

**Gibt es einen semantischen Beweis ?**

23. Oktober 2023

# Inhaltsverzeichnis

|          |                                                                  |           |
|----------|------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Überblick und Motivation</b>                                  | <b>4</b>  |
| <b>2</b> | <b>Grundlagen: Induktiv definierte Mengen</b>                    | <b>5</b>  |
| 2.1      | Definition (Regeln, Regelmenge)                                  | 5         |
| 2.2      | Definition verschiedener Regelmengen                             | 5         |
| 2.3      | Definition (Unter einer Regelmenge abgeschlossene Menge)         | 5         |
| 2.4      | Existenz der kleinsten über $R$ abgeschlossenen Menge            | 6         |
| 2.5      | Definition (Induktiv definierte Menge)                           | 6         |
| 2.6      | Definition (Iteration von Mengen)                                | 6         |
| 2.7      | Satz                                                             | 6         |
| 2.8      | Korollar 1                                                       | 6         |
| 2.9      | Korollar 2                                                       | 7         |
| 2.10     | Definition (Beweis, Beweisfolge, Beweisbaum)                     | 7         |
| 2.11     | Lemma 0                                                          | 7         |
| 2.12     | Lemma 1 (für e-Regelmengen)                                      | 8         |
| 2.13     | Satz (für e-Regelmengen)                                         | 8         |
| 2.14     | Satz (für u-Regelmengen)                                         | 9         |
| 2.15     | Satz (Entscheidbarkeit einer Beweisfolge)                        | 9         |
| 2.16     | Satz (Rekursive Aufzählbarkeit einer induktiv definierten Menge) | 11        |
| 2.16.1   | 1. Beweis:                                                       | 11        |
| 2.16.2   | 2. Beweis (Alternative):                                         | 12        |
| <b>3</b> | <b>Die Syntax der Arithmetik</b>                                 | <b>13</b> |
| 3.1      | Die Syntax der arithmetischen Terme                              | 13        |
| 3.1.1    | Definition arithmetische Terme                                   | 13        |
| 3.1.2    | Bemerkung: Metasprachliche Abkürzungen                           | 13        |
| 3.2      | Die Syntax der arithmetischen Formeln                            | 13        |
| 3.2.1    | Definition arithmetische Formeln                                 | 14        |
| <b>4</b> | <b>Semantik der Sprache der Arithmetik</b>                       | <b>15</b> |
| 4.1      | Struktur für $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$         | 15        |
| 4.2      | Definition Belegung                                              | 15        |
| 4.3      | Die Semantik der arithmetischen Terme                            | 15        |
| 4.3.1    | Definition arithmetische Formel mit Wahrheitswert                | 15        |
| 4.3.2    | Satz (Eindeutigkeit der Semantik der arithmetischen Terme)       | 15        |
| 4.4      | Die Semantik der arithmetischen Formeln                          | 16        |
| 4.4.1    | Satz (Eindeutigkeit der Semantik der arithmetischen Formeln)     | 16        |
| 4.4.2    | Definition (Gültigkeit)                                          | 16        |
| 4.4.3    | Definition (Gültige arithmetische Formeln)                       | 16        |
| 4.4.4    | Beispiel einer Beweisfolge                                       | 17        |
| 4.4.4.1  | Behauptung                                                       | 17        |
| 4.4.4.2  | 1. Möglichkeit der Darstellung des Beweises                      | 17        |
| 4.4.4.3  | 2. Möglichkeit der Darstellung des Beweises durch einen Baum     | 17        |
| 4.5      | Ziel                                                             | 17        |
| 4.5.1    | Strategie 1                                                      | 18        |
| 4.5.2    | Strategie 2                                                      | 18        |
| 4.5.3    | Strategie 3 (semantischer Beweis)                                | 18        |
| 4.6      | Anmerkungen zu $I_R$ Beweisen bzgl. einer u-Regelmenge           | 18        |
| 4.7      | Gödelscher Unvollständigkeitssatz                                | 18        |

|          |                                                     |           |
|----------|-----------------------------------------------------|-----------|
| <b>5</b> | <b>Axiomensystem von Peano</b>                      | <b>19</b> |
| 5.1      | Definitionen . . . . .                              | 19        |
| 5.2      | Axiome PA von Peano . . . . .                       | 19        |
| 5.3      | Die durch Peano induktiv definierte Menge . . . . . | 20        |

# 1 Überblick und Motivation

1) In der Mathematik spielt neben den Wahrheitswerten W bzw. F noch der klassische Beweis eine grosse Rolle.

Die Gültigkeit (Wahrheit) eines mathematischen Satzes, wie z.B. die Goldbachsche Vermutung wird "normalerweise" durch einen klassischen Beweis festgestellt:

Mit Hilfe eines klassischen Beweises wird ein Satz Schritt für Schritt rein mechanisch bewiesen (hergeleitet).

Könnte man statt dessen dazu auch die Semantik benutzen? Dies soll hier erörtert werden:

In dem von Prof. Ekkart Kindler verfassten Skript gibt es zu jedem Element der durch eine Regelmenge induzierten induktiv definierten Menge eine Herleitung (die eine Baumstruktur hat).

Statt einer Herleitung kann man auch den in diesem Skript ähnlichen Begriff Beweisfolge (bzw. Beweis) definieren, die eine flache Struktur hat und als Folge dargestellt wird.

Wenn man also eine induktiv definierte Menge verwendet, hat man automatisch auch den Begriff Beweis zur Verfügung.

Konkret:

Wenn man die Semantik durch eine induktiv definierte Menge definiert, hat man auch den Begriff des (semantischen) Beweises eingeführt.

Es wäre demnach rein theoretisch möglich, die Goldbachsche Vermutung nicht über einen klassischen Beweis, sondern nur über einen semantischen Beweis zu beweisen, d.h. über die Wahrheitswerte von arithmetischen Formeln

2) Da beim semantischen Beweis manche Regeln unendlich viele Voraussetzungen haben, kann nicht mehr von jeder arithmetischen Formel der Wahrheitswert abgeleitet werden:

Die Paare (arithmetische Formel, Wahrheitswert) sind nicht rekursiv aufzählbar.

Von einem klassischen Beweis erwartet man dagegen, dass er sogar entscheidbar ist.

Das ist der Nachteil eines semantischen Beweises gegenüber einem klassischen Beweis.

3) Induktiv definierte Mengen

Über induktiv definierte Mengen werden arithmetische Terme, arithmetische Formeln, die Wahrheitswerte von arithmetischen Formeln, usw.) definiert.

Deshalb eine kurze Erklärung dazu: (Ausführliches dazu siehe unten)

Eine Regelmenge  $R(X)$  filtert (bastelt) aus einer Basismenge  $X$  (z.B. einer Menge von Worten) eine neue Menge (Teilmenge von  $X$ )  $I_R$  von Objekten (wie z.B. Terme, Formeln, Paare von Formeln und Wahrheitswerten, usw.) die sich alle durch dazugehörige Beweisfolgen beweisen lassen.

