Stunden 5,6

Sunday, April 25, 2010
20:46

Berechnung für andere Bereiche als $\mathbb{N}$

Haben gesehen: Wir können Folgen natürlicher Zahlen $(x_0, \ldots, x_{n-1})$ als nat. Zahl $\langle x_0, \ldots, x_{n-1} \rangle$ kodieren.

Auf diese und ähnliche Weise können wir viele andere Bereiche kodieren und Berechenbarkeit, Entscheidbarkeit und r.e. für diese Bereiche kodieren.

Insbesondere:

$\mathbb{Z}$: kodiere $z = (-1)^a b$ als $\ulcorner z \urcorner = \langle a, b \rangle$ (um Fkt eindeutig zu machen: für $a \in \{0,1\}$ und $b > 0$ oder $a = b = 0$)

Sei $f : \mathbb{Z} \to \mathbb{Z}$. Def $\tilde{f} : \mathbb{N} \to \mathbb{N}$ sd.
$\tilde{f}(\ulcorner z \urcorner) = \ulcorner f(z) \urcorner$ (und zB $\tilde{f}(x) = 0$, falls x kein Code)

Def: f rekursiv gdw $\tilde{f}$ rekursiv.

Genauso: $A \subseteq \mathbb{Z}$ rekursiv $:\Leftrightarrow \{\ulcorner z \urcorner : z \in A\} \subseteq \mathbb{N}$ rek.
(und analog für r.e. etc).

Bem: (·) $A \subseteq \mathbb{Z}$ rek. $\Leftrightarrow K_A : \mathbb{Z} \to \mathbb{Z}$ rek.

(·) Hätten Registermaschinen so def. können dass in jedem Register Element von $\mathbb{Z}$ steht, das hätte zu selben Begriff von rek. geführt.

(·) Analog für Fkt: $\mathbb{Z}^n \to \mathbb{Z}^m$ etc

Bsp: natürlich sind Addition, Multiplikation, Division mit Rest, etc etc alles rek. Fkt

$\mathbb{Q}$: Kodiere $q = (-1)^a \frac{b}{c}$ als $\ulcorner q \urcorner = (a, b, c)$
für $(a = b = 0, c = 1)$ oder $a \in \{0,1\}, b, c > 0$, $ggT(b,c) = 1$

Rest analog wie für $\mathbb{Z}$

Stunden 5,6 (Forts.)

Sunday, April 25, 2010
21:05

$\mathbb{N}^n$: Wir haben bereits def. was es heißt dass $f: \mathbb{N}^n \to \mathbb{N}$ rekursiv ist (bzw dass $A \subseteq \mathbb{N}^n$ rek. ist). Äquivalent hätten wir verwenden können:

Für $f: \mathbb{N}^n \to \mathbb{N}$ def $\tilde{f}: \mathbb{N} \to \mathbb{N}$ durch

$$\tilde{f}(z) = \begin{cases} f(x_1 \ldots x_n), & \text{wenn } z = \langle x_1 \ldots x_n \rangle \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt: f rek. gdw $\tilde{f}$ rek.

Wir hätten uns also bei der Def von rek. gleich auf Fkt von $\mathbb{N}$ nach $\mathbb{N}$ beschränken können.

Polynome zB aus $\mathbb{Z}[X_1 \ldots X_{17}]$

Ein Monom π hat die Form $(-1)^a \cdot b \cdot X_1^{c_1} \cdots X_{17}^{c_{17}}$ für $a \in \{0,1\}$, $b, c_1, \ldots, c_{17} \in \mathbb{N}$

Der Code $\ulcorner \pi \urcorner$ von π sei $\langle a, b, c_1, \ldots, c_{17} \rangle$.

Der Code $\ulcorner p \urcorner$ eines Polynoms $p \in \mathbb{Z}[X_1 \ldots X_{17}]$ der Form $\sum_{i<n} \pi_i$ sei $\langle \ulcorner \pi_0 \urcorner, \ldots, \ulcorner \pi_{n-1} \urcorner \rangle$.

