Mathematische Logik

Universität Freiburg

WS 2005/2006

http://home.mathematik.uni-freiburg.de/flum/ws04log/index.html

Was ist ein mathematischer Beweis?

Analyse des Beweisbegriffes, der Beweise, wie wir sie in der Mathematik antreffen.

Der/Die Mathematiker/in muss seine/ihre Behauptungen beweisen.

- Wandel im Laufe der Jahrhunderte
- experimentelle Mathematik
- weitere Tätigkeiten
  - das Aufspüren wichtiger Zusammenhänge und Behauptungen
  - das Herauskristallisieren des mathematischen Kerns eines Problems
  - das geeignete Modellieren
  - die geschickte Einführung von Begriffen

Was ist ein mathematischer Beweis?

- Welches Interesse haben wir an der Behandlung dieser Frage?
- Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

Welches Interesse haben wir an der Behandlung dieser Frage?

Erkenntnistheoretisches Anliegen

Aristoteles (384 - 322 v. Chr.)

Welchen Nutzen ziehen wir aus der Behandlung dieser Frage?

1. Ist jede mathematische Aussage beweisbar?

   GOLDBACHSCHE VERMUTUNG: Jede gerade Zahl ≥ 4 ist die Summe von zwei Primzahlen.

2. Ist jede mathematische Aussage wahr oder falsch?

   KONTINUUMSHYPOTHESE (CH): Für jede nichtleere Teilmenge $X \subseteq \mathbb{R}$ gilt:
   Es gibt $f : \mathbb{N} \to X$ surjektiv oder es gibt $f : X \to \mathbb{R}$ surjektiv.

3. Ist die Mathematik widerspruchsfrei?

   Wenn die Mathematik widerspruchsfrei ist, dann läßt sich die Widerspruchsfreiheit nicht (mathematisch) beweisen

4. Kann man das Beweisen Computern überlassen?

   Gibt es also ein Programm, das folgendes leistet:

   INPUT: Axiome einer mathematischen Theorie und eine Behauptung (Vermutung)

   OUTPUT: Behauptung richtig (Beweis) oder Behauptung ist falsch (Gegenbeispiel).

Aristoteles (384 - 322 v. Chr.)

Schule der Sophisten

Achilles und die Schildkröte

> *Achilles und die Schildkröte laufen ein Wettrennen. Achilles gewährt der Schildkröte einen Vorsprung. Dann kann Achilles die Schildkröte niemals einholen.*

Zenon von Elea (490 - 425 v. Chr.) gibt folgende Begründung: Zu dem Zeitpunkt, an dem Achilles den Startpunkt der Schildkröte erreicht, ist die Schildkröte schon ein Stück weiter. Etwas später erreicht Achilles diesen Punkt, aber die Schildkröte ist schon etwas weiter. Wenn Achilles diesen Punkte erreicht, ist die Schildkröte wieder etwas weiter. So kann Achilles zwar immer näher an die Schildkröte herankommen, sie aber nie erreichen.

Der Barbier

In einem Städtchen wohnt ein Barbier, der genau diejenigen männlichen Einwohner rasiert, die sich nicht selbst rasieren.

Rasiert nun der Barbier sich selbst?

Antinomie des Lügners

Epimenides (Kreta, 600 v. Chr.)

Brief des Paulus an Titus 1:12-13:

> *Einer von ihren eigenen Landsleuten war ein Prophet, als er sagte: "Die Kreter lügen immer. Sie sind Raubtiere, liegen auf der faulen Haut und denken nur ans Fressen". Er hat die Wahrheit gesagt.*

Aus Don Quijote de la Mancha von Miguel de Cervantes (1517–1616)

Um eine gewisse Brücke zu überqueren, müssen alle Reisenden zunächst angeben, was ihr Ziel ist. Antworten sie wahrheitsgemäß, so dürfen sie die Brücke überqueren. Sonst werden sie gnadenlos an einem Galgen am Fuß der Brücke erhängt.

Eines Tages kommt ein Reisender, der angibt, sein Ziel sei es, am Galgen am Fuß der Brücke erhängt zu werden.

Aristoteles: Bemühen Überblick über die Regeln des Schließens (Syllogismen).

Prämisse:	Alle *Menschen* sind *sterblich*.
Prämisse:	*Sokrates* ist ein *Mensch*.
Konklusion:	*Sokrates* ist *sterblich*.

Prämisse:	Alle *Sura* sind *derung*.
Prämisse:	*Plarq* ist ein *Sura*.
Konklusion:	*Plarq* ist *derung*.

Prämisse:	Alle p sind q.
Prämisse:	a ist ein p.
Konklusion:	a ist q.

Ziel: Alle Schlußregeln.

R. Llullus (1235–1315)

G. W. Leibniz (1646–1716)

G. Boole (1815–1864)

G. Frege (1848–1925)

D. Hilbert (1862–1943)

B. Russell (1872–1970)

K. Gödel (1906–1978)

Ein Chinese hat das Pulver entdeckt.

Ein Chinese ist ein Asiat.

Eine differenzierbare Funktion ist Lösung der Gleichung $f'' + f = 0$.

Eine differenzierbare Funktion ist stetig.

Literatur:

Cori, Lascar: Mathematical Logic I, II. Oxford University Press.

Ebbinghaus, Flum, Thomas: Einführung in die mathematische Logik. Spektrum

Enderton: A mathematical introduction to logic. Academic Press

Prestel: Einführung in die mathematische Logik und Modelltheorie. Vieweg

Rautenberg: Einführung in die mathematische Logik. Vieweg

Σ Alphabet: Σ nichtleere Menge von Zeichen (Buchstaben, Symbolen)

bei grundlagentheoretischen Überlegungen: endliche Alphabete, konkrete Zeichen;

$\Sigma_1 = \{0, 1, \ldots, 9\}$; $\Sigma_2 = \{0, 1\}$; $\Sigma_3 = \{a, b, \ldots, x, y, z\}$; $\Sigma_4 = \{a, d, f, x, \int,), (\}$.

für weitere Anwendungen in der Mathematik: auch unendliche Alphabete:

$\Sigma_5 = \{c_0, c_1, \ldots\}$; $\Sigma_6 = \{c_r \mid r \in \mathbb{R}\}$.

Wort (Zeichenreihe) über Σ: endliche Aneinanderreihung von Buchstaben aus Σ.

Wörter: $u, v, w, \ldots$ leere Wort: λ;

Σ^* Menge der Wörter über dem Alphabet Σ.

$\int f(x)dx \in \Sigma_4^*$, $a \int \int dxd \in \Sigma_4^*$

$|w|$ Länge von w.

$|a \int \int dxd| = 6$ $|\lambda| = 0$.

$\Sigma_5 = \{c_0, c_1, \ldots\}$ ersetzen durch endliches Alphabet, etwa durch

$$\Sigma_7 := \{c, {}_0, {}_1, \ldots, {}_9\}.$$

Bei Identifikation von c_{25} mit $c\,{}_2\,{}_5$:

$$\Sigma_5 \subseteq \Sigma_7^* \quad \text{und} \quad \Sigma_5^* \subseteq \Sigma_7^*.$$

$\Sigma = \{a_0, \ldots, a_n\}$ mit paarweise verschiedenen (p.v.) $a_0, \ldots, a_n$.

Die lexikographische Ordnung $\leq_{\text{lex}}$ von Σ^* (bzgl. $a_0, \ldots, a_n$):

$$u \leq_{\text{lex}} v \quad \Longleftrightarrow \quad \Big(u = v \text{ oder } |u| < |v| \text{ oder}$$
$$(|u| = |v| \text{ und ex. } 1 \leq i < j \leq n,\ x, y, z \in \Sigma^*\colon u = x a_i y \text{ und } v = x a_j z)\Big).$$

$$u <_{\text{lex}} v \quad \Longleftrightarrow \quad (u \leq_{\text{lex}} v \text{ und } u \neq v)$$

$$\lambda, a_0, \ldots, a_n, a_0a_0, \ldots, a_0a_n, a_1a_0, \ldots, a_1a_n, \ldots, a_na_n, a_0a_0a_0, \ldots$$

Natürliche Zahlen als Wörter

$\Sigma := \{|\}$ $\quad n \mapsto \underbrace{|\ldots|}_{n}$ $\quad (:= [n]_1)$

$b \geq 2$, $\Sigma_b := \{0, \ldots, b-1\}$.

$$[\ ]_b : \mathbb{N} \to \Sigma_b^*$$

$$n \mapsto [n]_b \qquad b\text{-adische Darstellung von } n$$

$[25]_3 = 221$, da $25 = 2 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0$

$[81]_3 = 10000$, da $81 = 1 \cdot 3^4 + 0 \cdot 3^3 + 0 \cdot 3^2 + 0 \cdot 3^1 + 0 \cdot 3^0$

$[0]_3 = 0$

Für $n > 0$ und $b \geq 2$:

$$b^{\log_b n} = n \quad \text{und somit} \quad |[n]_b| = \lfloor \log_b n \rfloor + 1.$$

$$\log_b n < |[n]_b| \leq \log_b n + 1$$

Seien $a, b \in \mathbb{N}$, $a, b \geq 2$, $n > 0$

$$|[n]_b| \quad \leq \quad \log_b n + 1 = \log_b a \cdot \log_a n + 1 \leq \log_b a \cdot |[n]_a| + 1 \leq \underbrace{(\log_b a + 1)}_{c} \cdot |[n]_a|$$

Dagegen: $|[n]_1| = n = b^{\log_b n} \approx b^{|[n]_b|}$

Beispiele von Verfahren (Algorithmus):

1. zur Addition von natürlichen Zahlen (in Dezimaldarstellung);
2. zur Prüfung, ob vorgegebene Zahl eine Primzahl ist;
3. zur Auflistung der Primzahlen.

Unterschiede:

- mehrere, ein oder kein Input;
- stoppt mit Output; mit ja/nein Antwort; läuft unendlich lange und liefert unendlich viele Outputs.

Gemeinsamkeiten und Normierungen, die zu einem “mathematisch brauchbaren” intuitiven Begriff führen werden:

1. Ein Verfahren ist gegeben durch eine (endliche) Vorschrift. Ausführung, Verlauf und Ergebnis sind durch diese und die Inputs in allen Einzelheiten festgelegt (Reproduzierbarkeit).

2. Verfahren operiert schrittweise mit konkreten, handhabbaren Objekten; System hat diskrete Zustände.

$2'$. Verfahren operiert mit Zeichenreihen über einem (endlichen) Alphabet.

3. Kein Mangel an Zeit, Raum und Materie.

Σ sei ein endliches Alphabet und $W \subseteq \Sigma^*$.

1. Sei V ein Verfahren. V ist Entscheidungsverfahren für W, falls V bei jeder Eingabe $x \in \Sigma^*$ schließlich hält; ist $x \in W$, so steht dann λ in der Ergebniszeile sonst ein von λ verschiedenes Wort aus Σ^*.

2. W ist entscheidbar, falls es ein Entscheidungsverfahren für W gibt.

Σ sei ein Alphabet, $r \geq 1$, V ein Verfahren (Σ enthalte alle Buchstaben, die in V angesprochen werden). $f_{V,r}$ ist die Funktion mit $\mathrm{df}(f_{V,r}) \subseteq (\Sigma^*)^r$, $\mathrm{bd}(f_{V,r}) \subseteq \Sigma^*$ für die gilt:

$$(x_1, \ldots, x_r) \in \mathrm{df}(f_{V,r}) \quad \text{gdw} \quad \text{bei Eingabe } (x_1, \ldots, x_r) \text{ hält } V \text{ schließlich}$$

und für $(x_1, \ldots, x_r) \in \mathrm{df}(f_{V,r})$ und $y \in \Sigma^*$ gilt $f_{V,r}(x_1, \ldots, x_r) = y$, wenn V bei Eingabe $(x_1, \ldots, x_r)$ mit y in der Ergebniszeile hält.

Es gibt nur endlich viele natürliche Zahlen, welche in der deutschen Sprache mit einem Text der Länge ≤ 1000 definiert werden können.

Es gibt eine kleinste natürliche Zahl n_0, welche nicht in der deutschen Sprache mit einem Text der Länge ≤ 1000 definiert werden kann.

	n_0 ist die kleinste natürliche Zahl,
$(*)$	welche nicht in der deutschen Sprache
	mit einem Text der Länge ≤ 1000
	definiert werden kann.

$(*)$ ist eine Definition von n_0 in der deutschen Sprache mit einem Text der Länge ≤ 1000.

D. Hilbert (1862–1943)

Internationaler Mathematikerkongreß 1900 (Paris)

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoeffizienten sei vorgelegt; man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in den ganzen rationalen Zahlen lösbar ist.

Alan TURING (1912–1954)

http://www.turing.org.uk/turing/

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsanwsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsanwsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(3) $k\ R_i = [R_i)a \Rightarrow \ell; m$ $\qquad (k, i, \ell, m \in \mathbb{N},\ a \in \Sigma)$

Sprunganwsg.: Falls Wort in R_i mit a endet, gehe zu Zeile mit der Nummer ℓ sonst zur Zeile m.

(4) k PRINT R_i $\qquad (k, i \in \mathbb{N})$

Druckanwsg: Drucke Wort in R_i.

(5) k HALT $\qquad (k \in \mathbb{N})$

Halteanwsg: Halte.

Einem R-Programm P entspricht auf natürliche Weise ein Verfahren. Wir stellen uns dabei eine Rechenmaschine (Registermaschine) vor, die mit P programmiert ist und über die in P angesprochenen Register verfügt. Soll das Verfahren auf $(x_1, \ldots, x_r)$ angewendet werden, so sind zu Beginn der Berechnung alle Register leer, d.h. es steht in allen Registern das leere Wort, ausgenommen sind die Register $R_1, \ldots, R_r$, in denen sich $x_1, \ldots, x_r$ befinden. Die Berechnung erfolgt schrittweise; ein Schritt entspricht dabei der Ausführung einer Zeile. Beginnend mit der ersten Zeile wird dabei Zeile für Zeile abgearbeitet; es sei denn, dass durch eine Sprunganweisung eine andere Zeile aufgerufen wird. Ausgabewörter sind die evtl. bei Druckanweisungen ausgedruckten Wörter. Die Maschine hält, wenn die Halteanweisung erreicht wird.

P_1

0 $R_1 = [R_1)| \Rightarrow 1; ?$

1 $R_1 \leftarrow [R_1)$

2 $R_0 \leftarrow R_0 + 1$

3 $R_0 \leftarrow R_0 + 1$

4 $R_0 = [R_0)| \Rightarrow 0; 0$

5 HALT

P_1

0 $R_1 = [R_1)| \Rightarrow 1; 5$

1 $R_1 \leftarrow [R_1)$

2 $R_0 \leftarrow R_0 + 1$

3 $R_0 \leftarrow R_0 + 1$

4 $R_0 = [R_0)| \Rightarrow 0; 0$

5 HALT

P_2

0 PRINT R_1

1 $R_1 \leftarrow R_1 + 1$

2 $R_1 \leftarrow R_1 + 1$

3 $R_0 = [R_0)| \Rightarrow 0; 0$

4 HALT

P R-Programm, $r \geq 1$.

