2.3 ESO und der Satz von Fagin

Zur Erinnerung:

ESO-Formeln sind SO-Formeln der Form

$$\exists X_1 \cdots \exists X_\ell \; \varphi$$

mit $\ell \geq 0$, $X_1, \ldots, X_\ell$ Relationsvariablen beliebiger Stelligkeit und φ eine FO-Formel.

Definition 2.18 (Logische Beschreibung von Komplexitätsklassen)

Sei $\mathcal{K}$ eine Komplexitätsklasse (z.B. $\mathcal{K} = NP$), sei $\mathcal{L}$ eine Logik (z.B. ESO) und sei $\mathcal{S}$ eine unter Isomorphie abgeschlossene Klasse endlicher Strukturen (z.B. $\mathcal{S} = FIN :=$ die Klasse aller endlichen Strukturen über allen endlichen funktionenfreien Signaturen).

Wir sagen "$\mathcal{L}$ beschreibt $\mathcal{K}$ auf $\mathcal{S}$", falls die folgenden beiden Bedingungen erfüllt sind:

(1) Für jeden Satz $\varphi \in \mathcal{L}$ gehört das folgende Problem zur Komplexitätsklasse $\mathcal{K}$:

> $Eval_\varphi(\mathcal{S})$: Das Auswertungsproblem für φ auf $\mathcal{S}$:
> Eingabe: Eine endliche Struktur $\mathfrak{A} \in \mathcal{S}$
> Frage: Gilt $\mathfrak{A} \models \varphi$?

(2) Für jede endliche, funktionenfreie Signatur σ und jede unter Isomorphie abgeschlossene Klasse $C \subseteq S$ von σ-Strukturen gilt:
Falls das Problem

> Zugehörigkeit zu C:
> Eingabe: $\mathfrak{A} \in S$, $\mathfrak{A}$ eine σ-Struktur
> Frage: Ist $\mathfrak{A} \in C$?

zur Komplexitätsklasse $\mathcal{K}$ gehört, so gibt es einen $\mathcal{L}[\sigma]$-Satz φ, so dass gilt:

$$C = \underbrace{\{ \mathfrak{A} \in S : \mathfrak{A} \text{ ist eine } \sigma\text{-Struktur mit } \mathfrak{A} \models \varphi \}}_{=: \mathrm{Mod}_S(\varphi)}$$

Theorem 2.19 (Der Satz von Fagin, 1974)

ESO beschreibt NP auf der Klasse FIN aller endlichen Strukturen.

Der Beweis von Theorem 2.19 erfolgt in 2 Teilen:
Im 1. Teil zeigen wir, dass jeder ESO-Satz Φ bei Eingabe einer Struktur $\mathfrak{A}$ nichtdeterministisch in Zeit polynomiell in der Größe von $\mathfrak{A}$ ausgewertet werden kann (dies ist der "leichte Teil" des Beweises).

Im 2. Teil zeigen wir, dass jedes Problem, das in NP liegt, durch einen ESO-Satz beschrieben werden kann.

Das Berechnungsmodell, mit dem wir arbeiten, sind Turingmaschinen. Um die Details des Beweises von Theorem 2.19 ausarbeiten zu können, müssen wir festlegen, wie genau eine Struktur $\mathcal{A}$ als Eingabe einer Turingmaschine repräsentiert wird. Wir benutzen dazu die sog. Standardkodierung, die im Folgenden eingeführt wird.

Definition 2.20

Sei $A = \{a_0 < a_1 < \dots < a_{n-1}\}$ eine durch die Relation $<$ linear geordnete endliche Menge.

(a) Der Rang $rg_<(a)$ eines Elements $a \in A$ ist

$$rg_<(a) := |\{b \in A : b < a\}|$$

D.h.: $rg_<(a_i) = i$.

(b) Sei $r \in \mathbb{N}_{\geq 1}$. Die lexikographische Ordnung $<_{lex}$ auf A^r ist wie folgt definiert:

Für $\bar{b} = (b_1, \dots, b_r) \in A^r$ und $\bar{c} = (c_1, \dots, c_r) \in A^r$ ist

$$\bar{b} <_{lex} \bar{c} \iff \text{ex. } i \in \{1, \dots, r\} \text{ s.d. } b_i < c_i \text{ und f.a. } j < i \text{ ist } b_j = c_j$$

Klar: $<_{lex}$ ist eine lineare Ordnung auf A^r.

