2.1 Die Logik zweiter Stufe und der Satz von Fagin

Die erste solche Erweiterung ist die folgendermaßen definierte *Logik zweiter Stufe* (SO), die die Logik erster Stufe um Quantoren der Form $\exists X$ bzw. $\forall X$ erweitert, wobei X eine Relationsvariable ist.

2.1.1 Syntax und Semantik der Logik zweiter Stufe (SO)

2.3 Definition (Syntax der Logik zweiter Stufe SO). Sei σ eine Signatur.

(a) $\text{Var}_2 := \{\text{Var}_i^k \mid i, k \in \mathbb{N}_{\geqslant 1}\}$ ist die Menge alle *Variablen zweiter Stufe* (oder *Relationsvariablen*). Die Relationsvariable Var_i^k hat die *Stelligkeit* $ar(\text{Var}_i^k) = k$.
D.h. für jede Zahl k gibt es abzählbar viele Relationsvariablen der Stelligkeit k.

(b) Die Formelmenge $\text{SO}[\sigma]$ ist induktiv durch die Regeln (A1), (A2), (BC) und (Q1) der Logik erster Stufe (wobei "$\text{FO}[\sigma]$" jeweils durch "$\text{SO}[\sigma]$" ersetzt werden muss), sowie die beiden folgenden Regeln (A3) und (Q2) definiert:

(A3) Ist $X \in \text{Var}_2$ mit Stelligkeit $k := ar(X)$ und sind $v_1, .., v_k \in \text{Var}_1 \cup \{c \in \sigma \mid c \text{ ist ein Konstantensymbol}\}$, so gehört $X(v_1, .., v_k)$ zu $\text{SO}[\sigma]$.

(Q2) Ist ψ eine Formel in $\text{SO}[\sigma]$ und $X \in \text{Var}_2$, so gehören auch folgende Formeln zu $\text{SO}[\sigma]$:
- $\exists X\ \psi$ (Existenzquantor)
- $\forall X\ \psi$ (Allquantor).

(c) Die mit $(A1)$, $(A2)$ und $(A3)$ gebildeten Formeln heißen *atomare σ-Formeln*.

2.4 Bemerkungen.

(a) Analog zu Definition 1.8 bezeichnen wir mit

$$\textit{frei}(\varphi)$$

die Menge aller Variablen erster oder zweiter Stufe, die frei in einer $\text{SO}[\sigma]$-Formel φ vorkommen. Wir schreiben oft $\varphi(x_1, .., x_s, X_1, .., X_t)$ um anzudeuten, dass

$$\textit{frei}(\varphi) = \{x_1, .., x_s, X_1, .., X_t\}.$$

Eine $\text{SO}[\sigma]$-Formel φ heißt *Satz*, falls $\textit{frei}(\varphi) = \varnothing$, φ also keine freien Variablen erster Stufe und keine freien Relationsvariablen hat.

(b) Die *Semantik* der Logik zweiter Stufe ist auf die offensichtliche Weise definiert, z.B. gilt für eine σ-Struktur $\mathfrak{A}$, eine k-stellige Relationsvariable X und eine $\text{SO}[\sigma]$-Formel φ

$$\mathfrak{A} \models \exists X\, \varphi \iff \text{es gibt eine Relation } X^{\mathfrak{A}} \subseteq A^k, \text{ so dass } (\mathfrak{A}, X^{\mathfrak{A}}) \models \varphi.$$

Ist $\varphi(x_1,..,x_s,X_1,..,X_t)$ eine SO$[\sigma]$-Formel, $\mathfrak{A}$ eine σ-Struktur, $a_1,..,a_s \in A$ und $A_1,..,A_t$ Relationen über A mit $A_i \subseteq A^{ar(X_i)}$, so schreiben wir

$$\mathfrak{A} \models \varphi[a_1,..,a_s,A_1,..,A_t] \quad \text{bzw.} \quad (\mathfrak{A},A_1,..,A_t) \models \varphi[a_1,..,a_s]$$

falls die Formel φ in der Struktur $\mathfrak{A}$ *erfüllt* ist, wenn die freien Vorkommen der Variablen $x_1,..,x_s,X_1,..,X_t$ durch die Werte $a_1,..,a_s,A_1,..,A_t$ belegt werden.

