Achtung: Ich habe die Definition der Funktion $F_n(m)$ ein wenig geändert. Dies ändert nichts an dem bis hierher besprochenen, macht aber die folgenden Konstruktion deutlich einfacher. Ich bitte dies zu entschuldigen. Die neue Definition lautet

$$F_0(m) = m \text{ und } F_{n+1}(m) = F_n(m) \cdot 2^{F_n(m)} = F_n(m) \cdot 2^{F_n(m) \cancel{-} \cancel{1}}$$

Um die zu großen Automaten für L_n zu umgehen, ersetzen wir die problematische Relation L_n durch weitere synchron-rationale Relationen auf $\{0,1\}^*$, die durch „kleine“ Mehrbandautomaten akzeptiert werden können. Im Ergebnis werden wir Formeln $\lambda_k \in \Sigma_k$ erhalten, die in der so modifizierten Struktur die Relation L_k definieren (für alle $k \in \mathbb{N}$ und damit insbesondere für $k = n$).

Lemma 4.4. *Es existieren Formeln $\lambda_n(x) \in \Sigma_n$ (für alle $n \in \mathbb{N}$), so daß aus $m \in \mathbb{N}$ eine automatische Darstellung P_m in polynomieller Zeit berechnet werden kann mit*

$$L_n = \big\{ w \in \{0,1\}^* \mid \mathcal{A}(P_m) \models \lambda_n(w) \big\} \text{ für alle } n \in \mathbb{N}\,.$$

Notationen für $u = x_k x_{k-1} \dots x_0$ mit $x_i \in \{0,1\}$ setze $\mathrm{val}(u) = \sum_{0 \leq i \leq k} x_i 2^i$.

Wir beginnen jetzt mit dem umfangreichen Beweis von Lemma 4.4.

Zunächst definieren wir die automatische Struktur $\mathcal{B}_m$ mit Universum $\{0,1\}^*$ und den folgenden synchron-rationalen Relationen:

- $L_0 = 0^*\,1\,0^{m-1}\,1\,0^*$
- Measure $\subseteq \{0,1\}^* \times \{0,1\}^*$ mit $(x_1, x_2) \in$ Measure genau dann, wenn es $s_1, s_2, s_3 \in \mathbb{N}$ gibt mit $x_1 \in 0^{s_1}\,1\,\{0,1\}^{s_2}\,1\,0^{s_3}$ und $x_2 = 0^{s_1}\,1\,0^{s_2}\,1\,0^{s_3}$.

  Die Idee ist, daß x_2 den Abstand zwischen der ersten und der letzten 1 in x_1 „mißt“.
- Fill $\subseteq \{0,1\}^* \times \{0,1\}^*$ mit $(x_1, x_2) \in$ Fill genau dann, wenn es $s_1, s_2 \in \mathbb{N}$ und ein Wort u gibt mit $x_1 = 0^{s_1}\,1\,u\,1\,0^{s_2}$ und $x_2 \in \{0,1\}^{s_1}\,1\,u\,1\,\{0,1\}^{s_2}$.

  Die Idee ist, daß der Platz vor der ersten und nach der letzten Eins in x_1 beliebig „gefüllt“ werden kann.