$f_{P,r}$ sei die Funktion mit

$$\mathrm{df}(f_{P,r}) \subseteq (\Sigma^*)^r \text{ und } \mathrm{bd}(f_{P,r}) \subseteq \Sigma^*$$

für die gilt:

$$(x_1, \ldots, x_r) \in \mathrm{df}(f_{P,r}) \quad \text{gdw} \quad P : (x_1, \ldots, x_r) \to \mathit{halt}$$

und für $(x_1, \ldots, x_r) \in \mathrm{df}(f_{P,r})$:

$$f_{P,r}(x_1, \ldots, x_r) = y \quad \text{gdw} \quad P : (x_1, \ldots, x_r) \to y.$$

$W \subseteq (\Sigma^*)^r$, P R-Programm.

1. P entscheidet W gdw für $(x_1, \ldots, x_r) \in (\Sigma^*)^r$:

   $P : (x_1, \ldots, x_r) \to \lambda$, falls $(x_1, \ldots, x_r) \in W$,

   $P : (x_1, \ldots, x_r) \to y$ mit $y \neq \lambda$, falls $(x_1, \ldots, x_r) \notin W$.

2. W Register-entscheidbar (R-entscheidbar) gdw ex. R-Programm, das W entscheidet.

$W \subseteq \Sigma^*$, P R-Programm.

1. P zählt W auf gdw P angesetzt auf λ druckt genau alle Wörter aus W aus.
2. W R-aufzählbar gdw existiert ein R-Programm, das W aufzählt.
3. f mit $\mathrm{df}(f) \subseteq (\Sigma^*)^r$ und $\mathrm{bd}(f) \subseteq \Sigma^*$ ist R-berechenbar gdw exitiert ein R-Programm Q mit $f = f_{Q,r}$.

Bemerkungen und Beispiele I

1. $\Sigma = \{|\}$. Dann: $\{(n, k) \mid n < k\}$ ist R-entscheidbar.
2. $\{p \mid p \text{ Primzahl}\}$ ist R-entscheidbar.
3. Σ Alphabet, $r \geq 1$.
   - $(\Sigma^*)^r$ ist R-entscheidbar.
   - Jede endliche Teilmenge von $(\Sigma^*)^r$ ist R-entscheidbar.
   - Sind $W_1, W_2 \subseteq (\Sigma^*)^r$ R-entscheidbar, so auch $W_1 \cap W_2$, $W_1 \cup W_2$, $(\Sigma^*)^r \setminus W_1$ und $W_1 \setminus W_2$.

Beweis: Siehe § 2.

Bemerkungen und Beispiele II

1. $\Sigma = \{0, \ldots, 9\}$. Die Menge der Primzahlen ist R-aufzählbar.
2. $\Sigma = \{a_1, \ldots, a_n\}$. Es gibt ein R-Programm, das Σ^* in lexikographischer Reihenfolge (bzgl. $a_1, \ldots, a_n$) aufzählt.
3. Jede R-entscheidbare Menge ist R-aufzählbar.
4. $W \subseteq W_0 \subseteq (\Sigma^*)^r$, W_0 R-entscheidbar. Dann

   $$W \text{ R-entscheid.} \iff W \text{ und } W_0 \setminus W \text{ R-aufzählb.}$$

   Insbesondere

   $$W \text{ R-entscheid.} \iff W \text{ und } (\Sigma^*)^r \setminus W \text{ R-aufzählb.}$$

Beweis: Siehe § 2.

a)	$\{P \mid P \to \text{halt}\}$	$\mapsto$	$\{x_P \mid P \to \text{halt}\}$
b)	$ax + by = 0$	$\mapsto$	$a\|b\S c\|d$
	$cx + dy = 0$		
c)	Menge der Primzahlen	$\mapsto$	Menge der Primzahlen als Wörter über $\{\|\}$

Definition. H entscheidbare Menge handhabbarer Objekte, Σ Alphabet.

$G : H \to \Sigma^*$ ist eine Gödelisierung (von H):

1. G ist berechenbar.

2. G ist injektiv.

3. $\text{bd}(G)$ ist entscheidbar.

4. $G^{-1} : \text{bd}(G) \to H$ ist berechenbar.

$G(h)$ die (das) Gödelnummer (Gödelwort) von h.

Man kann nicht entscheiden, ob ein R-Programm $\underline{\underline{P}}$ angesetzt auf λ (leere Registerinhalte) schließlich hält.

Man kann nicht entscheiden, ob ein R-Programm $\underline{\underline{P}}$ angesetzt auf irgendwelche $\underline{\underline{\text{Inputs}}}$ schließlich hält.

Man kann nicht entscheiden, ob ein Verfahren $\underline{\underline{V}}$ angesetzt auf irgendwelche $\underline{\underline{\text{Inputs}}}$ schließlich hält.

Man kann nicht entscheiden, ob ein in einer genügend reichhaltigen Programmiersprache D geschriebenes $\underline{\underline{\text{Programm}}}$ angesetzt auf irgendwelche $\underline{\underline{\text{Inputs}}}$ schließlich hält.

PGN Menge der Polynome in mehreren Unbekannten mit ganzzahligen Koeffizienten, die eine ganzzahlige Nullstelle haben.

Satz von Matijasevic (1970):

PGN ist nicht R-entscheidbar.

Somit: Es ist nicht entscheidbar, ob ein Polynom $\underline{\underline{p(x_1,\ldots,x_l)}} \in \mathbb{Z}[x_1,\ldots,x_l]$ eine Nullstelle in $\mathbb{Z}$ besitzt (d.h. ob ex. $z_1,\ldots,z_l \in \mathbb{Z}$ mit $p(z_1,\ldots,z_l) = 0$).

Lemma von Matijasevic: $M \subseteq \mathbb{N}$ R-aufzählbar.
Dann ex. $l \geq 1$ und $p(x_1,\ldots,x_l) \in \mathbb{Z}[x_1,\ldots,x_l]$ mit

$$M = W_{\mathbb{N}}(p) := \{p(n_1,\ldots,n_l) \mid \bar{n} \in \mathbb{N},\ p(\bar{n}) \geq 0\}.$$

Es ist unentscheidbar, ob ein R-Programm $\underline{\underline{P}}$ angesetzt auf λ hält.

Es gibt kein Programm, dass angesetzt auf ein (endliches) <u><u>Axiomensystem</u></u> und eine <u><u>Behauptung</u></u> entscheidet, ob die Behauptung aus dem Axiomensystem folgt.

4) $f : (\Sigma^*)^r \to \Sigma^*$. P (bzw. V) ist *t-zeitbeschränktes* Berechnungsverfahren für f, wenn P (bzw. V) f berechnet und t-zeitbeschränkt ist.

5) $f : (\Sigma^*)^r \to \Sigma^*$. $f \in$ PTIME gdw ex. R-Programm P und $p \in \mathbb{N}[x]$ mit: P ist p-zeitbeschränktes Berechnungsverfahren für f.

6) Seien Σ und Γ Alphabete, $f : \Sigma^* \to \Gamma^*$. Dann $f \in$ PTIME gdw $\tilde{f} \in$ PTIME, wobei $\tilde{f} : (\Sigma \cup \Gamma)^* \to (\Sigma \cup \Gamma)^*$ gegeben ist durch:

$$\tilde{f}(x) := \begin{cases} f(x), & \text{für } x \in \Sigma^* \\ \lambda, & \text{sonst.} \end{cases}$$

Pr Menge der Primzahlen.

Entscheidungsverfahren: $\underline{\underline{n}}$

für $k = 2, \ldots, \sqrt{n}$ prüfe, ob $k|n$.

Also: $n^{\frac{1}{2}}$ Divisionen

- $\Sigma := \{|\}$. Dann $|n| = n$.

Jede Division $\leq c \cdot n^2$ Schritte.

Insgesamt: $\leq n^{\frac{1}{2}} \cdot c \cdot n^2 = c \cdot n^{\frac{5}{2}}$ Schritte.

polynomialer Algorithmus.

- $b \geq 2$, $\Sigma_b = \{0, 1, \ldots, b-1\}$. Dann $|[n]_b| \sim \log_b n$.

Divisionen: $n^{\frac{1}{2}} \sim b^{\frac{1}{2} \cdot \log_b n}$

exponentieller Algorithmus.

1 Operation $\approx 10^{-6}$ Sekunden

Laufzeit:

	10	30	60
n	10^{-5} Sek.	$3 \cdot 10^{-5}$ Sek.	$6 \cdot 10^{-5}$ Sek.
n^5	10^{-1} Sek.	$24,3$ Sek.	13 Min.
2^n	10^{-3} Sek.	17.9 Min.	366 Jht.

Größe des größten behandelbaren Problems:

	2005	$100 \times$ schneller	$1000 \times$ schneller
n	N_1	$100 \cdot N_1$	$1000 \cdot N_1$
n^5	N_2	$2,5 \cdot N_2$	$3,98 \cdot N_2$
2^n	N_3	$N_3 + 6,64$	$N_3 + 9,97$

- Wenn $p \in \mathbb{R}[x]$, so gibt es ein $q \in \mathbb{N}[x]$ mit

$$\text{für alle } m \in \mathbb{N}\text{:} \quad |p(m)| \leq q(m).$$

- Wenn $p \in \mathbb{N}[x]$, so ist p monoton ($n \leq m \implies p(n) \leq p(m)$).
- Wenn $p, q \in \mathbb{N}[x]$, so sind $p + q$, $p \cdot q$, $p \circ q$ (und für $c \in \mathbb{N}$) $c \cdot p$ in $\mathbb{N}[x]$.

$G = (P, K)$ Graph:

- P (endliche) Menge, die Menge der Punkte
- $K \subseteq \{\{a, b\} \mid a, b \in P,\ a \neq b\}$, die Menge der Kanten

C Clique in G:

$$\text{für alle } a, b \in C \text{ mit } a \neq b\text{: } \{a, b\} \in K.$$

Clique	*Input:*	Graph $G = (P, K)$ und $k \in \mathbb{N}$.
	Frage:	Gibt es in G eine Clique der Größe k (k-Clique)?

$$\textsc{Clique} := \{(G, k) \mid G \text{ Graph},\ k \in \mathbb{N},\ G \text{ hat } k\text{-Clique}\}$$

$$\textsc{VClique} := \{(G, k, C) \mid G \text{ Graph},\ k \in \mathbb{N},\ C \text{ ist } k\text{-Clique}\}$$

– $\textsc{VClique} \in \text{PTIME}$.

– $(G, k) \in \textsc{Clique} \iff \exists C (G, k, C) \in \textsc{VClique}$.

– Wenn $(G, k, C) \in \textsc{VClique}$, so $\|C\| \leq \|(G, k)\|$.

Ein Hamilton-Kreis in einem Graphen $G = (P, K)$ ist eine Folge

$$C: \ a_1, \ldots, a_n$$

paarweise verschiedener Punkte mit:

- $P = \{a_1, \ldots, a_n\}$
- $\{a_1, a_2\}, \{a_2, a_3\}, \ldots, \{a_{n-1}, a_n\}, \{a_n, a_1\} \in K$.

HAM	*Input:*	Graph $G = (P, K)$.
	Frage:	Besitzt G ein Hamilton-Kreis?

$$\textsc{Ham} := \{G \mid G \text{ Graph und } G \text{ hat Hamilton-Kreis}\}$$

$$\textsc{VHam} := \{(G, C) \mid G \text{ Graph und } C \text{ Hamilton-Kreis in } G\}$$

– $\textsc{VHam} \in \text{PTIME}$.

– $G \in \textsc{Ham} \iff \exists C (G, C) \in \textsc{VHam}$.

– Wenn $(G, C) \in \textsc{VHam}$, so $\|C\| \leq \|G\|$.

Quadratische Kongruenzen: $\mathrm{QK} \subseteq \mathbb{N}^3$.

QK	*Input:*	$a, b, c \in \mathbb{N}$
	Frage:	ex. $x \in \mathbb{N}$ $(x < c$ und $x^2 \equiv a \bmod b)$?

$$\mathrm{QK} \quad := \quad \{(a,b,c) \mid \text{ex. } x \in \mathbb{N}\colon (x < c \text{ und } x^2 \equiv a \bmod b)\}.$$

$$\mathrm{VQK} \quad := \quad \{(a,b,c,x) \mid x < c \text{ und } x^2 \equiv a \bmod b\}.$$

– $\mathrm{VQK} \in \mathrm{PTIME}$.

– $\mathrm{QK}\,abc \iff \exists x \mathrm{VQK}\,abcx$.

– Wenn $\mathrm{VQK}\,abcx$, so $x < c$.

Steve Smale (Fields Medaille 1966)

> ...it is the most important new problem in mathematics in the last half of this century.

Σ Alphabet. Anweisungen für nichtdeterministische R-Programme: Alle alten Anweisungen, jedoch werden die Sprunganweisungen

$$k\ R_i = [R_i)a \Rightarrow \ell; m$$

ersetzt durch

$$k\ R_i = [R_i)a \Rightarrow L; M \qquad (k, i \in \mathbb{N},\ L, M \subseteq \mathbb{N}, L, M \text{ endlich, nicht leer, } a \in \Sigma)$$

(Nichtdeterministische Sprunganweisungen: Falls Wort in R_i mit a endet, gehe zu einer Zeile mit Zeilennummer in L sonst zur Zeile mit Zeilennummer in M.)

Ein nichtdeterministisches R-Programm ist eine endliche Folge $\alpha_0, \ldots, \alpha_k$ von nichtdeterministischen Anweisungen mit:

(i) Für $i = 0, \ldots, k$: α_i hat die Zeilenr. i.

(ii) Jede (nichtdeterministische) Sprunganweisung verweist auf Zeilennummern $\leq k$.

(iii) Genau α_k ist eine Halteanweisung.

P nichtdeterministisches R-Programm, $\mathrm{Reg}(P) \subseteq \{0, \ldots, n\}$.

P wird auf $x_1, \ldots, x_r$ angesetzt (wie im det. Fall definiert).

Wird P auf $x_1, \ldots, x_r$ angesetzt, so kann es verschiedene Berechnungen geben.

$$\begin{array}{ccccccc} \lambda & x_1 & \ldots & x_r & \lambda & \ldots & \lambda \\ & & & \Downarrow P & & & \\ y_0 & y_1 & & \ldots & & & y_n \end{array}$$

bedeute: es gibt eine Berechnung von P angesetzt auf $x_1, \ldots, x_r$, die schließlich hält und dann stehen $y_0, \ldots, y_n$ in $R_0, \ldots, R_n$.

$W \subseteq (\Sigma^*)^r$. P akzeptiert (entscheidet) W gdw für alle $\bar{x} \in (\Sigma^*)^r$:

$$\bar{x} \in W \quad \Longleftrightarrow \quad \begin{array}{ccccccc} \lambda & x_1 & \ldots & x_r & \lambda & \ldots & \lambda \\ & & & \Downarrow P & & & \\ \lambda & * & & \ldots & & & * \end{array}$$

also: $\quad \bar{x} \in W \iff$ es gibt eine akzept. Berechnung von P angesetzt auf $\bar{x}$.

P nichtdeterministisches R-Programm, $t : \mathbb{N} \to \mathbb{N}$, $r \geq 1$.

P t-zeitbeschränkt gdw für alle $\bar{x} \in (\Sigma^*)^r$ endet jede Berechnung von P angesetzt auf $\bar{x}$ nach $\leq t(|\bar{x}|)$ Schritten.

$W \subseteq (\Sigma^*)^r$.

