Flußdiagramme

Seien die k-TM $\mathcal{M}_i = (Z_i, A_i, \delta_i, z_{0,i})$ $(1 \leq i \leq n)$ gegeben, wobei o.B.d.A. $i \neq j \Rightarrow Z_i \cap Z_j = \emptyset$. Wir wollen nun Flußdiagramme über diesen Maschinen erklären. Dazu bilden wir zunächst $\mathcal{M} := (Z, A, \delta, z_0)$ mit $Z := \bigcup_{1 \leq i \leq n} Z_i$, $A := \bigcup_{1 \leq i \leq n} A_i$ und $\delta := \bigcup_{1 \leq i \leq n} \delta_i$.

Ein Pfeil $\mathcal{M}_i \longrightarrow \mathcal{M}_j$ bedeutet nun, daß die „Endzustände“ von $\mathcal{M}_i$ mit dem Anfangszustand von $\mathcal{M}_j$ verbunden werden, daß also Übergänge $(z, a, z_{0,j}, a, \mathtt{N})$ zu δ hinzugefügt werden für alle $(z, a) \in Z_i \times A_i$ mit $\delta_i(z, a) = \emptyset$. Ein markierter Pfeil $\mathcal{M}_i \xrightarrow{\zeta} \mathcal{M}_j$ schränkt dies auf den speziellen Zustand ζ ein. Dann werden nur Übergänge $(\zeta, a, z_{0,j}, a, \mathtt{N})$ zu δ hinzugefügt für alle $a \in A_i$ mit $\delta_i(\zeta, a) = \emptyset$.

Mit $start \longrightarrow \mathcal{M}_i$ drücken wir aus, daß $z_0 := z_{0,i}$ sei. Durch $\mathcal{M}_i \longrightarrow stop$ bzw. $\mathcal{M}_i \xrightarrow{\zeta} stop$ verdeutlichen wir die Endzustände der neuen Maschine.

Beispiel: Sei N die Maschine zur Berechnung der Nachfolgerfunktion und $Test := (\{z_0, z_1, ja, nein\}, A, \delta, z_0)$ gegeben durch

(z', a', r)	0	1	$\sqcup$
z_0	$(nein, \mathtt{0}, \mathtt{N})$	$(z_1, \mathtt{1}, \mathtt{R})$	$(nein, \sqcup, \mathtt{N})$
z_1	$(nein, \mathtt{0}, \mathtt{L})$	$(ja, \mathtt{1}, \mathtt{L})$	$(nein, \sqcup, \mathtt{L})$

Diese Maschine hält genau dann im Zustand ja, wenn die Bandinschrift mit 11 beginnt, sonst mit $nein$. Sie plaziert den Kopf stets wieder auf dem ersten Zeichen der Eingabe!

Dann bezeichnet das folgende Flußdiagramm eine Maschine, die so lange die Bandinschrift aus $\{0,1\}^*$ um Eins erhöht, bis diese mit 11 beginnt.

$$\begin{tikzcd} start \arrow[r] & N \arrow[r] & Test \arrow[r, "ja"] \arrow[l, bend left, "nein"] & stop \end{tikzcd}$$

Gödelisierung von TM

Idee: Mache Beschreibungen von TM selbst zum Objekt von Berechnungen.

Sei $\mathcal{M} = (Z, A, \delta, z_0)$ eine det. 1-TM mit $Z = \{z_0, \ldots, z_n\}$ und $A = \{a_0, \ldots, a_m\}$; dabei sei $a_0 = 0$, $a_1 = 1$, $a_2 = \#$ und $a_3 = \sqcup$. Ordne nun jedem Tupel

$$(z_i, a_j, z_k, a_l, r) \in Z \times A \times Z \times A \times \{\mathtt{L}, \mathtt{N}, \mathtt{R}\}$$

seine Kodierung $w_{i,j,k,l,\hat{r}} :=$

$$\#\#bin(i)\#bin(j)\#bin(k)\#bin(l)\#bin(\hat{r})$$

über $\mathbb{A} := \{0, 1, \#\}$ zu, wobei

$$\hat{r} := \begin{cases} 0 & \text{falls } r = \mathtt{N}; \\ 1 & \text{falls } r = \mathtt{R}; \\ 2 & \text{falls } r = \mathtt{L}. \end{cases}$$

Jede Konkatenation $w \in \mathbb{A}^*$ all dieser Wörter beschreibt nun die TM $\mathcal{M}$ vollständig. Sei $g : \mathbb{A}^* \to \mathbb{B}^*$ der durch $g(0) := 00$, $g(1) := 01$ sowie $g(\#) := 11$ bestimmte Homomorphismus. Wir nennen $g(w) \in \mathbb{B}^*$ eine *Gödelisierung* von $\mathcal{M}$ und $bin^{-1}(g(w))$ eine *Gödelnummer* von $\mathcal{M}$.

