Zu Hilbert's 10. Problem nach Matijasevic 1975/80

(Exponential-diophantische Beschreibung einer kleinen universellen Turing-Machine (UTM).)

G. Hasenjaeger

A Vorgeschichte. Rekursiv aufzählbar (r.e.) (1935/6 Turing,Post) wurde sukzessive auf $\exists x(\forall y<x)\exists z_1..z_4$ "Pol"$(a,x,y,z_1,..z_4)$ $\exists\vec{x}$ "Expl"$(a,\vec{x})$ (Davis 1960) und auf $\exists\vec{x}$ "Pol"$(a,\vec{x})$ (Matijasevič 1970) reduziert. Ausführliche Darstellung in Davis (1973). Obwohl in der Exponential-Polynomgleichung "Expl" auch "u^v" erlaubt war, brauchte die "$(\forall y<x)$"-Version die im wesentlichen polynomiale Folgencodierung von Gödel (1931), (Reste nach teilerfremden Divisoren), um die Eigenschaft einer Berechnungsfolge durch "$(\forall y<x)$" auszudrücken. Vielleicht angeregt durch Singmaster (1974) gab Matijasevič (1975/80) eine Beschreibung des Verhaltens von Turingmaschinen durch zugeordnete Semi-Thue-Systeme, ~~die~~ mit einer einfachen Folgencodierung (die nicht so neu war) und einer Beschreibung von deren Verhalten, (die das wesentlich Neue ausmacht). Eine Variante für Minsky-Maschinen von Jones-Matijasevič (1980/84) wurde mir durch E. Börgers Vorträge (Bonn III.1982, Oberwolfach IV.1982) bekannt, nach dem Vortrag von Jones (Bonn 8.X.1982) ~~hier~~ über auch Matijasevič (1975/80). Nach Börgers Vorträgen hatte ich versucht, das Neue Werkzeug auf die Beschreibung einer kleinen UTM anzuwenden, und da meine Version hinreichend verschieden von Matijasevič (1975/80) ist, wird sie hier dargestellt.

B Das Werkzeug

$$dig(a,b,i)=c :\leftrightarrow \exists xy(a=x\cdot b^{i+1}+c\cdot b^i+y \wedge c<b \wedge y<b^i)$$

$$\binom{a}{b}=dig((2^a+2)^a,2^a+1,b)$$

$S_a := \{x \mid [{}^a/_{2^x}] \equiv 1 \bmod 2\}$, (im folgenden odd für ungerade),

$S_a \cap S_b = \emptyset \leftrightarrow \binom{a+b}{a}$ odd (Mat. 1975/80 nach Kummer 1852)

$S_b \subseteq S_a \leftrightarrow \binom{a}{b}$ odd (Mat. 1980/84 nach Lucas 1877)

Beweis auch durch Induktion über die Länge der Dual-Schreibweise von a,b für $S_b \subseteq S_a$, mit $2 \mid \binom{2a}{2b+1}$, $2 \mid \left(\binom{2a}{2b}-\binom{a}{b}\right)$. Dann auch $S_a \cap S_b = \emptyset \leftrightarrow S_a \subseteq S_{a+b}$.

Ich benutze außerdem eine "Zusammenfassung" beider "Beobachtungen":

$S_a \cap S_b = S_c \leftrightarrow S_c \subseteq S_a \wedge S_c \subseteq S_b \wedge S_a \cap S_b \cap S'_c = \emptyset$

Mit $S_x \subseteq S_y \rightarrow S_y \setminus S_x = S_{y-x}$ hat man

$S_a \cap S_b \cap S'_c = S_a \cap S_{b-c} = S_b \cap S_{a-c}$, also

$S_a \cap S_b = S_c \leftrightarrow \binom{a}{c} \cdot \binom{b}{c} \cdot \binom{a+b-c}{a} \cdot \binom{a+b-c}{b}$ odd

und wegen $\binom{a}{c} \cdot \binom{a+b-c}{a} = \dfrac{(a+b-c)!}{c!(a-c)!(b-c)!} = \binom{b}{c}\binom{a+b-c}{b}$

sogar $S_a \cap S_b = S_c \leftrightarrow \binom{a}{c} \cdot \binom{a+b-c}{a}$ odd, (z.B.).