$W \in$ NPTIME gdw ex. nichtdeterministisches Programm P und $p \in \mathbb{N}[x]$:

$$P \text{ ist } p\text{-zeitbeschränkt und akzeptiert } W.$$

Axiome der Theorie der Äquivalenzrelationen

(r) Für alle x: xRx.

(s) Für alle x, y: Wenn xRy, so yRx.

(t) Für alle x, y, z: Wenn xRy und yRz, so xRz.

Seien x, y gegeben und gelte für ein geeignetes u

$$xRu \text{ und } yRu.$$

Aus (s) erhalten wir dann

$$uRx \text{ und } uRy.$$

Aus xRu und uRy ergibt sich mit (t)

$$xRy, \tag{1}$$

und aus yRu und uRx, ebenfalls mit (t),

$$yRx. \tag{2}$$

Sei nun z beliebig gewählt. Gilt

$$xRz, \tag{3}$$

so erhalten wir aus (2) und (3) mit (t)

$$yRz.$$

Gilt umgekehrt

$$yRz, \tag{4}$$

so erhalten wir aus (1) und (4) mit (t) $\quad xRz.$

Für $S = \{\underset{2}{f}, \underset{1}{g}, c, \underset{3}{P}, \underset{4}{R}\}$ ist

$$g(f(c, v_7))$$

ein S-Term.

Ableitung:

1	c	(T2)
2	v_7	(T1)
3	$f(c, v_7)$	(T3) auf 1,2
4	$g(f(c, v_7))$	(T3) auf 3

1	v_7	(T1)
2	c	(T2)
3	$f(c, v_7)$	(T3) auf 2,1
4	$g(f(c, v_7))$	(T3) auf 3

Für $S = \{\underset{2}{+}, \underset{2}{\cdot}\}$ ist

$$+(v_3, \cdot(v_2, v_3))$$

ein S-Term.

Ableitung:

1	v_2	(T1)
2	v_3	(T1)
3	$\cdot(v_2, v_3)$	(T3) auf 1,2
4	$+(v_3, \cdot(v_2, v_3))$	(T3) auf 2,3

Für $S_{\text{Äq}} = \{\underset{2}{R}\}$ sind $S_{\text{Äq}}$-Ausdrücke:

$$\forall v_1 Rv_1v_1$$

$$\forall v_1 \forall v_2 (Rv_1v_2 \rightarrow Rv_2v_1)$$

$$\forall v_1 \forall v_2 \forall v_3 ((Rv_1v_2 \wedge Rv_2v_3) \rightarrow Rv_1v_3)$$

Ableitungen:

1	Rv_1v_1	(A2)
2	$\forall v_1 Rv_1v_1$	(A5) auf 1

1	Rv_1v_2	(A2)
2	Rv_2v_1	(A2)
3	$(Rv_1v_2 \rightarrow Rv_2v_1)$	(A4) auf 1,2
4	$\forall v_2(Rv_1v_2 \rightarrow Rv_2v_1)$	(A5) auf 3
5	$\forall v_1 \forall v_2(Rv_1v_2 \rightarrow Rv_2v_1)$	(A5) auf 4

Für $S := \{\underset{1}{P}, \underset{1}{f}, c\}$ ist ein S-Ausdruck:

$$(\forall x \exists x Px \wedge \forall y f(c) \equiv c)$$

Ableitung:

1	$f(c) \equiv c$	(A1)
2	$\forall y f(c) \equiv c$	(A5) auf 2
3	Px	(A2)
4	$\exists x Px$	(A5) auf 3
5	$\forall x \exists x Px$	(A5) auf 4
6	$(\forall x \exists x Px \wedge \forall y f(c) \equiv c)$	(A4) auf 5,2

Beweis durch Induktion über den Kalkül K: Will man zeigen, daß alle mit K ableitbaren Wörter eine Eigenschaft E haben, so genügt hierzu der Nachweis, daß

> für jede Regel
>
> $$\frac{\xi_1, \ldots, \xi_n}{\xi}$$
>
> des Kalküls K gilt: Wenn $\xi_1, \ldots, \xi_n$ in K ableitbar sind und die Eigenschaft E haben (*Induktionsvoraussetzung*), so hat auch ξ die Eigenschaft E.

Im Fall $n = 0$ müssen wir also zeigen, daß ξ die Eigenschaft E hat.

Induktion über den Aufbau der Terme: Um nachzuweisen, daß alle S-Terme eine Eigenschaft E haben, reicht es, zu zeigen:

(T1): Jede Variable hat die Eigenschaft E.

(T2): Jede Konstante aus S hat die Eigenschaft E.

(T3): Haben die S-Terme $t_1, \ldots, t_n$ die Eigenschaft E und ist $f \in S$ n-stellig, so hat $f(t_1, \ldots, t_n)$ die Eigenschaft E.

(T3): $t_1 = f(t'_1, \ldots, t'_r)$ mit r-stelligem f.

Dann beginnt s_1 mit f und somit gibt es Terme $s'_1, \ldots, s'_r$ mit $s_1 = f(s'_1, \ldots, s'_r)$. Daher

$$f(t'_1, \ldots, t'_r)t_2 \ldots t_m = f(s'_1, \ldots, s'_r)s_2 \ldots s_k\xi$$

und somit

$$t'_1, \ldots, t'_r)t_2 \ldots t_m = s'_1, \ldots, s'_r)s_2 \ldots s_k\xi$$

Da $|t'_1|, |s'_1| < |t_1 \ldots t_m|$ gilt nach Ind.vor. $t'_1 = s'_1$; entsprechend erhält man nacheinander

$$t'_2 = s'_2, \ldots, t'_r = s'_r.$$

Also insgesamt $t_1 = f(t'_1, \ldots, t'_r) = f(s'_1, \ldots, s'_r) = s_1$. Weiterhin ist

$$t_2 \ldots t_m = s_2 \ldots s_k\xi$$

Da $|t_2 \ldots t_m| < |t_1 \ldots t_m|$ und $m - 1 \leq k - 1$ gilt nach Ind.vor.

$$m - 1 = k - 1, \quad t_2 = s_2, \ldots, t_m = s_m \text{ und } \xi = \lambda.$$

Eindeutige Zerlegbarkeit von Termen. Jeder S-Term ist entweder

1. eine Variable oder
2. eine Konstante in S oder
3. ein Term der Gestalt $f(t_1, \ldots, t_n)$ für ein n-stelliges $f \in S$ und $t_1, \ldots, t_n \in T^S$.

   Dabei sind f und $t_1, \ldots, t_n$ eindeutig bestimmt.

Eindeutige Zerlegbarkeit von Ausdücken. Jeder S-Ausdruck ist entweder ein Ausdruck der Gestalt

(1)	$t_1 \equiv t_2$	oder	(2)	$Rt_1 \dots t_r$	oder
(3)	$\neg\varphi$	oder	(4)	$(\varphi \wedge \psi)$	oder
(5)	$(\varphi \vee \psi)$	oder	(6)	$(\varphi \rightarrow \psi)$	oder
(7)	$(\varphi \leftrightarrow \psi)$	oder	(8)	$\forall x\varphi$	oder
(9)	$\exists x\varphi$				

Dabei sind eindeutig bestimmt
$t_1, t_2 \in T^S$ in (1),
$R \in S$ und $t_1, \dots, t_r \in T^S$ in (2),
φ in (3),
φ und ψ in (4), (5), (6), (7)
x und φ in (8) und (9).

Bemerkung (Induktive Definitionen über den Aufbau der Terme). Um in eindeutiger Weise eine Funktion für alle S-Terme zu definieren, genügt es,

(T1)$'$: jeder Variable einen Wert zuzuordnen;

(T2)$'$: jeder Konstanten in S einen Wert zuzuordnen;

(T3)$'$: für jedes n-stellige $f \in S$ und beliebigen $t_1, \ldots, t_n \in T^S$ dem Term $f(t_1, \ldots, t_n)$ einen Wert zuzuordnen unter der Annahme, daß den Termen $t_1, \ldots, t_n$ bereits je ein Wert zugeordnet ist.

$$
\begin{aligned}
&\mathrm{fr}((\exists u Rxu \wedge \exists y \forall x (Ryx \vee Ryu))) \\
&\quad = \quad \mathrm{fr}(\exists u Rxu) \cup \mathrm{fr}(\exists y \forall x (Ryx \vee Ryu)) \\
&\quad = \quad (\mathrm{fr}(Rxu) \setminus \{u\}) \cup (\mathrm{fr}(\forall x (Ryx \vee Ryu)) \setminus \{y\}) \\
&\quad = \quad (\{x, u\} \setminus \{u\}) \cup (\mathrm{fr}((Ryx \vee Ryu)) \setminus \{y, x\}) \\
&\quad = \quad \{x\} \cup ((\mathrm{fr}(Ryx) \cup \mathrm{fr}(Ryu)) \setminus \{y, x\}) \\
&\quad = \quad \{x\} \cup ((\{y, x\} \cup \{y, u\}) \setminus \{y, x\}) \\
&\quad = \quad \{x\} \cup \{u\} \\
&\quad = \quad \{x, u\}.
\end{aligned}
$$

Für $S_{\text{Äq}} = \{\underset{2}{R}\}$ sind $S_{\text{Äq}}$-Ausdrücke:

$$\forall v_1 R v_1 v_1$$

$$\forall v_1 \forall v_2 (R v_1 v_2 \rightarrow R v_2 v_1)$$

$$\forall v_1 \forall v_2 \forall v_3 ((R v_1 v_2 \wedge R v_2 v_3) \rightarrow R v_1 v_3)$$

$$S = \{\underset{2}{g}\}, \quad \mathfrak{R} = (\mathbb{R}, \cdot), \quad \mathfrak{I} = (\mathfrak{R}, \beta) \text{ mit } \beta(v_n) = \begin{cases} n & n \text{ ungerade} \\ -n & \text{sonst} \end{cases}$$

$$\begin{aligned}
& \mathfrak{I} \models \neg\exists v_1 g(v_1, v_1) \equiv v_2 \\
\iff \quad & \text{nicht } \mathfrak{I} \models \exists v_1 g(v_1, v_2) \equiv v_2 \\
\iff \quad & \text{nicht ex. } r \in \mathbb{R} : \ \mathfrak{I}\frac{r}{v_1} \models g(v_1, v_1) \equiv v_2 \\
\iff \quad & \text{nicht ex. } r \in \mathbb{R} : \ \mathfrak{I}\frac{r}{v_1}(g(v_1, v_1)) = \mathfrak{I}\frac{r}{v_1}(v_2) \\
\iff \quad & \text{nicht ex. } r \in \mathbb{R} : \ \mathfrak{I}\frac{r}{v_1}(v_1) \cdot \mathfrak{I}\frac{r}{v_1}(v_1) = \beta\frac{r}{v_1}(v_2) \\
\iff \quad & \text{nicht ex. } r \in \mathbb{R} : \ \beta\frac{r}{v_1}(v_1) \cdot \beta\frac{r}{v_1}(v_1) = -2 \\
\iff \quad & \text{nicht ex. } r \in \mathbb{R} : \ r \cdot r = -2.
\end{aligned}$$

Somit $\mathfrak{I} \models \neg\exists v_1 g(v_1, v_1) \equiv v_2$.

Entsprechend: $\mathfrak{I} \models \neg\exists v_{116} g(v_{116}, v_{116}) \equiv v_2$.

Dagegen: $\mathfrak{I} \not\models \neg\exists v_1 g(v_1, v_1) \equiv v_3$, da

$$\mathfrak{I} \models \exists v_1 g(v_1, v_1) \equiv v_3.$$

$S_{\text{Äq}} = \{\underset{2}{R}\}$:

$$\Phi_{\text{Äq}} \begin{cases} \forall v_1 R v_1 v_1 \\ \forall v_1 \forall v_2 (R v_1 v_2 \rightarrow R v_2 v_1) \\ \forall v_1 \forall v_2 \forall v_3 ((R v_1 v_2 \wedge R v_2 v_3) \rightarrow R v_1 v_3) \end{cases}$$

$$
\begin{aligned}
\varphi^* &:= \varphi \quad \text{wenn } \varphi \text{ atomar}\\
[\neg\varphi]^* &:= \neg\ [\varphi]^*\\
(\varphi \wedge \psi)^* &:= \neg(\neg\ [\varphi]^* \vee \neg\ [\psi]^*)\\
(\varphi \vee \psi)^* &:= (\varphi^* \vee \psi^*)\\
(\varphi \rightarrow \psi)^* &:= (\neg\ [\varphi]^* \vee \psi^*)\\
(\varphi \leftrightarrow \psi)^* &:= \neg(\varphi^* \vee \psi^*) \vee \neg(\neg\ [\varphi]^* \vee \neg\ [\psi]^*)\\
[\forall x\varphi]^* &:= \neg\exists x\neg\ [\varphi]^*\\
[\exists x\varphi]^* &:= \exists x\ [\varphi]^*
\end{aligned}
$$

$$
\begin{aligned}
\forall x(Rx \rightarrow Pf(x))^* \quad &= \quad \neg\exists x\neg(Rx \rightarrow Pf(x))^*\\
&= \quad \neg\exists x\neg(\neg Rx^* \vee Pf(x)^*)\\
&= \quad \neg\exists x\neg(\neg Rx \vee Pf(x))
\end{aligned}
$$

(a) Induktion über den Termkalkül: Sei $t \in T^S$ und gelte $\beta_1 \upharpoonright \mathrm{var}(t) = \beta_2 \upharpoonright \mathrm{var}(t)$.

$$
\begin{array}{ll}
t = x: & \mathfrak{I}_1(x) = \beta_1(x) = \beta_2(x) = \mathfrak{I}_2(x). \\
t = c: & \mathfrak{I}_1(c) = c^{\mathfrak{A}_1} = c^{\mathfrak{A}_2} = \mathfrak{I}_2(c). \\
t = f(t_1, \ldots, t_n): & \mathfrak{I}_1(f(t_1, \ldots, t_n)) \;=\; f^{\mathfrak{A}_1}(\mathfrak{I}_1(t_1), \ldots, \mathfrak{I}_1(t_n)) \\
\quad \text{(Ind.vor.)} & = f^{\mathfrak{A}_1}(\mathfrak{I}_2(t_1), \ldots, \mathfrak{I}_2(t_n)) \\
\quad (\text{Vor. } f^{\mathfrak{A}_1} = f^{\mathfrak{A}_2}) & = f^{\mathfrak{A}_2}(\mathfrak{I}_2(t_1), \ldots, \mathfrak{I}_2(t_n)) \\
 & = \mathfrak{I}_2(f(t_1, \ldots, t_n)).
\end{array}
$$

(b) Induktion über den Ausdruckskalkül: Sei $\varphi \in L^S$ und gelte $\beta_1 \upharpoonright \mathrm{fr}(\varphi) = \beta_2 \upharpoonright \mathrm{fr}(\varphi)$.

$\varphi = Rt_1 \ldots t_r$:

$$
\begin{array}{rcl}
\mathfrak{I}_1 \models Rt_1 \ldots t_r & \iff & R^{\mathfrak{A}_1}\mathfrak{I}_1(t_1) \ldots \mathfrak{I}_1(t_r) \\
\text{(wegen (a))} & \iff & R^{\mathfrak{A}_1}\mathfrak{I}_2(t_1) \ldots \mathfrak{I}_2(t_r) \\
(\text{wegen } R^{\mathfrak{A}_1} = R^{\mathfrak{A}_2}) & \iff & R^{\mathfrak{A}_2}\mathfrak{I}_2(t_1) \ldots \mathfrak{I}_2(t_r) \\
 & \iff & \mathfrak{I}_2 \models Rt_1 \ldots t_r.
\end{array}
$$

$\varphi = \neg\psi$: $\quad \mathfrak{I}_1 \models \neg\psi$ gdw nicht $\mathfrak{I}_1 \models \psi$

gdw nicht $\mathfrak{I}_2 \models \psi$ (Ind.vor.)

gdw $\mathfrak{I}_2 \models \neg\psi$.

