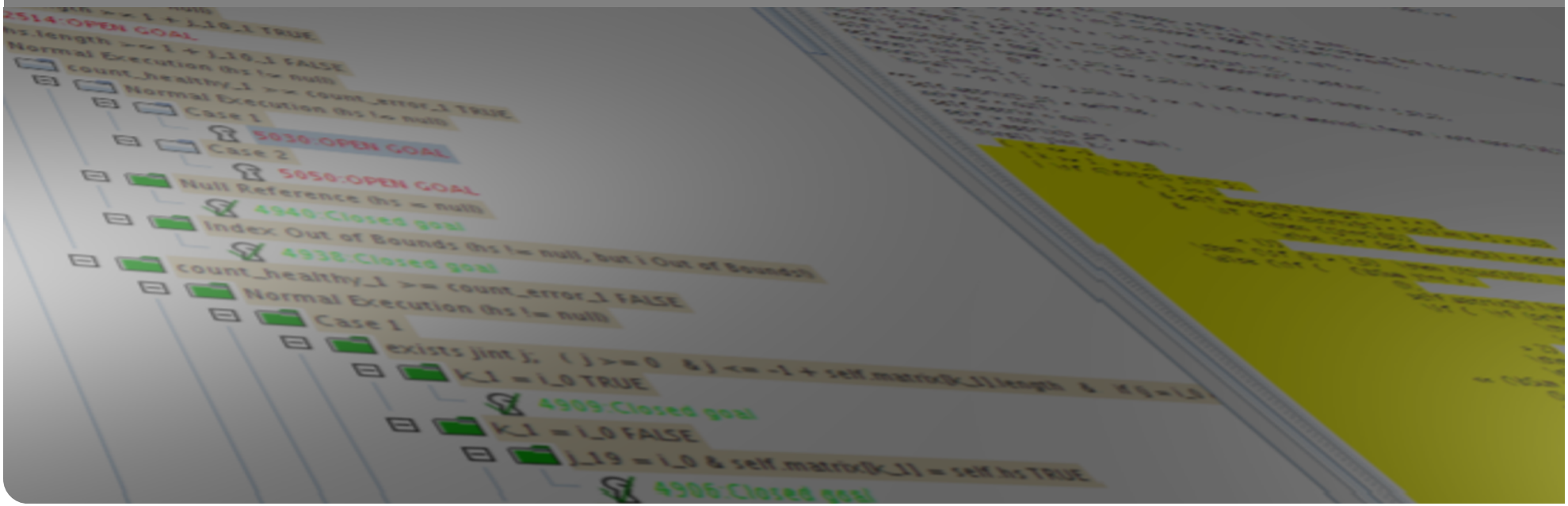
Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2018/2019

Reduktionssysteme

KIT – Institut für Theoretische Informatik



www.kit.edu

Gleichungslogik

Die *Gleichungslogik* ist der Spezialfall der Prädikatenlogik, bei dem nur Gleichungen, $s \doteq t$, betrachtet werden.
Das ist im striktesten Sinne zu verstehen: es gibt keine Ungleichungen, keine Disjunktion oder Konjunktion von Gleichungen.
Variablen können auftreten und sind implizit universell quantifiziert.
Für eine Gleichungsmenge E und Terme t, s gilt also