Vielleicht nützlich sind auch (mit $S_x \cap S_y = \emptyset \rightarrow S_x \cup S_y = S_{x+y}$)

$S_a \setminus S_b = S_c \leftrightarrow \binom{a}{c} \cdot \binom{b+c}{a}$ odd, auch $\leftrightarrow \binom{b}{a-c} \cdot \binom{b+c}{b}$ odd

und

$S_a \cup S_b = S_c \leftrightarrow \binom{c}{a} \cdot \binom{a}{c-b}$ odd, (z.B.)

Mehrstellige boolesche Beziehungen analog ohne Quantifikation für die Komposition auszudrücken, ist mir nicht gelungen. Vgl. aber G.

C Die Folgencodierung als Menge"gedacht"

Ist b eine Potenz von 2 und die Glieder a_0-a_K einer Folge als Dualzahlen gegeben, so lassen sich die benutzten Bedingungen für Folgencodierungen $c = \sum_{i \le k} a_i b^i$ ausdrücken als Bedingungen für die als S_c codierten Mengen, mit $a \subseteq b :\leftrightarrow S_a \subseteq S_b$

Wegen (z.B.) $\forall ab \exists^{=1} c$ $\binom{a}{c}\binom{a+b-c}{a}$ odd wird auch $a \subseteq b$ (ggf. auch

$a \tilde{>} b$, $a \tilde{\subset} b$) geschrieben, i.allg. sollen Großbuchstaben ausdrücken, daß Zahlen als (Darstellung von) Mengen $\subset \mathbb{N}$ zu denken sind.

Statt ein Band durch 2 "Keller" darzustellen und die Operation darauf ($2x$, $2x+1$, $\lceil x/2 \rceil$) zu programmieren, werde das Band an den "ungeraden" Stellen einer äquidistanten Folge A mit dem beobachteten Feld "aufgehängt", wobei die geraden Stellen B als Begrenzung dienen.

Sei $q=2^{m \cdot l+1}$, $\pi=2(m \cdot l+1)$, $b=2^{\pi}$, also $b=q^2$, wobei später l die Länge einer Programmschleife wird, π die Periode der Aufhänger-, bzw. Begrenzungspunkte. Dies wird durch $B = \sum_{i<e+1} b^i$, $A = q \cdot B$ erreicht. Die "lokale Maske" $M = \sum_{i+1<\pi} 2^{i+1}$ füllt gerade das Gebiet zwischen den beiden kleinsten "Punkten" von B . Ist nun T ein Protokoll der "Geschichte" des Bandes, so kann durch $T \cap B = 0$ oder durch $T \tilde{\subset} B \cdot M$ ausgedrückt werden, daß sich "Kopf" und "Schwanz" benachbarter Darstellungen nicht stören. (Die 2. Bedingung ist formal etwas stärker, da sie auch am oberen Ende der Darstellung (unwesentlich) einschränkt.) $M = q^2 - 2$.

Bem.: Abweichend von meiner Darstellung am 12.10. in Paderborn ist jetzt A+B eine "ordentliche" geometrische Summe, die Jones' Zahl/Menge I entspricht.

D. Die "Geschichte" eines Bandes

Eine "normierte Berechenbarkeit" (s. H.) soll das Argument x durch x+1 Einsen, codiert $(2^{x+1}-1)$, darstellen, deren letzte das "beobachtete Feld" ist. "x akzektiert" könnte durch Ende der Rechnung mit Wert = 0 , also $(2^{x+1}-1) \cdot 4+1$ mit der letzten Eins als beobachtetem Feld, sein. Dann soll eine Zusatzprozedur (Teil des normierten gelesenen Programms) das Argument löschen und zur einzigen 1 (die 0 darstellt) zurückkehren.

