Script generated by TTT

Title: seidl: Theoretische_Informatik (12.07.2012)

Date: Thu Jul 12 16:04:05 CEST 2012

Duration: 85:44 min

Pages: 73

PARTITION

Gegeben: Zahlen $a_1, \ldots a_n \in \mathbb{N}$.

RUCKSACK

Gegeben: Zahlen $a_1, \ldots a_n \in \mathbb{N}$ und $b \in \mathbb{N}$.

Problem: Gibt es $R \subseteq \{1, \ldots, n\}$ mit $\sum_{i \in R} a_i = b$?

Satz 5.33

RUCKSACK ist NP-vollständig.

Beweis:

3KNF-SAT $\leq_p$ RUCKSACK :

Sei $F = (z_{11} \vee z_{12} \vee z_{13}) \wedge \cdots \wedge (z_{m1} \vee z_{m2} \vee z_{m3})$, wobei

$$z_{ij} \in \{x_1, \ldots, x_n\} \cup \{\neg x_1, \neg x_2, \ldots, \neg x_n\}$$

D.h. $m =$ Anzahl der Klauseln und n Anzahl der vorkommenden Variablen.

Wir geben jetzt Zahlen $\vec{a} = a_1, \ldots, a_k$ und b an. b ist (etwa im Dezimalsystem)

$$b = \underbrace{44 \ldots 444}_{m}\underbrace{11 \ldots 11}_{n}$$

$\square$

PARTITION

Gegeben: Zahlen $a_1, \ldots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \ldots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34

PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^n a_i = 57,$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34

PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^n a_i = 57, \quad M - b + 1 = 20, \quad b + 1 = 39$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34

PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^n a_i = 57, \quad M - b + 1 = 20, \quad b + 1 = 39$

Das resultierende PARTITONS-Problem: $12, 7, 4, 9, 7, 3, 15, \ 20, 39$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34

PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^n a_i = 57, \quad M - b + 1 = 20, \quad b + 1 = 39$

Das resultierende PARTITONS-Problem: $12, 7, 4, 9, 7, 3, 15, \ 20, 39$

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^{n} a_i = 57, \quad M - b + 1 = 20, \quad b + 1 = 39$

Das resultierende PARTITONS-Problem: $12, 7, 4, 9, 7, 3, 15, \; 20, 39$

Lösung: $\{7, 9, 7, 15, 20\}$ und $\{12, 4, 3, 39\}$,

PARTITION

Gegeben: Zahlen $a_1, \dots a_n \in \mathbb{N}$.

Problem: Gibt es $I \subseteq \{1, \dots, n\}$ mit $\sum_{i \in I} a_i = \sum_{i \notin I} a_i$?

Satz 5.34
PARTITION ist NP-vollständig.

Beweis: RUCKSACK $\leq_p$ PARTITION

Beispiel: $\vec{a} = 12, 7, 4, 9, 7, 3, 15$ und $b = 38$.

Lösung: Die Zahlen $7, 9, 7, 15$, dh $R = \{2, 4, 5, 7\}$

RUCKSACK $\rightarrow$ PARTITION:

$M := \sum_{i=1}^{n} a_i = 57, \quad M - b + 1 = 20, \quad b + 1 = 39$

Das resultierende PARTITONS-Problem: $12, 7, 4, 9, 7, 3, 15, \; 20, 39$

Lösung: $\{7, 9, 7, 15, 20\}$ und $\{12, 4, 3, 39\}$, dh $I = \{2, 4, 5, 7, 8\}$.

Reduktion im Allgemeinen:

$$a_1, a_2, \dots, a_k, b \;\mapsto\; a_1, a_2, \dots, a_k, M - b + 1, b + 1 \qquad \square$$

BIN PACKING

Gegeben: Eine „Behältergröße“ $b \in \mathbb{N}$, die Anzahl der Behälter $k \in \mathbb{N}$ und „Objekte“ $a_1, a_2, \dots a_n$.

BIN PACKING

Gegeben: Eine „Behältergröße“ $b \in \mathbb{N}$, die Anzahl der Behälter $k \in \mathbb{N}$ und „Objekte“ $a_1, a_2, \dots a_n$.