Beispiel 2.21

Sei $A = \{0 < 1 < 2\}$. Für die lexikographische Ordnung $<_{lex}$ auf A^2 gilt:

$\bar{b} \in A^2$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)	(2,0)	(2,1)	(2,2)
$rg_{<_{lex}}(\bar{b})$	0	1	2	3	4	5	6	7	8

Definition 2.22 (Standardkodierung $enc_c(\mathfrak{A})$)

- Sei $\sigma = \{R_1, \dots, R_\ell, c_1, \dots, c_{\ell'}\}$ (mit $\ell, \ell' \geq 0$) eine endliche funktionenfreie Signatur, wobei für jedes $j \in \{1, \dots, \ell\}$ gilt: R_j ist ein Relationssymbol der Stelligkeit $r_j := ar(R_j)$.
  Sei $r := max\{r_1, \dots, r_\ell\}$ die maximale Stelligkeit der Relationssymbole in σ.

- Sei $\mathfrak{A}$ eine endliche σ-Struktur, sei $n := |A|$.
  Sei $<$ eine beliebige lineare Ordnung auf A und sei $\{a_0 < a_1 < \dots < a_{n-1}\} = A$.
  Im Folgenden identifizieren wir jedes $a_i \in A$ mit seinem Rang $i = rg_<(a_i)$, und wir identifizieren jedes r_j-Tupel $\bar{b} \in A^{r_j}$ mit seinem Rang $rg_{<_{lex}}(\bar{b}) \in \{0, 1, \dots, n^{r_j} - 1\}$.

- Für jedes $j \in \{1, \dots, \ell\}$ kodieren wir die Relation $R_j^{\mathfrak{A}}$ durch das Wort

$$enc_<(R_j^{\mathfrak{A}}) := w_0 w_1 \cdots w_{n^r-1} \in \{0,1\}^{(n^r)},$$

wobei

- f.a. $\bar{b} \in A^{r_j}$ gilt: $\bar{b} \in R_j^{\mathfrak{A}} \iff w_{rg_<^{(r)}(\bar{b})} = 1$
- f.a. $m \geq n^{r_j}$ gilt: $w_m = 0$

- Für jedes $j \in \{1, \dots, \ell'\}$ kodieren wir die Konstante $c_j^{\mathfrak{A}}$ durch das Wort

$$enc_<(c_j^{\mathfrak{A}}) := w_0 w_1 \cdots w_{n^r-1} \in \{0,1\}^{(n^r)}$$

wobei

- f.a. $m \in \{0, \dots, n^r-1\}$ gilt:

$$w_m = 1 \iff m = rg_<(c_j^{\mathfrak{A}})$$

- Die Mächtigkeit n des Universums von $\mathfrak{A}$ kodieren wir durch das Wort

$$enc_<(|A|) := 1^n 0^{(n^r-n)} \in \{0,1\}^{n^r}$$

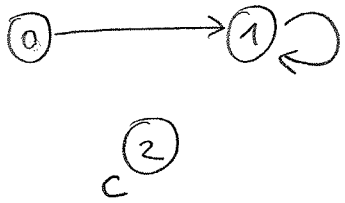
- Die Standardkodierung von $\mathfrak{A}$ bzgl $<$ ist das Wort

$$enc_<(\mathfrak{A}) := enc_<(|A|)\, enc_<(R_1^{\mathfrak{A}}) \cdots enc_<(R_\ell^{\mathfrak{A}})\, enc_<(c_1^{\mathfrak{A}}) \cdots enc_<(c_{\ell'}^{\mathfrak{A}})$$

$$\in \{0,1\}^{(1+\ell+\ell') \cdot n^r}.$$

Beispiel 2.22

Sei $\sigma = \{E, c\}$ die Signatur, die aus einem 2-stelligen Relationssymbol E und einem Konstantensymbol c besteht.
Wir betrachten die σ-Struktur $\mathfrak{A}$ mit

$\mathfrak{A} =$ 

D.h.: $\mathfrak{A} = (A, E^{\mathfrak{A}}, c^{\mathfrak{A}})$ mit $A = \{0,1,2\}$,
$E^{\mathfrak{A}} = \{(0,1), (1,1)\}$ und $c^{\mathfrak{A}} = 2$.
Sei $<$ die natürliche lineare Ordnung auf $\mathbb{N}$.
dann gilt: $r = 2$, $n = 3$, $n^r = 9$

$$enc_<(\mathfrak{A}) = \underbrace{111|000\,000}_{enc_<(|A|)}\ \underbrace{010|010|000}_{enc_<(E^{\mathfrak{A}})}\ \underbrace{001|000\,000}_{enc_<(c^{\mathfrak{A}})}$$