$\varphi = (\psi \vee \chi)$: $\mathfrak{I}_1 \models (\psi \vee \chi)$ gdw $(\mathfrak{I}_1 \models \psi$ oder $\mathfrak{I}_1 \models \chi)$

gdw $(\mathfrak{I}_2 \models \psi$ oder $\mathfrak{I}_2 \models \chi)$ (Ind.vor.)

gdw $\mathfrak{I}_2 \models (\psi \vee \chi)$.

$\varphi = \exists x\psi$: $\mathfrak{I}_1 \models \exists x\psi$ gdw es gibt ein $a \in A_1$: $\mathfrak{I}_1 \frac{a}{x} \models \psi$

gdw es gibt ein $a \in A_2\,(= A_1)$: $\mathfrak{I}_1 \dfrac{a}{x} \models \psi$

wegen $\text{fr}(\psi) \subseteq \text{fr}(\exists x\psi) \cup \{x\}$ stimmen $\mathfrak{I}_1 \frac{a}{x}$ und $\mathfrak{I}_2 \frac{a}{x}$ auf $\text{fr}(\psi)$ überein; somit nach Ind.vor.

gdw es gibt ein $a \in A_2$: $\mathfrak{I}_2 \dfrac{a}{x} \models \psi$

gdw $\mathfrak{I}_2 \models \exists x\psi$.

$\mathfrak{A}, \mathfrak{B}$ S-Strukturen

1. (a) $\pi : A \to B$, π ist Isomorphismus von $\mathfrak{A}$ nach (auf) $\mathfrak{B}$, $\pi : \mathfrak{A} \cong \mathfrak{B}$, wenn
   (1) π ist bijektiv;
   (2) Für $R \in S, R$ r-stellig, $a_1, \ldots, a_r \in A$:
   $$R^{\mathfrak{A}} a_1 \ldots a_r \iff R^{\mathfrak{B}} \pi(a_1) \ldots \pi(a_r);$$
   (3) Für $f \in S, f$ r-stellig, $a_1, \ldots, a_r \in A$:
   $$\pi(f^{\mathfrak{A}}(a_1, \ldots, a_r)) = f^{\mathfrak{B}}(\pi(a_1), \ldots, \pi(a_r));$$
   (4) Für $c \in S$: $\qquad \pi(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$.

   (b) $\mathfrak{A}$ und $\mathfrak{B}$ sind isomorph, $\mathfrak{A} \cong \mathfrak{B}$, gdw. ex. π mit $\pi : \mathfrak{A} \cong \mathfrak{B}$.

2. $\pi : A \to B$, π ist starker Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ gdw π erfüllt (2), (3) und (4).

3. $\pi : A \to B$, π Homomorphismus von $\mathfrak{A}$ nach $\mathfrak{B}$ gdw π erfüllt (3), (4) und

   (2′) für $R \in S, R$ r-stellig, $a_1, \ldots, a_r \in A$,
   $$\text{wenn } R^{\mathfrak{A}} a_1 \ldots a_r, \text{ so } R^{\mathfrak{B}} \pi(a_1) \ldots \pi(a_r).$$

Schreibweisen: $\pi : \mathfrak{A} \to \mathfrak{B}$ Isomorphismus (starker Homomorph., Homomorphismus).

Zu (b): Induktion über t:

x_j: $\pi(x_j^{\mathfrak{A}}[\bar{a}]) = \pi(a_j) = x_j^{\mathfrak{B}}[\pi(\bar{a})]$.

c: $\pi(c^{\mathfrak{A}}[\bar{a}]) = \pi(c^{\mathfrak{A}}) = c^{\mathfrak{B}} = c^{\mathfrak{B}}[\pi(\bar{a})]$.

$f(t_1, \ldots, t_r)$:

$$\begin{array}{rcl}
\pi(f(t_1, \ldots, t_r)^{\mathfrak{A}}[\bar{a}]) & = & \pi(f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[\bar{a}], \ldots, t_r^{\mathfrak{A}}[\bar{a}])) \\
(\pi \text{ Homom.}) & = & f^{\mathfrak{B}}(\pi(t_1^{\mathfrak{A}}[\bar{a}]), \ldots, \pi(t_r^{\mathfrak{A}}[\bar{a}])) \\
(\text{Ind.Vor.}) & = & f^{\mathfrak{B}}(t_1^{\mathfrak{B}}[\pi(\bar{a})], \ldots, t_r^{\mathfrak{B}}[\pi(\bar{a})]) \\
 & = & f(t_1, \ldots, t_r)^{\mathfrak{B}}[\pi(\bar{a})].
\end{array}$$

Zu (a): $t_1 = t_2$:

$$\begin{array}{rcl}
\mathfrak{A} \models t_1 = t_2[\bar{a}] & \Longleftrightarrow & t_1^{\mathfrak{A}}[\bar{a}] = t_2^{\mathfrak{A}}[\bar{a}] \\
(\Leftarrow, \text{ da } \pi \text{ inj.}) & \Longleftrightarrow & \pi(t_1^{\mathfrak{A}}[\bar{a}]) = \pi(t_2^{\mathfrak{A}}[\bar{a}]) \\
(\text{wegen (b)}) & \Longleftrightarrow & t_1^{\mathfrak{B}}[\pi(\bar{a})] = t_2^{\mathfrak{B}}[\pi(\bar{a})] \\
 & \Longleftrightarrow & \mathfrak{B} \models t_1 = t_2[\pi(\bar{a})].
\end{array}$$

$Rt_1 \dots t_r$:

$$\begin{aligned}
\mathfrak{A} \models Rt_1 \dots t_r[\bar{a}] \quad &\Longleftrightarrow \quad R^{\mathfrak{A}} t_1^{\mathfrak{A}}[\bar{a}] \dots t_r^{\mathfrak{A}}[\bar{a}] \\
&\Longleftrightarrow \quad R^{\mathfrak{B}} \pi(t_1^{\mathfrak{A}}[\bar{a}]) \dots \pi(t_r^{\mathfrak{A}}[\bar{a}]) \\
(\Rightarrow, \text{ da } \pi \text{ Hom.} \quad & \quad\quad\quad\;\; \Leftarrow, \text{ da } \pi \text{ starker Hom.}) \\
(\text{wegen (b)}) \quad &\Longleftrightarrow \quad R^{\mathfrak{B}} t_1^{\mathfrak{B}}[\pi(\bar{a})] \dots t_r^{\mathfrak{B}}[\pi(\bar{a})] \\
&\Longleftrightarrow \quad \mathfrak{B} \models Rt_1 \dots t_r[\pi(\bar{a})].
\end{aligned}$$

Sei $\varphi(x_1, \dots, x_n) = \exists y \psi$. Da $y \notin \mathrm{fr}(\varphi)$, können wir o.B.d.A. annehmen, dass $y \notin \{x_1, \dots, x_n\}$. Somit $\psi = \psi(x_1, \dots, x_n, y)$. Nun gilt:

$$\begin{aligned}
\mathfrak{A} \models \varphi[\bar{a}] \quad &\Longleftrightarrow \quad \text{ex. } a \in A\text{: } \mathfrak{A} \models \psi[\bar{a}, a] \\
(\text{Ind.vor.}) \quad &\Longleftrightarrow \quad \text{ex. } a \in A\text{: } \mathfrak{B} \models \psi[\pi(\bar{a}), \pi(a)] \\
(\Leftarrow \text{ da } \pi \text{ surjektiv}) \quad &\Longleftrightarrow \quad \text{ex. } b \in B\text{: } \mathfrak{B} \models \psi[\pi(\bar{a}), b] \\
&\Longleftrightarrow \quad \mathfrak{B} \models \varphi[\pi(\bar{a})].
\end{aligned}$$

$\mathfrak{A}$, $\mathfrak{B}$ S-Strukturen. $\mathfrak{A}$ ist Substruktur von $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B}$, wenn

1. $A \subseteq B$.
2. (a) für $R \in S$ n-st.: $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$, d.h. für $\bar{a} \in A^n$

   $$R^{\mathfrak{A}}\bar{a} \iff R^{\mathfrak{B}}\bar{a}$$

   (b) für $f \in S$ n-st.: $f^{\mathfrak{A}} = f^{\mathfrak{B}} \restriction A^n$, d.h. für $\bar{a} \in A^n$

   $$f^{\mathfrak{A}}(\bar{a}) = f^{\mathfrak{B}}(\bar{a})$$

   (c) für $c \in S$: $c^{\mathfrak{A}} = c^{\mathfrak{B}}$.

$$\Phi_{\mathrm{Ord}} \begin{cases} \forall x \forall y (x \leq y \vee y \leq x) \\ \forall x \forall y ((x \leq y \wedge y \leq x) \rightarrow x \equiv y) \\ \forall x \forall y \forall z ((x \leq y \wedge y \leq z) \rightarrow x \leq z). \end{cases}$$

$$\Phi_{\mathrm{Graph}} \quad \forall x \neg Exx \quad \forall x \forall y (Exy \rightarrow Eyx).$$

$$\Phi_{\mathrm{DG}} \quad \forall x \neg Exx$$

$$\Phi_{\mathrm{Kp}} \begin{cases} \forall x \forall y \forall z (x+y)+z \equiv x+(y+z) & \forall x\, x+0 \equiv x \\ \forall x \forall y \forall z (x \cdot y) \cdot z \equiv x \cdot (y \cdot z) & \forall x\, x \cdot 1 \equiv x \\ \forall x \exists y\, x+y \equiv 0 & \forall x (\neg x \equiv 0 \rightarrow \exists y\, x \cdot y \equiv 1) \\ \forall x \forall y\, x+y \equiv y+x & \forall x \forall y\, x \cdot y \equiv y \cdot x \\ \neg 0 \equiv 1 & \\ \forall x \forall y \forall z\, x \cdot (y+z) \equiv (x \cdot y)+(x \cdot z). & \end{cases}$$

$$\Phi_{\mathrm{gKp}} \begin{cases} \text{die Sätze von } \Phi_{\mathrm{Kp}} \text{ und } \Phi_{\mathrm{Ord}} \\ \forall x \forall y \forall z (x \leq y \rightarrow x+z \leq y+z) \\ \forall x \forall y \forall z ((x \leq y \wedge 0 \leq z) \rightarrow x \cdot z \leq y \cdot z). \end{cases}$$

$S_{\mathrm{BA}} = \{\underset{2}{\sqcap}, \underset{2}{\sqcup}, \underset{1}{\sim}, 0, 1\}$. Sei Φ_{BA} die Menge der folgenden S_{BA}-Sätze:

$\forall x \forall y\ x \sqcap y \equiv y \sqcap x$	$\sqcap$ kommutat.
$\forall x \forall y \forall z\ (x \sqcap y) \sqcap z \equiv x \sqcap (y \sqcap z)$	$\sqcap$ assoziat.
$\forall x \forall y\ x \sqcup y \equiv y \sqcup x$	$\sqcup$ kommutat.
$\forall x \forall y \forall z\ (x \sqcup y) \sqcup z \equiv x \cup (y \sqcup z)$	$\sqcup$ assoziat.
$\forall x \forall y \forall z\ x \sqcap (y \sqcup z) \equiv (x \sqcap y) \sqcup (x \sqcap z)$	distributiv
$\forall x \forall y \forall z\ x \sqcup (y \sqcap z) \equiv (x \sqcup y) \sqcap (x \sqcup z)$	distributiv
$\forall x \forall y\ (x \sqcup y) \sqcap y \equiv y$	Absorption
$\forall x \forall y\ (x \sqcap y) \sqcup y \equiv y$	Absorption
$\forall x\ x \sqcap 1 \equiv x$	1 neutral bei $\sqcap$
$\forall x\ x \sqcup 0 \equiv x$	0 neutral bei $\sqcup$
$\forall x \forall y\ x \sqcap \sim x \equiv 0$	Komplementgesetz
$\forall x\ x \sqcup \sim x \equiv 1$	Komplementgesetz.

Sind

$$(\exists y(Exy \vee \neg\neg Eyx) \vee \neg\neg Eyx))$$

und

$$(\exists y(Exy \vee Eyx) \vee \neg\neg Eyx))$$

logisch äquivalent?

Ersetzungslemma. (Intuitiv: Ersetzt man in φ einen Teilausdruck ψ durch einen zu ψ logisch äquivalenten Ausdruck, so erhält man einen zu φ logisch äquivalenten Ausdruck.)

Gelte $\varphi_1 \equiv \psi_1$ und $\varphi_2 \equiv \psi_2$; dann

$\neg\varphi_1 \equiv \neg\psi_1$, $(\varphi_1 \vee \varphi_2) \equiv (\psi_1 \vee \psi_2)$, $\exists x\varphi_1 \equiv \exists x\psi_1$.

$$\begin{aligned}
\neg\neg Eyx &\equiv Eyx \\
(Exy \vee \neg\neg Eyx) &\equiv (Exy \vee Eyx) \\
\exists y(Exy \vee \neg\neg Eyx) &\equiv \exists y(Exy \vee Eyx) \\
(\exists y(Exy \vee \neg\neg Eyx) \vee \neg\neg Eyx)) &\equiv (\exists y(Exy \vee \neg\neg Eyx) \vee Eyx))
\end{aligned}$$

S-Interpretation $\mathfrak{I} = (\mathfrak{A}, \beta)$, $x_1, \dots, x_m$ paarweise verschiedene Variable, $a_1, \dots, a_m \in A$

$$\mathfrak{I}\frac{a_1 \dots a_m}{x_1 \dots x_m} := (\mathfrak{A}, \beta\frac{a_1 \dots a_m}{x_1 \dots x_m}),$$

wobei $\beta\frac{a_1 \dots a_m}{x_1 \dots x_m}$ die Belegung in $\mathfrak{A}$ ist mit

$$\beta\frac{a_1 \dots a_m}{x_1 \dots x_m}(y) := \begin{cases} a_i & y = x_i \\ \beta(y) & y \neq x_1, \dots, y \neq x_m \end{cases}$$

also für Terme $t_1, \dots, t_m$:

$$\mathfrak{I}\frac{\mathfrak{I}(t_1) \dots \mathfrak{I}(t_m)}{x_1 \dots x_m}(y) = \begin{cases} \mathfrak{I}(t_i) & y = x_i \\ \mathfrak{I}(y) & y \neq x_1, \dots, y \neq x_m \end{cases}$$

Eine Abbildung

$$\sigma : V \to T^S$$

ist eine Substitution, wenn $\{x \mid \sigma(x) \neq x\}$ endlich ist.

Ist dann $\{x \mid \sigma(x) \neq x\} \subseteq \{x_1, \ldots, x_m\}$ mit paarweise verschiedenen x_i und ist $\sigma(x_1) = t_1, \ldots, \sigma(x_m) = t_m$, so schreiben wir für σ auch

$$\frac{t_1 \ldots t_m}{x_1 \ldots x_m}.$$

Ist $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine S-Interpretation und σ eine Substitution, so sei

$$\mathfrak{I}^\sigma := (\mathfrak{A}, \mathfrak{I} \circ \sigma).$$

Somit:

Ist $\sigma(x) = t$, so $\mathfrak{I}^\sigma(x) = \mathfrak{I} \circ \sigma(x) = \mathfrak{I}(t)$.

