Arithmetik ohne Exponentialfunktion

Die Unvollständigkeit von P.A - 1. Teil

Jan Flügge

Institut für Informatik
Humboldt-Universität zu Berlin

19. Juni 2007

Fahrplan

1. Einführung des Axiomensystems „Peano Arithmetik“(P.A.)
   - Ziel: Unvollständigkeit von P.A. zeigen
   - Ist $\tilde{\mathrm{P}}^*_{\mathrm{E}}$ arithmetisch ?

   $\Rightarrow$ Unvollständigkeit leitet sich aus P.E. ab, falls $x^y = z \in$ P.A.
2. Definition der Formelmengen und Relationen Σ_0, Σ_1 und Σ
3. Verkettung zur Basis einer Primzahl

Peano Arithmetik

Definition

- Sei das Axiomensystem P.A. (Peano Arithmetik) das Axiomensystem P.E. *ohne* die Axiome

$$\begin{aligned} N_{10} &: \quad (v_1 \mathbf{E} \overline{0}') \\ N_{11} &: \quad (v_1 \mathbf{E} v_2') = ((v_1 \mathbf{E} v_2) \cdot v_1) \end{aligned}$$

- Ein Term (Formel) ohne Exponentialfunktion **E** wird *arithmetisch* genannt.
- Eine arithmetische Relation (Menge) ist ausdrückbar durch eine arithmetische Formel.

atomare Σ_0-Formeln

Definition

Sei c_1, c_2 oder c_3 eine natürliche Zahl oder eine Variable.
Eine *atomare* Σ_0-Formel ist eine Formel der Art:

- $c_1 + c_2 = c_3$
- $c_1 \cdot c_2 = c_3$
- $c_1 = c_2$
- $c_1 \leq c_2$

atomare Σ_0-Formeln

Definition

Sei c_1, c_2 oder c_3 eine natürliche Zahl oder eine Variable.
Eine *atomare* Σ_0-Formel ist eine Formel der Art:

- $c_1 + c_2 = c_3$
- $c_1 \cdot c_2 = c_3$
- $c_1 = c_2$
- $c_1 \leq c_2$

atomare Σ_0-Formeln

Definition

Sei c_1, c_2 oder c_3 eine natürliche Zahl oder eine Variable.
Eine *atomare* Σ_0-Formel ist eine Formel der Art:

- $c_1 + c_2 = c_3$
- $c_1 \cdot c_2 = c_3$
- $c_1 = c_2$
- $c_1 \leq c_2$

atomare Σ_0-Formeln

Definition

Sei c_1, c_2 oder c_3 eine natürliche Zahl oder eine Variable.
Eine *atomare* Σ_0-Formel ist eine Formel der Art:

- $c_1 + c_2 = c_3$
- $c_1 \cdot c_2 = c_3$
- $c_1 = c_2$
- $c_1 \leq c_2$

atomare Σ_0-Formeln

Definition

Sei c_1, c_2 oder c_3 eine natürliche Zahl oder eine Variable.
Eine *atomare* Σ_0-Formel ist eine Formel der Art:

- $c_1 + c_2 = c_3$
- $c_1 \cdot c_2 = c_3$
- $c_1 = c_2$
- $c_1 \leq c_2$

Klasse der Σ_0-Formeln

Definition

Die Klasse der Σ_0-Formeln ist wie folgt Induktiv definiert:

1. Jede atomare Σ_0-Formel ist in Σ_0
2. Falls $F, G \in \Sigma_0$ dann $\sim F \in \Sigma_0$ und $F \supset G \in \Sigma_0$ (und damit auch $F \wedge G, F \vee G, F \equiv G \in \Sigma_0$)
3. Für jedes $F \in \Sigma_0$ gilt $\forall v_i(v_i \leq c \supset F) \in \Sigma_0$
   mit
   - v_i - Variable
   - c ist eine natürliche Zahl oder eine Variable *verschieden von* v_i

Klasse der Σ_0-Formeln

Definition

Die Klasse der Σ_0-Formeln ist wie folgt Induktiv definiert:

1. Jede atomare Σ_0-Formel ist in Σ_0
2. Falls $F, G \in \Sigma_0$ dann $\sim F \in \Sigma_0$ und $F \supset G \in \Sigma_0$ (und damit auch $F \wedge G, F \vee G, F \equiv G \in \Sigma_0$)
3. Für jedes $F \in \Sigma_0$ gilt $\forall v_i(v_i \leq c \supset F) \in \Sigma_0$
   mit
   - v_i - Variable
   - c ist eine natürliche Zahl oder eine Variable *verschieden von* v_i