Beachte: $enc_<(E^{\mathfrak{A}})$ ist die zeilenweise gelesene Adjazenzmatrix des Graphen $(A, E^{\mathfrak{A}})$: $\begin{pmatrix} 0&1&0 \\ 0&1&0 \\ 0&0&0 \end{pmatrix}$

Bemerkung 2.23

(a) Die Standardkodierung $enc_<(\mathfrak{A})$ hängt von der gewählten linearen Ordnung $<$ ab

(b) $|enc_<(\mathfrak{A})| = (1 + \ell + \ell') \cdot |A|^r$. D.h. für jede feste Signatur σ ist die Länge von $enc_<(\mathfrak{A})$ polynomiell in der Mächtigkeit $|A|$ der Struktur $\mathfrak{A}$.

(c) Sei $enc_<(\mathfrak{A}) = w_0 w_1 \cdots w_{(1+\ell+\ell^r)n^r-1}$

Für ein Tupel $\bar{b} \in A^r$ lässt sich die Information, ob $\bar{b} \in R_j^{\mathfrak{A}}$ ist, in $enc_<(\mathfrak{A})$ am Buchstaben w_m mit

$$m = j \cdot n^r + rg_{<_{lex}}(\bar{b})$$

ablesen.

Wir können nun den Beweis des Satzes von Fagin führen:

Beweis von Theorem 2.13 (Satz von Fagin)

Ziel: Zeige "ESO beschreibt NP auf FIN"

1. Teil: Sei σ eine Signatur und sei $\Phi = \exists X_1 \cdots \exists X_d \varphi$ ein ESO[σ]-Satz.

Wir müssen zeigen, dass das folgende Problem in NP gehört:

> $Eval_\Phi(FIN)$: Auswertungsproblem für Φ auf FIN
> Eingabe: Eine endliche σ-Struktur $\mathfrak{A}$
> Frage: Gilt $\mathfrak{A} \models \Phi$?

Ein nichtdeterministischer Polynomialzeit-Algorithmus kann bei Eingabe einer endlichen σ-Struktur $\mathfrak{A}$ wie folgt vorgehen, um zu testen, ob $\mathfrak{A} \models \Phi$:

1) Rate Belegungen der Relationsvariablen $X_1, \dots, X_d$, d.h. rate Relationen $X_1^{\mathfrak{A}} \subseteq A^{ar(X_1)}, \dots, X_d^{\mathfrak{A}} \subseteq A^{ar(X_d)}$

   Das geht in Zeit $O(d \cdot n^R)$, falls $n = |A|$ und R die maximale Stelligkeit der $X_1, \dots, X_d$.

2) Teste (deterministisch, in Polynomialzeit), ob $(\mathfrak{A}, X_1^{\mathfrak{A}}, \dots, X_d^{\mathfrak{A}}) \models \varphi$

   Dafür können wir den "naiven" Algorithmus benutzen, der rekursiv entlang der Definition der Semantik von FO vorgeht; siehe Vorlesung "Logik in der Informatik" / "Einführung in die formale Logik".

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

> "Zugehörigkeit zu C":
> 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 $F = F_{akz} \dot{\cup} F_{verw}$ 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 $\mathfrak{A}$ und jede lineare Ordnung $<$ auf A gilt:

- jeder Lauf von M bei Eingabe $enc_<(\mathfrak{A})$ 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 $enc_<(\mathfrak{A})$.

OBdA können wir annehmen, dass gilt:

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

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

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

Idee zur Konstruktion von Φ:

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

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

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

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

Analog wird jede Bandposition

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

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

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

Ein Lauf von M bei Eingabe $enc_<(\omega)$ wird durch folgende Relationen repräsentiert.