Analog dem klassischen Beweis kann man diese Beweisfolgen ebenso Beweise nennen

## 2 Grundlagen: Induktiv definierte Mengen

In dieser Ausarbeitung wurde das Skript von Prof. Ekkart Kindler benutzt.

### 2.1 Definition (Regeln, Regelmenge)

Sei  $X$  eine Menge.

Für eine **endliche** Teilmenge  $Y \subset X$  und ein Element  $x \in X$  nennt man das Paar  $(Y, x)$  eine Regelinstanz über  $X$ .

Die Elemente der Menge  $Y$  nennt man die Voraussetzungen der Regel, das Element  $x$  nennt man die Folgerung der Regelinstanz.

Eine Regelinstanz  $(\emptyset, x)$  nennt man Axiominstanz und  $x$  ein Axiom.

Eine Regel  $(Y, x)$  schreibt man auch in der folgenden Form:

$$\frac{Y}{x}$$

Im Folgenden redet man oft nur von Regeln und Axiomen, wenn man Regelinstanzen und Axiominstanzen meint.

Der Grund für die Unterscheidung zwischen dem Begriff der Regel und der Regelinstanz ist, daß man bei der Formulierung einer Regel meist unendlich viele Regelinstanzen bezeichnet.

Beispielsweise steht die folgende Regel über  $\mathbb{N} \times \mathbb{N}$ :

$$\frac{(a,b)}{a+b}$$

für unendlich viele Regelinstanzen: Für jedes  $a, b \in \mathbb{N}$  ist  $((a, b), a + b)$  eine Instanz dieser Regel.

Um zwischen der syntaktischen Repräsentation einer Regel und ihren oft unendlich vielen Instanzen unterscheiden zu können, hat man in der obigen Definition über Regelinstanzen geredet.

Im Folgenden wird nur noch von Regeln geredet, wenn man eigentlich Regelinstanzen meint.

Eine Teilmenge  $R(X) \subset \mathfrak{P}(X) \times X$  nennt man eine Regelmenge über  $X$ .

### 2.2 Definition verschiedener Regelmengen

1) Eine Regelmenge  $R$  heißt e-Regelmenge :gdw

alle Regeln aus  $R$  haben nur endlich viele Voraussetzungen

2) Eine Regelmenge  $R$  heißt u-Regelmenge :gdw

es gibt Regeln aus  $R$ , die unendlich viele Voraussetzungen haben

### 2.3 Definition (Unter einer Regelmenge abgeschlossene Menge)

Sei  $R(X)$  eine Menge von Regeln über  $X$ .

Eine Menge  $Q \subset X$  heißt abgeschlossen unter  $R$  (kurz  $R$ -abgeschlossen) gdw

für jede Regel(instanz)  $(Y, x) \in \mathfrak{R}(X)$  mit  $Y \subset Q$  auch  $x \in Q$  gilt.

## 2.4 Existenz der kleinsten über R abgeschlossenen Menge

1)

Sei  $(A_i)_{i \in I}$  eine Familie von R-abgeschlossenen Mengen, d. h. für jedes  $i \in I$  ist  $Q_i$  abgeschlossen unter R. Dann ist auch die Menge  $A = \bigcap_{i \in I} A_i$  unter R abgeschlossen.

2)

$\{\bigcap_{i \in I} A_i \mid A_i \text{ ist R-abgeschlossen}\}$  ist die bzgl. Mengeninklusion  $\subset$  kleinste R-abgeschlossene Menge, d.h:

Für alle R-abgeschlossenen Mengen M gilt:  $\{\bigcap_{i \in I} A_i \mid A_i \text{ ist R-abgeschlossen}\} \subset M$

Beweis:

1)

Sei  $Y \subset A$  und  $(Y, x) \in R$ . Dann gilt  $Y \subset A_k$  für alle  $k \in I$ .

Da  $A_k$  abgeschlossen, ist  $x \in A_k$ . Also  $x \in A$ .

2)

Alle R-abgeschlossene Mengen ist die Familie der Mengen  $(A_i)_{i \in I}$

Zeige für alle  $k \in I$ :  $\{\bigcap_{i \in I} A_i \mid A_i \text{ ist R-abgeschlossen}\} \subset A_k$  Dies gilt trivialerweise. Da nach 1) A abgeschlossen ist, ist A auch die kleinste R-abgeschlossene Menge.

## 2.5 Definition (Induktiv definierte Menge)

Sei R eine Regelmenge über X. Man nennt die (bzgl.  $\subset$ ) kleinste unter R abgeschlossene Menge die durch R induktiv definierte Menge und bezeichnet sie mit  $I_R$ :

$$I_R = \{\bigcap_{i \in I} A_i \mid A_i \text{ ist R-abgeschlossen}\}.$$

## 2.6 Definition (Iteration von Mengen)

$$\widehat{R}(Q) := \{x \in X \mid \exists Y \subset Q (Y, x) \in R\}$$

$$Q_0 := \emptyset$$

$$Q_1 := \{x \in X \mid (\emptyset, x) \in R\} = \widehat{R}(Q_0)$$

$$Q_2 := \{x \in X \mid (Y, x) \in R \wedge Y \subset Q_1\} = \widehat{R}(Q_1)$$

$$Q_3 := \{x \in X \mid (Y, x) \in R \wedge Y \subset Q_2\} = \widehat{R}(Q_2)$$

...

## 2.7 Satz

Sei R eine e-Regelmenge über X und  $Q_0, Q_1, Q_2, Q_3, \dots$  die Folge der o.g. Mengen.

Dann gilt:

$$I_R = \bigcup_{i=1}^{\infty} Q_i$$

## 2.8 Korollar 1

Für alle  $i \geq 0$  gilt:  $Q_i \subset Q_{i+1}$

Bemerkung: Gilt für e- und u-Regelmengen.

Beweis: (mit vollständiger Induktion)

1) Induktionsanfang:

$$Q_0 = \emptyset \subset Q_1$$

2) Induktionsvoraussetzung:  $Q_{i-1} \subset Q_i$

Sei  $x \in Q_i$ . Dann gibt es ein  $Y \subset Q_{i-1}$  mit  $(Y, x) \in R$ .

Nach Ind.Vor. gilt:  $Y \subset Q_i$ . Da  $(Y, x) \in R$ , folgt  $x \in Q_{i+1}$ .