Problem: Können die Objekte so auf die k Behälter verteilt werden, dass kein Behälter überläuft?

BIN PACKING

Gegeben: Eine „Behältergröße“ $b \in \mathbb{N}$, die Anzahl der Behälter $k \in \mathbb{N}$ und „Objekte“ $a_1, a_2, \dots a_n$.

Problem: Können die Objekte so auf die k Behälter verteilt werden, dass kein Behälter überläuft?

Satz 5.35
BIN PACKING ist NP-vollständig.

BIN PACKING

Gegeben: Eine „Behältergröße“ $b \in \mathbb{N}$, die Anzahl der Behälter $k \in \mathbb{N}$ und „Objekte“ $a_1, a_2, \dots a_n$.

Problem: Können die Objekte so auf die k Behälter verteilt werden, dass kein Behälter überläuft?

Satz 5.35
BIN PACKING ist NP-vollständig.

Beweis: PARTITION $\leq_p$ BIN PACKING

BIN PACKING

Gegeben: Eine „Behältergröße“ $b \in \mathbb{N}$, die Anzahl der Behälter $k \in \mathbb{N}$ und „Objekte“ $a_1, a_2, \dots a_n$.

Problem: Können die Objekte so auf die k Behälter verteilt werden, dass kein Behälter überläuft?

Satz 5.35
BIN PACKING ist NP-vollständig.

Beweis: PARTITION $\leq_p$ BIN PACKING

$$(a_1, \dots, a_n) \mapsto (b, k, 2a_1, \dots, 2a_n)$$

wobei $b := \sum_{i=1}^{k} a_i$ und $k := 2$. □

HAMILTON

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

HAMILTON

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

Satz 5.36
HAMILTON ist NP-vollständig.

HAMILTON

Gegeben: Ungerichteter Graph G

Problem: Enthält G einen Hamilton-Kreis, dh einen geschlossenen Pfad, der jeden Knoten genau einmal enthält?

Satz 5.36
HAMILTON ist NP-vollständig.

3KNF-SAT $\leq_p$ HAM

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

Satz 5.37

TSP ist NP-vollständig.

Beweis: HAMILTON $\leq_p$ TSP

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

Satz 5.37

TSP ist NP-vollständig.

Beweis: HAMILTON $\leq_p$ TSP

$$(\{1, \ldots, n\}, E) \;\mapsto\; (M, n)$$

wobei

$$M_{ij} \;:=\; \begin{cases} 1 & \text{falls } \{i, j\} \in E \\ 2 & \text{sonst} \end{cases}$$

$\square$

TRAVELLING SALESMAN (TSP)

Gegeben: Eine $n \times n$ Matrix $M_{ij} \in \mathbb{N}$ von „Entfernungen“ und eine Zahl $k \in \mathbb{N}$

Problem: Gibt es eine „Rundreise“ (Hamilton-Kreis) der Länge $\leq k$?

Satz 5.37

TSP ist NP-vollständig.

Beweis: HAMILTON $\leq_p$ TSP

$$(\{1, \ldots, n\}, E) \;\mapsto\; (M, n)$$

wobei

$$M_{ij} \;:=\; \begin{cases} 1 & \text{falls } \{i, j\} \in E \\ 2 & \text{sonst} \end{cases}$$

$\square$

FÄRBBARKEIT (COL)

Gegeben: Ein ungerichteter Graph (V, E) und eine Zahl k.

Problem: Gibt es eine Färbung der Knoten V mit k Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

FÄRBBARKEIT (COL)

Gegeben: Ein ungerichteter Graph (V, E) und eine Zahl k.

Problem: Gibt es eine Färbung der Knoten V mit k Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

Satz 5.38
FÄRBBARKEIT ist NP-vollständig für $k \geq 3$.

FÄRBBARKEIT (COL)

Gegeben: Ein ungerichteter Graph (V, E) und eine Zahl k.

Problem: Gibt es eine Färbung der Knoten V mit k Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

Satz 5.38
FÄRBBARKEIT ist NP-vollständig für $k \geq 3$.