- eine $2k$-stellige Relation K^ω mit

  $(\bar{t}, \bar{p}) \in K^\omega \iff$ 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_γ^ω mit

  $(\bar{t}, \bar{p}) \in B_\gamma^\omega \iff$ 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^ω mit

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

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

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

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

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

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:

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

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

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

- 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

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

und eine FO-Formel

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

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 $\mathrm{succ}_{<_{lex}}(\bar{x},\bar{y})$: 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. $\forall p_1 \dots \forall p_k$.

$$\varphi_{Schritt} := \forall \bar{t} \forall \bar{p} \bigwedge_{q \in Q \setminus F} \bigwedge_{\gamma \in \Gamma} \Big(\big(K(\bar{t},\bar{p}) \wedge Z_q(\bar{t}) \wedge B_\gamma(\bar{t},\bar{p}) \big) \rightarrow$$

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

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

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

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

$$\chi_1(\bar{p},\bar{p}') := succ_{Lex}(\bar{p},\bar{p}'),$$

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

$$\chi_{-1}(\bar{p},\bar{p}') := succ_{Lex}(\bar{p}',\bar{p}).$$

- 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 $enc_\Sigma(\sigma)$ 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 Worts $enc_\Sigma(\sigma) = w_0 w_1 \cdots w_{|enc_\Sigma(\sigma)|-1}$ eine 0 steht,
  - das Symbol 1, falls $w_p = 1$
  - das Blank-Symbol $\sqcup$, falls $p \geq |enc_\Sigma(\sigma)|$

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 $rg_{<ex}(\bar{p})$ 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:

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

Die Positionen $0, 1, \dots, 3n^2-1$ des Worts $enc_c(\mathcal{D})$ 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 $enc_c(\mathcal{D})$ 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 $enc_c(E^n)$"

  $\vee \big(\text{"}p_{k-2} \hat{=} a_2\text{"} \wedge p_{k-1} = z_0 \wedge p_k = c\big)\Big)$ ← "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:

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

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

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 und Levin, ≈ 1971)

Das aussagenlogische Erfüllbarkeitsproblem

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

ist NP-vollständig.

Beweis:

SAT $\in$ NP: Man kann leicht einen nichtdeterministischen Polynomialzeit-Algorithmus angeben, der bei Eingabe einer aussagenlogischen Formel α zunächst eine Belegung der in α vorkommenden aussagenlogischen Variablen mit Werten aus $\{0,1\}$ "rät" und danach überprüft, ob diese Belegung die Formel α tatsächlich erfüllt.

SAT ist NP-hart: Dazu muss man für jedes Problem L in NP zeigen, dass es eine Polynomialzeit-Reduktion auf SAT gibt. Jedes Problem L kann man, für eine geeignete Signatur σ, mit einer Klasse C endlicher σ-Strukturen identifizieren, so dass das Problem

> L:
> Eingabe: ein Wort $w \in \Sigma^*$
> Frage: $w \in L$?

äquivalent zum Problem

> Zugehörigkeit zu C:
> Eingabe: eine endliche σ-Struktur $\mathfrak{A}$
> Frage: $\mathfrak{A} \in C$?

Da gemäß Voraussetzung $L \in NP$ ist, liefert der Satz von Fagin (Theorem 2.19), dass es einen $ESO[\sigma]$-Satz Φ gibt, so dass für jede endliche σ-Struktur $\mathfrak{A}$ gilt:

$$\mathfrak{A} \in C \iff \mathfrak{A} \models \Phi.$$

Der Satz Φ ist von der Form

$$\Phi = \exists X_1 \cdots \exists X_d \, \varphi$$

wobei $d \geq 0$, $X_1, \ldots, X_d$ Relationsvariablen und φ ein $FO[\sigma \dot{\cup} \{X_1, \ldots, X_d\}]$-Satz ist.

Wir nutzen die Formel φ, um für jede endliche σ-Struktur $\mathfrak{A}$ eine aussagenlogische Formel $\alpha_{\varphi, \mathfrak{A}}$ zu konstruieren, so dass gilt:

$$\mathfrak{A} \models \varphi \quad \Leftrightarrow \quad \alpha_{\varphi, \mathfrak{A}} \text{ hat eine erfüllende Belegung.}$$

Die aussagenlogische Formel $\alpha_{\varphi, \mathfrak{A}}$ benutzt aussagenlogische Variablen aus der Menge

$$V := \{ v_{X_i, \bar{a}} : i \in \{1, \ldots, d\}, \ \bar{a} \in A^{ar(X_i)} \}$$

Die Idee dabei ist, dass einer Belegung, die der Variablen $v_{X_i, \bar{a}}$ den Wahrheitswert 1 zuordnet, aussagt, dass das Tupel $\bar{a}$ zur Relation X_i gehört.

Somit entspricht eine Belegung der aussagenlogischen Variablen aus V mit Werten aus $\{0,1\}$ gerade einer Belegung der Relationsvariablen $X_1, \ldots, X_d$ mit Relationen über dem Universum von $\mathfrak{A}$.