Ist $\sigma(x) = x$, so $\mathfrak{I}^\sigma(x) = \mathfrak{I} \circ \sigma(x) = \mathfrak{I}(x)$.

Ist daher $\sigma = \dfrac{t_1 \ldots t_m}{x_1 \ldots x_m}$, so $\mathfrak{I}^\sigma = \mathfrak{I}\dfrac{\mathfrak{I}(t_1) \ldots \mathfrak{I}(t_m)}{x_1 \ldots x_m}$.

Mit ι bezeichnen wir die identische Substitution, d.h. für alle Variable x gilt

$$\iota(x) = x.$$

$$
\begin{aligned}
t = x: &\qquad t^\sigma := \sigma(x) \\
t = c: &\qquad t^\sigma := c \\
t = f(t_1, \ldots, t_n): &\qquad t^\sigma := f(t_1^\sigma, \ldots, t_n^\sigma)
\end{aligned}
$$

$$
\begin{aligned}
\varphi = t_1 \equiv t_2: &\qquad \varphi^\sigma := t_1^\sigma \equiv t_2^\sigma \\
\varphi = Rt_1 \ldots t_n: &\qquad \varphi^\sigma := Rt_1^\sigma \ldots t_n^\sigma \\
\varphi = \neg\psi: &\qquad \varphi^\sigma := \neg\, \psi^\sigma \\
\varphi = (\psi \vee \chi): &\qquad \varphi^\sigma := (\psi^\sigma \vee \chi^\sigma)
\end{aligned}
$$

$\varphi = \exists x \psi$:

$$\varphi^{\sigma} := \exists u \left[\psi \frac{\sigma(y_1) \quad \ldots \quad \sigma(y_r) \quad u}{y_1 \quad \ldots \quad y_r \quad x}\right]$$

Dabei sind $y_1, \ldots, y_r$ paarweise verschieden mit

$$\{y_1, \ldots, y_r\} \quad := \quad \{y \mid y \in \mathrm{fr}(\exists x \psi) \text{ und } y \neq \sigma(y)\}$$

und

$$u := \begin{cases} x, & \text{falls } x \notin \mathrm{var}(\sigma(y_1)) \cup \ldots \cup \mathrm{var}(\sigma(y_r)) \\ \text{die erste Variable, die in} & \\ \psi, \sigma(y_1), \ldots, \sigma(y_r) \text{ nicht vorkommt,} & \text{sonst.} \end{cases}$$

Bemerkung.

$$y \in \mathrm{var}(t\frac{t_1 \dots t_r}{x_1 \dots x_r}) \iff \begin{array}{l}(y \in \mathrm{var}(t) \text{ und } y \neq x_1, \dots, y \neq x_r) \text{ oder} \\ \text{es gibt } i \in [r]\text{: } (x_i \in \mathrm{var}(t) \text{ und } y \in \mathrm{var}(t_i)).\end{array}$$

$$y \in \mathrm{fr}(\varphi\frac{t_1 \dots t_r}{x_1 \dots x_r}) \iff \begin{array}{l}(y \in \mathrm{fr}(\varphi) \text{ und } y \neq x_1, \dots, y \neq x_r) \text{ oder} \\ \text{es gibt } i \in [r]\text{: } (x_i \in \mathrm{fr}(\varphi) \text{ und } y \in \mathrm{var}(t_i)).\end{array}$$

Insbesondere: Ist $\varphi = \varphi(x_1, \dots, x_r)$, so ist für Konstantensymbole $c_1, \dots, c_r$

$$\varphi\frac{c_1 \dots c_r}{x_1 \dots x_r} \text{ ein Satz.}$$

1. $\neg\exists x\psi \equiv \forall x\neg\psi, \qquad \neg\forall x\psi \equiv \exists x\neg\psi$

2. $(\exists x\varphi\vee\psi) \equiv \exists y(\varphi\frac{y}{x}\vee\psi)$, wenn $y \notin \mathrm{fr}(\{\exists x\varphi, \psi\})$
   insbesondere $(\exists x\varphi\vee\psi) \equiv \exists x(\varphi\vee\psi)$, wenn $x \notin \mathrm{fr}(\psi)$
   $(\varphi\vee\exists x\psi) \equiv \exists y(\varphi\vee\psi\frac{y}{x})$, wenn $y \notin \mathrm{fr}(\{\varphi, \exists x\psi\})$
   $(\forall x\varphi\vee\psi) \equiv \forall y(\varphi\frac{y}{x}\vee\psi)$, wenn $y \notin \mathrm{fr}(\{\forall x\varphi, \psi\})$
   $(\varphi\vee\forall x\psi) \equiv \forall y(\varphi\vee\psi\frac{y}{x})$, wenn $y \notin \mathrm{fr}(\{\varphi, \forall x\psi\})$.

Beispiel: Sei

$$\varphi = (\neg\exists z Pxyz \vee \forall x\exists y Rxy).$$

Dann

$$\begin{aligned}
(\neg\exists z Pxyz \vee \forall x\exists y Rxy) &\overset{1}{\equiv} (\forall z\neg Pxyz \vee \forall x\exists y Rxy)\\
&\overset{2}{\equiv} \forall z(\neg Pxyz \vee \forall x\exists y Rxy)\\
&\overset{2}{\equiv} \forall z\forall u(\neg Pxyz \vee \exists y Ruy)\\
&\overset{2}{\equiv} \forall z\forall u\exists v(\neg Pxyz \vee Ruv).
\end{aligned}$$

Seien x, y gegeben und gelte für ein geeignetes u

$$xRu \text{ und } yRu.$$

Aus (s) erhalten wir dann

$$uRx \text{ und } uRy.$$

Aus xRu und uRy ergibt sich mit (t)

$$xRy, \tag{5}$$

und aus yRu und uRx, ebenfalls mit (t),

$$yRx. \tag{6}$$

Sei nun z beliebig gewählt. Gilt

$$xRz, \tag{7}$$

so erhalten wir aus (2) und (3) mit (t)

$$yRz.$$

Gilt umgekehrt

$$yRz, \tag{8}$$

so erhalten wir aus (1) und (4) mit (t) $\qquad xRz.$

(∃A) $\dfrac{\Gamma\, \varphi\frac{y}{x}\, \psi}{\Gamma\, \exists x\varphi\, \psi}$ $y \notin \mathrm{fr}(\Gamma, \exists x\varphi, \psi)$ ist korrekt:

Beweis: Gelte

$$\Gamma, \varphi\frac{y}{x} \models \psi \tag{9}$$

und sei $\mathfrak{I} \models \Gamma$ und $\mathfrak{I} \models \exists x\varphi$, wobei $\mathfrak{I} = (\mathfrak{A}, \beta)$ (z.z.: $\mathfrak{I} \models \psi$). Dann

$$\text{ex. } a \in A\text{: } \mathfrak{I}\frac{a}{x} \models \varphi.$$

Ist $y \neq x$, so $y \notin \mathrm{fr}(\varphi)$ nach Vor. $y \notin \mathrm{fr}(\exists x\varphi)$; somit nach Koinzidenzlemma

$$\text{ex. } a \in A\text{: } (\mathfrak{I}\frac{a}{x})\frac{a}{y} \models \varphi$$

(für $y = x$ gilt dies trivialerweise). Somit

$$\text{ex. } a \in A\text{: } (\mathfrak{I}\frac{a}{y})\frac{\mathfrak{I}\frac{a}{y}(y)}{x} \models \varphi.$$

Daher nach Substitutionslemma

$$\text{ex. } a \in A\text{: } \mathfrak{I}\frac{a}{y} \models \varphi\frac{y}{x}.$$

Da $\mathfrak{I}\frac{a}{y} \models \Gamma$ (weil $y \notin \mathrm{fr}(\Gamma)$), gilt mit (9) $\mathfrak{I}\frac{a}{y} \models \psi$ und daher $\mathfrak{I} \models \psi$ (weil $y \notin \mathrm{fr}(\psi)$).

$\vdash (\varphi \vee \neg\varphi)$

1.	φ	φ	(Vor)
2.	φ	$(\varphi \vee \neg\varphi)$	$(\vee S)$ auf 1
3.	$\neg\varphi$	$\neg\varphi$	(Vor)
4.	$\neg\varphi$	$(\varphi \vee \neg\varphi)$	$(\vee S)$ auf 3
5.		$(\varphi \vee \neg\varphi)$	(FU) auf 2,4

Rechtfertigung für (Wid'):

1. $\Gamma\,\psi$ (Prämisse)
2. $\Gamma\,\neg\psi\,\neg\varphi\,\psi$ (Ant) auf 1
3. $\Gamma\,\neg\psi\,\neg\varphi\,\neg\psi$ (Vor)
4. $\Gamma\,\neg\psi\,\varphi$ (Wid) auf 2,3

Rechtfertigung für (KS):

1. $\Gamma\,\varphi\,\psi$ (Prämisse)
2. $\Gamma\,\varphi$ (Prämisse)
3. $\Gamma\,\neg\varphi\,\psi$ (Wid') auf 2
4. $\Gamma\,\psi$ (FU) auf 1,3

Rechtfertigung für (MP):

1.	$\Gamma\,(\neg\varphi \vee \psi)$	(Prämisse)
2.	$\Gamma\,\varphi$	(Prämisse)
3.	$\Gamma\,\neg\varphi\,\psi$	(Wid') auf 2
4.	$\Gamma\,\psi\,\psi$	(Vor)
5.	$\Gamma\,(\neg\varphi \vee \psi)\,\psi$	($\vee$A) auf 3,4
6.	$\Gamma\,\psi$	(KS) auf 5,1

1.	$\Gamma\psi_1$	(Prämisse)
	$\vdots$	
n.	$\Gamma\psi_n$	(Prämisse)
$n+1$.	$\psi_1 \ldots \psi_n\varphi$	(Prämisse)(!)
$n+2$.	$\Gamma\psi_1 \ldots \psi_n\varphi$	(Ant) auf $n+1$
$n+3$.	$\Gamma\psi_1 \ldots \psi_{n-1}\psi_n$	(Ant) auf n
$n+4$.	$\Gamma\psi_1 \ldots \psi_{n-1}\varphi$	(KS) auf $n+2$, $n+3$
$n+5$.	$\Gamma\psi_1 \ldots \psi_{n-2}\psi_{n-1}$	(Ant) auf $n-1$
$n+6$.	$\Gamma\psi_1 \ldots \psi_{n-2}\varphi$	(KS) auf $n+4$, $n+5$
	$\vdots$	
	$\Gamma\varphi$	

$\vdash t_1 \equiv t_2\ t_2 \equiv t_1$

Wähle x neu:

1. $t_1 \equiv t_1$ (≡S)
2. $t_1 \equiv t_2\ t_2 \equiv t_1$ (≡A) auf 1, da $t_1 \equiv t_1 = [x \equiv t_1]\frac{t_1}{x}$ und $t_2 \equiv t_1 = [x \equiv t_1]\frac{t_2}{x}$

$\vdash t_1 \equiv t_2\ t_2 \equiv t_3\ t_1 \equiv t_3$

Wähle x neu:

1. $t_1 \equiv t_2\ t_1 \equiv t_2$ (Vor)
2. $t_1 \equiv t_2\ t_2 \equiv t_3\ t_1 \equiv t_3$ (≡A) auf 1, da $t_1 \equiv t_2 = [t_1 \equiv x]\frac{t_2}{x}$ und $t_1 \equiv t_3 = [t_1 \equiv x]\frac{t_3}{x}$

$\vdash Rt_1 \ldots t_r\ t_1 \equiv t_1' \ldots t_r \equiv t_r'\ Rt_1' \ldots t_r'$

Wähle $x_1, \ldots, x_r$ neu:

1. $Rt_1 \ldots t_r\ Rt_1 \ldots t_r$ (Vor)
2. $Rt_1 \ldots t_r\ t_1 \equiv t_1' \ldots t_r \equiv t_r'\ Rt_1' \ldots t_r'$ (≡S) auf 1, da $Rt_1 \ldots t_r = [Rx_1 \ldots x_r]\frac{t_1 \ldots t_r}{x_1 \ldots x_r}$ und $Rt_1' \ldots t_r' = [Rx_1 \ldots x_r]\frac{t_1' \ldots t_r'}{x_1 \ldots x_r}$

$\Phi \subseteq L^S$. $\sim\, \subseteq T^S \times T^S$ $\;(\sim_\Phi)\;$ sei gegeben durch

$$t{\sim}t' \quad \text{gdw} \quad \Phi \vdash t \equiv t'.$$

§ 8, Folg. aus Bem 2:

$$\text{Wenn} \vdash \varphi_1 \ldots \varphi_n \psi \text{ und } \Phi \vdash \varphi_i \text{ für } i \in [n], \text{ so } \Phi \vdash \psi.$$

Beweis: $\sim$ reflexiv: $t \sim t$, da $\vdash t \equiv t$ und somit $\Phi \vdash t \equiv t$.

$\sim$ symmetrisch: Gelte $t_1 \sim t_2$; somit $\Phi \vdash t_1 \equiv t_2$. Wegen $\vdash t_1 \equiv t_2\, t_2 \equiv t_1$ und § 8, Folg. aus Bem 2: $\Phi \vdash t_2 \equiv t_1$; somit $t_2 \sim t_1$.

$\sim$ transitiv: Gelte $t_1 \sim t_2$ und $t_2 \sim t_3$; somit $\Phi \vdash t_1 \equiv t_2$ und $\Phi \vdash t_2 \equiv t_3$. Wegen $\vdash t_1 \equiv t_2\, t_2 \equiv t_3\, t_1 \equiv t_3$ und § 8, Folg. aus Bem 2: $\Phi \vdash t_1 \equiv t_3$; somit $t_1 \sim t_3$.

2 (ii): Nach Vor.

$$\Phi \vdash t_1 \equiv t_1', \ldots, \Phi \vdash t_r \equiv t_r'.$$

Nach § 8:

$$\vdash Rt_1 \ldots t_r\, t_1 \equiv t_1' \ldots t_r \equiv t_r'\, Rt_1' \ldots t_r'.$$

Wenn also $\Phi \vdash Rt_1 \ldots t_r$, so nach § 8, Folg. aus Bem 2: $\Phi \vdash Rt_1' \ldots t_r'$.

Lemma 3. Sei $\mathfrak{I} = (\mathfrak{A}, \beta)$ eine Interpretation mit

$$A = \{\mathfrak{I}(t) \mid t \in T^S\}. \tag{10}$$

Dann

$$\mathfrak{I} \models \exists x_1 \ldots \exists x_n \varphi \iff \text{ex. } t_1, \ldots, t_n \in T^S\colon \mathfrak{I} \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}$$

$$\mathfrak{I} \models \forall x_1 \ldots \forall x_n \varphi \iff \text{f.a. } t_1, \ldots, t_n \in T^S\colon \mathfrak{I} \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}.$$

Beachte: (10) ist für jede Henkininterpretation erfüllt.