$$E \models s \doteq t$$

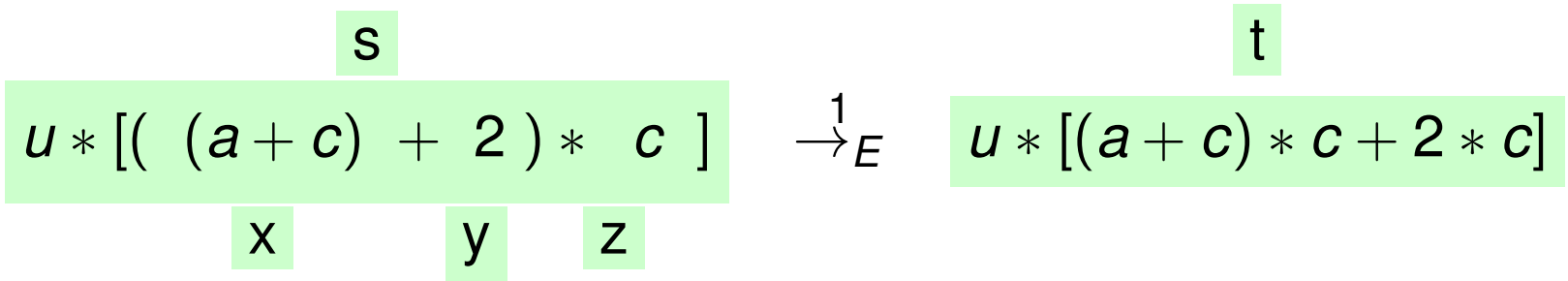
genau dann, wenn für jede Struktur $\mathcal{M}$, mit
$\mathcal{M} \models \forall \bar{x}(s' \doteq t')$ für jede Gleichung $s' \doteq t'$ in E
auch $\mathcal{M} \models \forall \bar{x}(s \doteq t)$ gilt.
Dabei steht $\bar{x}$ jeweils für alle in der nachfolgenden Gleichung vorkommenden Variablen.

Ersetzung von Gleichem durch Gleiches

Gegeben sei eine Menge E von Gleichungen in der Signatur Σ

$s \xrightarrow{1}_E t \quad \Leftrightarrow$ es gibt eine Gleichung $l \doteq r \in E$
und eine Substitution σ, so daß gilt:
$\sigma(l)$ ist Unterterm von s
t entsteht aus s, indem dort der Unterterm $\sigma(l)$
an genau einer Stelle ersetzt wird durch $\sigma(r)$

Beispiel: $E = \{(x + y) * z = x * z + y * z\}$



Iteration der Ersetzung

$s \overset{1}{\rightarrow}_E t$ *gdw* wie gesehen

$t \rightarrow_E r$ gdw r wird durch mehrfache Anwendung von $\overset{1}{\rightarrow}_E$ von links nach rechts, erhalten

$t \leftrightarrow_E r$ gdw r wird durch mehrfache Anwendung von $\overset{1}{\rightarrow}_E$ in beiden Richtungen, erhalten

Satz von Birkhoff

Für jedes Gleichungssystem E und zwei beliebige Terme s, t gilt

$$E \models s \doteq t \quad \Leftrightarrow \quad s \leftrightarrow_E t$$

Garrett Birkhoff
On the structure of abstract algebras
Proc.Cambrigde Phil.Soc., 1935
Vol. 31, pp 433–454

Das Skript enthält auch einen Beweis in den Übungsaufgaben zum Kapitel über Gleichungslogik.

Termersetzungssysteme

Nach dem Satz von Birkhoff können wir uns auf das Studium der Relation $\leftrightarrow_E$ konzentrieren.

Die automatische Berechnung von $\leftrightarrow_E$ ist äußerst aufwendig. Es ist unmöglich vorherzusehen, welche Gleichungsanwendungen am Ende zum Ziel führen werden. Die Vermeidung nutzloser Schleifen ist ein weiteres Problem.

Termersetzungssysteme

Idee:

Um $t \doteq s$ zu beweisen, berechnen wir Normalformen t_0, s_0 mit

$$t \to_E t_0 \text{ und } s \to_E s_0$$

Es gilt:

$$t_0 = s_0 \text{ impliziert } t \doteq s$$

Falls Normalformen *existieren* und *eindeutig* sind:

$$t_0 = s_0 \text{ gdw } t \doteq s$$

Funkioniert nicht für alle E. Für welche?

Die Idee eindeutiger Normalformen ist weit über die Gleichungslogik hinaus fruchtbar. Wir präsentieren sie deshalb zunächst in dem allgemeinen Kontext der *Reduktionssysteme* und kehren danach zum Studium von $\leftrightarrow_E$ zurück.

Reduktionssysteme

Definition

Ein **Reduktionssystem** $(D, \succ)$ besteht aus einer nichtleeren Menge D und einer beliebigen, binären Relation $\succ$ auf D.