Die aussagenlogische Formel $\alpha_{\varphi,\mathfrak{A}}$ entsteht nun aus φ, indem man nacheinander die folgenden Ersetzungen durchführt:

1) Ersetze jede Teilformel der Form $\exists x\, \psi(x,\dots)$ durch $\bigvee_{a \in A} \psi(a,\dots)$.

2) Ersetze jede Teilformel der Form $\forall x\, \psi(x,\dots)$ durch $\bigwedge_{a \in A} \psi(a,\dots)$.

3) Ersetze jedes Konstantensymbol c durch die zugehörige Konstante $c^{\mathfrak{A}}$.

4) Ersetze jedes "Atom" der Form $R(\bar{a})$, für $R \in \sigma$ und $\bar{a} \in A^{ar(R)}$, durch den Wahrheitswert
$$\begin{cases} 1, & \text{falls } \bar{a} \in R^{\mathfrak{A}} \\ 0, & \text{falls } \bar{a} \notin R^{\mathfrak{A}} \end{cases}$$

5) Ersetze jedes "Atom" der Form $X_i(\bar{a})$, für $i \in \{1,\dots,d\}$ und $\bar{a} \in A^{ar(X_i)}$, durch die aussagenlogische Variable $v_{X_i,\bar{a}}$

6) Ersetze jede Gleichung der Form $a = b$, für $a, b \in A$, durch den Wahrheitswert

$$\begin{cases} 1, & \text{falls } a = b \\ 0, & \text{falls } a \neq b. \end{cases}$$

Gemäß dieser Konstruktion gilt für alle endlichen σ-Strukturen $\mathfrak{A}$:

- $\mathfrak{A} \models \Phi \iff \alpha_{\Phi,\mathfrak{A}}$ ist erfüllbar, und
- Bei Eingabe der Struktur $\mathfrak{A}$ kann man in polynomieller Zeit (also in Zeit $|A|^k$, für ein $k \in \mathbb{N}$) die Formel $\alpha_{\Phi,\mathfrak{A}}$ erzeugen.

Somit ist die Abbildung f, die jeder endlichen σ-Struktur $\mathfrak{A}$ die Formel $\alpha_{\Phi,\mathfrak{A}}$ zuordnet, eine Polynomialzeit-Reduktion von dem Problem "Zugehörigkeit zu C" (d.h. von dem Problem L) auf das aussagenlogische Erfüllbarkeitsproblem SAT.

Insgesamt haben wir also gezeigt, dass SAT NP-vollständig ist. □

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.

Definition 2.25 ($\mathrm{FIN}_<$)

(a) Eine geordnete Struktur ist eine Struktur $\mathfrak{A}$ über einer endlichen funktionenfreien Signatur, die das 2-stellige Relationssymbol $<$ enthält, und bei der dieses Symbol durch eine lineare Ordnung $<^{\mathfrak{A}}$ auf $\mathfrak{A}$ interpretiert wird.

(b) Die Klasse aller endlichen geordneten Strukturen bezeichnen wir mit $\mathrm{FIN}_<$.

Definition 2.26 (Horn-Klauseln und ESO-Horn)

(a) Eine aussagenlogische Horn-Klausel ist eine Disjunktion von aussagenlogischen Literalen (d.h. aussagenlogische Variablen bzw. negierte aussagenlogische Variablen), in der höchstens eine der Variablen unnegiert vorkommt.

Beachte: • Eine aussagenlogische Horn-Klausel der Form $(\neg X_1 \vee \neg X_2 \vee \cdots \vee \neg X_\ell \vee X_{\ell+1})$ lässt sich schreiben als Implikation $(X_1 \wedge \cdots \wedge X_\ell) \to X_{\ell+1}$.

• Die Hornklausel $(\neg X_1 \vee \cdots \vee \neg X_\ell)$ lässt sich schreiben als Implikation $(X_1 \wedge \cdots \wedge X_\ell) \to \mathrm{false}$

(5) Sei σ eine funktionenfreie Signatur, seien $X_1, \dots, X_d$ Relationsvariablen und sei

$$\sigma' := \sigma \cup \{X_1, \dots, X_d\}$$

Eine <u>σ'-Horn-Klausel bzgl $X_1, \dots, X_d$</u> ist eine Disjunktion von $FO[\sigma]$-Formeln (in denen keins der Symbole $X_1, \dots, X_d$ vorkommt) atomaren oder negierten atomaren Formeln über $\{X_1, \dots, X_d\}$, wobei höchstens <u>ein</u> über $\{X_1, \dots, X_d\}$ gebildetes Atom <u>unnegiert</u> vorkommt.