## 2.9 Korollar 2

Sei  $R$  eine u-Regelmenge. Dann gilt:

$$\bigcup_{i=1}^{\infty} Q_i \subset I_R$$

Beweis: (mit vollständiger Induktion über  $i$ )

zeige dazu:

$Q_i \subset I_R$  für alle  $i \geq 0$

1) Induktionsvoraussetzung:  $i=0$ :

$$Q_0 = \emptyset \subset I_R$$

2) Zeige:  $Q_{i+1} \subset I_R$

sei  $x \in Q_{i+1}$  dann existiert ein  $Y \subset Q_i$  mit  $(Y, x) \in R$ .

Da nach Ind.Vor. gilt:  $Q_i \subset I_R$  folgt:

$Y \subset Q_i \subset I_R$ , also  $Y \subset I_R$ .

Da  $I_R$  abgeschlossen und  $(Y, x) \in R$ , folgt  $x \in I_R$ .

## 2.10 Definition (Beweis, Beweisfolge, Beweisbaum)

1) Für e-Regelmengen wird definiert: Für ein  $x \in X$  nennt man die endliche Folge (Beweisfolge)  $(a_1, a_2, \dots, a_n)$  aus  $X$  mit  $a_n = x$  einen  $I_R$ -Beweis für  $x$  bzgl. einer Regelmenge  $R$  (in der alle Regeln nur endlich viele Voraussetzungen haben), wobei jedes Folgenglied  $a_k \in X$  mit  $1 \leq k \leq n$ :  
entweder ein Axiom ist (also durch eine Axiomeninstanz hervorgeht) oder  
 $a_k$  entsteht aus früheren Gliedern der Folge durch Anwendung einer Regel der Regelmenge  $R(X)$ .

2) Für beliebige Regelmengen (e-Regelmengen u-Regelmengen) wird definiert:

Für ein  $x \in X$  nennt man einen Baum (Beweisbaum) mit endlicher Höhe mit Wurzel  $x$

einen  $I_R$ -Beweis für  $x$  bzgl.  $R \iff$

Jeder Knoten des Baums ist Element aus  $X$  und entsteht aus den Söhnen durch Anwendung einer Regel der Regelmenge  $R(X)$  oder

ist ein Blatt, falls der Knoten durch eine Axiomeninstanz hervorgeht.

Beispiel eines Beweisbaum siehe: 4.4.4.3 auf Seite 17

## 2.11 Lemma 0

Für alle  $n \geq 1$  gilt:

I) Für jede Beweisfolge  $(x_0, x_1, \dots, x_n)$  sind die Folgenglieder  $x_i$  der Beweisfolge Element von  $Q_{n+1}$

II) Alle Knoten eines beliebigen Beweisbaums der Höhe  $h$  liegen in  $Q_{h-1}$

Beweis: (vollständige Induktion über  $n \geq 1$ )

I) 1) Induktionsanfang:  $n=1$ :

Sei  $(x_0)$  eine Beweisfolge für  $x_0$ , Dann gilt:  $x_0 \in Q_1$

2) Induktionsvoraussetzung gelte für  $n$ .

Sei  $(x_0, x_1, \dots, x_{n+1})$  eine Beweisfolge für  $x_{n+1}$ .

Dann ist  $(x_0, x_1, \dots, x_n)$  eine Beweisfolge für  $x_n$ .

Nach Induktionsvoraussetzung gilt dann für alle  $i \leq k$ :  $x_i \in Q_{n+1}$

$x_{n+1}$  entsteht durch die Anwendung einer Regel auf eine Teilmenge der in  $(x_0, x_1, \dots, x_n)$  enthaltenen Elemente  $\subset Q_{n+1}$ .

Also gilt:  $x_{n+1} \in Q_{n+2}$

II) Vollständige Induktion (über Höhe  $h \geq 2$  des Beweisbaums)

1) Induktionsanfang:  $h=2$ :

Dann muss  $x$  als Voraussetzung die leere Menge haben, also  $x \in Q_1$ .

2) Induktionsvoraussetzung gelte für  $h$ .

Sei  $B$  ein Beweisbaum für  $x$  der Höhe  $h+1$ , also mit Wurzel  $x$ .

$x$  besitzt die Unterbäume der Höhe  $h$  mit Wurzeln  $x_0, x_1, \dots, x_n$ .

Nach Induktionsvoraussetzung liegen alle Knoten (da sie die Höhe  $h$  haben) in  $Q_{h-1} \subset Q_h$ .

Speziell sind auch die Knoten  $x_0, x_1, \dots, x_n$  aus  $Q_{h-1} \subset Q_h$ .

Da  $x$  durch die Anwendung einer Regel auf  $\{x_0, x_1, \dots, x_n\} \subset Q_{h-1}$  entsteht, muss  $x \in Q_h$  sein.

Damit sind alle Knoten (Elemente) des Beweisbaums für  $x$  aus  $Q_h$ .

## 2.12 Lemma 1 (für e-Regelmengen)

Für alle  $n \geq 1$  gilt:

$z \in Q_n \Leftrightarrow z \in \{x \in X \mid \text{es existiert eine Beweisfolge für } x \text{ bzgl. } R\}$

Beweis:

$\Rightarrow$ :

I) Vollständige Induktion über  $n \geq 1$

Induktionsanfang:  $n=1$ :

Sei  $x \in Q_1$ . Dann ist  $(x)$  eine Beweisfolge.

2) Induktionsvoraussetzung gelte für  $n$ .

Sei  $x \in Q_{n+1}$ . Dann existiert eine Folge  $(v_0, v_1, \dots, v_k, x)$  mit  $(\{v_0, v_1, \dots, v_k\}, x) \in R$

mit  $\{v_0, v_1, \dots, v_k\} \subset Q_n$ .

Nach Induktionsvoraussetzung existieren aber für  $v_0, v_1, \dots, v_k$  Beweisfolgen  $\langle b_0 \rangle, \langle b_1 \rangle, \dots, \langle b_k \rangle$ .

Die Folge  $\langle b_0 \rangle, \langle b_1 \rangle, \dots, \langle b_k \rangle, v_0, v_1, \dots, v_k, x$  ist dann eine Beweisfolge für  $x$  bzgl.  $R$ .

$\Leftarrow$ :

Sei nun  $b$  eine Beweisfolge für  $x$ . Nach Lemma 0 existiert ein  $n$  so dass für alle Folgenglieder  $x_i$  von  $b$  gilt:  $x_i \in Q_n$ , also auch  $x \in Q_n$

## 2.13 Satz (für e-Regelmengen)

$\{x \in X \mid \text{es existiert eine Beweisfolge für } x \text{ bzgl. einer e-Regelmenge } R\} = I_R$

Beweis:

$\Rightarrow$ :

Sei  $x \in I_R$ . Dann existiert ein  $k \geq 1$  mit  $x \in D_k$ . Mit Lemma 1 folgt dann die Behauptung.

