2. Teil: Sei $\sigma = \{R_1, \dots, R_\ell, c_1, \dots, c_\ell\}$ eine Signatur und sei C eine unter Isomorphie abgeschlossene Klasse endlicher σ-Strukturen, so dass das Problem

Eingabe: eine endliche σ-Struktur $\mathfrak{A}$

Frage: Ist $\mathfrak{A} \in C$?

in NP liegt.

D.h. es gibt eine NTM

$$M = (Q, \Sigma, \Gamma, \Delta, q_0, F)$$

mit $F = \text{Fakz} \dot{\cup} \text{Fvers}$ und eine Konstante $k \in \mathbb{N}$, s.d. M bei Eingabe (der Kodierung) einer endlichen σ-Struktur $\mathfrak{A}$ entscheidet, ob $\mathfrak{A} \in C$ ist und dabei weniger als n^k Schritte macht, für $n := |A|$.

D.h: für jede endliche σ-Struktur $\mathfrak{A}$, jede lineare Ordnung $<$ auf A gilt:

- jeder Lauf von M bei Eingabe $\text{enc}_<(\mathfrak{A})$ endet nach weniger als n^k Schritten (mit $n = |A|$), und
- $\mathfrak{A} \in C$ $\Leftrightarrow$ es gibt einen akzeptierenden Lauf von M bei Eingabe $\text{enc}_<(\mathfrak{A})$.

OBdA können wir annehmen, dass gilt:

- q_{akz} besteht aus genau einem Zustand, q_{akz}
- $n^k \geq |enc_<(\mathfrak{A})|$
- jeder Lauf von M bei Eingabe einer Struktur $\mathfrak{A}$ mit $|A| \geq 2$ hält nach genau $n^k - 1$ Schritten.

Ziel: Finde einen ESO[σ]-Satz Φ, s.d. $C = Mod_{FIN}(C)$, d.h. für jede endliche σ-Struktur $\mathfrak{A}$ gilt:

$$\begin{aligned} \mathfrak{A} \models \Phi &\iff \mathfrak{A} \in C \\ &\iff M \text{ akzeptiert } \mathfrak{A} \\ &\iff \text{es gibt eine lineare Ordnung } < \text{ auf } A \text{ und einen Lauf von } M \text{ bei Eingabe } enc_<(\mathfrak{A}), \text{ der nach } n^k - 1 \text{ Schritten im Zustand } q_{akz} \text{ endet} \end{aligned}$$

Idee zur Konstruktion von Φ:

Ähnlich wie im Beweis des Satzes von Trakhtenbrot. Jetzt wird aber jeder Zeitpunkt

$$t \in \{0, 1, \dots, n^k - 1\}$$

durch das k-Tupel $\bar{t} = (t_1, \dots, t_k) \in A^k$ kodiert, für das gilt:

$$rg_{<_{lex}}(\bar{t}) = t.$$

Analog wird jede Bandposition

$p \in \{0, 1, \dots, n^k - 1\}$

durch das k-Tupel $\bar{p} = (p_1, \dots, p_k) \in A^k$

kodiert, s.d. $rg_{<_{lex}}(\bar{p}) = p$.

Ein Lauf von M bei Eingabe $enc_<(\mathcal{A})$ wird durch folgende Relationen repräsentiert:

- eine $2k$-stellige Relation $K^{\mathcal{A}}$ mit

  $(\bar{t}, \bar{p}) \in K^{\mathcal{A}} \iff$ zum Zeitpunkt $\bar{t}$ steht der Kopf von M auf Bandposition $\bar{p}$

- für jedes $\gamma \in \Gamma$ gibt es eine $2k$-stellige Relation $B_\gamma^{\mathcal{A}}$ mit

  $(\bar{t}, \bar{p}) \in B_\gamma^{\mathcal{A}} \iff$ zum Zeitpunkt $\bar{t}$ steht auf Bandposition $\bar{p}$ das Symbol γ

- für jeden Zustand $q \in Q$ gibt es eine k-stellige Relation $Z_q^{\mathcal{A}}$ mit

  $\bar{t} \in Z_q^{\mathcal{A}} \iff$ zum Zeitpunkt $\bar{t}$ ist M in Zustand q

Beachte: Um Zahlen aus $\{0, 1, \dots, n^k - 1\}$ durch k-Tupel $\bar{t}, \bar{p} \in A^k$ zu repräsentieren, benutzen wir eine lineare Ordnung $<^{\mathcal{A}}$ auf A.

Außerdem wird es sich als hilfreich erweisen, die zu $<^{\mathfrak{A}}$ gehörige Nachfolgerrelation $succ^{\mathfrak{A}}$, sowie Elemente $z_0^{\mathfrak{A}}$ und $z_{max}^{\mathfrak{A}}$ für das kleinste und das größte Element in A bzgl $<^{\mathfrak{A}}$ zu nutzen.