(Bem: man kann noch eine Ordnung einführen, um jedem Polynom einen eindeutigen, von der Ordnung unabhängigen, Code zu geben)

Eine Fkt $f: \mathbb{Z}[X_1, \ldots, X_{17}] \to \mathbb{Z}[X_1 \ldots X_{17}]$ ist rek, wenn $\tilde{f}: \ulcorner p \urcorner \mapsto \ulcorner f(p) \urcorner$ (od 0, falls kein Code) rek. ist.

Genauso: $A \subseteq \mathbb{Z}[X_1 \ldots X_{17}]$ entscheidbar (= rekursiv), wenn $\{\ulcorner p \urcorner : p \in A\} \subseteq \mathbb{N}$ entscheidbar.

Stunden 5,6 (Forts.)

Sunday, April 25, 2010
21:18

10. Hilbertsches Problem / Satz von Matijasevitch:

Satz: $N = \{ \ulcorner p \urcorner \in \mathbb{Z}[X_1 .. X_{17}] : p$ hat zumindest eine ganzzahlige Nullstelle $\}$ ist nicht entscheidbar (aber natürlich r.e.).

(Ohne Beweis. Beweisidee: Konstruiere auf effiziente (= rekursive) Art zu jeder Maschine M ein Polynom p sd: M hält auf Input $\ulcorner M \urcorner$ gdw p hat ganzz. NS.
(D.h. finde $f: \mathbb{N} \to \mathbb{N}$ rek. sdass für alle x gilt $f(x) \in N$ gdw $x \in H$. Wäre N rek., dann auch H, Widerspruch.
Diese Konstruktion braucht etwas (elementare) Zahlentheorie.)

Ähnliche Ergebnisse gibt es in anderen Gebieten, zB Wortproblem in Gruppen:
Sei G erzeugt durch $a_1 \dots a_n$. Ein Wort w hat die Form $b_1^{e_1} \cdot b_2^{e_2} \cdots b_m^{e_m}$, wobei $b_i \in \{a_1 \dots a_n\}$ und $e_i \in \mathbb{Z}$ für alle $i \leq m$.

Satz (ohne Bew.)

Es gibt Gruppe G die def ist durch endl. viele Erzeuger $a_1 \dots a_n$ und endl. viele Relationen $w_1 = 1$, $w_2 = 1$, $\dots$ $w_N = 1$ so dass das Wortproblem: (Ist $w = 1$?) unentscheidbar ist.
(Bem: Auch hier kann man eine Übersetzung finden von Computer M in Wort w^M sd. M hält gdw $w^M = 1$)
Bem: Wortproblem ist natürl. r.e. (wieso?)

Stunden 5,6 (Forts.)

Sunday, April 25, 2010
21:28

<u>Zeichenketten</u>

Man kann auch (was dem Begriff des math. Algorithmus vielleicht besser entspricht) ganz allgemein Zeichenketten (zu einem recht umfassenden mathematischen Alphabet) kodieren:
(Alphabet: Menge von Buchstaben)

Dann wäre das Polynom "$-17 \cdot X \wedge 12 + 3 \cdot X \wedge 5$" eine Folge
$(-, 1, 7, \cdot, X, \wedge, 1, 2, +, 3, \cdot, X, \wedge, 5)$

Jeder Buchstabe bekommt eine eindeutige Zahl, zB

$(11, 1, 7, 12, 20, 13, 1, 2, 14, 3, 12, 20, 13, 5)$

und diese Folge von Zahlen kodiert man mit der üblichen $\langle\,\rangle$ Fkt als einzige Zahl.

(Auf diese Weise kann man zu jedem endl. Alphabet Σ den Zeichenketten (= endliche Folge von Buchstaben) Σ^* codes in $\mathbb{N}$ zuordnen.)

Auch so kann rek. zB für $\mathbb{Z}[X_1 .. X_{17}]$ def., natürlich mit demselben Ergebnis.

Im Ziegler-Skr. sind Registermaschinen so def., daß sie mit Zeichenketten operieren.

Es gilt: $f: \Sigma^* \to \Sigma^*$ ist Ziegler-Skript-berechenbar $\Longleftrightarrow$ $\tilde{f}: \mathbb{N} \to \mathbb{N}$ $\ulcorner \sigma \urcorner \mapsto \ulcorner f(\sigma) \urcorner$ ist berechenbar