$\Leftarrow$ :

Sei  $x \in \{x \in X \mid \text{es existiert eine Beweisfolge für } x \text{ bzgl. } e-R\}$

Nach Lemma 0 gilt dann für alle Folgenglieder der Beweisfolge  $b$  mit Länge  $m$  und demnach auch für  $x$ :  $x \in Q_m \subset I_R$



## 2.14 Satz (für u-Regelmengen)

$\{x \in X \mid \text{es existiert ein Beweisbaum für } x \text{ bzgl. einer u-Regelmenge } R\}$   
 $= \bigcup_{i=1}^{\infty} Q_i \subset I_R$

Beweis:

$\Rightarrow$ :

Sei  $x \in \{x \in X \mid \text{es existiert ein Beweisbaum für } x \text{ bzgl. u-R}\}$

Nach Lemma 0 gilt dann für alle Knoten des Beweisbaums der Höhe  $h$  und demnach auch für  $x$ :

$x \in Q_{h-1} \subset I_R$

$\Leftarrow$ :

1) Unterbehauptung:

Für alle  $i \geq 1$  gilt:

$Q_i \subset \{x \in X \mid \text{es existiert ein Beweisbaum für } x \text{ bzgl. u-R}\}$

Unterbeweis: (vollständige Induktion)

a) Induktionsanfang  $i=1$ :

Sei  $x \in Q_1$ . Dann existiert der Beweisbaum  $(\emptyset, x)$  für  $x$ .

b) Induktionsvoraussetzung:

Sei  $x \in Q_{i+1}$ . Dann existieren  $x_0, x_1, \dots, x_n$  mit  $(\{x_0, x_1, \dots, x_n\}, x) \in R$  und  $\{x_0, x_1, \dots, x_n\} \subset Q_i$

Nach Induktionsvoraussetzung gibt es Beweisbäume für  $x_0, x_1, \dots, x_n$ .

Diese Beweisbäume bilden mit der Wurzel  $x$  einen neuen Beweisbaum für  $x$ .

2) Sei nun  $x \in \bigcup_{i=1}^{\infty} Q_i$ . Also existiert ein  $k$  mit  $x \in Q_k$ .

Mit der Unterbehauptung folgt die Behauptung.

3) mit Korollar 2:  $\bigcup_{i=1}^{\infty} Q_i \subset I_R$

## 2.15 Satz (Entscheidbarkeit einer Beweisfolge)

Sei  $R$  eine e-Regelmenge über  $X$ , die entscheidbar ist.

Behauptung:

Die Menge aller Beweisfolgen für  $x$  bzgl.  $R$  ist entscheidbar.

Beweis:

0) Notationen:

$|s|$  := Länge einer endlichen Folge  $s$

$s[\text{last}]$  := Das letzte Folgenglied der endlichen Folge  $s$   $s_i^j$  := Die Teilfolge  $(s_i, s_{i+1}, \dots, s_j)$  der Folge  $(s_1, s_2, \dots, s_i, \dots, s_j)$

$M[i]$  := Das  $i$ -te Element einer durchnummerierten (Nummerierung beginnt mit 1) endlichen Menge.

1) Unterbehauptung 1:

$\mathfrak{P}_{fin}(M)$  := Die Menge aller Teilmengen einer endlichen Menge  $M$  ist entscheidbar.

Unterbeweis 1:

Vorbedingung:

$T$  endlich und  $M$  endlich

Zusicherung:

$T \in \mathfrak{P}_{fin}(M)$ , d.h.  $T$  ist Teilmenge von  $M$  ? return 1 sonst 0

istTeilmenge(Menge  $T$ , Menge  $M$ ):

```

for(i=0, ..., Anzahl Elemente von T) do {
    if(T[i] kein Element von M)
        return 0
}
return 1

```

## 2) Unterbehauptung 2:

Die Menge aller endlichen Folgen, bei denen das letzte Folgenglied durch eine Regel aus früheren Folgengliedern hervorgeht (oder durch eine Axiomeninstanz) ist entscheidbar.

Unterbeweis 2:

Zusicherung:

$s[\text{last}]$  geht aus früheren Folgengliedern hervor oder ist Axiom: return 1 sonst 0

`istFolgerung(Folge s):`

```
// Nach Unterbehauptung 1 ist die Menge aller Teilmengen von {s[1], ..., s[last-1]}
// rekursiv aufzählbar. Also gibt es eine Funktion f, die diese aufzählt.
for(i=0, ..., Anzahl Teilmengen der Menge {s[1], ..., s[last-1] } ) do {
    if( (f[i],s[last]) ist Regel oder s[last] ein Axiom)      // T[i]: das i-te Element von T
        return 1
}
return 0
```

## 3) Unterbehauptung 3:

Behauptung: Die Menge aller Beweisfolgen ist entscheidbar.

Unterbeweis 3:

Zusicherung:

b ist Beweisfolge ? return 1 sonst 0

`istBeweisfolge(Folge b):`

```
for(i=0, ..., |b|) do {
    if( nicht istFolgerung ( $b_1^i$ ))
        return 0
}
return 1
```

## 2.16 Satz (Rekursive Aufzählbarkeit einer induktiv definierten Menge)

Sei  $R$  eine e-Regelmenge über  $X$ , die entscheidbar ist.

Behauptung:  $I_R$  ist rekursiv aufzählbar.

Bemerkungen:

B1) // bedeutet bei allen Programmen den Beginn einer Kommentarzeile

B2)  $Q_i$  seien die Mengen aus obigem Satz:  $I_R = \bigcup_{i=1}^{\infty} Q_i$

B3) P-RV(r) sei das Programm, das von einer Regel  $r$  die Voraussetzungen berechnet.

(Von der Regel  $(\{x_1, x_2, \dots, x_n\}, x)$  wird also  $\{x_1, x_2, \dots, x_n\}$  geliefert).

B4) P-RF(r) sei das Programm, das von einer Regel  $r$  die Folgerung berechnet.

(Von der Regel  $(\{x_1, x_2, \dots, x_n\}, x)$  wird also  $x$  geliefert).

B5) Per Definition der Entscheidbarkeit gilt:

$R$  besteht aus endlichen Folgen (also muss  $R$  eine e-Regelmenge sein) und  $X$  besteht aus endlichen Worten.

### 2.16.1 1. Beweis:

1) Unterbehauptung 0:

$\mathfrak{P}_{fin}(Q_i) :=$  Die Menge aller endlichen Teilmengen von  $Q_i$  ist entscheidbar.

Vorbedingung:

Sei  $Q_i$  rekursiv aufzählbar und  $T$  endlich.

Zusicherung:

$T \subset Q_i$  ? return 1

istTeilmenge(Menge T)

```

for(i=0, ..., Anzahl Elemente von T) do {
    // Da  $Q_i$  nach Voraussetzung rekursiv aufzählbar ist,
    // ist  $Q_i$  durch eine Funktion  $q_i$  rekursiv aufzählbar.
    for (j=0,1,2,..) do {
        if( $T[i] == q_i(j)$ )
            break; // d.h. gehe zur äußeren for-Schleife
    }
}
return 1;

```

2) Unterbehauptung 1:

$Q_i$  ist rekursiv aufzählbar für alle  $i \geq 1$ , d.h es gibt ein Programm, das 1 zurückgibt, wenn  $x \in Q_i$

Unterbeweis 1: (vollständige Induktion)

a) Induktionsvoraussetzung:  $Q_1$  ist rekursiv aufzählbar.