Mit l = Band ein Feld nach links

r = " " " " rechts

č = Wechsel des vorliegenden Feldinhalts (1/0, 0/1)

j = bei Beobachtung 1 Sprung in die Programmschleife

h = " " halt und Löschen der letzten 1

hat man statt des vorläufigen"halt"die Programmfolge

r r̆ j l č l j l h s. L_a am Ende von H.

Durch $S_o = T_{\Omega}A$ wird die Folge der bei A beobachteten Felder des Bandes beschrieben (2-Zeichenalfabet {0,1}).
(Größeres Alfabet, $\leq 2^k$, durch k Bänder mit gleichem Bewegungsgesetz möglich.)

Sei $K \subseteq B$, also $q \cdot K \subseteq A$, eine Beschreibung der Stellen/Zeitpunkte, an denen das Band nicht nach rechts bewegt wird, ebenso $L \subseteq B$, also $q \cdot L \subseteq A$, eine Beschreibung der Stellen, an denen das Band nach links bewegt wird. Ferner seien $E, F \subseteq A$ Beschreibungen der Stellen, an denen 1 durch 0 (eraze) bzw. 0 durch 1 (fill) ersetzt wird.
Ferner seien $T_K = T_{\Omega}(K \cdot M)$, $T_L = T_{\Omega}(L \cdot M)$ die durch K bzw. L mittels der lokalen Maske aus der Geschichte des Bandes ausgeblendeten Teile. Damit ist die definierende Bedingung für die Geschichte des Bandes:

$$T = (q^2/2) \cdot (T + T_K) + q^2 \cdot (T_L + F - E) + q(2^{x+1} - 1)$$

(Durch das Verlegen des "Aufräumens" in die Programmcodierung kann hier die aufwendigere linke Seite

$T + (q^2)^{e+1} \cdot ((2^{x+1} - 1) \cdot 4 + 1)$ e beschreibt das Ende der Rechnung

vermieden werden.) Die Rechtsverschiebung (eine Stelle weniger als π) wird gerade durch T_K aufgehoben, die Linksverschiebung (eine Stelle mehr als π) wird durch Addition von T_L bewirkt.

Die Verwendung von F und E entspricht der Operation + 1 bzw. - 1 bei Jones/Mat. (1980/84), wobei hier aber ein Übertrag durch die Definitionen von F und E ausgeschlossen sein muß.

E. Übersetzung einer Maschinentafel. Dies könnte analog zu Jones-Mat. (1980/84) geschehen. Die univereelle Maschine, die eine Programmschleife aus "Elementarmaschinen" liest, erscheint (mir) einfacher.

F. Lesen einer Programmschleife. Das Programm soll als Schleife aus l 2-Bit-Signalen gegeben sein, "also" als Zahl p mit $p<2^{2a}$. Mit $P = p\cdot\sum_{i<} 2^{2a\cdot i}$ wird p so oft wiederholt, daß es an allen"Stellen 3A" zur Verfügung steht. Entsprechend zum jeweils beobachteten Feld des Bandes

$$S_o = T_{\wr}A$$

werden 2 benachbarte Stellen der Schleife durch

$$S_1 = P_{\wr}A \quad \text{und} \quad 2S_2 = P_{\wr}2A$$

beschrieben ("3A" setzt jeweils eine Maske für 2 benachbarte Stellen, der Wert der linken Stelle wird durch S_2 wieder an der Stelle A angegeben.) Das Programm ist dann ein zyklisch wiederholtes "Fourletter-word", dessen Anfang "bei q", als kleinsten"Punkt" von A, vorliegen soll. Die Länge von (Vorwärts!)-Sprüngen "bei 1" werde in einem Zähler J registriert, der "bei q" auf 0 steht und dessen 0-Stellung durch $S_3 \subsetneq A$, (d.h. die Stelle von $S_3 = 0 \leftrightarrow$ der lokale Teil von J = 0), durch

$$A\cdot 2^{1-J} \subsetneq A\cdot 2^{1-S_3}$$

angezeigt wird (jeder Sprung ist kürzer als die Schleife). Schließlich werde durch $S_{\ }$, $S_{\ } \subsetneq A$, angezeigt, ob das Verhalten der Maschine von S_3 (Zähler 0 bzw. $\neq 0$) oder von S_0 (Feld von T) abhängt (also 2 Zustände möglich).