Wir benutzen die folgenden Bezeichnungen:

- $\to$ die reflexive, transitive Hülle von $\succ$
- $\overset{+}{\to}$ die transitive Hülle von $\succ$
- $\leftrightarrow$ die reflexive, transitive, symmetrische Hülle von $\succ$

Das Standardbeispiel ist

$$s \succ t \Leftrightarrow s \overset{1}{\to}_E t$$

Weitere Beispiele für Reduktionssysteme

- Polynomreduktion
- β-Reduktion im λ-Kalkül
- Wortersetzung (Semi-Thue-Systeme)
- etc

Einschränkende Eigenschaften

von Reduktionssystemen

Definition

1. Ein Reduktionssystem $(D, \succ)$ heißt **konfluent**, wenn für jedes Tripel $s, s_1, s_2 \in D$ mit $s \to s_1$, $s \to s_2$ ein $t \in D$ existiert mit $s_1 \to t$ und $s_2 \to t$.
2. $(D, \succ)$ heißt **lokal konfluent**, wenn für alle $s, s_1, s_2 \in D$ mit $s \succ s_1$, $s \succ s_2$ ein $t \in D$ mit $s_1 \to t$ und $s_2 \to t$ existiert.
3. $(D, \succ)$ heißt **noethersch** (oder **wohlfundiert** oder **terminierend**), wenn es keine unendlichen Folge $s_0 \succ s_1 \ldots \succ s_i \succ \ldots$ gibt.
4. Ein konfluentes und noethersches Reduktionssystem heißt **kanonisch**.
5. Ein Element $s \in D$ heißt **irreduzibel** (oder eine **Normalform**) in $(D, \succ)$, wenn kein $t \in D$ existiert mit $s \succ t$.
6. Sei $s \in D$. Ein Element $s_0 \in D$ heißt eine **Normalform für s** in $(D, \succ)$, wenn s_0 irreduzibel ist und $s \to s_0$ gilt.

Kanonische Reduktionssysteme

Theorem

Sei $(D, \succ)$ ein kanonisches Reduktionssystem. Dann gilt:

1. *Zu jedem $s \in D$ gibt es eine eindeutige Normalform. Diese bezeichnen wir mit $irr(s)$.*
2. *Für $s, t \in D$ gilt*

$$s \leftrightarrow t \text{ gdw } irr(s) = irr(t)$$

3. *$(D, \succ)$ sei berechenbar im folgenden Sinne: Es gibt einen Algorithmus, der zu jedem $t \in D$ ein t' mit $t \succ t'$ liefert, wenn ein solches existiert, und andernfalls ausgibt „t ist irreduzibel“, Dann ist die Relation $\leftrightarrow$ entscheidbar.*

Beweis

Eindeutigkeit und Existenz der Normalform

Eindeutigkeit

Angenommen es gäbe für $s \in D$ zwei Normalformen s_1, s_2.
D.h. es gilt $s \to s_1$ und $s \to s_2$.
Wegen der Konfluenz von $(D, \succ)$ gibt es $t \in D$ mit
$s_1 \to t$ und $s_2 \to t$.
Das widerspricht der Irreduzibilität von s_1, s_2.

Existenz

für $s \in D$:
Setze $s_0 = s$ und wählen ein s_{i+1} mit $s_i \succ s_{i+1}$, solange s_i nicht irreduzibel ist.
Da $(D, \succ)$ noethersch ist, wird nach endlich vielen Schritten ein irreduzibles s_i erreicht.

Beweis

$s \leftrightarrow t$ gdw $irr(s) = irr(t)$

Die Implikation von rechts nach links ist trivial.
Gelte jetzt $s \leftrightarrow t$.
Nach Definition von $\leftrightarrow$ gibt es eine Folge $s = s_0, s_1, \ldots, s_n = t$, so dass für alle $0 \leq i < n$ entweder $s_i \succ s_{i+1}$ oder $s_{i+1} \succ s_i$ gilt.
Nachweis von $irr(s) = irr(t)$ durch Induktion über n.