Zeige:  $Q_1$  ist semi-entscheidbar.

Zusicherung:

$x \in Q_i$  ? return 1

ist-x-in-Q1(x)

```
//Da R entscheidbar ist, ist R auch durch eine Funktion r rekursiv aufzählbar.
for (i=0,1,2,..) do {
    V = P-RV(r(i))
    F = P-RF(r(i))
    if (V==∅ and F ==x) // x ∈ Q1
        return(1)
}
```

b) Induktionsvoraussetzung:  $Q_i$  ist rekursiv aufzählbar.

Zeige:  $Q_{i+1}$  ist rekursiv aufzählbar, zeige dazu  $Q_{i+1}$  ist semi-entscheidbar.

Zeige dazu:

Wenn  $x \in Q_{i+1}$ , dann gibt das Programm P-Qi+1 den Wert 1 zurück.

Zusicherung:

Wenn  $x \in Q_{i+1}$  ? return 1

ist-x-in-Qi+1(x)

```
//Da R entscheidbar ist, ist R auch durch eine Funktion r rekursiv aufzählbar.
for (i=0,1,2,..) do {
    V = P-RV(r(i))
    F = P-RF(r(i))
    if (istTeilmenge(V)==1 and F==x) // x ∈ Qi+1
        return 1
}
```

3) Unterbehauptung 2:

Laut Wikipedia gilt:

Die Vereinigung einer rekursiv aufzählbaren Menge von rekursiv aufzählbaren Mengen ist rekursiv aufzählbar.

Damit ist  $I_R = \bigcup_{i=1}^{\infty} Q_i$  rekursiv aufzählbar.

### 2.16.2 2. Beweis (Alternative):

Zusicherung:

Ist x aus IR ? return 1 sonst 0

ist-x-in-IR(x):

```
// Nach Satz (Entscheidbarkeit einer Beweisfolge), ist die Menge aller Beweisfolgen
// rekursiv aufzählbar. Also gibt es eine Funktion f, die diese Menge X rekursiv aufzählt.
for(i=0, ... , do {
    b=f(i)
    if(b[last]==x)
        return 1
}
```

# 3 Die Syntax der Arithmetik

## 3.1 Die Syntax der arithmetischen Terme

Mit  $L := \{\bar{0}, \bar{1}, \oplus, \otimes\}$  wird eine Sprache der Prädikatenlogik 1. Stufe festgelegt.

Grundmenge  $G_T := L \cup \{x, 0, 1, 2, \dots, 9, (, )\}$

$X_T := G_T^* :=$  Menge aller Worte aus  $G_T$

Bemerkung:  $\mathbb{V} := \{xi \mid i \in \mathbb{N}\} \subset X_T$  nennt man Variablenmenge.

Im Skript wird  $x_i$  statt  $xi$  geschrieben.

Regelmenge  $R_T$  mit:

$R_T :=$

$\{(\emptyset, \bar{0}) \mid n \in \mathbb{N}\} \cup$

$\{(\emptyset, \bar{1}) \mid n \in \mathbb{N}\} \cup$

$\{(\emptyset, x_i) \mid i \in \mathbb{N}\} \cup$

$\{(\{t_1, t_2\}, (t_1 \oplus t_2)) \mid t_1, t_2 \in X_T\} \cup$

$\{(\{t_1, t_2\}, (t_1 \otimes t_2)) \mid t_1, t_2 \in X_T\}$

Um Klammergebirge zu vermeiden, werden manchmal (wenn es im Kontext klar ist) die äußeren Klammern weggelassen, also z.B:  $t_1 \oplus t_2$  statt  $(t_1 \oplus t_2)$ .

Regelmenge in Kurzschreibweise:

$\frac{\emptyset}{0} \quad \frac{\emptyset}{1} \quad \frac{\emptyset}{x_i} \quad \frac{t_1, t_2}{(t_1 \oplus t_2)} \quad \frac{t_1, t_2}{(t_1 \otimes t_2)}$

Bemerkung: Die Regeln können noch durch weitere Junktoren (wie z.B.  $\rightarrow$ ) ergänzt werden.

### 3.1.1 Definition arithmetische Terme

Menge aller durch die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  bestimmten arithmetischen Terme  $:= I_{R_T}$

### 3.1.2 Bemerkung: Metasprachliche Abkürzungen

spezielle Terme

$\bar{2} := (\bar{1} \oplus \bar{1})$

$\bar{3} := (\bar{2} \oplus \bar{1}) = (\bar{1} \oplus (\bar{1} \oplus \bar{1}))$

usw.

allgemein definiert man für alle  $n > 1$ :

$\bar{n} := (\overline{n-1} \oplus \bar{1})$

## 3.2 Die Syntax der arithmetischen Formeln

Grundmenge  $G_F := G_T \cup \{\neg, \wedge, \vee, \exists, \forall, \equiv\}$

$X_F := G_F^* :=$  Menge aller Worte aus  $G_F$

Regelmenge  $R_F$  mit:

$R_F :=$

$\{(\emptyset, (t_1 \equiv t_2)) \mid t_1, t_2 \in R_T\} \cup$

$\{(\{\alpha, \beta\}, (\alpha \wedge \beta)) \mid \alpha, \beta \in X_F\} \cup$

$\{(\{\alpha, \beta\}, (\alpha \vee \beta)) \mid \alpha, \beta \in X_F\} \cup$

$\{(\{\alpha\}, (\neg \alpha)) \mid \alpha \in X_F\} \cup$

$\{(\{\alpha\}, (\exists x \alpha)) \mid \alpha \in X_F \text{ und } x \in \mathbb{V}\} \cup$

$\{(\{\alpha\}, (\forall x \alpha)) \mid \alpha \in X_F \text{ und } x \in \mathbb{V}\}$

Um Klammergebirge zu vermeiden, werden manchmal (wenn es im Kontext klar ist) die äußeren Klammern weggelassen, also z.B.:  $\alpha \vee \beta$  statt  $(\alpha \vee \beta)$ .

Regelmenge in Kurzschreibweise:

$$\frac{}{(t_1 \equiv t_2)} \quad \frac{\alpha, \beta}{(\alpha \wedge \beta)} \quad \frac{\alpha, \beta}{(\alpha \vee \beta)} \quad \frac{\alpha}{(\neg \alpha)} \quad \frac{\alpha}{(\exists x \alpha)} \quad \frac{\alpha}{(\forall x \alpha)}$$

Bemerkung: Die Regeln können noch durch weitere Junktoren (wie z.B.  $\rightarrow$ ) ergänzt werden.