Beweis:
3KNF-SAT $\leq_p$ 3FÄRBBARKEIT □

Satz 5.39
2FÄRBBARKEIT $\in$ P

FÄRBBARKEIT (COL)

Gegeben: Ein ungerichteter Graph (V, E) und eine Zahl k.

Problem: Gibt es eine Färbung der Knoten V mit k Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

Satz 5.38
FÄRBBARKEIT ist NP-vollständig für $k \geq 3$.

Beweis:
3KNF-SAT $\leq_p$ 3FÄRBBARKEIT □

Satz 5.39
2FÄRBBARKEIT $\in$ P

FÄRBBARKEIT (COL)

Gegeben: Ein ungerichteter Graph (V, E) und eine Zahl k.

Problem: Gibt es eine Färbung der Knoten V mit k Farben, so dass keine zwei benachbarten Knoten die gleiche Farbe haben?

Satz 5.38
FÄRBBARKEIT ist NP-vollständig für $k \geq 3$.

Beweis:
3KNF-SAT $\leq_p$ 3FÄRBBARKEIT □

Satz 5.39
2FÄRBBARKEIT $\in$ P

Die NP-Bibel, der NP-Klassiker:

Michael Garey and David Johnson.
Computers and Intractability: A Guide to the Theory of NP-Completeness. 1979.

Die NP-Bibel, der NP-Klassiker:

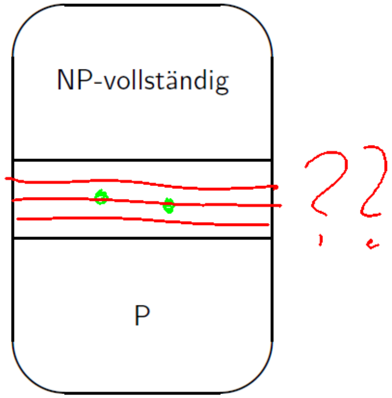
Michael Garey and David Johnson.
Computers and Intractability: A Guide to the Theory of NP-Completeness. 1979.

> *Despite the 23 years that have passed since its publication, I consider Garey and Johnson the single most important book on my office bookshelf.*

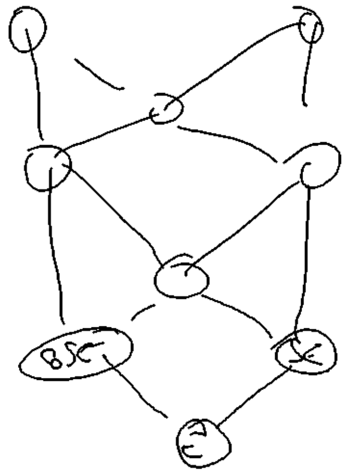
Lance Fortnow, 2002.

Man weiß nicht ob $P = NP$. Aber man weiß (Ladner 1975)

$P \neq NP \implies NP =$



Kurt Gödel.
Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatshefte für Mathematik, 1931.



Kurt Gödel.
Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatshefte für Mathematik, 1931.

Kurt Gödel
1906 (Brünn) –
1978 (Princeton)

5.5 Die Unvollständigkeit der Arithmetik

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$
Formeln:	F	$(T=T)\ \neg F\ (F\wedge F)\ (F\vee F)$
		$\exists V.\, F$

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$ $\quad 1 \quad 1+3$
Formeln:	F	$(T=T)\ \neg F\ (F\wedge F)\ (F\vee F)$ $\quad x*(1+y)$
		$\exists V.\, F$

$\exists x.\ 0 = x^2 + x + 17$

false

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$
Formeln:	F	$(T=T)\ \neg F\ (F\wedge F)\ (F\vee F)$
		$\exists V.\, F$

Wir betrachten $\forall x.\, F$ als Abk. für $\neg\exists\, x.\neg F$.

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$
Formeln:	F	$(T=T)\ \neg F\ (F\wedge F)\ (F\vee F)$
		$(\exists V.\, F)$

Wir betrachten $\forall x.\, F$ als Abk. für $\neg\exists\, x.\neg F$.

Definition 5.40

Ein Vorkommen einer Variablen x in einer Formel F ist **gebunden** gdw das Vorkommen in einer Teilformel der Form $\exists x.\, F'$ oder $\forall x.\, F'$ in der Teilformel F' liegt.