Klasse der Σ_0-Formeln

Definition

Die Klasse der Σ_0-Formeln ist wie folgt Induktiv definiert:

1. Jede atomare Σ_0-Formel ist in Σ_0
2. Falls $F, G \in \Sigma_0$ dann $\sim F \in \Sigma_0$ und $F \supset G \in \Sigma_0$ (und damit auch $F \wedge G, F \vee G, F \equiv G \in \Sigma_0$)
3. Für jedes $F \in \Sigma_0$ gilt $\forall v_i(v_i \leq c \supset F) \in \Sigma_0$
   mit
   - v_i - Variable
   - c ist eine natürliche Zahl oder eine Variable *verschieden von* v_i

Klasse der Σ_0-Formeln

Definition

Die Klasse der Σ_0-Formeln ist wie folgt Induktiv definiert:

1. Jede atomare Σ_0-Formel ist in Σ_0
2. Falls $F, G \in \Sigma_0$ dann $\sim F \in \Sigma_0$ und $F \supset G \in \Sigma_0$ (und damit auch $F \wedge G, F \vee G, F \equiv G \in \Sigma_0$)
3. Für jedes $F \in \Sigma_0$ gilt $\forall v_i(v_i \leq c \supset F) \in \Sigma_0$
   mit
   - v_i - Variable
   - c ist eine natürliche Zahl oder eine Variable *verschieden von* v_i

Σ_0-Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$
\begin{aligned}
&\Longrightarrow && F \in \Sigma_0 \\
&\overset{(2)}{\Longrightarrow} && \sim F \in \Sigma_0 \\
&\overset{(3)}{\Longrightarrow} && (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\overset{(2)}{\Longrightarrow} && \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\Longrightarrow && (\exists v_i \leq c)F \in \Sigma_0
\end{aligned}
$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Σ_0-Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$
\begin{aligned}
&\longrightarrow F \in \Sigma_0 \\
&\overset{(2)}{\longrightarrow} \sim F \in \Sigma_0 \\
&\overset{(3)}{\longrightarrow} (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\overset{(2)}{\longrightarrow} \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\longrightarrow (\exists v_i \leq c)F \in \Sigma_0
\end{aligned}
$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Σ_0-Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$\begin{aligned} &\longrightarrow && F \in \Sigma_0 \\ &\xrightarrow{(2)} && \sim F \in \Sigma_0 \\ &\xrightarrow{(3)} && (\forall v_i \leq c) \sim F \in \Sigma_0 \\ &\xrightarrow{(2)} && \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\ &\longrightarrow && (\exists v_i \leq c)F \in \Sigma_0 \end{aligned}$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Σ_0-Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$\begin{aligned} &\longrightarrow && F \in \Sigma_0 \\ &\xrightarrow{(2)} && \sim F \in \Sigma_0 \\ &\xrightarrow{(3)} && (\forall v_i \leq c) \sim F \in \Sigma_0 \\ &\xrightarrow{(2)} && \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\ &\longrightarrow && (\exists v_i \leq c)F \in \Sigma_0 \end{aligned}$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Σ_0−Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$
\begin{aligned}
&\longrightarrow && F \in \Sigma_0 \\
&\xrightarrow{(2)} && \sim F \in \Sigma_0 \\
&\xrightarrow{(3)} && (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\xrightarrow{(2)} && \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\
&\longrightarrow && (\exists v_i \leq c)F \in \Sigma_0
\end{aligned}
$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Σ_0—Formeln - nützliche Abkürzungen

- $\forall v_i(v_i \leq c \supset F) \leftrightarrow (\forall v_i \leq c)F$
  - Damit gilt nach (3): $(\forall v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
- $\sim (\forall v_i \leq c) \sim F \leftrightarrow (\exists v_i \leq c)F$
  - Behauptung: $(\exists v_i \leq c)F \in \Sigma_0 \Leftrightarrow F \in \Sigma_0$
    - Beweis:

$$\begin{array}{cl} \longrightarrow & F \in \Sigma_0 \\ \xrightarrow{(2)} & \sim F \in \Sigma_0 \\ \xrightarrow{(3)} & (\forall v_i \leq c) \sim F \in \Sigma_0 \\ \xrightarrow{(2)} & \sim (\forall v_i \leq c) \sim F \in \Sigma_0 \\ \longrightarrow & (\exists v_i \leq c)F \in \Sigma_0 \end{array}$$

- Die Quantoren $(\exists v_i \leq c)$ und $(\forall v_i \leq c)$ werden auch *beschränkte Quantoren* genannt.

