≤ n Regeln, die schließlich hält, bei Input leeres Band zurücklegen kann, ist nicht rekursiv (sonst wäre „Busy-Beaver" rekursiv)

Wenn H rekursiv wäre, dann auch G; man müsste nur diejenigen Maschinen die stehenbleiben werden, ablaufen lassen und Ergebnisse vergleichen.

2009-01-30

Churchsche These (Church's Thesis)

Die durch Turing-Maschinen berechenbaren Funktionen entsprechen genau den Funktionen, für die ein Algorithmus existiert, der sie berechnet. (Da diese Formulierung nicht exakt ist, sondern intuitiv-umgangssprachlich, nicht beweisbar.)

Plausibel wird Church's Thesis durch die Tatsache, dass alle bisherigen Versuche Berechenbarkeit zu formalisieren die selbe Klasse von Funktionen geliefert haben.

zB.:

1) Turing-Maschinen
2) Berechenbarkeit durch Register-Maschinen.

Registermaschine hat Register R_i, $i \in \mathbb{N}$ in denen jeweils eine Zahl $\in \mathbb{N}_0$ stehen kann (zu Beginn in R_1 der Input, sonst 0) und endl. viele mit $1, \dots, n$ nummerierte Instruktionen I_k; jedes I_k von einer der folgenden Formen:

$R_i := 0$

$R_j := R_j + 1$

$R_j := R_i$

IF $R_j := R_i$ THEN GOTO I_k
ELSE GOTO I_e

3) Klasse der rekursiven Funktionen tatsächlich rekursiv definieren:

Zuerst eine Teilmenge „primitiver rekursiven Funktionen"

Initialfunktionen: $f: \mathbb{N}_0^n \to \mathbb{N}_0$ der Form

$f(k) = c$ Konstante Funktion

$f(k) = k+1$ Nachfolger

$f(k_1, \dots, k_n) = k_i$ für $1 \leq i \leq n$ Projektion auf i-te Koordinate

Zusammensetzung (Komposition) von Funktionen:

für $g: \mathbb{N}_0^m \to \mathbb{N}_0$, $h_i: \mathbb{N}_0^n \to \mathbb{N}_0$ $i = 1, \dots, m$ sei f def. als:

$f(x_1, \dots, x_n) = g(h_1(x_1, \dots, x_n), \dots, h_m(x_1, \dots, x_n))$

$f: \mathbb{N}_0^n \to \mathbb{N}_0$

Primitive Rekursionen:

$g: \mathbb{N}_0^n \to \mathbb{N}_0$, $h: \mathbb{N}_0^{n+2} \to \mathbb{N}_0$ definieren ein $f: \mathbb{N}_0^{n+1} \to \mathbb{N}_0$ wie folgt:

$f(0, x_1, \dots, x_n) = g(x_1, \dots, x_n)$

$f(k+1, x_1, \dots, x_n) = h(k, x_1, \dots, x_n, f(k, x_1, \dots, x_n))$

Kleinste Klasse von Funktionen, die initiale Fkt. enthält und bzgl. Zusammensetzung, primitiver Rekursion abgeschlossen ist. (Durchschnitt aller solcher Mengen von Fkt) heißt Klasse der „primitiv-rekursiven" Funktionen

Beispiel für rekursive, aber nicht primitiv rekursive Funktionen (nach Ackermann)

$A_0(x) = x+1$ $\quad A_{n+1}(x+1) = A_n(A_{n+1}(x))$

$A_{n+1}(0) = A_n(1)$

$A(n,x) = A_n(x)$ $\quad A: \mathbb{N}_0^2 \to \mathbb{N}$ nicht primitiv rekursiv. (aber rec n. Church)

$\forall f: \mathbb{N}_0^2 \to \mathbb{N}$ prim. rec. $\exists n: \forall a,b: f(a,b) < A_n(\max(a,b))$

Unbeschränkte Suche: gegeben $f: \mathbb{N}_0^{k+1} \to \mathbb{N}_0$ definieren $g: \mathbb{N}_0^k \to \mathbb{N}_0$ sodass $g(x_1,\dots,x_k) = y \Leftrightarrow f(x_1,\dots,x_k,y) = 0$ und $\forall z < y: f(x_1,\dots,x_k,z)$ definiert $\neq 0$.

$$g(x_1,\dots,x_n) = \begin{cases} \min\{y \mid f(x_1,\dots,x_k,y) = 0,\ f(x_1,\dots,x_k,z)\downarrow \text{ für } z<y\} \\ \text{undefiniert wenn } \nexists y: f(x_1,\dots,x_k,y) = 0 \text{ oder} \\ \quad \exists y: f(x_1,\dots,x_k,y)\uparrow \text{ und } f(x_1,\dots,x_k,z) \neq 0 \text{ für } z<y \end{cases}$$

(Partiell) Rekursive Funktionen: die kleinste Menge von Funktionen, die die initialen Fkt. enthält und bzgl. Zusammensetzung prim. Rek. und unbeschränkter Suche abgeschlossen ist.
[Def. von Zusammensetzung, prim. Rek. adaptieren auf partielle Fkt.:
f definiert genau dann, wenn alle Fkt auf der rechten Seite def. sind]
f berechenbar; $x_1,\dots,x_k$ fix: berechnen $g(x_1,\dots,x_n)$: für $y = 0,1,2,\dots$ $f(x_1,\dots,x_k,y)$ berechnen: entweder man kommt (erstmals) zu einer Nullstelle, einem y mit $f(x_1,\dots,x_k,y) = 0$, setze $g(x_1,\dots,x_k) = y$ oder Berechnung läuft ewig (entweder keine Nullstelle, oder man gerät an ein y sodass Berechnung von $f(x_1,\dots,x_n,y)$ ewig läuft) – dann g undefiniert.

