4.2 Ausdruckskomplexität

Wir untersuchen die Komplexität von $\mathrm{MC}(\mathcal{P}, \Sigma_{n+1})$ mit $\mathcal{P} = \{P\}$. Korollar 4.2 ergibt $\mathrm{MC}\big(\{P\}, \Sigma_{n+1}\big) \in n\mathsf{-EXPSPACE}$. Wir konstruieren eine einzige automatische Präsentation P so, daß, für alle $n \in \mathbb{N}$, das Auswerungsproblem $\mathrm{MC}\big(\{P\}, \Sigma_{n+1}\big)$ vollständig für $n\mathsf{-EXPSPACE}$ ist.

Idee Konstruiere feste automatische Struktur $\mathcal{A}$, in der $\mathcal{A}(P_w)$ für jedes w interpretiert werden kann. Da P_w aber auch von der TM M (und damit von n) abhängt, müssen wir genauer $\mathcal{A}(P_w)$ für alle w und beliebig komplizierte M in $\mathcal{A}$ interpretieren können.

Notationen Sei U eine wie üblich konstruierte universelle TM, d.h. bei Eingabe von w und dem Code einer TM M hält U genau dann, wenn $w \in L(M)$. Ist M f-platzbeschränkt, so verwendet U den Platz $f(|w|) + |M|$.

Lemma 4.5. *Sei $n \in \mathbb{N}$ beliebig und fest.*

*Das folgende Problem ist vollständig für $n-$*EXPSPACE*:*
Eingabe: x
Ausgabe: Hält U bei Eingabe von x mit Platzbedarf $F_n(|x|) - 2$?

Beweis:
Offensichtlich ist obiges Problem in $n-$EXPSPACE.

Sei nun M TM mit Platzbedarf $F_n(|w| - |M|) - 2 - |M|$, so daß $L(M)$ ein $n-$EXPSPACE-vollständiges Problem ist. Dann ist $w \mapsto (w, M) =: x$ Polynomialzeitreduktion von $L(M)$ auf unser Problem (denn $|(w, M)| = |w| + |M|$). $\square$

Notationen Q Zustandsmenge, q_0 Initialzustand, q_f akzeptierender Zustand, Γ Bandalphabet und $\diamond$ Leerzeichen von U,
$\$, 0, 1 \notin Q \cup \Gamma$, $\Delta = \{\$\} \cup Q \cup \Gamma$

Wir konstruieren jetzt eine (feste) automatische Struktur $\mathcal{A}$ mit Universum $\big(\Delta \cup \{0,1\}\big)^*$. Sie enthält die Konstante $\$q_0$ und die folgenden synchron-rationalen Relationen:

- StepInBlocks$'$ umfaßt alle Paare (c, c') mit
  - $c = \$c_0\$c_1\$\ldots\$c_k\$$ und $c' = \$c'_0\$c'_1\$\ldots\$c'_k\$$ für Konfigurationen $c_i, c'_i \in \Gamma^* Q \Gamma^+$,
  - $c_i \vdash c'_i$ und $|c_i| = |c'_i|$ für alle $0 \leq i \leq k$,
  - $\cancel{c_0 \in q_0 w \diamond^*}$,
  - $c'_k \in \Gamma^* q_f \Gamma^+$
- EqLet
- Replace
- $\cancel{L_n = 0^* 1 0^{F_n(m)-1} 1 0^*}$
- der Längenvergleich $|u| \leq |v|$

- $\cancel{L_0 = 0^* 1 0^{m-1} 1 0^*}$
- Measure
- Fill
- IncBlocks
- ~~DiffBit~~
- EqBit
- die Präfixrelation $\sqsubseteq$
- $S_a = \big\{(u, ua) \bigm| u \in (\Delta \cup \{0,1\})^*\big\}$ für $a \in \Delta \cup \{0,1\}$

  Für $(x, y) \in S_a$ schreiben wir in Formeln kürzer $y = xa$.
- $E = \{(x, y) \mid y \in x\,1\,0^*\}$

  Für $(x, y) \in E$ schreiben wir in Formeln kürzer $y \in x\,1\,0^*$.

- $I^{\otimes} = (0,0)^* \big((1,1)\,(0,0)^*\,(0,1)\,(0,0)^*\big)^+\,(1,1)\,(0,0)^*$

  Ein Paar von Wörtern (u,v) gehört zu I, wenn das Wort$u \in \{0,1\}^*$ aus dem Wort $v \in \{0,1\}^*$ entsteht, indem jede zweite Eins durch Null ersetzt wird und dabei die erste und letzte Eins erhalten bleiben.

- $H = \big\{(x,c) \;\big|\; \text{es gibt } k \in \mathbb{N}, \text{ so daß } x \diamond^k \$ \text{ Präfix von } c \text{ ist}\big\}$

- die unären Relationen 0^* und $0^*\,1^+\,1\,0^*$ und die Konstante $\$q_0$.

Sei P eine automatische Präsentation dieser Struktur $\mathcal{A}$.

Lemma 4.6. *Sei $n \geq 1$. Aus $m \in \mathbb{N}$ kann eine Formel $\lambda_{m,n}(x) \in \Sigma_n$ in polynomieller Zeit berechnet werden mit*

$$\mathcal{A} \models \lambda_{m,n}(w) \iff w \in 0^*\,1\,0^{F_n(m)-1}\,1\,0^*\,.$$

Beweis:
Der Beweis erfolgt induktiv über n.

