

# Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2017/2018

Reduktionssysteme

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



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  $\Sigma$

$s \xrightarrow{1}_E t \Leftrightarrow$  es gibt eine Gleichung  $l \doteq r \in E$   
und eine Substitution  $\sigma$ , 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:  $E = \{(x + y) * z = x * z + y * z\}$

$$\begin{array}{ccc} & \mathbf{s} & \\ & \boxed{u * [(a + c) + 2] * c} & \\ & \mathbf{x} \quad \mathbf{y} \quad \mathbf{z} & \\ & & \mathbf{t} \\ & \boxed{u * [(a + c) * c + 2 * c]} & \end{array} \xrightarrow{1}_E$$

- $s \xrightarrow{1}_E t$  gdw wie gesehen
- $t \xrightarrow{1}_E r$  gdw  $r$  wird durch mehrfache Anwendung von  $\xrightarrow{1}_E$  von links nach rechts, erhalten
- $t \leftrightarrow_E r$  gdw  $r$  wird durch mehrfache Anwendung von  $\xrightarrow{1}_E$  in beiden Richtungen, erhalten

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. Cambridge Phil. Soc., 1935

Vol. 31, pp 433–454

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

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

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

Es gilt:

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

Falls Normalformen *existieren* und *eindeutig* sind:

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

Funktioniert 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.

## Definition

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

Wir benutzen die folgenden Bezeichnungen:

- $\rightarrow$  die reflexive, transitive Hülle von  $\succ$
- $\rightarrow^+$  die transitive Hülle von  $\succ$
- $\leftrightarrow$  die reflexive, transitive, symmetrische Hülle von  $\succ$

Das Standardbeispiel ist

$$s \succ t \Leftrightarrow s \xrightarrow{1}_E t$$



# Weitere Beispiele für Reduktionssysteme

- ▶ Polynomreduktion
- ▶  $\beta$ -Reduktion im  $\lambda$ -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  $s \rightarrow s_1, s \rightarrow s_2$  ein  $t \in D$  existiert mit  $s_1 \rightarrow t$  und  $s_2 \rightarrow t$ .
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  $s_1 \rightarrow t$  und  $s_2 \rightarrow t$  existiert.
3.  $(D, \succ)$  heißt **noethersch** (oder **wohlfundiert** oder **terminierend**), wenn es keine unendlichen Folge  $s_0 \succ s_1 \dots \succ s_i \succ \dots$  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  $s \rightarrow s_0$  gilt.

## Theorem

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

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

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

- 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  $s \rightarrow s_1$  und  $s \rightarrow s_2$ .

Wegen der Konfluenz von  $(D, \succ)$  gibt es  $t \in D$  mit

$s_1 \rightarrow t$  und  $s_2 \rightarrow t$ .

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  $s_j$  erreicht.

# Beweis

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

Die Implikation von rechts nach links ist trivial.

Gelte jetzt  $s \leftrightarrow t$ .

Nach Definition von  $\leftrightarrow$  gibt es eine Folge  $s = s_0, s_1, \dots, s_n = t$ , 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  $\text{irr}(s) = \text{irr}(t)$  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  $\text{irr}(s_1) = \text{irr}(t)$ .

Im Fall  $s_0 \succ s_1$  gilt offensichtlich  $\text{irr}(s_0) = \text{irr}(s_1)$ , und wir sind fertig.

Falls  $s_1 \succ s_0$  gilt, folgt aus der Konfluenz, dass ebenfalls  $\text{irr}(s_0) = \text{irr}(s_1)$  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  $s_0 \succ s_1 \succ s_2 \succ \dots$ , 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  $s_m = irr(s)$ .

Entsprechend erhält man  $irr(t)$  aus  $t$ .

Nach (2) ist  $s \leftrightarrow t$  genau dann, wenn  $irr(s) = irr(t)$ .

## 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  $X = D$ .*

## Proof.

Angenommen es gibt  $a_0 \in D \setminus X$ . 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

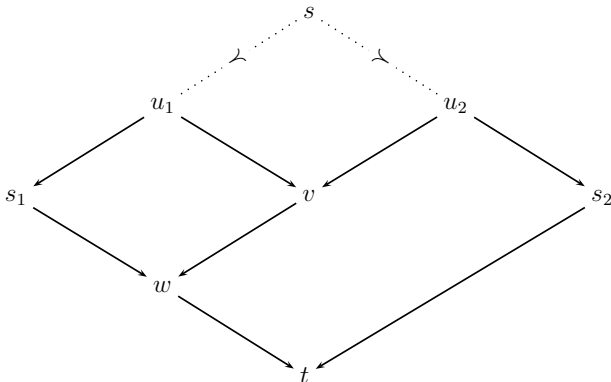
$$a_0 \succ a_1 \succ a_2, a_2 \notin X$$

Führt 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.  $\square$



## Theorem

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



Wir verwenden noethersche Induktion bezüglich der Menge

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

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

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

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

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

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

Nachweis von

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

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

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

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

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

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

Wir haben  $s_1 \rightarrow t$  und  $s_2 \rightarrow t$  und somit  $s \in \text{Confl}$ , was zu beweisen war.