Eigenschaften der Gödelisierung

Satz: Haben $\mathcal{M}$ und $\mathcal{M}'$ eine gemeinsame Gödelisierung, so hält $\mathcal{M}$ angesetzt auf $v \in \mathbb{A}^*$ genau dann, wenn $\mathcal{M}'$ dies tut. Ist $f_{\mathcal{M}}(v) \in \mathbb{A}^*$, so ist $f_{\mathcal{M}}(v) = f_{\mathcal{M}'}(v)$.

Beweis: $\mathcal{M}$ und $\mathcal{M}'$ unterscheiden sich nur in trivialer Weise, nämlich durch die Numerierung von $Z \setminus \{z_0\}$ und $A \setminus \{0, 1, \#, \sqcup\}$.

Lemma: Eine Zeichenreihe $u \in \mathbb{B}^*$ ist genau dann Gödelisierung einer det. 1-TM, falls

- $u = g(w)$ für ein $w \in \mathbb{A}^*$;
- w besteht aus Wörtern $w_{i,j,k,l,\widehat{r}}$;
- kommen $w_{i,j,k,l,\widehat{r}}$ und $w_{i',j',k',l',\widehat{r}'}$ in w vor, so ist $(i, j) \neq (i', j')$.

„Umkehrung" der Gödelisierung

Wir ordnen nun einem Wort $u \in \mathbb{B}^*$ eine 1-TM $\mathcal{M}_u$ zu: Ist u nicht Gödelisierung einer 1-TM, so sei $\mathcal{M}_u$ eine Maschine, die für keine Eingabe hält. Andernfalls sei $w := g^{-1}(u)$ und $\mathcal{M}_u := (Z, A, \delta, z_0)$, $Z := \{z_0, \ldots, z_n\}$, $A := \{a_0, \ldots, a_m\}$. δ sei die Menge aller Tupel (z_i, a_j, z_k, a_l, r), deren Kodierung $w_{i,j,k,l,\widehat{r}}$ in w vorkommt, und n bzw. m seien die maximale Nummer eines Zustands bzw. Zeichens in diesen Tupeln.

Ist u Gödelisierung irgendeiner 1-TM, so auch von $\mathcal{M}_u$.

Korollar: Ist u Gödelisierung von $\mathcal{M}$, so hält $\mathcal{M}$ angesetzt auf $v \in \mathbb{A}^*$ genau dann, wenn $\mathcal{M}_u$ dies tut. Ist $f_{\mathcal{M}}(v) \in \mathbb{A}^*$, so ist $f_{\mathcal{M}}(v) = f_{\mathcal{M}_u}(v)$.

Universelle 1-TM

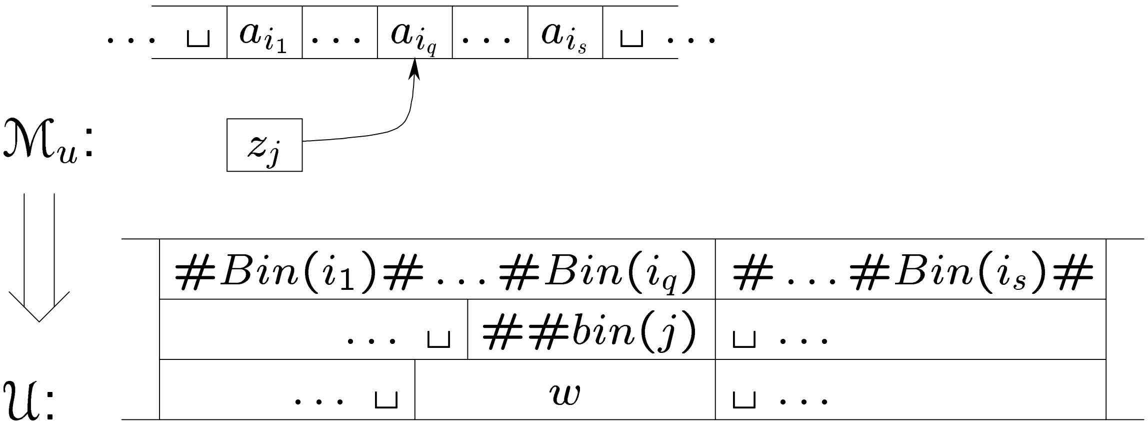
Satz: Es gibt eine 1-TM $\mathcal{U}$, so daß für $u \in \mathbb{B}^*$ und $v \in \mathbb{A}^*$ gilt:

- $\mathcal{U}$ angesetzt auf $u\#v$ hält genau dann, wenn $\mathcal{M}_u$ angesetzt auf v hält. Ist $f_{\mathcal{M}_u}(v) \in \mathbb{A}^*$, so ist $f_{\mathcal{U}}(u\#v) = f_{\mathcal{M}_u}(v)$.
- Benutzt $\mathcal{M}_u$ angesetzt auf v s Felder und macht t Schritte, so benutzt $\mathcal{U}$ angesetzt auf $u\#v$ $O(|u| \cdot s)$ Felder und macht $O(|u|^2(|v|^2 + t + l^2))$ Schritte, wobei $l := |f_{\mathcal{M}_u}(v)|$.

Idee: $\mathcal{U}$ angesetzt auf $u\#v$ testet zunächst, ob u Gödelisierung einer TM ist. Falls ja, simuliert $\mathcal{U}$ die Maschine $\mathcal{M}_u$ angesetzt auf v Schritt für Schritt; ansonsten hält $\mathcal{U}$ nicht.

Beweis: Sei $\mathcal{M}_u = (Z, A, \delta, z_0)$, $A = \{a_0, \ldots, a_m\}$ und $w := g^{-1}(u)$. $\mathcal{U}$ hat ein festes Alphabet und muß daher a_i durch $Bin(i)$ kodieren, die Binärdarstellung von i der Länge $\lfloor \log m \rfloor + 1$.

Die Bandbelegung ist wie folgt:



Simulation eines Schrittes:

- Hänge $\#bin(i_q)\#$ an Spur 2 an.
- Suche $\#\#bin(j)\#bin(i_q)\#$ auf Spur 3 (enthält w ein Wort $w_{j,i_q,j',i_{q'},\widehat{r}}$?) und ersetze die Inschrift von Spur 2 durch $\#\#bin(j')\#bin(i_{q'})\#bin(\widehat{r})\#$.
- Verschiebe Spur 2, bis $bin(j')$ und w rechtsbündig sind.
- Überschreibe $Bin(i_q)$ auf Spur 1 durch $Bin(i_{q'})$.
- Merke r und lösche $\#bin(i_{q'})\#bin(\widehat{r})\#$ auf Spur 2. Falls $r \neq \mathtt{N}$, müssen Spur 2 und 3 entsprechend verschoben werden.

Analyse: $\mathcal{U}$ benutzt höchstens $|u| + s \cdot (\lfloor \log m \rfloor + 2) + 3$ Felder. Wegen $\lfloor \log m \rfloor < |u|$ folgt die Behauptung: $O(|u| \cdot s)$ Felder.

Für den Test, ob u Gödelisierung einer TM ist, genügt Zeit $O(|u|^2)$ (Übung). Für das Präparieren der Bandbelegung (insbesondere $a_i \mapsto Bin(i)$) genügt Zeit $O((|u| \cdot |v|)^2)$.

Die meiste Zeit bei der Simulation eines Schrittes erfordert das Verschieben von Spur 2 und 3; deren Inschriften sind maximal $|u|$ lang und werden um $O(|u|)$ Felder verschoben: Zeit $O(|u|^2)$.

Das Rückgewinnen des Ergebnisses auf Spur 1 dauert analog zum Präparieren $O((|u| \cdot l)^2)$. Insgesamt: $O(|u|^2(|v|^2 + t + l^2))$.