### 3.2.1 Definition arithmetische Formeln

Menge aller durch die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  bestimmten arithmetischen Formeln  $:= I_{R_F}$

# 4 Semantik der Sprache der Arithmetik

## 4.1 Struktur für $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$

Als Struktur für die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  wählt man:

$$\mathfrak{N} = (\mathbb{N}, 0, 1, +, \cdot)$$

mit den natürlichen Zahlen  $\mathbb{N}$  als Trägermenge und den bekannten Funktionen  $+$ ,  $\cdot$  und den Konstanten 0 und 1.

## 4.2 Definition Belegung

1) Eine Abbildung  $h$  über der Variablenmenge  $\mathbb{V}$  in die Trägermenge nennt man eine Belegung.

Hier konkret:  $h: \mathbb{V} \rightarrow \mathbb{N}$

2) Die Menge aller Abbildungen  $h: \mathbb{V} \rightarrow \mathbb{N}$  wird mit  $\mathbb{N}^{\mathbb{V}}$  bezeichnet.

3) Sei  $x$  eine Variable und  $\kappa$  ein Element der Trägermenge. Dann wird definiert:

$$h_x^\kappa(z) = \begin{cases} h(z), & z \neq x \\ \kappa, & z = x \end{cases}$$

## 4.3 Die Semantik der arithmetischen Terme

$$X_{ST} := I_{R_T} \times \mathbb{N}^{\mathbb{V}} \times \mathbb{N}$$

Regelmenge  $R_{ST}$ :

$$R_{ST} :=$$

$$\{(\emptyset, (\bar{0}, h, 0) \mid v \in \mathbb{V}\} \cup$$

$$\{(\emptyset, (\bar{1}, h, 1) \mid v \in \mathbb{V}\} \cup$$

$$\{(\emptyset, (v, h, h(v)) \mid v \in \mathbb{V}\} \cup$$

$$\{(\{(t_1, h, w_1), (t_2, h, w_2)\}, (t_1 \oplus t_2, h, t_1 + t_2)) \mid t_1, t_2 \in X_{ST}\} \cup$$

$$\{(\{(t_1, h, w_1), (t_2, h, w_2)\}, (t_1 \otimes t_2, h, t_1 \cdot t_2)) \mid t_1, t_2 \in X_{ST}\}$$

e-Regelmenge in Kurzschreibweise:

$$\frac{\emptyset}{(\bar{0}, h, 0)} \quad \frac{\emptyset}{(\bar{1}, h, 1)} \quad \frac{\emptyset}{(v, h, h(v))} \quad \frac{(t_1, h, w_1), (t_2, h, w_2)}{(t_1 + t_2, h, t_1 + t_2)} \quad \frac{(t_1, h, w_1), (t_2, h, w_2)}{(t_1 \cdot t_2, h, t_1 \cdot t_2)}$$

### 4.3.1 Definition arithmetische Formel mit Wahrheitswert

Menge aller durch die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  bestimmten Paare (arithmetischen Term, Wert)  $:= I_{R_{ST}}$

### 4.3.2 Satz (Eindeutigkeit der Semantik der arithmetischen Terme)

Zu jedem  $(t, h) \in I_{R_T} \times \mathbb{N}^{\mathbb{V}}$  existiert genau ein  $n \in \mathbb{N}$  mit  $(t, h, n) \in I_{R_{ST}}$

Das bedeutet, dass jeder Term mit einer bestimmten Belegung genau eine natürliche Zahl als Wert besitzt.

Damit existiert eine Abbildung:

$$w_{\mathfrak{N}}: I_{R_T} \times \mathbb{N}^{\mathbb{V}} \rightarrow \mathbb{N}$$

## 4.4 Die Semantik der arithmetischen Formeln

$$X_{SF} := I_{R_F} \times \mathbb{N}^{\mathbb{V}} \times \{W, F\}$$

u-Regelmenge  $R_{SF}$ :

$$R_{SF} :=$$

$$\begin{aligned} & \{(\emptyset, ((t_1 \equiv t_2), h, eq(w_{\mathbb{N}}(t_1, h), w_{\mathbb{N}}(t_2, h))) \mid t_1, t_2 \in I_{R_T}\} \cup \\ & \{((\alpha, h, w_1), (\beta, h, w_2)), ((\alpha \wedge \beta), and(w_1, w_2))) \mid \alpha, \beta \in I_{R_F}, h \in \mathbb{N}^{\mathbb{V}}, w_1, w_2 \in \{W, F\}\} \cup \\ & \{((\alpha, h, w_1), (\beta, h, w_2)), ((\alpha \vee \beta), or(w_1, w_2))) \mid \alpha, \beta \in I_{R_F}, h \in \mathbb{N}^{\mathbb{V}}, w_1, w_2 \in \{W, F\}\} \cup \\ & \{((\alpha, h, w), (\neg\alpha, h, non(w))) \mid \alpha \in I_{R_T}, h \in \mathbb{N}^{\mathbb{V}}, w \in \{W, F\}\} \cup \\ & \{((\alpha, h_x^{\kappa}, w_{\kappa}) \mid \kappa \in \mathbb{N} \wedge w_{\kappa} \in \mathbb{N}), (\exists x \alpha, h, max\{\pi_3(M)\})) \mid \alpha \in I_{R_F}, h \in \mathbb{N}^{\mathbb{V}}\} \cup \\ & \{((\alpha, h_x^{\kappa}, w_{\kappa}) \mid \kappa \in \mathbb{N} \wedge w_{\kappa} \in \mathbb{N}), (\forall x \alpha, h, min\{\pi_3(M)\})) \mid \alpha \in I_{R_F}, h \in \mathbb{N}^{\mathbb{V}}\} \end{aligned}$$

wobei:

$$M := \{(\alpha, h_x^{\kappa}, w_{\kappa}) \mid \kappa \in \mathbb{N} \wedge w_{\kappa} \in \mathbb{N}\}$$

$$\mathfrak{W} := \{W, F\}$$

$min \mathfrak{W} := F$  und  $max \mathfrak{W} = W$  und

$$or(w_1, w_2) = F \quad :gdw \quad w_1 = F \text{ und } w_2 = F$$

$$and(w_1, w_2) = W \quad :gdw \quad w_1 = W \text{ und } w_2 = W$$

$$non(w) = W \quad :gdw \quad \text{nicht } w = F$$

$\pi_3(M)$  die Projektion der Menge M in die 3. Komponente ist.