Der ESO[σ]-Satz Φ, der in jeder endlichen σ-Struktur $\mathfrak{A}$ die Berechnung von M bei Eingabe $enc_<(\mathfrak{A})$ beschreibt, wird wie folgt gewählt:

$$\Phi := \exists K \, (\exists B_\gamma)_{\gamma \in \Gamma} \, (\exists Z_q)_{q \in Q} \; \exists R_< \exists R_{succ} \; \exists z_0 \exists z_{max} \; \Big(\varphi_{<,succ,0,max}(R_<, R_{succ}, z_0, z_{max}) \wedge \varphi_{Band} \wedge \varphi_{Kopf} \wedge \varphi_{Zustand} \wedge \varphi_{Start} \wedge \varphi_{Schritt} \wedge \varphi_{akzeptiere} \Big)$$

wobei $\varphi_{<,succ,0,max}(R_<, R_{succ}, z_0, z_{max}) :=$

$$\varphi_{<,succ,0}(R_<, R_{succ}, z_0) \wedge \forall x \, \big(R_<(x, z_{max}) \vee x = z_{max} \big)$$

die bereits in Beispiel 2.4 (d) genutzte FO-Formel ist, die in ihren Modellen erzwingt, dass

$R_<$ mit einer diskreten linearen Ordnung,
R_{succ} mit deren Nachfolgerrelation und
t_0 und t_{max} mit deren kleinstem und
größtem Element belegt wird.

Die restlichen in Φ vorkommenden FO-Formeln sind wie folgt gewählt:

- φ_{Band} besagt, dass zu jedem Zeitpunkt auf jeder Bandposition genau ein Symbol des Arbeitsalphabets Γ steht:

$$\varphi_{Band} := \forall t_1 \dots \forall t_k \forall p_1 \dots \forall p_k \Big(\bigvee_{\gamma \in \Gamma} \Big(B_\gamma(\bar{t}, \bar{p}) \wedge \bigwedge_{\substack{\gamma' \in \Gamma, \\ \gamma' \neq \gamma}} \neg B_{\gamma'}(\bar{t}, \bar{p}) \Big) \Big)$$

(hier steht $\bar{t}$ bzw $\bar{p}$ für $t_1, \dots, t_k$ bzw $p_1, \dots, p_k$).

- φ_{Kopf} besagt, dass der Kopf von M zu jedem Zeitpunkt auf genau einer Bandposition steht:

$$\varphi_{Kopf} := \forall t_1 \dots \forall t_k \exists p_1 \dots \exists p_k \Big(K(\bar{t}, \bar{p}) \wedge \forall p'_1 \dots \forall p'_k \big(K(\bar{t}, \bar{p}') \leftrightarrow \bigwedge_{i=1}^{k} p'_i = p_i \big) \Big)$$

- φ_{Zustand} besagt, dass M zu jedem Zeitpunkt in genau einem Zustand aus Q ist:

$$\varphi_{\text{Zustand}} := \forall t_1 \dots \forall t_k \bigvee_{q \in Q} \left(Z_q(\bar{t}) \wedge \bigwedge_{\substack{q' \in Q, \\ q' \neq q}} \neg Z_{q'}(\bar{t}) \right)$$

- $\varphi_{\text{akzeptiere}}$ besagt, dass M zum Zeitpunkt $n^k - 1$ (wird repräsentiert durch das Tupel $(z_{max}, \dots, z_{max})$) im Zustand q_{akz} ist:

$$\varphi_{\text{akzeptiere}} := Z_{q_{akz}}(z_{max}, \dots, z_{max})$$

- φ_{schritt} besagt, dass für jeden Zeitpunkt $\bar{t}$ gilt: Falls $\bar{t}$ nicht das Ende der Berechnung ist, so ist M im Zeitpunkt $\bar{t}' := \bar{t} + 1$ in einem laut Übergangsrelation Δ zulässigen Zustand q' und hat das entsprechende Symbol auf's Band geschrieben und den Kopf an die richtige Stelle gesetzt und die Beschriftung aller anderen Bandpositionen nicht verändert.

Dazu benutzt φ_{schritt} die Formel

$$\text{equal}(x_1, \dots, x_k, y_1, \dots, y_k) := \bigwedge_{i=1}^{k} x_i = y_i$$

und eine FO-Formel

$\mathrm{succ}_{\mathrm{Lex}}(x_1,\dots,x_k,y_1,\dots,y_k)$,

die besagt, dass das k-Tupel $\bar{y}=(y_1,\dots,y_k)$ mit dem unmittelbaren Nachfolger (bzgl. der aus $R_<$ gebildeten lexikographischen Ordnung) des Tupels $\bar{x}=(x_1,\dots,x_k)$ belegt ist (Konstruktion der Formel $\mathrm{succ}_{\mathrm{Lex}}(\bar{x},\bar{y})$: Übung!)