Definition: Teilmenge $S \subseteq \mathbb{N}_0$ heißt rekursiv, wenn ihre charakteristische Funktion $\chi_S: \mathbb{N}_0 \to \{0,1\}$ def. durch $\chi_S(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$, rekursiv ist.
$S \subseteq \mathbb{N}_0$ heißt rekursiv aufzählbar, wenn $\exists f$:
f partiell rekursiv: $\operatorname{dom} f \subseteq \mathbb{N}_0 \to \mathbb{N}_0$ sodass $S = \operatorname{Im} f = f(\mathbb{N}_0)$
[r.e. recursively enumerable, e.e. effectively enumerable]

Bemerkung: r.e. Menge $\neq \emptyset$ auch durch total rekursive Funktion aufzählbar.
f partiell rek. mit $f(\mathbb{N}) = S$: konstruieren total rek. g:
1) 1. Schritt der Berechnung von $f(0)$
2) 2. Schritt der Berechnung von $f(0)$, 1. Schr. d. Berechn. v. $f(1)$
n) n-ter Schritt d. Berechnung von $f(0)$, .. 1. Schr. d. Berechn. v. $f(n)$

sobald erstmals die Berechnung eines $f(k)$ abbricht und einen Wert liefert, $g(0) := f(k)$, ab diesem Schritt $g(n)$ setzen auf den beim aktuellen Schritt aufgetauchten Wert von f, sonst auf $g(n-1)$.

Satz: S rekursiv $\Leftrightarrow$ S und $\mathbb{N}_0 \setminus S$ beide r.e.

Beweis: Ü [egal welche Def. von Berechenbarkeit man zugrunde liegt: intuitiv klar]

Beispiel: r.e. Menge, nicht rekursiv: die Nummern jener Turing Maschinen, die bei 0 halten.

Diophantische Mengen

Definition: $S \subseteq \mathbb{N}^k$ heißt Diophantisch, wenn $\exists$ Polynom $p \in \mathbb{Z}[x_1, \dots, x_k, y_1, \dots, y_m]$ sodass $(a_1, \dots, a_k) \in S \Leftrightarrow p(a_1, \dots, a_k; y_1, \dots, y_m)$ Nst in $\mathbb{Z}^m$ hat.

Satz (ohne Bew.) Matiyasievich et. al. (Robinson, ...)
Die diophantischen Mengen sind genau die r.e. Mengen

Folgerung: Hilberts 10. Problem „gibt es einen Alg. zur Entscheidung ob ein Polynom in mehreren Var. mit koeff $\in \mathbb{Z}$ $p \in \mathbb{Z}[y_1, \dots, y_m]$ eine Nullstelle in $\mathbb{Z}^m$ hat?" hat Antwort NEIN.

Bemerkung: ob man Nullst. in $\mathbb{Z}^m$ oder $\mathbb{N}_0^m$ betrachtet egal:
$f \in \mathbb{Z}[y_1, \dots, y_m]$ hat Nst in $\mathbb{N}_0^m$ genau dann, wenn
$g = f(y_{11}^2 + y_{12}^2 + y_{13}^2 + y_{14}^2, \dots, y_{m1}^2 + y_{m2}^2 + y_{m3}^2 + y_{m4}^2)$ eine Nullstelle in $\mathbb{Z}^{4m}$ hat und
$f \in \mathbb{Z}[y_1, \dots, y_m]$ hat Nullst. in $\mathbb{Z}^m$ genau dann, wenn
$g = f(y_{11} - y_{12}, y_{21} - y_{22}, \dots, y_{m1} - y_{m2})$ eine Nullst. in $\mathbb{N}_0^{2m}$ hat.

Unlösbarkeit von Hilberts 10. Probl. folgt aus Satz „ r.e. $\Leftrightarrow$ diophantisch" so:

wähle $S \subseteq \mathbb{N}_0$, S r.e., nicht rekursiv, dann $\exists p \in \mathbb{Z}[x, y_1, \ldots, y_m]$ sodass $p(s, y_1, \ldots, y_m)$ Nullst. in $\mathbb{Z}^m$ hat genau dann, wenn $s \in S$.

Hätte man Entsch.alg. für Existenz ganzzahliger Nullst. von $p(s, y_1, \ldots, y_m)$, wäre S rekursiv.

Folgerung: $S \subseteq \mathbb{N}_0$ ist r.e. genau dann, wenn $\exists f \in \mathbb{Z}[x_1, \ldots, x_n]$ sodass $S = \mathbb{N}_0 \cap f(\mathbb{Z}^n)$. Sei S r.e. $Q \in \mathbb{Z}[x, y_1, \ldots, y_m]$ sodass $Q(s, y_1, \ldots, y_m)$ Nullst. hat $\Leftrightarrow s \in S$. $P(x, y_1 \ldots y_m) = (x+1)(1 - Q(x, y_1, \ldots, y_m)^2) - 1$

für x einsetzen $\in \mathbb{N}_0$, für $y_1, \ldots, y_m \in \mathbb{Z}$ einsetzen; s tritt als Wert von $P(\mathbb{N}_0 \times \mathbb{Z}^n) \cap \mathbb{N}_0$ auf genau dann, wenn $s \in S$; für x einsetzen $x_1^2 + x_2^2 + x_3^2 + x_4^2$