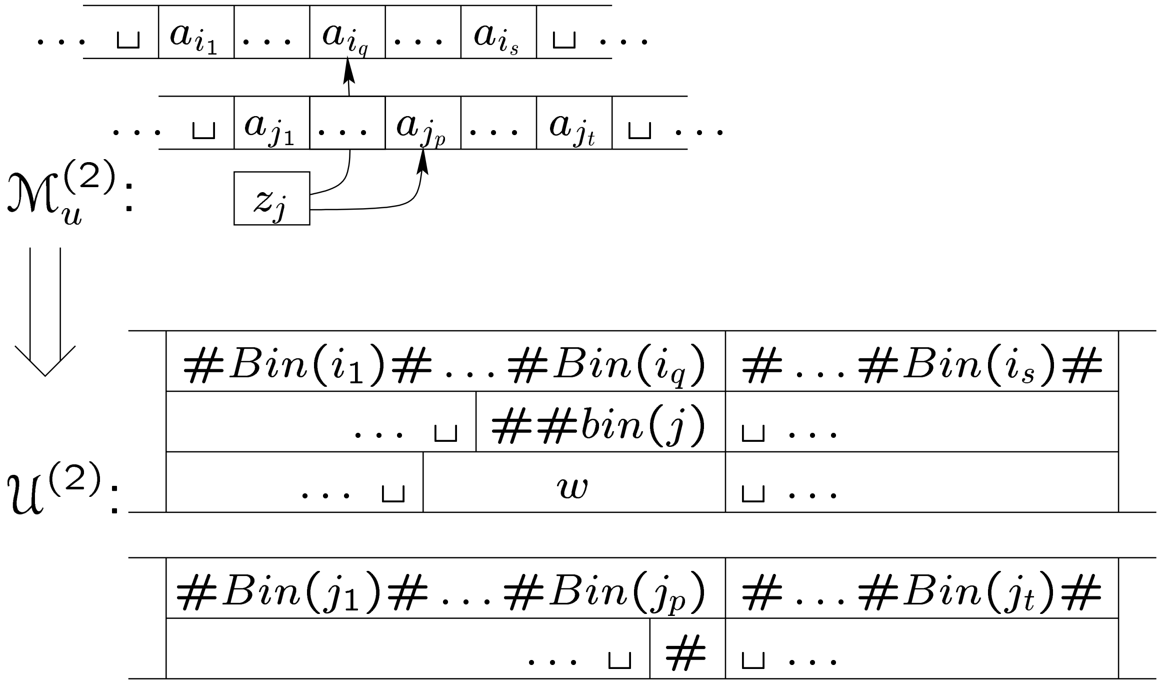
Universelle k-TM

Verallgemeinere Gödelisierungen auf k-TM für $k > 1$ und bezeichne die Umkehrung mit $\mathcal{M}_u^{(k)}$. Dann gilt der

Satz: Es gibt eine k-TM $\mathcal{U}^{(k)}$, so daß für $u \in \mathbb{B}^*$ und $v \in \mathbb{A}^*$ gilt:

- $\mathcal{U}^{(k)}$ angesetzt auf $u\#v$ hält genau dann, wenn $\mathcal{M}_u^{(k)}$ angesetzt auf v hält. Ist $f_{\mathcal{M}_u^{(k)}}(v) \in \mathbb{A}^*$, so ist $f_{\mathcal{U}^{(k)}}(u\#v) = f_{\mathcal{M}_u^{(k)}}(v)$.
- Benutzt $\mathcal{M}_u^{(k)}$ angesetzt auf v s Felder und macht $t \geq |v|$ Schritte, so benutzt $\mathcal{U}^{(k)}$ angesetzt auf $u\#v$ $O(|u| \cdot s)$ Felder und macht $O(|u|^2 \cdot t)$ Schritte.

Idee: Analog zum Fall $k = 1$, hier illustriert für $k = 2$:



Analyse: Mit Hilfe von 2 Bändern kann die Eingabe schon in Zeit $O(|u| \cdot |v|)$ präpariert und die Ausgabe in Zeit $O(|u| \cdot l)$ zurückgewonnen werden. Wegen $|v| \leq t$ und $l \leq |v| + t$ folgt: $O(|u|^2 \cdot t)$.

Entscheidbarkeit und Aufzählbarkeit

Definition: Eine Teilmenge $L \subset M$ (hier: $M = A^*$ oder $M = \mathbb{N}^k$) heißt genau dann *entscheidbar*, wenn ihre *charakteristische Funktion*

$$\chi_L : M \to \mathbb{B},\ x \mapsto \begin{cases} 1 & \text{falls } x \in L; \\ 0 & \text{sonst.} \end{cases}$$

berechenbar ist.

L heißt *rekursiv aufzählbar*, falls $L = \emptyset$ oder

$\exists\, f : M \to M$ berechenbar mit $f(M) = L$.

Sprechweise: f zählt L auf. Äquivalent: berechenbare Surjektion $\mathbb{N} \to L$.

Satz: L ist genau dann entscheidbar, wenn L und $\overline{L} := M \setminus L$ rekursiv aufzählbar sind.

Beweis: Übung.