Der Induktionsanfang $n = 0$, d.h. $s = t$ ist trivial.

Induktionsschritt:
Sei die Behauptung für Folgen der Länge $n - 1$ schon bewiesen. Also gilt $irr(s_1) = irr(t)$.
Im Fall $s_0 \succ s_1$ gilt offensichtlich $irr(s_0) = irr(s_1)$, und wir sind fertig.
Falls $s_1 \succ s_0$ gilt, folgt aus der Konfluenz, dass ebenfalls $irr(s_0) = irr(s_1)$ gelten muss

Beweis

Entscheidbarkeit von $\leftrightarrow$

Zu gegebenem s, t wird wie folgt entschieden, ob $s \leftrightarrow t$.
Beginnend mit $s_0 := s$, liefert der vorausgesetzte Algorithmus Elemente s_i mit $s_0 \succ s_1 \succ s_2 \succ \ldots$, bis hierbei ein irreduzibles s_m erreicht ist.
Da $(D, \succ)$ noethersch ist, tritt das auf jeden Fall ein und wird durch „s_m ist irreduzibel“ mitgeteilt, ferner gilt $s_m = \mathit{irr}(s)$.
Entsprechend erhält man $\mathit{irr}(t)$ aus t.
Nach (2) ist $s \leftrightarrow t$ genau dann, wenn $\mathit{irr}(s) = \mathit{irr}(t)$.

Noethersche Induktion

Theorem

Für ein noethersches Reduktionssystem $(D, \succ)$ gilt das folgende Beweisprinzip der Noetherschen Induktion:
Es sei $X \subseteq D$, so dass für alle $a \in D$ gilt

$$\{b \mid a \succ b\} \subseteq X \Rightarrow a \in X.$$

Dann ist $X = D$.

Noethersche Induktion

Proof.

Angenommen es gibt $a_0 \in D \backslash X$. Nach Annahme über X gilt $\{b \mid a_0 \succ b\} \not\subseteq X$.
Es gibt also ein a_1 mit

$$a_0 \succ a_1, a_1 \notin X$$

Nach Annahme über X gilt wieder $\{b \mid a_1 \succ b\} \not\subseteq X$ und es gibt ein a_2 mit

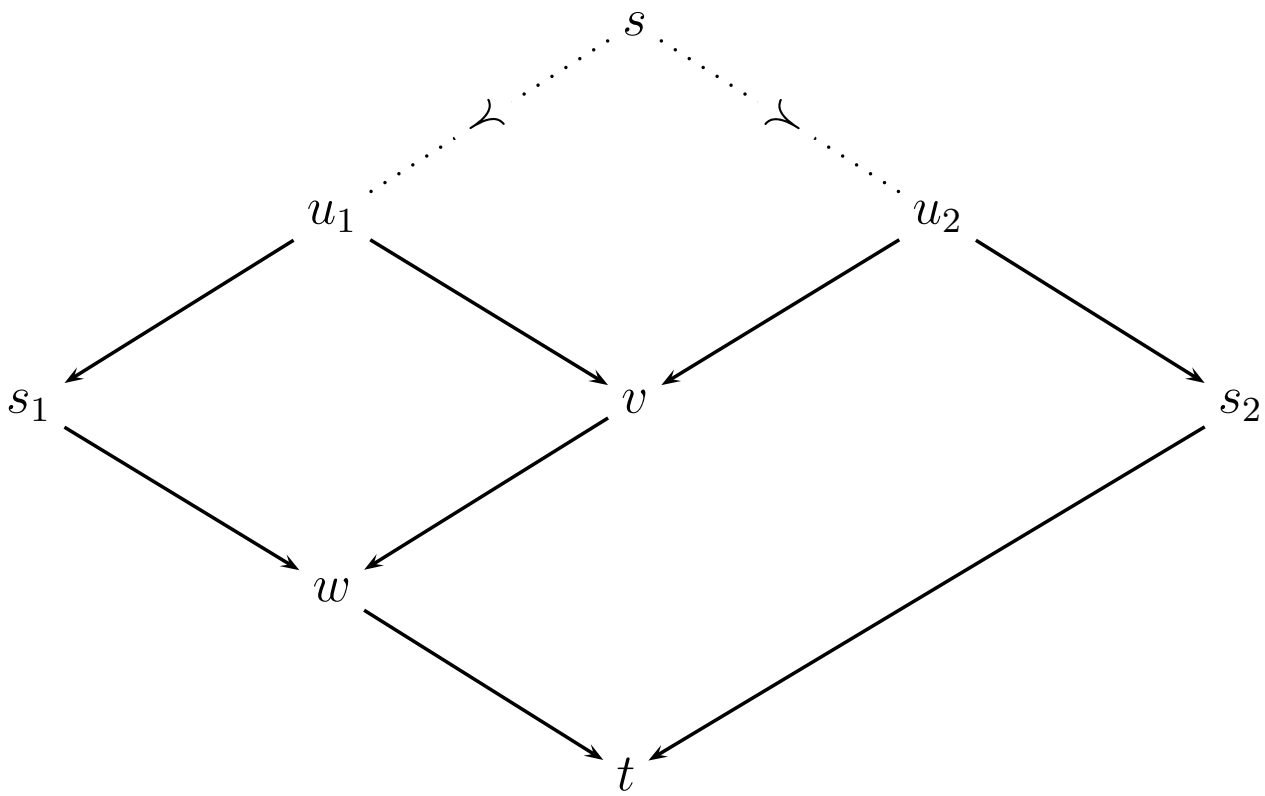
$$a_0 \succ a_1 \succ a_2, a_2 \notin X$$