<u>Beachte:</u> Jede σ'-Horn-Klausel bzgl. $X_1, \dots, X_d$ lässt sich schreiben als

(1) $X_i(\bar{y})$ mit $X_i \in \{X_1, \dots, X_d\}$, $\bar{y} \in Var_1 \cup \{c : c \in \sigma\}$

(2) $(\beta_1 \wedge \dots \wedge \beta_m) \rightarrow X_i(\bar{y})$ mit

$m \geq 1$, $X_i(\bar{y})$ wie in (1), f.a. $j \in \{1, \dots, m\}$ ist β_j eine $FO[\sigma]$-Formel (in der $X_1, \dots, X_d$ nicht vorkommen) oder von der Form $X_k(\bar{z})$ mit $X_k \in \{X_1, \dots, X_d\}$ und $\bar{z} \in (Var_1 \cup \{c : c \in \sigma\})^{ar(X_k)}$

(3) $(\beta_1 \wedge \dots \wedge \beta_m) \rightarrow$ false mit $m \geq 1$ und $\beta_1, \dots, \beta_m$ wie in (2).

(c) Die Klasse ESO-Horn besteht aus allen ESO-Sätzen Φ der Form

$$\exists X_1 \cdots \exists X_d \quad \forall y_1 \cdots \forall y_{d'} \quad \varphi ,$$

wobei $d, d' \geq 0$, $X_1, \ldots, X_d$ Relationsvariablen, $y_1, \ldots, y_{d'}$ Individuenvariablen und φ eine Konjunktion von σ'-Horn-Klauseln bzgl $X_1, \ldots, X_d$ ist (mit $\sigma' = \sigma \cup \{X_1, \ldots, X_d\}$, wobei σ die Signatur von Φ ist).

Theorem 2.27 (Satz von Grädel, 1991)

ESO-Horn beschreibt P auf der Klasse $FIN_<$ aller geordneten endlichen Strukturen.

(Hier bezeichnet P die Klasse aller deterministisch in Polynomialzeit lösbaren Probleme.)

Beweis:

1. Teil: Sei Φ ein ESO-Horn-Satz

zu zeigen: Das Problem

$\text{Eval}_{FIN_<}(\Phi)$

Eingabe: Eine endliche geordnete Struktur $\mathfrak{A}$

Frage: Gilt $\mathfrak{A} \models \Phi$?

ist in Polynomialzeit lösbar.

Idee: (1) Bei Eingabe von $\mathfrak{A}$ gehe ähnlich wie im obigen Beweis des Satzes von Cook-Levin vor, um Φ in Polyn.-Zeit in eine aussagenlogische Formel α umzuwandeln, für die gilt:

α ist erfüllbar $\iff \mathfrak{A} \models \Phi$.

(2) Wandle α um in eine Konjunktion von aussagenlogischen Horn-Klauseln.

(3) Zeige, dass das aussagenlogische Erfüllbarkeitsproblem für Horn-Klauseln in Polynomialzeit lösbar ist.

Details: Übung!

2. Teil:

Sei $\sigma = \{<, R_1, \dots, R_\ell, c_1, \dots, c_r\}$ eine Signatur und sei C eine unter Isomorphie abgeschlossene Klasse endlicher geordneter σ-Strukturen, so dass das Problem

Eingabe: eine endliche geordnete σ-Struktur $\mathfrak{A}$ (repräsentiert durch $enc_{<}(\mathfrak{A})$)

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

in P liegt, d.h. durch eine deterministische TM $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$ gelöst wird, für die es eine Zahl $k \in \mathbb{N}$ gibt, s.d. M bei Eingabe von $enc_{<}(\mathfrak{A})$ weniger als n^k Schritte macht, für $n = |A|$.

Gehe ähnlich vor wie im Beweis des 2. Teils des Satzes von Fagin, um einen ESO-Horn-Satz Φ zu konstruieren, s.d. f.a. endlichen geordneten σ-Strukturen $\mathfrak{A}$ gilt:

$\mathfrak{A} \models \Phi$ $\iff$ M akzeptiert $enc_{<}(\mathfrak{A})$.

Details: Übung!

□