Zur besseren Lesbarkeit schreiben wir im Folgenden

$\exists \bar{t}$ bzw. $\forall \bar{p}$

als Abkürzung für

$\exists t_1 \dots \exists t_k$ bzw. $\forall p_1 \dots \forall p_k$.

$$\varphi_{\mathrm{Schritt}} := \forall \bar{t} \forall \bar{p} \bigwedge_{q\in Q^{\mathrm{TF}}} \bigwedge_{\gamma\in\Gamma} \Big(\big(K(\bar{t},\bar{p}) \wedge z_q(\bar{t}) \wedge B_\gamma(\bar{t},\bar{p}) \big) \rightarrow$$

$$\exists \bar{t}' \exists \bar{p}' \Big(\mathrm{succ}_{\mathrm{Lex}}(\bar{t},\bar{t}') \wedge K(\bar{t}',\bar{p}') \wedge$$

$$\Big(\forall \bar{p}'' \Big(\mathrm{equal}(\bar{p}'',\bar{p}) \vee \bigwedge_{\gamma''\in\Gamma} \big(B_{\gamma''}(\bar{t}',\bar{p}'') \leftrightarrow B_{\gamma''}(\bar{t},\bar{p}'') \big) \Big)$$

$$\wedge \bigvee_{\substack{q',\gamma',m:\\ (q,\gamma,q',\gamma',m)\in\Delta}} \big(z_{q'}(\bar{t}') \wedge B_{\gamma'}(\bar{t}',\bar{p}) \wedge \chi_m(\bar{p},\bar{p}') \big) \Big) \Big)$$

wobei die Formel $\chi_m(\bar{p},\bar{p}')$ die jeweilige Kopfbewegung für $m\in\{-1,0,1\}$ beschreibt:

$$\chi_1(\bar{p},\bar{p}') := \mathrm{succ}_{<_{lex}}(\bar{p},\bar{p}'),$$

$$\chi_0(\bar{p},\bar{p}') := \mathrm{equal}(\bar{p},\bar{p}'),$$

$$\chi_{-1}(\bar{p},\bar{p}') := \mathrm{succ}_{<_{lex}}(\bar{p}',\bar{p}).$$

- ψ_{start} besagt, dass M zum Zeitpunkt 0 (der durch das Tupel $(z_0,\dots,z_0)$ kodiert wird) in der Startkonfiguration von M bei Eingabe $enc_c(\sigma\tau)$ ist, d.h. M ist im Startzustand q_0, der Kopf steht auf Bandposition 0 (die durch das k-Tupel $\bar{z}_0 = (z_0,\dots,z_0)$ kodiert wird), und für jedes $\bar{p} \in A^k$ gilt:
  Auf Bandposition $p := rg_{<_{lex}}(\bar{p}) \in \{0,1,\dots,n^k-1\}$ steht
  - das Symbol 0, falls an der p-ten Stelle w_p des Wort $enc_c(\sigma\tau) = w_0 w_1 \cdots w_{|enc_c(\sigma\tau)|-1}$ steht eine 0
  - das Symbol 1, falls $w_p = 1$
  - das Blank-Symbol $\sqcup$, falls $p \geq |enc_c(\sigma\tau)|$

Dies wird durch die folgende FO-Formel ausgedrückt:

$$\varphi_{Start} := z_{q_0}(\bar{z}_0) \wedge K(\bar{z}_0, \bar{z}_0) \wedge$$

$$\forall \bar{p} \Big(\big(B_0(\bar{z}_0, \bar{p}) \leftrightarrow \xi_0(\bar{p}) \big) \wedge$$

$$\big(B_1(\bar{z}_0, \bar{p}) \leftrightarrow \xi_1(\bar{p}) \big) \wedge$$

$$\big(B_\square(\bar{z}_0, \bar{p}) \leftrightarrow \neg(\xi_0(\bar{p}) \vee \xi_1(\bar{p})) \big) \Big)$$

Dabei sind $\xi_0(\bar{p})$ und $\xi_1(\bar{p})$ geeignete FO-Formeln, die ausdrücken, dass im 0-1-Wort $enc_<(\mathfrak{A})$ an Position $rg_{<ext}(\bar{p})$ eine 0 bzw 1 steht.