$\exists x.\ x = 5 \wedge x = 7$

5.5 Die Unvollständigkeit der Arithmetik

Syntax der Arithmetik:

Variablen:	V	$x\ y\ z\ \ldots$
Zahlen:	N	$0\ 1\ 2\ \ldots$
Terme:	T	$V\ N\ (T+T)\ (T*T)$
Formeln:	F	$(T=T)\ \neg F\ (F\wedge F)\ (F\vee F)$
		$\exists V.\, F$

Wir betrachten $\forall x.\, F$ als Abk. für $\neg\exists\, x.\neg F$.

Definition 5.40

Ein Vorkommen einer Variablen x in einer Formel F ist gebunden gdw das Vorkommen in einer Teilformel der Form $\exists x.\, F'$ oder $\forall x.\, F'$ in der Teilformel F' liegt.

Ein Vorkommen ist frei gdw es nicht gebunden ist.

$\forall x. \quad x=0 \vee \neg(x=0)$

Notation: $F(x_1,\ldots,x_k)$ bezeichnet eine Formel F, in der höchstens $x_1,\ldots,x_k$ frei vorkommen.

Notation: $F(x_1,\ldots,x_k)$ bezeichnet eine Formel F, in der höchstens $x_1,\ldots,x_k$ frei vorkommen.

Sind $n_1,\ldots,n_k$ $\mathbb{N}$ so ist $F(n_1,\ldots,n_k)$ das Ergebnis der Substitution von $n_1,\ldots,n_k$ für die freien Vorkommen von $x_1,\ldots,x_k$.

Notation: $F(x_1,\ldots,x_k)$ bezeichnet eine Formel F, in der höchstens $x_1,\ldots,x_k$ frei vorkommen.

Sind $n_1,\ldots,n_k$ $\mathbb{N}$ so ist $F(n_1,\ldots,n_k)$ das Ergebnis der Substitution von $n_1,\ldots,n_k$ für die freien Vorkommen von $x_1,\ldots,x_k$.

Beispiel 5.41

$$F(x,y) \quad = \quad (x=y\ \wedge\ \exists x.\, x=y)$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k$ $\mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 5.41

$$\begin{array}{rcl} F(x, y) & = & (x = y \;\wedge\; \exists x.\, x = y) \\ F(5, 7) & = & (5 = 7 \;\wedge\; \exists x.\, x = 7) \end{array}$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k$ $\mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 5.41

$$\begin{array}{rcl} F(x, y) & = & (x = y \;\wedge\; \exists x.\, x = y) \\ F(5, 7) & = & (5 = 7 \;\wedge\; \exists x.\, x = 7) \end{array}$$

Ein Satz ist eine Formel ohne freie Variablen.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k$ $\mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 5.41

$$\begin{array}{rcl} F(x, y) & = & (x = y \;\wedge\; \exists x.\, x = y) \\ F(5, 7) & = & (5 = 7 \;\wedge\; \exists x.\, x = 7) \end{array}$$

Ein Satz ist eine Formel ohne freie Variablen.

Beispiel 5.42

$$\exists x.\, \exists y.\, x = y \qquad \exists y.\, \exists x.\, x = y$$

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k$ $\mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 5.41

$$\begin{array}{rcl} F(x, y) & = & (x = y \;\wedge\; \exists x.\, x = y) \\ F(5, 7) & = & (5 = 7 \;\wedge\; \exists x.\, x = 7) \end{array}$$

Ein Satz ist eine Formel ohne freie Variablen.

Beispiel 5.42

$$\exists x.\, \exists y.\, x = y \qquad \exists y.\, \exists x.\, x = y$$

Mit S bezeichnen wir die Menge der arithmetischen Sätze.

Notation: $F(x_1, \ldots, x_k)$ bezeichnet eine Formel F, in der höchstens $x_1, \ldots, x_k$ frei vorkommen.

Sind $n_1, \ldots, n_k$ $\mathbb{N}$ so ist $F(n_1, \ldots, n_k)$ das Ergebnis der Substitution von $n_1, \ldots, n_k$ für die freien Vorkommen von $x_1, \ldots, x_k$.