Sei $\lambda_{m,1}(x)$ die folgende Formel:

$$\begin{aligned}\exists x_0, x_1, (y_i)_{0\le i\le m+1}, (z_i)_{0\le i\le m}:&\\ x_0 \in 0^* \wedge x_1 \in x_0\,1\,0^* \wedge x \in x_1\,1\,0^*&\\ \wedge\, y_0 = x_0 \wedge \bigwedge_{0\le i\le m} y_{i+1} \in y_i\,1\,0^* \wedge |x_1| = |y_m|&\\ \wedge\, z_m = y_{m+1} \wedge \bigwedge_{0\le i<m} I(z_{i+1}, z_i) \wedge z_0 \in 0^*\,1^+\,1\,0^*&\end{aligned}$$

Sie gehört zu Σ_1 und kann in Zeit polynomiell in m aus m berechnet werden.

Wir überlegen wieder, warum jedes Wort x, das $\lambda_{m,1}$ erfüllt, zu $0^*\,1\,0^{F_1(m)-1}\,1\,0^*$ gehört: Nach der ersten Zeile existieren $a, b, c \in \mathbb{N}$ mit $x = 0^a\,1\,0^b\,1\,0^c$. Nach der zweiten Zeile existieren Zahlen $s_0, s_1, \ldots, s_m, s_{m+1} \in \mathbb{N}$ mit $y_m = 0^{s_0}\,1\,0^{s_1}\,1\,0^{s_2} \cdots 1\,0^{s_m}$ und $y_{m+1} = y_m\,1\,0^{s_{m+1}}$. Außerdem gelten $s_0 = a$ (wegen $x_0 = y_0$) und

$$a + 1 + b = |x_1| = |y_m| = a + (1 + s_1) + (1 + s_2) + \cdots + (1 + s_m) = a + \sum_{1\le i\le m} (1 + s_i)$$

und daher

$$b = \sum_{1 \le i \le m} (1 + s_i) - 1\,.$$

Jetzt betrachten wir $z_0 \in 0^*\,1^+\,1\,0^*$. Es gibt also $k, \ell \in \mathbb{N}$ mit $z_0 \in 0^k\left(1\,0^{2^0-1}\right)^+ 1\,0^\ell$. Wegen $I(z_1, z_0)$ entsteht z_1 aus z_0, indem jede zweite Eins durch 0 ersetzt wird und dabei die erste und letzte Eins erhalten bleiben. Also gilt

$$z_1 \in 0^k\big(1\,0\big)^+ 1\,0^\ell = 0^k\big(1\,0^{2^1-1}\big)^+ 1\,0^\ell\,.$$

Induktiv erhält man

$$z_m \in 0^k\big(1\,0^{2^m-1}\big)^+ 1\,0^\ell\,.$$

Wegen $z_m = y_{m+1} \in 0^a\,1\,0^{s_1}\,1\,0^{s_2} \cdots 1\,0^*$ gilt also $s_i = 2^m - 1$ für alle $1 \le i \le m$. Also haben wir

$$b = \sum_{1 \le i \le m} \big(1 + 2^m - 1\big) - 1 = m \cdot 2^m - 1 = F_1(m) - 1\,,$$

d.h. tatsächlich $x \in 0^*\,1\,0^{F_1(m)-1}\,1\,0^*$.

Damit ist der Induktionsanfang gesichert.

Der Induktionsschritt folgt dem aus dem Beweis von Lemma 4.4: Aus $\lambda_{m,n+1}$ konstruieren wir $\sigma_{m,n+1}$ und $\lambda_{m,n+2}$ so, wie dort aus λ_{n+1} die Formeln σ_{n+1} und λ_{n+2} konstruiert wurden. □

Bemerkung. Das obige Lemma behauptet die Existenz von unendlich vielen polynomiellen Algorithmen, einen für jedes $n \geq 1$. Der Beweis liefert aber sogar, daß es einen einzige Algorithmus gibt, der aus m und n die Formel $\lambda_{m,n}$ berechnet (die Konstruktion von $\lambda_{m,n}$ ist „uniform“). Die Laufzeit dieses Algorithmus ist aber nur polynomiell in $m \cdot 2^n$. Für unsere Zwecke stört das aber nicht, da wir n als konstant annehmen.

Satz 4.7. *Sei P eine automatische Präsentation der Struktur $\mathcal{A}$.*

Für alle $n \in \mathbb{N}$ ist $\mathrm{MC}\big(\{P\}, \Sigma_{n+1}\big)$ vollständig für $(n+1)-\mathsf{EXPSPACE}$.

Beweis:
Wir verwenden das $n-\mathsf{EXPSPACE}$-vollständige Problem aus Lemma 4.5. Sei also $w = a_1 a_2 \cdots a_m$ eine Eingabe für U. Dann gilt $(c, c') \in \mathrm{StepInBlocks}$ genau dann, wenn diese

Struktur $\mathcal{A}$ die Formel

$$\sigma(c, c') = \exists x_0, x_1, \ldots, x_m \colon x_0 = \$q_0 \wedge \bigwedge_{1 \leq i \leq m} S_{a_i}(x_{i-1}, x_i) \wedge H(x_m, c) \wedge \mathrm{StepInBlocks}'(c, c')$$

erfüllt. Ersetze nun in der Formel φ_n aus Satz 4.3 die Teilformeln StepInBlocks(x, c) durch $\sigma(x, c)$ und die Formel $\lambda_n(x)$ durch $\lambda_{m,n}(x)$. Für das Ergebnis φ_n' dieser Ersetzungen gilt: $\mathcal{A}(P) \models \varphi_n' \iff \mathcal{A}(P_w) \models \varphi_n$. Außerdem folgt $\varphi_n' \in \Sigma_{n+1}$. $\square$