Regelmenge in Kurzschreibweise:

$$\begin{aligned} (RSF1) \quad & \frac{\emptyset}{(v, h, h(v))} \quad (RSF2) \quad \frac{(\alpha, h, w_1), (\beta, h, w_2)}{(\alpha \wedge \beta, h, and(\alpha, \beta))} \quad (RSF3) \quad \frac{(\alpha, h, w_1), (\beta, h, w_2)}{(\alpha \vee \beta, h, or(\alpha, \beta))} \quad (RSF4) \quad \frac{(\alpha, h, w_1)}{(\neg\alpha, h, non(\alpha))} \\ (RSF5) \quad & \frac{(\alpha, h_x^{\kappa}, w_{\kappa})}{(\exists x \alpha, h, max\{w_{\kappa} \mid \kappa \in \mathbb{N}\})} \quad (RSF6) \quad \frac{(\alpha, h_x^{\kappa}, w_{\kappa})}{(\forall x \alpha, h, min\{w_{\kappa} \mid \kappa \in \mathbb{N}\})} \end{aligned}$$

Menge aller durch die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  und der Regelmenge  $R_{SF}(X_{SF})$  bestimmten Paare (arithmetische Formel, Wahrheitswert)  $:= I_{R_{SF}}$

### 4.4.1 Satz (Eindeutigkeit der Semantik der arithmetischen Formeln)

Zu jedem  $(\alpha, h) \in I_{R_F} \times \mathbb{N}^{\mathbb{V}}$  existiert genau ein  $v \in \{W, F\}$  mit  $(t, h, v) \in I_{R_{SF}}$

Das bedeutet, dass jede arithmetische Formel mit einer bestimmten Belegung genau einen Wahrheitswert besitzt.

Damit existiert eine Abbildung:

$$W_{\mathfrak{N}}: I_{R_F} \times \mathbb{N}^{\mathbb{V}} \rightarrow \{W, F\}$$

### 4.4.2 Definition (Gültigkeit)

Die Formel  $\alpha$  ist in der Struktur  $\mathfrak{N}$  gültig, kurz:  $\models_{\mathfrak{N}} \alpha$  gdw

$$W_{\mathfrak{N}}(\alpha, h) = W \text{ für alle } h \in \mathbb{N}^{\mathbb{V}}$$

### 4.4.3 Definition (Gültige arithmetische Formeln)

Mit  $WA := Th(\mathfrak{N}) :=$  Theorie der natürlichen Zahlen mit Addition und Multiplikation  $:= \{\alpha \in I_{R_F} \mid \models_{\mathfrak{N}} \alpha\}$  wird die Menge aller in  $\mathfrak{N}$  gültigen arithmetischen Formeln bezeichnet.



#### 4.4.4 Beispiel einer Beweisfolge

##### 4.4.4.1 Behauptung

Für alle  $h \in \mathbb{N}^{\mathbb{V}}$  gilt:

$$W_{\mathfrak{N}}(\forall x \, x \otimes x \equiv x \oplus x \wedge \exists x \, x \otimes x \equiv x \oplus x, h) = F$$

Begründung:

Es gilt für beliebige  $h \in \mathbb{N}^{\mathbb{V}}$ :

##### 4.4.4.2 1. Möglichkeit der Darstellung des Beweises

(Beweisfolge untereinander angeordnet, mit Nummerierung und Angabe der verwendeten Regeln)

- (1)  $(x \otimes x \equiv x \oplus x, h_x^0, F)$  (RSF1)
- (2)  $(x \otimes x \equiv x \oplus x, h_x^1, F)$  (RSF1)
- (3)  $(x \otimes x \equiv x \oplus x, h_x^2, W)$  (RSF1)
- (4)  $(x \otimes x \equiv x \oplus x, h_x^3, F) \dots$  (RSF1)
- (5)  $(\exists x \, x \otimes x \equiv x \oplus x, h, W)$  (RSF5) auf (1) bis (4) angewendet
- (6)  $(\forall x \, x \otimes x \equiv x \oplus x, h, F)$  (RSF6) auf (1) bis (4) angewendet
- (7)  $(\forall x \, x \otimes x \equiv x \oplus x \wedge \exists x \, x \otimes x \equiv x \oplus x, h, F)$  (RSF2) auf (5) und (6) angewendet

also:

$$W_{\mathfrak{N}}(\forall x \, x \otimes x \equiv x \oplus x \wedge \exists x \, x \otimes x \equiv x \oplus x) = F$$

##### 4.4.4.3 2. Möglichkeit der Darstellung des Beweises durch einen Baum

Bemerkung:

In dem Baumbeweis unten geht die Liste:

$$\begin{array}{ccc} \emptyset & & \emptyset \dots \\ (x \otimes x \equiv x \oplus x, h_x^0, F) & (x \otimes x \equiv x \oplus x, h_x^1, F) & \dots \end{array}$$

weiter mit:

$$\begin{array}{cccc} \emptyset & \emptyset & \emptyset & \emptyset \dots \\ (x \otimes x \equiv x \oplus x, h_x^0, F) & (x \otimes x \equiv x \oplus x, h_x^1, F) & (x \otimes x \equiv x \oplus x, h_x^2, W) & (x \otimes x \equiv x \oplus x, h_x^3, F) \dots \end{array}$$

Beweisbaum:

$$\begin{array}{c} \begin{array}{cccc} \emptyset & \emptyset \dots & \emptyset & \emptyset \dots \\ \hline (x \otimes x \equiv x \oplus x, h_x^0, F) & (x \otimes x \equiv x \oplus x, h_x^1, F) \dots & (x \otimes x \equiv x \oplus x, h_x^0, F) & (x \otimes x \equiv x \oplus x, h_x^1, F) \dots \\ \hline (\exists x \, x \otimes x \equiv x \oplus x, h, W) \quad \underline{(RSF5)} & & (\forall x \, x \otimes x \equiv x \oplus x, h, F) \quad \underline{(RSF6)} & \\ \hline (\forall x \, x \otimes x \equiv x \oplus x \wedge \exists x \, x \otimes x \equiv x \oplus x, h, F) \quad \underline{(RSF2)} \end{array} \end{array}$$

## 4.5 Ziel

Mathematiker waren schon immer an der Axiomatisierung (Kalkülisierung) von Theorien (wie z.B. WA) interessiert.

Die Korrektheit eines Beweises muss auf mechanische Weise verifiziert werden können.

D.h. die Menge aller zulässigen Beweise müssen entscheidbar (im Sinne der theoretischen Informatik) sein. Damit sind unendlich große Beweise keine Beweise in diesem Sinne, da Entscheidbarkeit von endlichen Worten ausgeht.

Um die Menge WA (vielleicht sogar nur eine Teilmenge davon) erfassen zu können, gibt es 3 Strategien:

### 4.5.1 Strategie 1

Das maximale Ziel ist, ein Beweissystem  $B$  zu finden, das  $WA$  liefert, d.h. eine Regelmenge  $R(I_{R_F})$  über den arithmetischen Formeln  $I_{R_F}$  zu finden mit:

$$R(I_{R_F}) = WA$$

Leider ist dies nach dem Gödelschen Unvollständigkeitssatz nicht möglich (siehe unten).