J_+ bzw. J_- beschreibe die Stellen, an denen zum Zähler 1 addiert bzw. subtrahiert wird. Am Ende der Rechnung soll der Zähler auf 0 stehen. Dann wird die "Geschichte" des Zählers (nach dem Vorbild von Jones-Mat.(1980/84) beschrieben durch

$$J = q^2(J+J_+-J_-)$$

Die Operationen auf das Band und auf den Zähler sind "bei A" lokal als boolesche Funktionen von $S_0,\ldots,S_3,S$ zu beschreiben.

G. Boolesche Funktionen "bei A"

Rationeller als durch Komposition der Funktionen gemäß **B**, lassen sich die booleschen Hilfsfunktionen (von $S_0,\ldots,S_3,S$) K,L,E,F,J_+ wie folgt bestimmen (J_- und $S_{"neu"}$ haben eine etwas andere Struktur). Für $X_i \subseteq A$, $Y \subseteq A$ ist $Y = \bigvee_{i<8} X_i$ bestimmt durch

$$8A-\Sigma X_i \subseteq 8A-Y$$

Bei Anwendungen sind ggf. auch einige X_i durch $A-X_i$ bzw. Y durch A-Y zu ersetzen (unbenutzte Variable durch 0 bzw. A-0). Der volle "Reichtum" konjunktiver oder disjunktiver Normalformen tritt hier nicht auf; ob sich die speziellen einfacheren Lösungen (die hier nicht benutzt werden) für $\leftrightarrow$, $\nleftrightarrow$

$Z = X \leftrightarrow Y$ ausgedrückt durch $A-Z \subseteq X+Y \subseteq 3A-Z$ $\quad Z \subseteq A$

$W = X \nleftrightarrow Y$ " " $W \subseteq X+Y \subseteq 2A+W$ $\quad W \subseteq A$

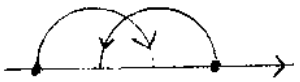
verallgemeinern lassen, konnte ich noch nicht klären.

H. Normierte Berechenbarkeit (Variante von Hermes' "keit³")

Die Zahl x wird durch x+1 Einsen dargestellt; ausgezeichnetes Feld ist aber das letzte (rechts) in der Zahl. Programme sind(zunächst) Folgen aus $\{\varepsilon,l,r,j\}$, die hier nach rechts fortschreitend gelesen werden (die Beziehung zwischen l und π kehrt dies später um, Dies geht in die Bestimmung von p ein ; das Programm wird dann nach rechts geschoben).

Die Sprungziele von

j : if$\langle S_0 \rangle$=1, then goto... (d.h. wo S_0"1" zeigt,...)

anzuzeigen, genügen 2 Klammerkonventionen, da  nicht stört und  nicht vorkommen.

"(...j)" bezeichne den Sprung ... nach "(", also rückwärts,

"j[...]" " " Sprung ... nach "]", also vorwärts.

Nachdem am Ende des Programms "halt bei $\langle S_0 \rangle$=1", also $\delta\alpha$, angefügt und die Schleife geschlossen ist (č,l,r sind α,β,γ!), sind alle j durch $\delta^k\beta$ zu ersetzen, mit den k , die sich durch die Interpretation der (...j) , j[...] ergeben.

Hilfsprozeduren

$K_n = (rj)^n l(č(lj)^{n+1} č(rj)^{n+1} člj)(lj)^2 r$

kopiert hinter die letzte von mindestens n Zahl(darstellung)en die von rechts gezählt n-te.

$L_1 = (črj)r$ löscht die letzte Zahl(...) und geht auf die vorige.

$L_2 = (rj)r(člč(lj)rč(rj)rj)lč(lj)rčr$

löscht die vorletzte Zahl(...) und rückt die letzte heran.

Grundfunktionen

$O = L^2č$ Null (ggf.) hinter die letzte Zahl gesetzt,

$S = K_1 lč$ Nachfolger der letzten Zahl hinter diese gesetzt,

$P_i^n = K_{n+1-i}$ Die Projektion wie üblich.