Entscheidbarkeit von Σ_0-Sätzen

Behauptung

Jeder $\Sigma_0 - Satz$ ist entscheidbar

Beweis.

- jede atomare Σ_0-Formel ist entscheidbar
- Seien X und Y entscheidbare Σ_0-Sätze, so sind auch $\sim X$ und $X \supset Y$ entscheidbar
- $(\forall v_i \leq c)F(v_i)$ ist entscheidbar, da für jedes mögliche $v_i = k$ mit $k \in \{\overline{n} | n \in \mathbb{N} \wedge n \leq c\}$ effektiv auf wahr oder falsch getestet werden kann.
  - gleiches gilt auch für $(\exists v_i \leq c)F(v_i)$

$\square$

Σ_1 Relationen

Definition

Eine Σ_1 Relation ist eine Formel der Art $\exists v_{n+1} F(v_1, \ldots, v_n, v_{n+1})$, mit $F(v_1, \ldots, v_n, v_{n+1}) \in \Sigma_0$.

- Sei $R(x_1, \ldots, x_n) \in \Sigma_1$ und $S(x_1, \ldots, x_n, y) \in \Sigma_0$, dann gilt für gleiche $x_1, \ldots, x_n$:

$$R(x_1, \ldots, x_n) \leftrightarrow \exists y S(x_1, \ldots, x_n, y)$$

Bemerkung

Eine Σ_1-Formel beginnt mit einem *unbeschränkten* Existenzquantor. Die restlichen Quantoren sind beschränkt.

Σ-Formeln

Definition

Die Menge der Σ-Formeln ist induktiv definiert durch:

1. Jede Σ_0-Formel ist eine Σ-Formel
2. Wenn $F \in \Sigma$ dann gilt für jede Variable v_i : $\exists v_i F \in \Sigma$
3. Wenn $F \in \Sigma$, dann gilt für jede Variable $v_i, v_j (v_i \neq v_j)$ und für jede Zahl n:
   - $(\exists v_i \leq v_j) F \in \Sigma$
   - $(\forall v_i \leq v_j) F \in \Sigma$
   - $(\exists v_i \leq \overline{n}) F \in \Sigma$
   - $(\forall v_i \leq \overline{n}) F \in \Sigma$
4. Wenn $F, G \in \Sigma$ dann auch $F \wedge G, F \vee G \in \Sigma$
5. Wenn $F \in \Sigma_0$ und $G \in \Sigma$ dann ist $F \supset G \in \Sigma$

Bemerkung

Eine Relation (Menge) ist in Σ, wenn sie durch Σ-Formeln ausdrückbar ist.

nützliche Σ_0-Relationen

1. $x < y \in \Sigma_0$

Beweis.

- $x < y \leftrightarrow x \leq y \land x \neq y$

$\square$

2. für jedes $R(x, y, z_1, \ldots, z_n) \in \Sigma_0$ gilt:
   $(\forall x < y) R(x, y, z_1, \ldots, z_n) \in \Sigma_0$

Beweis.

- $(\forall x < y) R(x, y, z_1, \ldots, z_n)$
  $\leftrightarrow (\forall x \leq y)(x \neq y \supset R(x, y, z_1, \ldots, z_n))$

$\square$

Verkettung zur Basis einer Primzahl

Fahrplan

- Ziel: Zeigen der Unvollständigkeit von P.A.
- Idee: Lässt sich der Unvollständigkeitsbeweis von P.E. nach P.A. übertragen ?
- Ist der Beweis für $P \in$ P.E. auch arithmetisch ?
  - $\Leftrightarrow$ $xB_by, xE_by, xP_by \in$ P.A.
  - $\Leftrightarrow$ $x *_b y = z \in$ P.A.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \textbf{ E } v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2(b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b}\ \mathbf{E}\ v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \mathbf{E} v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \mathbf{E} v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

- $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
- $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
- $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \textbf{ E } v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \ \mathbf{E} \ v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Bemerkung

- Für jede Basis ≥ 2 ist die Verkettungsfunktion $x *_b y = z$ Arithmetisch
- Die Exponentialfunktion E wurde in der Definition der Funktion $Pow_b(v_1) := \exists v_2(v_1(\overline{b} \ \mathbf{E} \ v_2))$ benötigt.