- IncBlocks $\subseteq \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$ mit $(x_1, x_2, x_3) \in$ IncBlocks genau dann, wenn es Zahlen $\ell \geq 1$ und $s_0, s_1, \ldots, s_{\ell+1} \in \mathbb{N}$ gibt mit
  - $x_1 = 0^{s_0}\,1\,0^{s_1}\,1\,0^{s_2}\,\cdots\,1\,0^{s_{\ell+1}}$,
  - $x_2 = 0^{s_0}\,x_{2,1}\,x_{2,2}\,\cdots\,x_{2,\ell}\,1\,0^{s_{\ell+1}}$ mit $x_{2,i} \in \{0,1\}^{s_i+1}$ für alle $1 \leq i \leq \ell$,
  - $x_3 = 0^{s_0}\,x_{3,1}\,x_{3,2}\,\cdots\,x_{3,\ell}\,1\,0^{s_{\ell+1}}$ mit $x_{3,i} \in \{0,1\}^{s_i+1}$ für alle $1 \leq i \leq \ell$,
  - $\mathrm{val}(x_{2,i}) + 1 = \mathrm{val}(x_{3,i}) \pmod{2^{s_i+1}}$ für alle $1 \leq i \leq \ell$,
  - $x_{2,i} \in 0^* \iff i = 1$ für alle $1 \leq i \leq \ell$ und
  - $x_{2,i} \in 1^* \iff i = \ell$ für alle $1 \leq i \leq \ell$.

- DiffBit $\subseteq \{0,1\}^* \times \{0,1\}^*$ mit $(x_1, x_2) \in$ DiffBit genau dann, wenn $x_1 = u_1\,a\,u_2$, $x_2 = v_1\,b\,v_2$, $|u_1| + m = |v_1|$ und $\{a, b\} = \{0, 1\}$.

  Die Idee ist, daß x_1 und x_2 sich an Stellen k und $k + m$ unterscheiden.

  Wir werden die Formel $\neg\mathrm{DiffBit}(x_1, x_2)$ verwenden, wobei $|x_1| = |x_2|$ gilt. Sie gilt genau dann, wenn $x_1 = uv$ und $x_2 = wu$ mit $|v| = |w| = m$.

- EqBit $\subseteq \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^*$ mit $(x_1, x_2, x_2) \in$ EqBit genau dann, wenn es $a \in \{0,1\}$ gibt mit

  - $x_1 \in 0^{s_1}\,1\,0^{s_2}\,1\,0^*$,
  - $x_2 \in \{0,1\}^{s_1}\,a\,\{0,1\}^*$ und
  - $x_3 \in \{0,1\}^{s_1+1+s_2}\,a\,\{0,1\}^*$.
- Der Präfixrelation $\sqsubseteq$.

Es ist nicht schwer zu sehen, daß aus $m \in \mathbb{N}$ in Zeit polynomiell in m eine automatische Darstellung dieser Struktur berechnet werden kann.

Es bleiben die Formeln $\lambda_n(x)$ zu definieren. Zunächst definieren wir die Sprachen

$$L_n = 0^*\,1\,0^{F_n(m)-1}\,1\,0^* \text{ und } S_n = 0^*\left(1\,0^{F_n(m)-1}\right)^+\,1\,0^*\,.$$

Wir werden induktiv Formeln $\lambda_n \in \Sigma_n$ und $\sigma_n \in \Sigma_{n+1}$ konstruieren, die L_n bzw. S_n in der Struktur $\mathcal{B}_m$ definieren.

<u>Induktionsanfang $n = 0$:</u> Setze zunächst $\lambda_0(x) = \big(L_0(x)\big)$.

Betrachte weiterhin die folgende Formel

$$\begin{aligned}\sigma_0(x) = \exists y_1, y_2\colon\; & y_1 \sqsubseteq x \wedge \lambda_0(y_1)\\ & \wedge \mathrm{Fill}(x, y_2)\\ & \wedge \neg\mathrm{DiffBit}(y_2, y_2)\end{aligned}$$

Wir zeigen, daß jedes Wort x, das diese Formel erfüllt, zu S_0 gehört; die umgekehrte Implikation bleibt als Übung hier unbewiesen.

Nach der ersten Zeile gilt $x \in 0^{s_1}\,1\,0^{m-1}\,1\,\{0,1\}^*$. Nach der zweiten Zeile gelten $x = 0^{s_1}\,1\,0^{m-1}\,1\,v\,1\,0^{s_2}$ und $y_2 = u\,1\,0^{m-1}\,1\,v\,1\,w$ mit $|u| = s_1$ und $|v| = s_2$. Nach der dritten Zeile ist das Wort y_2 m-periodisch (d.h. es gibt ein Wort h mit $|h| = m$ und y_2 ist Präfix eines Wortes aus h^*). Dann muß aber auch der Faktor $1\,0^{m-1}\,1\,v\,1$ m-periodisch sein, also zu $\big(1\,0^{m-1}\big)^+\,1$ gehören.