Normierte Einsetzung H zu $h(\vec{x}) = g(f_1(\vec{x}),\ldots,f_n(\vec{x}))$ mit G zu g, F_i zu f_i

$H = F_1 K_{m+1}^m F_2 L_2^m K_{m+2}^m F_3 \ldots L_2 K_{m+n-1}^n F_n L_2^m G L_2^n$

Primitive Rekursion H zu $h(0,\vec{y}) = f(\vec{y})$, $h(Sx,\vec{y}) = g(x,\vec{y},h(x,\vec{y}))$ mit F,G zu f,g

$H = F(rj)^{n+1} r^2 čj[č(č(lj)^{n+2} rGL_2 (rj)^{n+2} γrj)č]č(lj)^{n+2} r$

Kleinstzahloperator H zu $h(\vec{x}) = \mu y f(\vec{x},y) = 0$ mit F zu f

$H = l[(L,]lčFčrj)r$

Aufräumen bei Ende der Rechnung mit f(x) = 0; Löschen des Arguments L_a = r(rj)1(ćlj)1

Einfacher als L_2; führt ebenso wie L_2 für f(x)≠0 auf eine durch die Bedingung für T nicht akzeptierte Situation.

I. Die Maschinentafel

Zeile	T S_0	P S_1	P S_2	J S_3	S	Operationen auf T	J	S	
0	{0 {1	1	1	0	1	ć {1 {0		1	α=(1,1) für ć
1		1	0	0	1	l		1	β=(1,0) " l
2		0	1	0	1	r		1	γ=(0,1) " r
3		0	0	0	1			0	δ=(0,0) " "if..."
4	1	1	1	(0)	0	ć 0		(?)	δα für halt bei 1
5	1	1	0		0			1	$\delta^S\beta$ " Sprunglänge
(6)	1	0	1		0				(Reserve)
7	1	0	0		0		+1	0	$\delta^S \to J$
8		1	1	1	1		-1	1	NoOp on T
9		1	0	1	1		-1	1	Countdown on J
10		0	1	1	1		-1	1	1 auf S_3 für $\dot{J}\neq 0$
11		0	0	1	1			1	($\dot{J}$ für J local?)
12	0	1	1		0			1	NoOp on T
13	0	1	0		0			1	zum nächsten
(14)	0	0	1		0				Befehl auf P
15	0	0	0		0			0	

Für qL, J_+, F, qK, J_-, S (neu), E, etwa nach Einfachheit geordnet, ergibt sich hieraus:

$qL = S_1 \wedge \neg S_2 \wedge \neg S_3 \wedge S$ $\quad J_+ = S_0 \wedge \neg S_1 \wedge \neg S_2 \wedge \neg S$ $\quad F = \neg S_0 \wedge S_1 \wedge S_2 \wedge \neg S_3 \wedge S$

$qK = \neg(\neg S_1 \wedge S_2 \wedge \neg S_3 \wedge S) = S_1 \vee \neg S_2 \vee S_3 \vee \neg S$

$J_- = (S_1 \vee S_2) \wedge S_3 \wedge S$ $\quad S\ (neu) = S_1 \vee S_2 \vee (S_3 \wedge S)$

$E = S_0 \wedge S_1 \wedge S_2 \wedge (\neg S_3 \vee \neg S)$. Berücksichtigt man aber, daß bei "legalen" Programmen Zeile 7 nicht vor Zeile 4 wirksam wird, so liefert die "(0)" einfacher $E = S_0 \wedge S_1 \wedge S_2 \wedge \neg S_3$.

K. Ziel: $x \in C \leftrightarrow \exists \vec{y} E(p,l,x,\vec{y})$, Konjunktion von Exponential-Polynomen E .

Programm *fünf C*

Variablen, die Abkürzungen für mehrfach benutzte Teilterme sind, können z.T. vermieden werden; nicht, wenn die Zwischenwerte nur relational definiert sind wie bei $\Omega, \tilde{\Omega}$.