Beispiel 5.41

$$\begin{aligned} F(x, y) &= (x = y \ \wedge \ \exists x.\, x = y) \\ F(5, 7) &= (5 = 7 \ \wedge \ \exists x.\, x = 7) \end{aligned}$$

Ein Satz ist eine Formel ohne freie Variablen.

Beispiel 5.42

$$\exists x.\ \exists y.\, x = y \qquad \exists y.\ \exists x.\, x = y$$

Mit S bezeichnen wir die Menge der arithmetischen Sätze.

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$ gdw t_1 und t_2 den selben Wert haben.

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$ gdw t_1 und t_2 den selben Wert haben.

$\neg F\ W$ gdw $F\ W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$ gdw t_1 und t_2 den selben Wert haben.

$\neg F\ W$ gdw $F\ W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F\ W$	gdw	$F\ W$
$(F \wedge G)\ W$	gdw	$F\ W$ und $G\ W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$	gdw	t_1 und t_2 den selben Wert haben.

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F\ W$	gdw	$F\ \cancel{W}$ $\notin W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F\ W$	gdw	$F \notin W$
$(F \wedge G)\ W$	gdw	$F\ W$ und $G\ W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$$\begin{array}{rll} (t_1 = t_2)\ W & \text{gdw} & t_1 \text{ und } t_2 \text{ den selben Wert haben.} \\ \neg F\ W & \text{gdw} & F\ W \\ (F \wedge G)\ W & \text{gdw} & F\ W \text{ und } G\ W \\ (F \vee G)\ W & \text{gdw} & F\ W \text{ oder } G\ W \\ \exists x.\, F(x) & \text{gdw} & \text{es } n\ \mathbb{N} \text{ gibt, so dass } F(n)\ W \end{array}$$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$$\begin{array}{rll} (t_1 = t_2)\ W & \text{gdw} & t_1 \text{ und } t_2 \text{ den selben Wert haben.} \\ \neg F\ W & \text{gdw} & F\ W \\ (F \wedge G)\ W & \text{gdw} & F\ W \text{ und } G\ W \\ (F \vee G)\ W & \text{gdw} & F\ W \text{ oder } G\ W \\ \exists x.\, F(x) & \text{gdw} & \text{es } n\ \mathbb{N} \text{ gibt, so dass } F(n)\ W \end{array}$$

Fakt 5.44

Für jeden Satz F gilt entweder $F\ W$ oder $\neg F\ W$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$$\begin{array}{rll} (t_1 = t_2)\ W & \text{gdw} & t_1 \text{ und } t_2 \text{ den selben Wert haben.} \\ \neg F\ W & \text{gdw} & F\ W \\ (F \wedge G)\ W & \text{gdw} & F\ W \text{ und } G\ W \\ (F \vee G)\ W & \text{gdw} & F\ W \text{ oder } G\ W \\ \exists x.\, F(x) & \text{gdw} & \text{es } n\ \mathbb{N} \text{ gibt, so dass } F(n)\ W \end{array}$$

Fakt 5.44

Für jeden Satz F gilt entweder $F\ W$ oder $\neg F\ W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$$\begin{array}{rll} (t_1 = t_2)\ W & \text{gdw} & t_1 \text{ und } t_2 \text{ den selben Wert haben.} \\ \neg F\ W & \text{gdw} & F\ W \\ (F \wedge G)\ W & \text{gdw} & F\ W \text{ und } G\ W \\ (F \vee G)\ W & \text{gdw} & F\ W \text{ oder } G\ W \\ \exists x.\, F(x) & \text{gdw} & \text{es } n\ \mathbb{N} \text{ gibt, so dass } F(n)\ W \end{array}$$

Fakt 5.44

Für jeden Satz F gilt entweder $F\ W$ oder $\neg F\ W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

$$\exists x.\, x + x = y$$

Die Menge der wahren Sätze der Arithmetik nennen wir W:

Definition 5.43

$(t_1 = t_2)\ W$	gdw	t_1 und t_2 den selben Wert haben.
$\neg F\ W$	gdw	$F\ W$
$(F \wedge G)\ W$	gdw	$F\ W$ und $G\ W$
$(F \vee G)\ W$	gdw	$F\ W$ oder $G\ W$
$\exists x.\, F(x)$	gdw	es $n\ \mathbb{N}$ gibt, so dass $F(n)\ W$

Fakt 5.44

Für jeden Satz F gilt entweder $F\ W$ oder $\neg F\ W$

NB Ob eine Formel mit freien Variablen wahr ist, kann vom Wert der freien Variablen abhängen:

$$\{y \mapsto 2\} \qquad \exists x.\, x + x = y \qquad W$$

Daher haben wir Wahrheit nur für Sätze definiert.