Fährt man in dieser Weise fort, so erhält man eine unendliche Folge $(a_i)_{i \in \mathbb{N}}$ mit $a_i \succ a_{i+1}$ für alle i. Das ist ein Widerspruch, denn $(D, \succ)$ war als noethersch vorausgesetzt. □

Von lokaler Konfluenz zu Konfluenz

Theorem

Wenn $(D, \succ)$ ein noethersches und lokal konfluentes Reduktionssystem ist, dann ist $(D, \succ)$ konfluent, d. h. kanonisch.



Beweis

Wir verwenden noethersche Induktion bezüglich der Menge

$$\begin{aligned} \mathit{Confl} \quad := \quad & \{s \mid \text{für alle } s_1, s_2 \\ & \text{mit } s \to s_1, s \to s_2 \\ & \text{existiert ein } t \text{ mit } s_1 \to t, s_2 \to t\} \end{aligned}$$

Dazu müssen wir also zeigen, dass für alle s gilt:

$$\{s' \mid s \succ s'\} \subseteq \mathrm{Confl} \Rightarrow s \in \mathrm{Confl}$$

Es seien s, s_1, s_2 gegeben mit $s \to s_1$, $s \to s_2$.

Im Falle $s = s_1$ oder $s = s_2$ ist man fertig. (Etwa: $s_1 = s \to s_2$).

Sei also $s \neq s_1$, $s \neq s_2$.

Beweis (Forts.)

Nachweis von

$$\{s' \mid s \succ s'\} \subseteq \text{Confl} \Rightarrow s \in \text{Confl}$$

im Falle $s \to s_1$, $s \to s_2$ mit $s \neq s_1$, $s \neq s_2$.

Es existieren u_1, u_2 mit $s \succ u_1 \to s_1$ und $s \succ u_2 \to s_2$.

Wegen der lokalen Konfluenz von $(D, \succ)$ existiert ein v mit $u_1 \to v, u_2 \to v$.

Nach Voraussetzung („Induktionsannahme“) liegt u_1 in Confl. Also gibt es ein w mit $s_1 \to w$ und $v \to w$.

Entsprechend schließen wir aus der Induktionsannahme $u_2 \in$ Confl, dass ein Term t existiert mit $s_2 \to t$ und $w \to t$.

Wir haben $s_1 \to t$ und $s_2 \to t$ und somit $s \in$ Confl, was zu beweisen war.