$x \in C \leftrightarrow \exists qmreBAPS_0S_1S_2S_3JUVSW\ J_-J_+LFKET_kT_L[p,l,x,..]$ d.i.

$$
\begin{aligned}
&[q = 2^{1+ml} \wedge (2^{2l}-1)\cdot r = 2^{2l\cdot 2em}-1 \\
&\wedge (q^2-1)\cdot B = q^{2(e+1)}-1 \wedge A = q\cdot B \wedge P = r\cdot p \\
&\wedge T_{\tilde{\Omega}}E = 0 \wedge S_0 = T_{\tilde{\Omega}}A \wedge S_1 = P_{\tilde{\Omega}}A \wedge 2S_2 = P_{\tilde{\Omega}}2A \\
&\wedge S_3 \subsetneq A \wedge A\cdot 2^l - J \subsetneq A2^l - S_3 \wedge U = S_1 \tilde{\cup} S_2 \wedge V' = S_3 \tilde{\Omega} S \\
&\wedge W = U \tilde{\cup} V \wedge S = q^2(W - q^{2e+1}) + q \wedge J_- = U_{\tilde{\Omega}}V \\
&\wedge J_+ \subsetneq A \wedge 7A + S_0 - S_1 - S_2 - S \subsetneq 7A + J_+ \\
&\wedge L \subsetneq B \wedge 6A + S_1 - S_2 - S_3 + S \subsetneq 7A + qL \\
&\wedge F \subsetneq A \wedge 5A - S_0 + S_1 + S_2 - S_3 + S \subsetneq 7A + F \\
&\wedge K \subsetneq B \wedge 6A - S_1 + S_2 - S_3 + S \subsetneq 8A - qK \\
&\wedge E \subsetneq A \wedge 5A + S_0 + S_1 + S_2 - S \subsetneq 7A + E \\
&\wedge J = q^2(J + J_+ - J_-) \wedge T_K = T_{\tilde{\Omega}}K\cdot(q^2-2) \\
&\wedge T_L = T_{\tilde{\Omega}}L\cdot(q^2-2)\ldots \wedge T = q^2/2\cdot(T+T_K) + q^2(T_L+F-E) + q(2^{x+1}-1)]
\end{aligned}
$$

L. Literatur

* Davis (1973) Hilbert's tenth problem is unsolvable , Amer. Math Monthly 80 233-269.

Singmaster (1974) "Notes on binomial coefficients, I,II,II," J. London Math. Soc.,8,No. 3, 545-548,549-554,

* Matijasević (1975/80) A NEW PROOF OF THE THEOREM ON EXPONENTIAL DIOPHANTINE REPRESENTATION OF ENUMERABLE SETS* Jour. Soviet Math. 14(1980), 1475-1486 Resultat 1975 angekündigt.

Jones-Matijasevič (1980/84) Preprint für JSL 1984

*Darin ausführliche Bibliographie.

[1] Wegen $p<2^{2^l}$ ist $p^*=p+2^{2^l}$ als Programmnummer geeignet; damit "einfacher"

$x\in C_{p^*} \leftrightarrow \exists p l(p^*=p+2^{2^l} \wedge p<2^{2^l} \wedge \exists\vec{y}E(p,l,x,\vec{y}))$

$\leftrightarrow \exists\vec{y}E^*(p^*,x,\vec{y})$

Dann mit $x\in D \leftrightarrow x\in C_x$ wie üblich:

zwar d mit $x\in C_d \leftrightarrow x\in D$ prinzipiell definierbar, aber

$\overline{d}$ mit $x\in C_{\overline{d}} \leftrightarrow x\notin D$ unmöglich.

[2] Etwas einfacher, S und A-S auszutauschen.

[3] Von der Kombination von
Jones-Matijasevič (1980/84) DIRECT TRANSLATION OF REGISTER MACHINES INTO EXPONENTIAL DIOPHANTINE EQUATIONS

mit

Gregušová/Korec SMALL UNIVERSAL MINSKY MÁCHINES in Mathematical Foundations of Computer Science 1979, pp. 308-316

unter Verwendung der hier benutzten Techniken ist eine Lösung gleicher Größenordnung zu erwarten.