Beweis: Es gilt

$$\begin{aligned}
\mathfrak{I} \models \exists x_1 \ldots \exists x_n \varphi \quad & \iff \quad \text{ex } a_1, \ldots, a_n \in A: \ \mathfrak{I}\frac{a_1 \ldots a_n}{x_1 \ldots x_n} \models \varphi \\
& \overset{\text{(Vor.)}}{\iff} \quad \text{ex } t_1, \ldots, t_n \in T^S : \ \mathfrak{I}\frac{\mathfrak{I}(t_1) \ldots \mathfrak{I}(t_n)}{x_1 \ldots x_n} \models \varphi \\
& \overset{\text{(SL)}}{\iff} \quad \text{ex } t_1, \ldots, t_n \in T^S : \ \mathfrak{I} \models \varphi \frac{t_1 \ldots t_n}{x_1 \ldots x_n}.
\end{aligned}$$

Lemma 5. S höchstens abzählbar, $\mathrm{fr}(\Phi)$ endlich, Wf Φ. Dann

$$\text{ex. } \Psi\big(\Phi \subseteq \Psi \subseteq L^S, \text{ Wf } \Psi \text{ und } \Psi \text{ enthält Beispiele}\big).$$

Lemma 6. S höchstens abzählbar, Wf Ψ. Dann

$$\text{ex. } \Theta\big(\Psi \subseteq \Theta \subseteq L^S, \text{ Wf } \Theta \text{ und } \Theta \text{ negationstreu}\big).$$

Folgerung. S höchstens abzählbar, $\mathrm{fr}(\Phi)$ endlich, Wf Φ. Dann

$$\text{Erf } \Phi \text{ und } \Phi \text{ hat ein Modell mit höchstens abzählbarem Träger.}$$

Hilfssatz. Wf Φ, $\exists x\psi \in L^S$, $y \notin \mathrm{fr}(\Phi \cup \{\exists x\psi\}$. Dann

$$\text{Wf } \Phi \cup \{(\exists x\psi \rightarrow \psi\frac{y}{x})\}.$$

Zunächst definieren wir ψ^* für Ausdrücke der Gestalt $t \equiv x$ durch Induktion über t:

$$\begin{aligned}
y \equiv x^* \quad &:= \quad y \equiv x \\
c \equiv x^* \quad &:= \quad c \equiv x \\
f(t_1, \ldots, t_n) \equiv x^* \quad &:= \quad \exists x_1 \ldots \exists x_n (t_1 \equiv x_1{}^* \wedge \ldots \wedge t_n \equiv x_n{}^* \wedge f(x_1, \ldots, x_n) \equiv x)
\end{aligned}$$

($x_1, \ldots, x_n$ neu, etwa die ersten n Variablen, die in $f(t_1, \ldots, t_n) \equiv x$ nicht vorkommen).

Induktion über ψ für alle anderen ψ:

$\psi = t_1 \equiv t_2$ und t_2 keine Variable:

$$t_1 \equiv t_2{}^* \quad := \quad \exists x (t_1 \equiv x^* \wedge t_2 \equiv x^*) \quad x \text{ neu (s.o.).}$$

$$Rt_1 \ldots t_n{}^* \quad := \quad \exists x_1 \ldots \exists x_n (t_1 \equiv x_1{}^* \wedge \ldots \wedge t_n \equiv x_n{}^* \wedge Rx_1 \ldots x_n) \quad x_1, \ldots, x_n \text{ neu (s.o.).}$$

$$\neg\varphi^* := \neg\, \varphi^*, \qquad (\varphi_1 \vee \varphi_2)^* := (\varphi_1^* \vee \varphi_2^*), \qquad \exists x \varphi^* := \exists x\, \varphi^*$$

$$\Phi_I := \{\exists x \varphi_{S_1}(x)\} \ \cup \ \{\exists^{=1} x(\varphi_{S_1}\frac{x}{x} \wedge \varphi_c(x)) \mid c \in S_1\} \ \cup \{\forall x_1 \ldots \forall x_n \Big((\varphi_{S_1}\frac{x_1}{x} \wedge \ldots \wedge \varphi_{S_1}\frac{x_n}{x}) \to \exists^{=1} y(\varphi_{S_1}\frac{y}{x} \wedge \varphi_f(x_1, \ldots, x_n, y))\Big) \mid n \geq 1,\ f \in S_1 \ n\text{-stellig}\}$$

Beachte: $\Phi_I \subseteq L_0^S$.

Falls $\varphi_{S_1}(x) = x \equiv x$, so $\Phi_I \approx \{\exists^{=1} x \varphi_c(x) \mid c \in S_1\} \cup$

$$\{\forall x_1 \ldots \forall x_n \exists^{=1} y \varphi_f(x_1, \ldots, x_n, y))\Big) \mid n \geq 1,\ f \in S_1 \ n\text{-stellig}\}$$

Falls $\varphi_{S_1}(x) = x \equiv x$ und S_1 relational, so $\Phi_I \approx \emptyset$.

Ist $\mathfrak{A}$ eine S-Struktur, $\mathfrak{A} \models \Phi_I$, so sei $\mathfrak{A}^{-I}$ die S_1-Struktur

- $A^{-I} := \{a \in A \mid \mathfrak{A} \models \varphi_{S_1}[a]\}$;
- für n-st. $R \in S_1$, $\bar{a} \in A^{-I}$: $\quad R^{A^{-I}}\bar{a} \iff \mathfrak{A} \models \varphi_R[\bar{a}]$;
- für n-st. $f \in S_1$, $\bar{a}, a \in A^{-I}$: $\quad f^{A^{-I}}(\bar{a}) = a \iff \mathfrak{A} \models \varphi_f[\bar{a}, a]$;
- für $c \in S$, $a \in A^{-I}$: $\quad c^{A^{-I}} = a$ gdw $\mathfrak{A} \models \varphi_c[a]$.

Wir definieren ψ^I für termreduziertes ψ (für nicht termreduziertes ψ setzen wir $\psi^I := (\psi^*)^I$):

ψ	ψ^I
$Ru_1 \dots u_n$	$\varphi_R \frac{u_1 \dots u_n}{x_1 \dots x_n}$
$x \equiv y$	$x \equiv y$
$c \equiv u$	$\varphi_c \frac{u}{x}$
$f(u_1, \dots, u_n) \equiv v$	$\varphi_f \frac{u_1 \dots u_n v}{x_1 \dots x_n y}$
$\neg\varphi$	$\neg\ \varphi^I$
$(\varphi_1 \vee \varphi_2)$	$(\varphi_1^I \vee \varphi_2^I)$
$\exists u\varphi$	$\exists u(\varphi_{S_1} \frac{u}{x} \wedge \varphi^I)$

$\psi(u_1,\ldots,u_m) := \exists u\varphi \qquad \psi^I := \exists u(\varphi_{S_1}\frac{u}{x} \wedge \varphi^I)$.

O.B.d.A. $u \neq u_1,\ldots,u \neq u_m$. Dann $\varphi = \varphi(u_1,\ldots,u_m,u)$ und nach Ind.vor.

$$(\varphi_{S_1}\frac{u}{x} \wedge \varphi^I) = (\varphi_{S_1}\frac{u}{x} \wedge \varphi^I)(u_1,\ldots,u_m,u)$$

Sei $\mathfrak{A}$ S-Struktur, $\mathfrak{A} \models \Phi_I$ und $a_1,\ldots,a_m \in A^{-I}$:

$$\begin{aligned}
\mathfrak{A} \models [\exists u\varphi]^I[a_1,\ldots,a_m] \quad &\text{gdw} \quad \mathfrak{A} \models \exists u(\varphi_{S_1}\frac{u}{x} \wedge \varphi^I)[a_1,\ldots,a_m] \\
&\text{gdw} \quad \text{ex. } a \in A\text{: } \mathfrak{A} \models (\varphi_{S_1}\tfrac{u}{x} \wedge \varphi^I)[a_1,\ldots,a_m,a] \\
&\underset{\text{SL}}{\text{gdw}} \quad \text{ex. } a \in A\ (\mathfrak{A} \models \varphi_{S_1}[a] \text{ und } \mathfrak{A} \models \varphi^I[a_1,\ldots,a_m,a]) \\
&\underset{\text{IV. auf } \varphi}{\text{gdw}} \quad \text{ex. } a \in A\ (a \in A^{-I} \text{ und } \mathfrak{A}^{-I} \models \varphi[a_1,\ldots,a_m,a]) \\
&\text{gdw} \quad \text{ex. } a \in A^{-I} : \mathfrak{A}^{-I} \models \varphi[a_1,\ldots,a_m,a] \\
&\text{gdw} \quad \mathfrak{A}^{-I} \models \exists u\varphi[a_1,\ldots,a_m].
\end{aligned}$$

(P1) $\forall x \neg \underline{\sigma}(x) \equiv x$

(P2) $\forall x \forall y (\underline{\sigma}(x) \equiv \underline{\sigma}(y) \rightarrow x \equiv y)$

(P3) $\forall X((X0 \land \forall y(Xy \rightarrow X\underline{\sigma}(y))) \rightarrow \forall z Xz)$

1. Ziel: Jede mathematische Aussage läßt sich in einer für das Universum geeigneten Sprache der ersten Stufe wiedergeben (symbolisieren).

Erfahrungstatsache 1: Es ist möglich, die ganze Vielfalt der Objekte des "mathematischen Universums" auf den Mengenbegriff zurückzuführen: Man kann annehmen, das Universum besteht nur aus Mengen.

Erfahrungstatsache 2: Jede mathematische Aussage läßt sich als Aussage über die Gesamtheit der Mengen auffassen und in $L^{\{\underline{\in}\}}$ symbolisieren.

2. Ziel: Jeder mathematische Beweis läßt sich mit den Regeln des Sequenzenkalküls nachvollziehen.

Erfahrungstatsache 3: Die Eigenschaften des Universums, die Mathematiker/innen verwenden, sind in ZFC, ZFC $\subseteq L_0^{\{\epsilon\}}$, "enthalten" und die Mathematiker/innen akzeptieren die Eigenschaften von ZFC.

Erfahrungstatsache 4: Für $\varphi \in L_0^{\{\epsilon\}}$ gilt:

$$\mathrm{ZFC} \vdash \varphi \quad \Longleftrightarrow \quad \varphi \text{ ist Symbolisierung einer mathematisch beweisbaren Aussage.}$$

Extensionalitätsaxiom: φ_{EXT} : $\forall x \forall y (\forall z (z \underline{\in} x \leftrightarrow z \underline{\in} y) \rightarrow x \equiv y)$

Paarmengenaxiom: φ_{PAAR} : $\forall x \forall y \exists z \forall w (w \underline{\in} z \leftrightarrow (w \equiv x \vee w \equiv y))$

Vereinigungsmengenaxiom: φ_{VER} : $\forall x \exists y \forall z (z \underline{\in} y \leftrightarrow \exists w (w \underline{\in} x \wedge z \underline{\in} w))$

Potenzmengenaxiom: φ_{POT} : $\forall x \exists y \forall z (z \underline{\in} y \leftrightarrow \forall w (w \underline{\in} z \rightarrow w \underline{\in} x))$

Schema der Aussonderung: Zu $n \geq 0$, $\psi \in L_{n+1}^{\{\underline{\in}\}}$ das Axiom
$(x = v_{n+1}, y = v_{n+2}, z = v_{n+3})$

$$\varphi_{\text{AUS}(\psi)} : \quad \forall v_1 \ldots \forall v_n \forall y \exists z \forall x (x \underline{\in} z \leftrightarrow (x \underline{\in} y \wedge \psi(\bar{v}, x)))$$

Schema der Ersetzung: Zu $n \geq 0$, $\psi \in L_{n+2}^{\{\underline{\in}\}}$ das Axiom
$(x = v_{n+1}, y = v_{n+2}, u = v_{n+3}, v = v_{n+4})$

$$\varphi_{\text{ERS}(\psi)} : \quad \forall v_1 \ldots \forall v_n (\forall x \exists^{=1} y\, \psi(\bar{v}, x, y) \rightarrow \forall u \exists v \forall y (y \underline{\in} v \leftrightarrow \exists x (x \underline{\in} u \wedge \psi(\bar{v}, x, y))))$$

Unendlichkeitsaxiom: φ_{INF} : $\exists x (\underline{\emptyset} \,\underline{\in}\, x \wedge \forall y (y \underline{\in} x \rightarrow y \,\underline{\cup}\, \underline{\{} y \underline{\}} \,\underline{\in}\, x))$

Auswahlaxiom: φ_{AC}

$$\forall x((\neg \underline{\emptyset} \underline{\in} x \wedge \\ \forall u \forall v((u \underline{\in} x \wedge v \underline{\in} x \wedge \neg u \equiv v) \rightarrow u \underline{\cap} v \equiv \underline{\emptyset})) \rightarrow \exists y \forall w(w \underline{\in} x \rightarrow \exists^{=1} z\, z \underline{\in} w \underline{\cap} y))$$

SYNTAX: 1) A l p h a b e t. Zusätzliche Zeichen:

für $n \geq 1$, n-stellige Relationsvariable: $V_1^n, V_2^n, \ldots$ $\qquad$ $X^n, Y^n, X, Y, \ldots$

($n = 1$: Mengenvariable)

für $n \geq 1$, n-stellige Funktionssvariable: $h_1^n, h_2^n, \ldots$ $\qquad$ $h^n, h, \ldots$

2) T e r m k a l k ü l. Zusätzliche Regel:

$$\frac{t_1, \ldots, t_n}{h^n(t_1, \ldots, t_n)}$$

3) A u s d r u c k s k a l k ü l. Zusätzliche Regeln:

$$\frac{}{X^n t_1 \ldots t_n}, \qquad \frac{\varphi}{\exists X \varphi} \qquad \frac{\varphi}{\exists h \varphi}$$

T_{II}^S Menge der S-Terme der 2. Stufe

L_{II}^S Menge der S-Ausdrücke der 2. Stufe

Abkürzungen wie früher:

$$
\begin{array}{rcl}
(\varphi \rightarrow \psi) & \text{für} & (\neg\varphi \vee \psi) \\
(\varphi \leftrightarrow \psi) & \text{für} & (\neg(\varphi \vee \psi) \vee \neg(\neg\varphi \vee \neg\psi)) \\
(\varphi \wedge \psi) & \text{für} & \neg(\neg\varphi \vee \neg\psi) \\
\forall x\varphi & \text{für} & \neg\exists x\neg\varphi \\
\forall X\varphi & \text{für} & \neg\exists X\neg\varphi \\
\forall h\varphi & \text{für} & \neg\exists h\neg\varphi
\end{array}
$$

SEMANTIK: Eine S-Interpretation der 2. Stufe

$$\mathfrak{I} = (\mathfrak{A}, \gamma)$$

besteht aus einer S-Struktur $\mathfrak{A}$ und einer Belegung zweiter Stufe γ.