$\Rightarrow$ Erinnerung:

  - $x \cdot b^{\ell_b(y)} + y = z \leftrightarrow \exists z_1 \exists z_2 (b^{\ell_b(y)} = z_1 \wedge x \cdot z_1 = z_2 \wedge z_2 + y = z)$
  - $b^{\ell_b(x)} = y \leftrightarrow (x = 0 \wedge y = b) \vee (x \neq 0 \wedge s(x, y))$
  - $s(x, y) = Pow_b(y) \wedge x < y \wedge \forall z((Pow_b(z) \wedge x < z) \supset y \leq z)$

- Der restliche Teil der Definition von $x *_b y = z$ ist bereits arithmetisch.

Verkettung zur Basis einer Primzahl

Behauptung

Für jede **Primzahl** p kann $Pow_p(x)$ ohne Benutzung der Exponentialfunktion definiert werden. Damit ist für jede Primzahl die Funktion $x *_p y = z$ arithmetisch (sogar Σ_0)

Verkettung zur Basis einer Primzahl

Lemma 1

Für jede Primzahl sind folgende Ausdrücke in Σ_0:

1. x div y $\leftrightarrow$(x teilt y)
2. $Pow_p(x) \leftrightarrow$ (x ist eine Potenz von p)
3. $y = p^{\ell_p}(x) \leftrightarrow$ (y ist der kleinste positive Exponent von p größer als x)

Beweis.

1. x div y $\leftrightarrow (\exists z \leq y)(x \cdot z = y)$
2. $Pow_p(x) \leftrightarrow (\forall z \leq x)((z \text{ div } x \wedge z \neq 1) \supset p \text{ div } z)$
3. $y = p^{\ell_p(x)} \leftrightarrow (Pow_p(y) \wedge y > x \wedge y > 1) \wedge$
$(\forall z < y) \sim (Pow_p(z) \wedge z > x \wedge z > 1)$

$\square$

Verkettung zur Basis einer Primzahl

Satz A

Für jede Primzahl p gilt: $x *_p y = z \in \Sigma_0$

Beweis.

$$
\begin{aligned}
x *_b y = z \quad &\leftrightarrow \quad x \cdot p^{\ell_p(y)} + y = z \\
&\leftrightarrow \quad (\exists w_1 \leq z)(\exists w_2 \leq z)(w_1 = p^{\ell_p(y)} \wedge w_2 = x \cdot w_1 \wedge \\
&\qquad\; w_2 + y = z)
\end{aligned}
$$

Nach vorherigem Lemma gilt $w_1 = p^{\ell_p(y)} \in \Sigma_0$ $\square$

Verkettung zur Basis einer Primzahl

Satz B

Für jede Primzahl p sind die folgenden Relationen in Σ_0:

1. xB_py, xE_py, xP_py
   (y beginnt mit x, y endet mit x, x ist Teil von y)
2. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n = y$
   (y ist die Verkettung von $x_1, \ldots, x_n$)
3. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n P_p y$
   ($x_1, \ldots, x_n$ ist Teil von y)

Verkettung zur Basis einer Primzahl

Satz B

Für jede Primzahl p sind die folgenden Relationen in Σ_0:

1. xB_py, xE_py, xP_py
   (y beginnt mit x, y endet mit x, x ist Teil von y)
2. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n = y$
   (y ist die Verkettung von $x_1, \ldots, x_n$)
3. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n P_p y$
   ($x_1, \ldots, x_n$ ist Teil von y)

Verkettung zur Basis einer Primzahl

Satz B

Für jede Primzahl p sind die folgenden Relationen in Σ_0:

1. xB_py, xE_py, xP_py
   (y beginnt mit x, y endet mit x, x ist Teil von y)
2. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n = y$
   (y ist die Verkettung von $x_1, \ldots, x_n$)
3. Für jedes $n \geq 2$, die Relation $x_1 *_p \ldots *_p x_n P_p y$
   ($x_1, \ldots, x_n$ ist Teil von y)

Verkettung zur Basis einer Primzahl

Satz B

Für jede Primzahl p sind die folgenden Relationen in Σ_0:

1. xB_py, xE_py, xP_py
   (y beginnt mit x, y endet mit x, x ist Teil von y)
2. Für jedes $n \geq 2$, die Relation $x_1 *_p \dots *_p x_n = y$
   (y ist die Verkettung von $x_1, \dots, x_n$)
3. Für jedes $n \geq 2$, die Relation $x_1 *_p \dots *_p x_n P_p y$
   ($x_1, \dots, x_n$ ist Teil von y)