Halteproblem

Definition: Die Menge

$$H_d := \{u \in \mathbb{B}^* \mid \mathcal{M}_u \text{ angesetzt auf } u \text{ hält}\}$$

heißt das *spezielle Halteproblem*.

Satz: Das spezielle Halteproblem ist unentscheidbar, d.h. $\chi_{H_d} : \mathbb{B}^* \to \mathbb{B}$ ist keine turingberechenbare Funktion.

Beweis: Durch Diagonalisierung. Angenommen, $\mathcal{M}$ sei eine TM mit

$$f_{\mathcal{M}}(u) = \begin{cases} 1 & \text{falls } \mathcal{M}_u \text{ angesetzt auf } u \text{ hält;} \\ 0 & \text{sonst.} \end{cases}$$

Daraus erhält man leicht eine Maschine $\mathcal{M}'$ mit

$$f_{\mathcal{M}'}(u) = \begin{cases} 1 & \text{falls } f_{\mathcal{M}}(u) = 0; \\ \text{undefiniert} & \text{sonst.} \end{cases}$$

[Fortsetzung des Beweis] Sei nun u' eine Gödelisierung von $\mathcal{M}'$:

$$\begin{array}{ll} & \mathcal{M}' \text{ angesetzt auf } u' \text{ hält} \\ \Longleftrightarrow & f_{\mathcal{M}}(u') = 0 \\ \Longleftrightarrow & \mathcal{M}_{u'} \text{ angesetzt auf } u' \text{ hält nicht} \\ \Longleftrightarrow & \mathcal{M}' \text{ angesetzt auf } u' \text{ hält nicht.} \end{array}$$

Korollar: Auch die Menge

$$H := \{u\#v \mid u \in \mathbb{B}^*,\ v \in \mathbb{A}^* \\ \mathcal{M}_u \text{ angesetzt auf } v \text{ hält}\},$$

das (allgemeine) *Halteproblem*, ist unentscheidbar.

Beweis: Die Abbildung $d : \mathbb{B}^* \to \mathbb{A}^*$ mit $d(u) := u\#u$ ist turingberechenbar und $\chi_{H_d} = \chi_H \circ d$.

Reduzierbarkeit

Definition: Sind $L, L' \subset A^*$ und es gibt eine berechenbare Funktion $f : A^* \to A^*$ mit

$$\forall\, w \in A^* : \;\; w \in L \iff f(w) \in L',$$

dann heißt L vermittels f *reduzierbar* auf L'. Schreibweise: $L \leq L'$.

Satz: • Die Relation $\leq$ ist transitiv.

- Ist $L \leq L'$ und L unentscheidbar, so ist auch L' unentscheidbar.

Beispiel: $H_d \leq H$ vermittels d. Auch

$$H_0 := \{u \in \mathbb{B}^* \mid \mathcal{M}_u \text{ angesetzt auf } \varepsilon \text{ hält}\}$$

ist unentscheidbar, wie man durch Reduktion von H auf H_0 zeigt (Übung).

Übrigens: H_0, H_d, H sind rekursiv aufzählbar!

Satz von Rice

Sei $\mathcal{T}$ die Menge aller turingberechenbaren Funktionen und $L \subset \mathcal{T}$ beliebig. Dann ist $\hat{L} := \{u \mid f_{\mathcal{M}_u} \in L\}$ genau dann entscheidbar, wenn $L = \emptyset$ oder $L = \mathcal{T}$.

Beweis: Sei $L \neq \emptyset$ und $L \neq \mathcal{T}$ sowie ω die überall undefinierte Funktion.

$\omega \in L$: Sei $f \in \overline{L}$ mit TM $\mathcal{M}$. $w \in \mathbb{B}^*$ wird eine TM $\mathcal{M}(w)$ zugeordnet: Angesetzt auf $v \in \mathbb{B}^*$ ignoriert $\mathcal{M}(w)$ zunächst die Eingabe und verhält sich wie $\mathcal{M}_w$ angesetzt auf ε. Hält $\mathcal{M}_w$, so verhält sich $\mathcal{M}(w)$ anschließend wie $\mathcal{M}$ angesetzt auf v; dann ist $f_{\mathcal{M}(w)} = f \notin L$ und sonst ist $f_{\mathcal{M}(w)} = \omega \in L$.
Man kann aus w effektiv eine Gödelisierung von $\mathcal{M}(w)$ berechnen, daher ist $\overline{H_0} \leq \hat{L}$.

$\omega \notin L$: Analog: $H_0 \leq \hat{L}$.