Da offensichtlich $\lambda_0 \in \Sigma_0$ und $\sigma_0 \in \Sigma_1$ gelten, ist der Induktionsanfang $n = 0$ gesichert.

Leider müssen wir die Formel λ_1 gesondert behandeln, der eigentliche Induktionsschritt erfolgt danach. Wir setzen

$$\begin{aligned}\lambda_1(x) = \exists x_1, x_2, x_3 \colon\, & \sigma_0(x_1) \\ & \wedge \mathrm{Measure}(x_1, x) \\ & \wedge \mathrm{IncBlocks}(x_1, x_2, x_3) \\ & \wedge \neg \mathrm{DiffBit}(x_3, x_2)\,.\end{aligned}$$

Dann gilt offensichtlich $\lambda_1 \in \Sigma_1$.

Wir zeigen, daß jedes Wort x, das diese Formel erfüllt, zu L_1 gehört; die umgekehrte Implikation bleibt auch hier als Übung unbewiesen.

Nach den ersten beiden Zeilen existiert ein Wort $x_1 = 0^{s_0}\left(1\,0^{m-1}\right)^{\ell} 1\,0^{s_{\ell+1}}$ mit $\ell \geq 1$ und $x = 0^{s_0}\,1\,0^{\ell \cdot m-1}\,1\,0^{s_{\ell+1}}$.

(Da wir $x \in L_1$ zeigen wollen, bleibt also $\ell \cdot m = F_1(m)$ und damit $\ell = 2^m$ zu zeigen.)

Nach der dritten Zeile gelten

- $x_2 = 0^{s_0}\, x_{2,1}\, x_{2,2} \cdots x_{2,\ell}\, 0^{s_{\ell+1}}$ mit $x_{2,i} \in \{0,1\}^m$ für alle $1 \leq i \leq \ell$,
- $x_3 = 0^{s_0}\, x_{3,1}\, x_{3,2} \cdots x_{3,\ell}\, 0^{s_{\ell+1}}$ mit $x_{3,i} \in \{0,1\}^m$ für alle $1 \leq i \leq \ell$,
- $\mathrm{val}(x_{2,i}) + 1 = \mathrm{val}(x_{3,i}) \pmod{2^m}$ für alle $1 \leq i \leq \ell$,
- $x_{2,i} \in 0^* \iff i = 1$ für alle $1 \leq i\mathrm{el}\ell$ und
- $x_{2,i} \in 1^* \iff i = \ell$ für alle $1 \leq i \leq \ell$.

Nach der vierten Zeile ist der k-te Buchstabe von x_3 gleich dem Buchstaben Nummer $k + m$ von x_2 (für alle k). Insbesondere folgt $x_{3,i} = x_{2,i+1}$ für alle $1 \leq i < \ell$.

Wir betrachten die Folge

$$\mathrm{val}(x_{2,1}), \mathrm{val}(x_{2,2}), \ldots, \mathrm{val}(x_{2,\ell})$$

von Werten aus $\{0, 1, \ldots, 2^m - 1\}$. Für $1 \leq i < \ell$ gilt wegen $\mathrm{val}(x_{3,i}) = \mathrm{val}(x_{2,i+1})$ auch

$$\mathrm{val}(x_{2,i}) + 1 \equiv \mathrm{val}(x_{2,i+1}) \pmod{2^m}.$$

Da $\mathrm{val}(x_{2,i}) = 0 \iff i = 0$, hat die Folge also die Form

$$0, 1, 2, \ldots, \ell - 1\,,$$

insbesondere also $\ell - 1 = \mathrm{val}(x_{2,\ell}) = \mathrm{val}(1^m) = 2^m - 1$ bzw. $\ell = 2^m$ und damit tatsächlich $x \in L_1$.