Eine Belegung zweiter Stufe γ in der Struktur $\mathfrak{A}$ ordnet zu:

$$\begin{aligned} x \mapsto \gamma(x) &\quad \text{mit} \quad \gamma(x) \in A \\ h^n \mapsto \gamma(h^n) &\quad \text{mit} \quad \gamma(h^n) : A^n \to A \\ X^n \mapsto \gamma(X^n) &\quad \text{mit} \quad \gamma(X^n) \subseteq A^n. \end{aligned}$$

Für $t \in T_{\mathrm{II}}^S$ wird $\mathfrak{I}(t)$ mit $\mathfrak{I}(t) \in A$ durch Induktion über den Termkalkül wie früher definiert mit der zusätzlichen Festlegung:

$$\mathfrak{I}(h^n(t_1, \ldots, t_n)) := \gamma(h^n)(\mathfrak{I}(t_1), \ldots, \mathfrak{I}(t_n)).$$

M o d e l l b e z i e h u n g. Für $\varphi \in L_{\mathrm{II}}^{S}$ wird $\mathfrak{I} \models \varphi$ ($\mathfrak{I}$ ist ein Modell von φ) durch Induktion über den Ausdruckskalkül wie früher definiert mit den zusätzlichen Festlegungen:

$$\mathfrak{I} \models X^n t_1 \dots t_n \iff \beta(X^n)\mathfrak{I}(t_1) \dots \mathfrak{I}(t_n);$$

$$\mathfrak{I} \models \exists X^n \varphi \iff \text{ex. } n\text{-stellige Relation } \mathcal{R} \text{ auf } A\text{: } \mathfrak{I}\frac{\mathcal{R}}{X^n} \models \varphi.$$

$$\mathfrak{I} \models \exists h^n \varphi \iff \text{ex. } n\text{-stellige Funktion } \mathfrak{f} \text{ auf } A\text{: } \mathfrak{I}\frac{\mathfrak{f}}{h^n} \models \varphi.$$

Für $\varphi \in L_{\mathrm{II}}^S$ sei $\mathrm{fr}(\varphi)$ die Menge der in φ frei vorkommenden (Individuen)Variable, Funktions- und Relationsvariable.

φ ist ein Satz: $\quad \mathrm{fr}(\varphi) = \emptyset$.

Es gilt das Analogon des Koinzidenzlemmas, insbesondere:

$$\text{wenn } \gamma_1 \restriction \mathrm{fr}(\varphi) = \gamma_2 \restriction \mathrm{fr}(\varphi), \text{ so} \qquad (\mathfrak{A}, \gamma_1) \models \varphi \iff (\mathfrak{A}, \gamma_2) \models \varphi$$

Für einen Satz φ ist daher $\mathfrak{A} \models \varphi$ sinnvoll.

Es gilt das Analogon des Isomorphielemmas, insbesondere:

$$\text{Ist } \varphi \text{ ein Satz, } \mathfrak{A} \models \varphi \text{ und } \mathfrak{A} \cong \mathfrak{B}, \text{ so } \mathfrak{B} \models \varphi.$$

$A \sim B$, A und B sind gleichmächtig:

$$\text{existiert } f : A \longrightarrow B \text{ bijektiv}$$

Existieren $L_{\mathrm{II}}^{\emptyset}$-Sätze

$$\varphi_{\mathrm{endl}},\ \varphi_{\sim\mathbb{N}},\ \varphi_{\sim\mathbb{R}}$$

und $L_{\mathrm{II}}^{\emptyset}$-Ausdrücke

$$\psi_{\mathrm{endl}}(Z), \psi_{\sim\mathbb{N}}(Z), \psi_{\sim\mathbb{R}}(Z) \qquad (Z \text{ einstellig})$$

mit: Für alle S und alle S-Interpretationen $\mathfrak{I} = (\mathfrak{A}, \gamma)$ zweiter Stufe:

$$\begin{array}{lrll}
a) & \mathfrak{A} \models \varphi_{\mathrm{endl}} & \text{gdw} & A \text{ endlich} \\
b) & \mathfrak{A} \models \varphi_{\sim\mathbb{N}} & \text{gdw} & A \sim \mathbb{N} \\
c) & \mathfrak{A} \models \varphi_{\sim\mathbb{R}} & \text{gdw} & A \sim \mathbb{R} \\
d) & (\mathfrak{A}, \gamma) \models \psi_{\mathrm{endl}}(Z) & \text{gdw} & \gamma(Z) \text{ endlich} \\
e) & (\mathfrak{A}, \gamma) \models \psi_{\sim\mathbb{N}}(Z) & \text{gdw} & \gamma(Z) \sim \mathbb{N} \\
f) & (\mathfrak{A}, \gamma) \models \psi_{\sim\mathbb{R}}(Z) & \text{gdw} & \gamma(Z) \sim \mathbb{R}.
\end{array}$$

$$\varphi_{\text{endl}} := \text{“Jede injektive Funktion ist surjektiv”}$$
$$= \forall h\Big(\forall x\forall y(h(x) \equiv h(y) \to x \equiv y) \to \forall y\exists x h(x) \equiv y)\Big)$$

$$\psi_{\text{endl}}(Z) := \text{“Jede injektive Funktion auf } Z \text{ ist surjektiv”}$$
$$= \forall h\Big(\big(\forall x(Zx \to Zh(x)) \land \forall x\forall y((Zx \land Zy \land h(x) \equiv h(y)) \to x \equiv y)\big)$$
$$\to \forall y(Zy \to \exists x(Zx \land h(x) \equiv y))\Big)$$

$$\varphi_P := \text{“(P1)} \land \text{(P2)} \land \text{(P3)”} = \forall x\neg\underline{\sigma}(x) \equiv 0 \land \forall x\forall y(\underline{\sigma}(x) \equiv \underline{\sigma}(y) \to x \equiv y)$$
$$\land \forall X((X0 \land \forall y(Xy \to X\underline{\sigma}(y))) \to \forall y Xy)$$

$$\varphi_{\sim\mathbb{N}} := \exists z\exists h\text{“}\varphi_P\frac{hz}{\underline{\sigma}0}\text{''} = \exists z\exists h\forall x\neg h(x) \equiv z \land \forall x\forall y(h(x) \equiv h(y) \to x \equiv y)$$
$$\land \forall X((Xz \land \forall y(Xy \to Xh(y))) \to \forall y Xy)$$

$\psi_{\sim\mathbb{N}}(Z) :=$ "es gibt eine zu $(\mathbb{N}, \sigma, 0)$ isomorphe Struktur mit Träger Z"

Zu b): Aufzählungsverfahren: Für $n = 1, 2, \ldots$ stelle man die ersten n Terme und Ausdrücke her in der lexikographischen Reihenfolge und bilde die endlich vielen Ableitungen einer Länge $\leq n$, die nur diese Ausdrücke und Terme verwenden und aus höchstens n-gliedrigen Sequenzen bestehen.

Zu c): Setze Aufzählungsverfahren $\mathfrak{V}_1$ für Φ und $\mathfrak{V}_2$ für $\{\Gamma\varphi \mid \vdash \Gamma\varphi\}$ in Gang.

Für $n = 1, 2 \ldots$: Sind nach n Schritten von $\mathfrak{V}_1$ ausgegeben

$$\psi_1, \ldots, \psi_k$$

und von $\mathfrak{V}_2$ ausgegeben

$$\Gamma_1\varphi_1, \ldots, \Gamma_\ell\varphi_\ell,$$

so prüfe für $i = 1, \ldots, \ell$, ob

$$\Gamma_i \subseteq \{\psi_1, \ldots, \psi_k\}$$

und gib ggf. φ_i aus.

(1) $k\ R_i \leftarrow R_i + a$ $\qquad (k, i \in \mathbb{N},\ a \in \Sigma)$

Verlängerungsanwsg.: Füge a an Wort in R_i.

(2) $k\ R_i \leftarrow [R_i)$ $\qquad (k, i \in \mathbb{N})$

Verkürzungsanwsg: Streiche letzten Buchstaben in R_i; falls λ in R_i, so bleibt λ in R_i.

(3) $k\ R_i = [R_i)a \Rightarrow \ell; m$ $\qquad (k, i, \ell, m \in \mathbb{N},\ a \in \Sigma)$

Sprunganwsg.: Falls Wort in R_i mit a endet, gehe zu Zeile mit der Nummer ℓ sonst zur Zeile m.

(4) k PRINT R_i $\qquad (k, i \in \mathbb{N})$

Druckanwsg: Drucke Wort in R_i.

(5) k HALT $\qquad (k \in \mathbb{N})$

Halteanwsg: Halte.

P_0:

0 $R_0 \leftarrow R_0 + 1$

1 $R_2 \leftarrow R_2 + 1$

2 PRINT R_2

3 $R_2 = [R_2)| \Rightarrow 0; 1$

4 HALT

(2) (a) $\mathfrak{A}_P \models \psi_P$.

(b) Ist $\mathfrak{A}$ eine S-Struktur mit $\mathfrak{A} \models \psi_P$ und $(\ell, m_0, \ldots, m_n)$ die Konfiguration von P nach s Schritten, so $\mathfrak{A} \models R\overline{s}\overline{\ell}\overline{m_0}\ldots\overline{m_n}$ und $\overline{0}^{\mathfrak{A}}, \overline{1}^{\mathfrak{A}}, \ldots, \overline{s}^{\mathfrak{A}}$ sind paarweise verschieden.

$$\psi_P := \psi_O \wedge R\bar{0}\ldots\bar{0} \wedge \psi_{\alpha_0} \wedge \ldots \wedge \psi_{\alpha_{k-1}}$$

$$\begin{aligned}\psi_O \quad := \quad & \text{“}\leq \text{ Ordnung mit kleinsten Element } \bar{0}\text{”} \wedge \\ & \forall x(x \leq f(x) \wedge \forall x(\exists y\, x < y \to (x < f(x) \wedge \forall z(x < z \to f(x) \leq z)))\end{aligned}$$

$$\alpha : \ \ell\, R_i \leftarrow R_i + |$$

$$\psi_\alpha \quad := \quad \forall x \forall y_0 \ldots \forall y_n (Rx\bar{\ell}y_0 \ldots y_n \to (x < f(x) \wedge Rf(x)\overline{\ell + 1}y_0 \ldots y_{i-1} f(y_i) y_{i+1} \ldots y_n))$$

$$\alpha : \ \ell\, R_i \leftarrow [R_i)$$

$$\begin{aligned}\psi_\alpha \quad := \quad & \forall x \forall y_0 \ldots \forall y_n (Rx\bar{\ell}y_0 \ldots y_n \to (x < f(x) \wedge ((y_i \equiv \bar{0} \wedge Rf(x)\overline{\ell + 1}y_0 \ldots y_n) \vee \\ & (\neg y_i \equiv \bar{0} \wedge \exists u(f(u) \equiv y_i \wedge Rf(x)\overline{\ell + 1}y_0 \ldots y_{i-1} u y_{i+1} \ldots y_n)))))\end{aligned}$$

$$\alpha : \ \ell\, R_i \leftarrow [R_i)| \Rightarrow m_1; m_2$$

$$\begin{aligned}\psi_\alpha \quad := \quad & \forall x \forall y_0 \ldots \forall y_n (Rx\bar{\ell}y_0 \ldots y_n \to (x < f(x) \wedge \\ & ((\neg y_i \equiv \bar{0} \wedge Rf(x)\bar{m}_1 y_0 \ldots y_n) \vee (y_i \equiv \bar{0} \wedge Rf(x)\bar{m}_2 y_0 \ldots y_n))))\end{aligned}$$

$$\alpha : \ \ell\,\mathrm{PRINT}\,R_i$$

$$\psi_\alpha \quad := \quad \forall x \forall y_0 \ldots \forall y_n (Rx\bar{\ell}y_0 \ldots y_n \rightarrow (x < f(x) \wedge Rfx\overline{\ell + 1}y_0 \ldots y_n))$$

SYNTAX: Alphabet:

- Aussagenvariable: $p_1, p_2, \ldots$ $\qquad p, q, r, \ldots$
- Junktoren: $\neg, \vee$
- Hilfszeichen: $), ($

Ausdruckskalkül:

$$\frac{}{p_i} \qquad \frac{\alpha}{\neg\alpha} \qquad \frac{\alpha, \beta}{(\alpha \vee \beta)}$$

AA Menge der aussagenlogischen Ausdrücke. $\quad$ $\mathrm{AV} = \{p_1, p_2, \ldots\}$.

$\mathrm{var}(\alpha)$ Menge der Aussagenvariablen in α.

$\alpha(q_1, \ldots, q_n)$ bedeute $\mathrm{var}(\alpha) \subseteq \{q_1, \ldots, q_n\}$ und $q_1, \ldots, q_n$ paarweise verschieden.

$\mathrm{AA}_n = \{\alpha \mid \mathrm{var}(\alpha) \subseteq \{p_1, \ldots, p_n\}\}$.

SEMANTIK Aussagenlogische Belegung:

$$b : \mathrm{AV} \to \{W, F\}. \qquad\qquad b : \mathrm{AV} \to \{1, 0\}$$

Erweitern auf alle aussagenlogische Ausdrücke durch Vorschrift:

$$b(\neg\alpha) \quad := \begin{cases} W & \text{wenn } b(\alpha) = F \\ F & \text{wenn } b(\alpha) = W \end{cases} \qquad b(\alpha \vee \beta) \quad := \begin{cases} F & \text{wenn } b(\alpha) = b(\beta) = F \\ W & \text{sonst.} \end{cases}$$

Statt $b(\alpha) = 1$ auch $b \models \alpha$ oder $\alpha[b]$.

Koinz.lemma. Für Belegungen b, b': wenn $b \restriction \mathrm{var}(\alpha) = b' \restriction \mathrm{var}(\alpha)$ so $b(\alpha) = b'(\alpha)$.

Daher setzen wir für $\alpha = \alpha(q_1, \ldots, q_n)$ und $b_1, b_2, \ldots \in \{W, F\}$

$$\alpha[b_1, \ldots, b_n] := \alpha[b]$$

für eine (alle) Belegung(en) b mit $b(q_1) = b_1, \ldots,\ b(q_n) = b_n$.

Zum Zeitpunkt t ist P in genau einem Zustand:

$$\{q[t,\ell] \mid \ell \leq k\} \qquad t \leq t_0;$$

$$\{\neg q[t,\ell], \neg q[t,m]\} \qquad t \leq t_0,\ \ell, m \leq k,\ \ell \neq m.$$

Zum Zeitpunkt t enthält R_i an jeder Stelle genau einen Buchstaben aus $\Sigma \cup \{*\}$:

$$\{r_i[t,n,a] \mid a \in \Sigma \cup \{*\}\} \qquad i \in R_P,\ t \leq t_0,\ n \leq 2 \cdot t_0;$$

$$\{\neg r_i[t,n,a], \neg r_i[t,n,b]\} \qquad i \in R_P,\ t \leq t_0,\ n \leq 2 \cdot t_0,\ a, b \in \Sigma \cup \{*\},\ a \neq b.$$

Für $t = 0$ wird "P auf x angesetzt": $\{q[0,0]\}$

$$\{r_1[0,n,a_n]\} \qquad n < |x| \text{ (wobei } x = a_0 \dots a_{|x|-1});$$

$$\{r_1[0,n,*]\} \qquad |x| \leq n \leq 2 \cdot t_0;$$

$$\{r_i[0,n,*]\} \qquad i \in R_P, i \neq 1,\ n \leq 2 \cdot t_0;$$

Für $t = t_0$ steht P mit Antwort "ja": $\{q[t_0,k]\}$, $\{r_0[t_0,0,*]\}$.