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$\begin{aligned}
xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\
&\qquad (x \cdot w) *_p z = y)) \\
xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\
xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz)
\end{aligned}$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_nP_py \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

□

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$
\begin{aligned}
xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\
&\quad (x \cdot w) *_p z = y)) \\
xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\
xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz)
\end{aligned}
$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_n P_p y \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

□

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$
\begin{aligned}
xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\
&\quad (x \cdot w) *_p z = y)) \\
xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\
xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz)
\end{aligned}
$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_n P_p y \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

□

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$\begin{aligned} xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\ &\quad (x \cdot w) *_p z = y)) \\ xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\ xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz) \end{aligned}$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_n P_p y \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

□

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$
\begin{aligned}
xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\
&\quad (x \cdot w) *_p z = y)) \\
xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\
xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz)
\end{aligned}
$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_n P_p y \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

□

Verkettung zur Basis einer Primzahl

Beweis.

1. Die Relationen xB_py, xE_py, xP_py lassen sich schreiben als..

$$
\begin{aligned}
xB_py &\leftrightarrow x = y \wedge (x \neq 0 \wedge (\exists z \leq y)(\exists w \leq y)(Pow_p(w) \wedge \\
&\quad (x \cdot w) *_p z = y)) \\
xE_py &\leftrightarrow x = y \vee (\exists z \leq y)(z *_p x = y) \\
xP_py &\leftrightarrow (\exists z \leq y)(zE_py \wedge xB_pz)
\end{aligned}
$$

2. Beweis über Induktion von $n \geq 2$
   - Nach Satz A gilt: $x *_p y = z \in \Sigma_0$
   - Induktionsannahme: $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$.
   - Induktionsschritt: $x_1 *_p \ldots *_p x_n *_p x_{n+1} = y$ läßt sich schreiben als: $(\exists z \leq y)(x_1 *_p \ldots *_p x_n = z \wedge z *_p x_{n+1} = y) \in \Sigma_0$
3. $x_1 *_p \ldots *_p x_n P_p y \leftrightarrow (\exists z \leq y)(x_1 *_p \ldots *_p = z \wedge zP_py) \in \Sigma_0$

$\square$

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_py, xE_py, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_p y, xE_p y, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_p y, xE_p y, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_py, xE_py, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_p y, xE_p y, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Zusammenfassung

Relationen in Σ_0

1. $Pow_p(x) \in \Sigma_0$ (Lemma 1)
2. $x *_p y = z \in \Sigma_0$ (Satz A)
3. $xB_py, xE_py, xP_p \in \Sigma_0$ (Satz B)
4. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n = y \in \Sigma_0$ (Satz B)
5. Für jedes $n \geq 2$ ist $x_1 *_p \ldots *_p x_n P_p y \in \Sigma_0$ (Satz B)

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x, y, z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

$\square$

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x, y, z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

$\square$

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x, y, z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

$\square$

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x, y, z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

$\square$

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x, y, z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

□

Schlußfolgerungen

Für p= 13

Folgende Bedingungen aus P.E. sind dann arithmetisch:

- $Seq(y), x \in y$ und $x \prec_z y$
- $Sb(x), Var(x), Num(x), R_1(x,y,z), \ldots, P_E(x), R_E(X)$

Beweis.

- $Pow_{13}(x), x *_p y = z \in \Sigma_0$
- Die Exponentialfunktion **E** wird in anderen Definitionen nicht verwendet
- Insbesondere gilt P_E und $R_E \in \Sigma$, da der ungebundene Allquantor nicht verwendet wird.

$\square$

Schlußfolgerungen

- $\mathrm{P_E}$ und $\overset{\sim}{\mathrm{P}}_\mathrm{E}$ ist arithmetisch
- für einen Gödelsatz von $\overset{\sim}{\mathrm{P}}_\mathrm{E}$ muß gezeigt werden, dass $\overset{\sim}{\mathrm{P}}^*_\mathrm{E}$ arithmetisch.
- Diagonalisierungsfunktion:

$$d(x) = r(x, x) = z \leftrightarrow \exists w(w = 13^x \wedge z = k * w * 8 * x * 3))$$

$\Rightarrow$ zu Zeigen: $13^x = y$ ist arithmetisch

  - der existenzielle Beweis existiert bereits..(es gibt eine Zahl)
  - es wird jedoch ein konstruktiver Beweis benötigt (wie gross ist die Zahl?)

Theorem

$$x^y = z \in \Sigma_1$$