<u>Induktionsvoraussetzung:</u> Seien die Formeln $\sigma_n \in \Sigma_{n+1}$ und $\lambda_{n+1} \in \Sigma_{n+1}$ bereits definiert.

<u>Induktionsschritt:</u> Setze

$$\begin{aligned}\sigma_{n+1}(x) = \exists y_1, y_2 \colon\ & y_1 \sqsubseteq x \wedge \lambda_{n+1}(y_1) \\ & \wedge \mathrm{Fill}(x, y_2) \\ & \wedge \neg\exists z \colon \big(\lambda_{k+1}(z) \wedge \neg\mathrm{EqLet}(z, y_2, y_2)\big)\,.\end{aligned}$$

Wegen $\lambda_{n+1} \in \Sigma_{n+1}$ erhalten wir $\sigma_{n+1} \in \Sigma_{n+2}$.

Setze weiterhin

$$\begin{aligned}\lambda_{n+2}(x) = \exists x_1, x_2, x_3 \colon\ & \sigma_{n+1}(x_1) \\ & \wedge \mathrm{Measure}(x_1, x) \\ & \wedge \mathrm{IncBlocks}(x_1, x_2, x_3) \\ & \wedge \neg\exists z \colon \big(\lambda_{k+1}(z) \wedge \neg\mathrm{EqLet}(z, x_3, x_2)\big) \,.\end{aligned}$$

Aus $\sigma_{n+1}, \lambda_{n+1} \in \Sigma_{n+1}$ folgt $\lambda_{n+2} \in \Sigma_{n+2}$.

Um zu zeigen, daß σ_{n+1} und λ_{n+2} die Mengen S_{n+1} bzw. L_{n+2} definieren, geht man wie oben vor.

Damit ist der Beweis von Lemma 4.4 abgeschlossen $\square$

Damit können wir Satz 4.3 beweisen: Sei $w \in \Gamma^*$ und $m = |w|$. Wir betrachten die Struktur $\mathcal{C}_w$ als Vereinigung der Struktur $\mathcal{A}_w$ aus der letzten Vorlesung (ohne die Relation L_n) und $\mathcal{B}_{|w|}$ (aus Lemma 4.4). Dann kann aus w in Zeit polynomiell in $|w|$ eine automatische Darstellung P_w dieser Struktur berechnet werden.

Sei weiter ψ der oben konstruierte Satz. Er ist äquivalent zu

$$\begin{aligned}\varphi_n = \exists c, c'\colon &\mathrm{StepInBlocks}(c, c')\\ &\wedge \exists x\colon \mathrm{Replace}(c, x) \wedge \lambda_n(x)\\ &\wedge \neg\exists x'\colon \big(\lambda_n(x') \wedge |x'| \leq |c'| \wedge \neg\mathrm{EqLet}(x', c', c)\big)\end{aligned}$$

Wegen $\lambda_n \in \Sigma_n$ gilt $\varphi_n \in \Sigma_{n+1}$.

Wir haben

$$w \in L(M_n) \iff \mathcal{C}_w \models \varphi_n \iff \mathcal{A}(P_w) \models \varphi_n$$

d.h. $w \mapsto P_w$ ist eine Polynomialzeitreduktion von $L(M_n)$ auf $\mathrm{MC}\big(\mathrm{AutPr}, \{\varphi_n\}\big)$. Da die Sprache $L(M_n)$ aber $n-\mathsf{EXPSPACE}$-vollständig ist, ist $\mathrm{MC}\big(\mathrm{AutPr}, \{\varphi_n\}\big)$ hart für die Klasse $n-\mathsf{EXPSPACE}$ (und damit vollständig wegen Korollar 4.2).