### 4.5.2 Strategie 2

Nach dem Vollständigkeitssatz gilt für jede Formelmenge  $\Sigma$  der Sprache  $L$ :

Wenn  $\Sigma \vdash_L \alpha$  dann  $\Sigma \models \alpha$

Daraus folgt:

Wenn  $\Sigma \vdash_L \alpha$  und  $\Sigma$  ist eine wahre arithmetische Formelmenge (d.h.  $\mathfrak{N}$  ist ein Modell von  $\Sigma$ ), dann ist  $\alpha$  eine wahre arithmetische Formel.

Also sucht man eine möglichst "große, mächtige" wahre, arithemische Formelmenge, wie z.B. die Peano-Axiome  $PA$  (siehe unten).

Wenn man dann zeigen will, dass eine arithemische Formel  $\alpha$  wahr ist, genügt zu zeigen:  $PA \vdash_L \alpha$ .

### 4.5.3 Strategie 3 (semantischer Beweis)

Will man zeigen, dass  $\alpha$  eine wahre arithmetische Formel ist,

genügt es einen  $I_{R_{SF}}$ -Beweis für  $(\alpha, W)$  zu finden.

Statt eines  $I_{R_{SF}}$ -Beweises wird hier der Begriff semantischer Beweis verwendet. Vielleicht kann man auch die Begriffe Semantikkalkül bzw. Pseudosemantikkalkül benutzen.

## 4.6 Anmerkungen zu $I_R$ Beweisen bzgl. einer u-Regelmenge

Da ein  $I_{R_S}$ -Beweis bzgl. einer u-Regelmenge gilt, also auch aus nicht endlichen Worten besteht, ist er per Definition nicht rekursiv aufzählbar.

Da nur gilt:  $\bigcup_{i=1}^{\infty} Q_i \subset$  (siehe: 2.13 auf Seite 9) kann es durchaus sein, dass  $\bigcup_{i=1}^{\infty} Q_i \neq I_{R_{SF}}$  ist.

Es könnte also ein  $(\alpha, W) \in I_{R_{SF}}$  geben, das nicht  $I_{R_{SF}}$ -beweisbar ist.

Von  $\alpha$  könnte also - mittels sematischem Beweis - nicht der Wahrheitswert bestimmt werden.

## 4.7 Gödelscher Unvollständigkeitssatz

Jedes Beweissystem für die Menge  $WG$  aller in  $\mathfrak{N}$  gültigen arithmetischen Formeln ist unvollständig in dem Sinn, dass es in  $\mathfrak{N}$  gültige arithmetische Formeln gibt, die nicht beweisbar sind.

Beweis:

mit Hilfsmitteln aus der theoretischen Informatik. Siehe dazu:

Uwe Schöning "Theoretische Informatik Kurz Gefasst".

Im Folgenden wird noch ein mögliches Axiomensystem vorgestellt: Das Axiomensystem von Peano.

# 5 Axiomensystem von Peano

## 5.1 Definitionen

Das Axiomensystem von Peano wird durch eine Sprache  $L := \{\bar{0}, \bar{1}, \oplus, \otimes\}$  der Prädikatenlogik ersten Stufe formalisiert.

Diese besteht aus den 2 Konstanten  $\bar{0}, \bar{1}$  und den 2 Funktionssymbolen  $\oplus, \otimes$ .

Für alle L-Modelle  $\mathfrak{M} = (M, \bar{0}^M, \bar{1}^M, \oplus^M, \otimes^M)$  von PA und alle  $z \in \mathbb{N}$  wird definiert:  
 $\bar{z}^M = \bar{1}^M \oplus^M \dots \oplus^M \bar{1}^M$  z - Mal

M bedeutet dabei die Trägermenge und die Funktionssymbole zusammen mit den hochgestellten M's bedeuten die zu den Funktionssymbolen zugehörigen Interpretationen.

Mit  $\mathfrak{N} = (\mathbb{N}, 0, 1, +, *)$  wird das Standardmodell (ein L-Modell) von PA bezeichnet.

Mit  $\mathbb{N}$  werden dabei die interpretierten natürlichen Zahlen aus  $\mathbb{N}$  bezeichnet. Also:

$$\mathbb{N} = \{\bar{0}^N, \bar{1}^N, \bar{2}^N, \dots\}$$

wobei  $\bar{0}^N := 0, \bar{1}^N := 1, \bar{2}^N := 2$ , usw.

## 5.2 Axiome PA von Peano

Voraussetzungen:

y kommt in einer beliebigen Formel P frei vor, t und s sind beliebige Terme.

Axiomenschema Pax1:

Für alle Formeln A, in denen y frei vorkommt, sind die Formeln der folgenden Form Axiome:

$$(A(\bar{0}) \wedge \forall y(A(y) \rightarrow A(y+1))) \rightarrow \forall y A(y)$$

$$\text{Axiom Pax2: } t \oplus \bar{1} = s \oplus \bar{1} \rightarrow t = s$$

$$\text{Axiom Pax3: } \neg(t \oplus \bar{1}) = \bar{0}$$

$$\text{Axiom Pax4: } t = s \rightarrow t \oplus \bar{1} = s \oplus \bar{1}$$

$$\text{Axiom Pax5: } t \oplus \bar{0} = t$$

$$\text{Axiom Pax6: } t \oplus (s \oplus \bar{1}) = (t \oplus s) \oplus \bar{1}$$

$$\text{Axiom Pax7: } t \otimes \bar{0} = \bar{0}$$

$$\text{Axiom Pax8: } t \otimes (s \oplus \bar{1}) = (t \otimes s) \oplus \bar{1}$$

Die Menge der Axiome des Peanoschen Axiomensystems wird mit PA abgekürzt.

PA induziert die zugehörigen Regeln (Axiomeninstanzen)

$$R_A := \{(\emptyset, a) | a \in PA\}$$

### 5.3 Die durch Peano induktiv definierte Menge

Zu der Menge  $I_{R_F}$  aller durch die Sprache  $L = \{\bar{0}, \bar{1}, \oplus, \otimes\}$  bestimmten arithmetischen Formeln wird nun die Regelmengende  $R_P(I_{R_F})$  hinzugefügt, die aus den Regeln eines Syntaxkalküls der Prädikatenlogik und die Axiome (Axiominstanzen)  $R_A$  von Peano bestehen. Dadurch wird die Menge  $I_{R_P}$  erzeugt, also die Menge aller durch das Axiomensystem beweisbaren ( $I_{R_P}$ -beweisbaren) Formeln.

Nach dem Vollständigkeitssatz gilt speziell für PA:

Wenn  $PA \vdash_L \alpha$  dann  $PA \models \alpha$