Wir geben hier die Formeln $\xi_0(\bar{p})$ und $\xi_1(\bar{p})$ für den Spezialfall an, dass $\sigma = \{E, c\}$ aus einem 2-stelligen Relationssymbol E und einem Konstantensymbol c besteht (der allgemeine Fall mit $\sigma = \{R_1, \dots, R_\ell, c_1, \dots, c_\ell\}$ kann analog behandelt werden).

Für $\sigma = \{E, c\}$, jede σ-Struktur $\mathfrak{A}$ mit $n := |A|$ und jede lineare Ordnung $<$ auf A ist $enc_<(\mathfrak{A})$ von der folgenden Form:

$$enc_<(\mathfrak{A}) = \underbrace{1\,0^{n^2-n}}_{\text{Länge } n^2} \; \underbrace{enc_<(E^{\mathfrak{A}})}_{\text{Länge } n^2} \; \underbrace{enc_<(c^{\mathfrak{A}})}_{\text{Länge } n^2} \in \{0,1\}^{3n^2}.$$

Die Positionen $0, 1, \dots, 3n^2-1$ des Worts $enc_c(\mathcal{A})$ werden durch genau diejenigen k-Tupel $\bar{p} = (p_1, \dots, p_k) \in A^k$ mit $A = \{a_0 < a_1 < \dots < a_{m-1}\}$ kodiert, für die gilt:

$$p_1 = \dots = p_{k-3} = a_0, \quad p_{k-2} \in \{a_0, a_1, a_2\}, \quad p_{k-1}, p_k \in A$$

Daher erzwingen die folgenden Formeln $\xi_1(\bar{p})$ und $\xi_0(\bar{p})$, dass in ihren Modellen die Variablen $\bar{p}$ mit Werten belegt sind, die Positionen kodieren, an denen in $enc_c(\mathcal{A})$ eine 1 bzw eine 0 steht:

- $\xi_1(p_1, \dots, p_k) := \bigwedge_{i=1}^{k-3} p_i = z_0 \wedge \Big($
  $(p_{k-2} = z_0 \wedge p_{k-1} = z_0)$ ← "Anfangsblock $1^n 0^{n^2-n}$"
  $\vee \big(\underbrace{R_{succ}(z_0, p_{k-2})}_{\text{"}p_{k-2} \hat{=} a_1\text{"}} \wedge E(p_{k-1}, p_k) \big)$ ← "Teilstück $enc_c(\mathcal{E}^n)$"
  $\vee \big(\text{"}p_{k-2} \hat{=} a_2\text{"} \wedge p_{k-1} = z_0 \wedge p_k = c \big) \Big)$ ← "Teilstück $enc_c(c^n)$"

- $\xi_0(p_1, \dots, p_k) := \neg \xi_1(p_1, \dots, p_k) \wedge$
  $\bigwedge_{i=1}^{k-3} p_i = z_0 \wedge \big(p_{k-2} = z_0 \vee \underbrace{\text{"}p_{k-2} = a_1\text{"}}_{R_{succ}(z_0, p_{k-2})} \vee \text{"}p_{k-2} = a_2\text{"} \big)$

wobei "$p_{k-2} = a_2$" die Formel $\exists x \big(R_{succ}(z_0, x) \wedge R_{succ}(x, p_{k-2}) \big)$ ist

Insgesamt sind wir nun fertig mit der Konstruktion der ESO-Formel Φ.

Per Induktion nach den Zeitpunkten $0, 1, \ldots, n^k - 1$ kann man leicht nachprüfen, dass für jede endliche σ-Struktur $\mathfrak{A}$ und jede lineare Ordnung $<$ auf A gilt:

$\mathfrak{A} \models \Phi$ $\Leftrightarrow$ es gibt einen Lauf von M bei Eingabe $\mathrm{enc}_<(\mathfrak{A})$, der nach $n^k - 1$ Schritten im akzeptierenden Zustand q_{akz} endet

$\Leftrightarrow$ $\mathfrak{A} \in C$.

Damit sind wir fertig mit dem Beweis des Satzes von Fagin. $\square$

Unter Verwendung des Satzes von Fagin
lässt sich leicht der Satz von Cook und Levin beweisen
(der allerdings bereits vor dem Satz von Fagin bekannt war):

Theorem 2.24 (Satz von Cook-Levin, ≈1971)

Das aussagenlogische Erfüllbarkeitsproblem

SAT
Eingabe: Eine aussagenlogische Formel α
Frage: Ist α erfüllbar?

ist NP-vollständig.

Beweis: Siehe Skript [S], Theorem 2.9.

Auf ähnliche Art wie den Satz von Fagin kann
man auch den folgenden Satz von Grädel
beweisen, der eine logische Charakterisierung
aller (deterministisch) in Polynomialzeit lösbaren
Probleme auf geordneten Strukturen liefert.

Zur Formulierung des Satzes von Grädel benötigen
wir einige Notationen.