Definition 5.45

Eine partielle Funktion $f : \mathbb{N}^k\ \mathbb{N}$ ist arithmetisch repräsentierbar gdw es eine Formel $F(x_1, \dots, x_k, y)$ gibt, so dass für alle $n_1, \dots, n_k, m\ \mathbb{N}$ gilt:

$$f(n_1, \dots, n_k) = m \quad \text{gdw} \quad F(n_1, \dots, n_k, m)\ W$$

Definition 5.45

Eine partielle Funktion $f : \mathbb{N}^k\ \mathbb{N}$ ist arithmetisch repräsentierbar gdw es eine Formel $F(x_1, \dots, x_k, y)$ gibt, so dass für alle $n_1, \dots, n_k, m\ \mathbb{N}$ gilt:

$$f(n_1, \dots, n_k) = m \quad \text{gdw} \quad F(n_1, \dots, n_k, m)\ W$$

Satz 5.46

Jede WHILE-berechenbare Funktion ist arithmetisch repräsentierbar.

Definition 5.45

Eine partielle Funktion $f : \mathbb{N}^k\ \mathbb{N}$ ist arithmetisch repräsentierbar gdw es eine Formel $F(x_1, \dots, x_k, y)$ gibt, so dass für alle $n_1, \dots, n_k, m\ \mathbb{N}$ gilt:

$$f(n_1, \dots, n_k) = m \quad \text{gdw} \quad F(n_1, \dots, n_k, m)\ W$$

Satz 5.46

Jede WHILE-berechenbare Funktion ist arithmetisch repräsentierbar.

Satz 5.47
W *ist nicht entscheidbar.*

Korollar 5.48
W *ist nicht semi-entscheidbar.*

Satz 5.47
W *ist nicht entscheidbar.*

Korollar 5.48
W *ist nicht semi-entscheidbar.*

Wir kodieren Beweise als Zahlen.

Definition 5.49
Ein Beweissystem für die Arithmetik ist ein entscheidbares Prädikat

$$Bew : \mathbb{N} \times S \;\to\; \{0, 1\}$$

wobei wir $Bew(b, F)$ lesen als „b ist Beweis für Formel F“.
Ein Beweissystem Bew ist korrekt gdw

$$Bew(b, F) \implies F\ W.$$

Ein Beweissystem Bew ist vollständig gdw

$$F\ W \implies \text{es gibt } b \text{ mit } Bew(b, F).$$

Wir kodieren Beweise als Zahlen.

Definition 5.49
Ein Beweissystem für die Arithmetik ist ein entscheidbares Prädikat

$$Bew : \mathbb{N} \times S \;\to\; \{0, 1\}$$

wobei wir $Bew(b, F)$ lesen als „b ist Beweis für Formel F“.
Ein Beweissystem Bew ist korrekt gdw

$$Bew(b, F) \implies F\ W.$$

Ein Beweissystem Bew ist vollständig gdw

$$F\ W \implies \text{es gibt } b \text{ mit } Bew(b, F).$$

Satz 5.50 (Gödel)

Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.

Beweis:
Denn mit jedem korrekten und vollständigen Beweissystem kann man $\chi'_W(F)$ programmieren:

$b := 0$
while $Bew(b, F) = 0$ **do** $b := b + 1$
output(1)

□

Satz 5.50 (Gödel)

Es gibt kein korrektes und vollständiges Beweissystem für die Arithmetik.

Beweis:
Denn mit jedem korrekten und vollständigen Beweissystem kann man $\chi'_W(F)$ programmieren:

$b := 0$
while $Bew(b, F) = 0$ **do** $b := b + 1$
output(1)

□