Wenn "$\ell\ R_i = R_i + a$"$\in P$, so:

$\{\neg q[t,\ell], q[t+1,\ell+1]\}$ $t < t_0$;

$\{\neg q[t,\ell], \neg r_j[t,n,b], r_j[t+1,n,b]\}$ $t < t_0,\ n \leq 2 \cdot t_0,$
$j \in R_P, ((j \neq i,\ b \in \Sigma \cup \{*\})$ oder $(j = i, b \in \Sigma))$;

$\{\neg q[t,\ell], \neg r_i[t,0,*], r_i[t+1,0,a]\}$ $t < t_0$;

$\{\neg q[t,\ell], \neg r_i[t,n,b], \neg r_i[t,n+1,*], r_i[t+1,n+1,a]\}$ $t < t_0,\ n < 2 \cdot t_0, b \in \Sigma$;

$\{\neg q[t,\ell], \neg r_i[t,n,*], r_i[t,n+1,*], r_i[t+1,n+1,*]\}$ $t < t_0,\ n < 2 \cdot t_0$;

Wenn "$\ell\ R_i = [R_i)a \Rightarrow L; M$"$\in P$, so:

$\{\neg q[t,\ell], \neg r_i[t,n,a], \neg r_i[t,n+1,*]\} \cup \{q[t+1,\ell'] \mid \ell' \in L\}$ $t < t_0,\ n < 2 \cdot t_0$;

$\{\neg q[t,\ell], \neg r_i[t,n,b], \neg r_i[t,n+1,*]\} \cup \{q[t+1,m] \mid m \in M\}$ $t < t_0,\ n < 2 \cdot t_0,\ a \neq b \in \Sigma$

$\{\neg q[t,\ell], \neg r_i[t,0,*]\} \cup \{q[t+1,m] \mid m \in M\}$ $t < t_0$;

$\{\neg q[t,\ell], \neg r_j[t,n,b], r_j[t+1,n,b]\}$ $t < t_0,\ n \leq 2 \cdot t_0,\ i \in R_P,\ b \in \Sigma \cup \{*\}$.

Da "k HALT"$\in P$:

$$\{\neg q[t,k], \neg q[t+1,k]\} \quad t < t_0;$$

$$\{\neg q[t,k], \neg r_i[t,n,a], r_i[t+1,n,a]\} \quad t < t_0,\ n \leq 2 \cdot t_0,\ i \in R_P,\ b \in \Sigma \cup \{*\}.$$

$T \subseteq L_0^S$ Theorie: $\qquad$ ex. $\Phi \subseteq L_0^S$ (Erf Φ und $\Phi^{\models} = T$).

T Theorie, T R-axiomatisierbar: $\qquad$ ex. $\Phi \subseteq L_0^S$ (Φ R-entscheidbar und $\Phi^{\models} = T$).

Bemerkung. Eine R-axiomatisierbare Theorie ist R-aufzählbar.

$\Phi \subseteq L_0^S$, Φ vollständig: $\qquad$ für alle $\psi \in L_0^S$ ($\Phi \models \psi$ oder $\Phi \models \neg\psi$).

Beweis. $\text{KLEIN} := \{(b_0, \ldots, b_n) \mid \text{für alle } i \leq n : \; b_i < d_i\}$

$$|\text{KLEIN}| = d_0 \cdot \ldots \cdot d_n = d.$$

Für $c \in \mathbb{N}$: $R(c) := (r(c, d_0), \ldots, r(c, d_n)) \in \text{KLEIN}$. Somit

$$\{0, \ldots, d-1\} \xrightarrow{R} \text{KLEIN}.$$

Genügt z.z.:

$$\text{Wenn } 0 \leq c < c' < d, \text{ so } R(c) \neq R(c').$$

Dann ist nämlich R auf $\{0, \ldots, d-1\}$ injektiv und damit surjektiv, die Beh.

Ang. $0 \leq c < c' < d$ und $R(c) = R(c')$.

$\Rightarrow$: Für $i = 0, \ldots, n$: $\quad r(c, d_i) = r(c', d_i)$.

$\Rightarrow$: Für $i = 0, \ldots, n$: $\quad d_i | c' - c$.

$\overset{d_i \text{ paarweise tf.}}{\Rightarrow}$: $\quad d_0 \cdot \ldots \cdot d_n | c' - c$, also $d | c' - c$.

$\overset{0 \leq c' - c < d}{\Rightarrow}$: $c = c'$.

$$\chi_P(u_0,\ldots,u_n,z,w_0,\ldots,w_n) \;:=\; \exists s\exists c\exists t\exists c_0\exists t_0\ldots\exists c_n\exists t_n$$

$$\Big(\varphi_\beta(c,t,\bar{0},\bar{0}) \wedge \varphi_\beta(c_0,t_0,\bar{0},u_0) \wedge \ldots \wedge \varphi_\beta(c_n,t_n,\bar{0},u_n) \wedge$$

$$\varphi_\beta(c,t,s,z) \wedge \varphi_\beta(c_0,t_0,s,w_0) \wedge \ldots \wedge \varphi_\beta(c_n,t_n,s,w_n) \wedge$$

$$\forall i(i < s \rightarrow \text{“}C_i \rightarrow_P C_{i+1}\text{''})\Big)$$

mit

$$\text{“}C_i \rightarrow_P C_{i+1}\text{''} :=$$

$$\bigwedge_{\nu=0}^{k-1} \forall x_0\ldots\forall x_n((\varphi_\beta(c,t,i,\bar{\nu}) \wedge \varphi_\beta(c_0,t_0,i,x_0) \wedge \ldots \wedge \varphi_\beta(c_n,t_n,i,x_n)) \rightarrow \psi_\nu),$$

wobei etwa für “$\nu\ R_j = R_j + |$'' $\in P$:

$$\psi_\nu \;:=\; (\varphi_\beta(c,t,i+1,\overline{\nu+1})\wedge$$

$$\varphi_\beta(c_0,t_0,i+1,x_0) \wedge \ldots \wedge \varphi_\beta(c_j,t_j,i+1,x_j+1) \wedge \ldots \wedge \varphi_\beta(c_n,t_n,i+1,x_n)).$$

$$\begin{aligned} \text{wenn } \mathfrak{Q} n_1 \ldots n_r, \text{ so} \quad & \Phi \vdash \psi(\bar{n}_1, \ldots, \bar{n}_r) \\ \text{wenn nicht } \mathfrak{Q} n_1 \ldots n_r, \text{ so} \quad & \Phi \vdash \neg\psi(\bar{n}_1, \ldots, \bar{n}_r) \end{aligned}$$

$$\begin{aligned} \text{wenn } F(n_1, \ldots, n_r) = k, \text{ so} \quad & \Phi \vdash \psi(\bar{n}_1, \ldots, \bar{n}_r \bar{k}) \\ \text{wenn nicht } F(n_1, \ldots, n_r) \neq k, \text{ so} \quad & \Phi \vdash \neg\psi(\bar{n}_1, \ldots, \bar{n}_r, \bar{k}) \\ & \Phi \vdash \exists^{=1} y \psi(\bar{n}_1, \ldots, \bar{n}_r, y) \end{aligned}$$

$$P \mapsto \chi_P(u_0, \ldots, u_n, z, w_0, \ldots, w_n)$$

$$(0, \tilde{k}) \Rightarrow_P (\ell, \tilde{m}) \iff \mathfrak{N} \models \chi_P[\tilde{k}, \ell, \tilde{m}]$$

Beweis. Definiere $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ durch

$$F(n,m) := \begin{cases} n_{\chi(\bar{m})}, & \text{falls } n = n_\chi \text{ für ein } \chi \in L_1^S; \\ 0, & \text{sonst.} \end{cases}$$

F ist berechenbar. Für $\chi \in L_1^S$ gilt: $\quad F(n_\chi, m) = n_{\chi(\bar{m})}$ (1)

Da F berechenbar und Repr Φ ex. $\alpha \in L_3^S$: $\alpha(x,y,z)$ repräsentiert F in Φ. (2)

Sei nun $\psi \in L_1^S$ gegeben. Setze: $\quad \beta(x) := \forall z(\alpha(x,x,z) \to \psi(z))$. (3)

Wegen (1): $\quad F(n_\beta, n_\beta) = n_{\beta(\bar{n}_\beta)} = n_\varphi$ für (4)

$$\varphi := \beta(\bar{n}_\beta) = \forall z(\alpha(\bar{n}_\beta, \bar{n}_\beta, z) \to \psi(z)) \quad (\in L_0^S). \tag{5}$$

Wegen (4) und (2): $\Phi \vdash \alpha(\bar{n}_\beta, \bar{n}_\beta, \bar{n}_\varphi)$. (6)

Behauptung. $\Phi \vdash \varphi \leftrightarrow \psi(\bar{n}_\varphi)$.

$\to$: Wegen (5) $\Phi \cup \{\varphi\} \vdash \alpha(\bar{n}_\beta, \bar{n}_\beta, \bar{n}_\varphi) \to \psi(\bar{n}_\varphi)$, wegen (6) daher $\quad \Phi \vdash \varphi \to \psi(\bar{n}_\varphi)$.

$\leftarrow$: Wegen (2) $\Phi \vdash \exists^{=1} z \alpha(\bar{n}_\beta, \bar{n}_\beta, z)$, wegen (6) daher $\Phi \vdash \forall z(\alpha(\bar{n}_\beta, \bar{n}_\beta, z) \to z = \bar{n}_\varphi)$.

Somit $\Phi \vdash \psi(\bar{n}_\varphi) \to \underbrace{\forall z(\alpha(\bar{n}_\beta, \bar{n}_\beta, z) \to \psi(z))}_{\varphi}$.

Voraussetzungen: S effektiv gegeben, $n \mapsto \bar{n}$, $\quad \varphi \mapsto n_\varphi$, $\quad \ulcorner\varphi\urcorner := \bar{n}_\varphi$
$\Phi \in L_0^S$, Φ R-entscheidbar und Repr Φ

$$Hnm \iff \text{“}m \text{ ist Beweis von } n \text{ aus } \Phi\text{”}$$

die m-te Ableitung endet mit Sequnez $\psi_1 \ldots \psi_k \varphi$,

wobei $\psi_1 \ldots \psi_k \in \Phi$ und $n_\varphi = n$

$\varphi_H(x, y)$ repräsentiere H in Φ; $\mathrm{Bew}_\Phi(x) := \exists y \varphi(x, y)$.

Mit Fixpunktsatz wähle $\varphi_0 \in L_0^S$ mit

$$(*) \qquad \Phi \vdash \varphi_0 \leftrightarrow \neg \mathrm{Bew}_\Phi(\ulcorner\varphi_0\urcorner)$$

$$(2) \qquad \text{Wenn Wf } \Phi, \text{ so nicht } \Phi \vdash \varphi_0.$$

PGN Menge der Polynome in mehreren Unbekannten mit ganzzahligen Koeffizienten, die eine ganzzahlige Nullstelle haben.

Satz von Matijasevic (1970):

PGN ist nicht R-entscheidbar.

Somit: Es ist nicht entscheidbar, ob ein Polynom $\underline{\underline{p(x_1, \dots, x_l)}} \in \mathbb{Z}[x_1, \dots, x_l]$ eine Nullstelle in $\mathbb{Z}$ besitzt (d.h. ob ex. $z_1, \dots, z_l \in \mathbb{Z}$ mit $p(z_1, \dots, z_l) = 0$).

Lemma von Matijasevic: $M \subseteq \mathbb{N}$ R-aufzählbar.
Dann ex. $l \geq 1$ und $p(x_1, \dots, x_l) \in \mathbb{Z}[x_1, \dots, x_l]$ mit

$$M = W_{\mathbb{N}}(p) := \{p(n_1, \dots, n_l) \mid \bar{n} \in \mathbb{N}, \, p(\bar{n}) \geq 0\}.$$

$$\Delta_k^S \quad := \quad \{\psi \in L_k^S \mid \psi \text{ hat Gestalt } x = y, Rx_1 \ldots x_r, f(x_1, \ldots, x_n) = y \text{ oder } c = y\}.$$

Beweis. Induktion über m: $m = 0$:

$$\begin{aligned} \mathfrak{B} \models \varphi_{\bar{a}}^0[\bar{b}] &\overset{\text{L. 3.4)}}{\iff} \bar{a} \mapsto \bar{b} \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B}) \\ &\overset{\text{L. 1a)}}{\iff} \text{II gew. } G_0(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b}). \end{aligned}$$

$m > 0$:

$$\begin{aligned} & \text{II gew. } G_m(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b}) \\ \overset{\text{L. 1b)}}{\iff} \quad & \forall a \in A \exists b \in B : \text{ II gew. } G_{m-1}(\mathfrak{A}, \bar{a}a, \mathfrak{B}, \bar{b}b) \text{ und} \\ & \forall b \in B \exists a \in A : \text{ II gew. } G_{m-1}(\mathfrak{A}, \bar{a}a, \mathfrak{B}, \bar{b}b) \\ \overset{\text{Ind.Vor.}}{\iff} \quad & \forall a \in A \exists b \in B : \mathfrak{B} \models \varphi_{\bar{a}a}^{m-1}[\bar{b}b] \text{ und } \forall b \in B \exists a \in A : \mathfrak{B} \models \varphi_{\bar{a}a}^{m-1}[\bar{b}b] \\ \iff \quad & \mathfrak{B} \models \bigwedge_{a \in A} \exists v_{k+1} \varphi_{\bar{a}a}^{m-1}[\bar{b}] \text{ und } \mathfrak{B} \models \forall v_{k+1} \bigvee_{a \in A} \varphi_{\bar{a}a}^{m-1}[\bar{b}] \\ \iff \quad & \mathfrak{B} \models \varphi_{\bar{a}}^m[\bar{b}]. \end{aligned}$$

Lemma 1. a) II gew. $G_0(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$ gdw. $\bar{a} \mapsto \bar{b} \in \mathrm{Part}(\mathfrak{A}, \mathfrak{B})$.

b) Sei $m > 0$. Dann

$$\begin{aligned} \text{II gew. } G_m(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b}) \quad &\Longleftrightarrow \quad \forall a \in A \exists b \in B: \ \text{II gew. } G_{m-1}(\mathfrak{A}, \bar{a}a, \mathfrak{B}, \bar{b}b) \\ &\quad\ \text{und} \quad\ \forall b \in B \exists a \in A: \ \text{II gew. } G_{m-1}(\mathfrak{A}, \bar{a}a, \mathfrak{B}, \bar{b}b). \end{aligned}$$

c) Ist $m' < m$ und II gew. $G_m(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$, so II gew. $G_{m'}(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$.

Lemma 3. 1) S endlich. Dann ist

$$\mathrm{IT}_k^m := \{\varphi_{\mathfrak{A}, \bar{a}}^m \mid \mathfrak{A} \ S\text{-Struktur}, \bar{a} \in A^k\}$$

endlich.

Lemma von Ehrenfeucht. (+) und S endlich. Dann sind äquivalent:

(i) II gew. $G_m(\mathfrak{A}, \bar{a}, \mathfrak{B}, \bar{b})$.

(ii) $\mathfrak{B} \models \varphi_{\mathfrak{A}, \bar{a}}^m[\bar{b}]$.

(iii) Für alle termreduzierten $\varphi \in L_k^S$ mit $\mathrm{qr}(\varphi) \leq m$:

$$\mathfrak{A} \models \varphi[\bar{a}] \iff \mathfrak{B} \models \varphi[\bar{b}].$$

Was ist ein mathematischer Beweis?

1. Ist jede mathematische Aussage beweisbar?
2. Ist jede mathematische Aussage wahr oder falsch?
3. Ist die Mathematik widerspruchsfrei?
4. Kann man das Beweisen Computern überlassen?