(c) Für eine Signatur $\sigma = \{R_1,..,R_k,c_1,..,c_\ell\}$ schreiben wir oft SO$[R_1,..,R_k,c_1,..,c_\ell]$ an Stelle von SO$[\{R_1,..,R_k,c_1,..,c_\ell\}]$, um die Klasse aller SO$[\sigma]$-Formeln zu bezeichnen.

2.5 Beispiele (Graphprobleme).
Sei $\sigma := \{E\}$ die Signatur für Graphen, E also ein 2-stelliges Relationssymbol.

(a) Die Formel $\Phi_{\text{3-col}}$ aus Beispiel 0.2 ist ein SO$[\sigma]$-Satz, der in einem Graphen $G = (V,E)$ genau dann gilt, wenn der Graph 3-färbbar ist.
Also gilt: $\text{Mod}_{\mathsf{Fin}}(\Phi_{\text{3-col}}) = \{G \mid G \text{ ist ein 3-färbbarer Graph}\}$.

(b) Die Formel

$$\begin{aligned}\Phi_{\text{conn}} \;:=\; \forall X \Big(\big(\exists x\, X(x) \wedge \exists y\, \neg X(y)\big) \;\rightarrow \\ \exists u\, \exists v\, \big((E(u,v) \vee E(v,u)) \wedge X(u) \wedge \neg X(v)\big)\Big)\end{aligned}$$

besagt in ihren Modellen $G = (V,E)$, dass für jede nicht-leere Knotenmenge $X \neq V$ gilt: Es gibt eine Kante zwischen einem Knoten in X und einem Knoten außerhalb von X. Somit gilt für alle Graphen G:

$$\begin{aligned} G \not\models \Phi_{\text{conn}} \quad &\iff \quad \text{es gibt eine Knotenmenge } X \text{ mit } \varnothing \neq X \neq V, \text{ so} \\ & \quad \text{dass keine Kante zwischen } X \text{ und } V \setminus X \text{ verläuft} \\ &\iff \quad G \text{ ist nicht zusammenhängend.} \end{aligned}$$

Also gilt: $\text{Mod}_{\mathsf{Fin}}(\Phi_{\text{conn}}) = \{G \mid G \text{ ist ein zusammenhängender Graph}\}$.

(c) Ein *Hamiltonkreis* in einem Graphen $G = (V,E)$ ist eine Folge $v_0,v_1,..,v_{n-1}$ von Knoten, so dass $V = \{v_0,..,v_{n-1}\}$ und es eine Kante von v_n nach v_1 und eine Kante von v_i nach v_{i+1}, für alle $i < n$, gibt. Aus der Komplexitätstheorie ist bekannt, dass das Problem

HAMILTONKREIS:
Eingabe: Ein Graph G.
Frage: Hat G einen Hamiltonkreis?

NP-vollständig ist.
Wir geben nun einen SO-Satz Φ_{Ham} an, so dass

$$\text{Mod}_{\mathsf{Fin}}(\Phi_{\text{Ham}}) \;=\; \{G \mid G \text{ hat einen Hamiltonkreis}\}.$$

Die Formel Φ_{Ham} ist von der Form

$$\exists R_< \;\exists R_{succ}\;\exists z_0\;\exists z_{max}\;\Big(\;\varphi_{<,succ,0,max}(R_<, R_{succ}, z_0, z_{max}) \;\wedge\; E(z_{max}, z_0) \;\wedge\; \forall x\,\forall y\,\big(R_{succ}(x,y) \to E(x,y)\big)\Big),$$

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 Formel $\varphi_{<,succ,0}$ aus dem Beweis von Theorem 1.59 benutzt, um in ihren Modellen zu erzwingen, dass $R_<$ eine lineare Ordnung, R_{succ} deren Nachfolger-Relation, z_0 deren kleinstes und z_{max} deren größtes Element ist. Die letzte Zeile der Formel Φ_{Ham} besagt, dass die Folge $v_0, v_1, \ldots, v_{n-1}$, die man beim Durchlaufen der Knotenmenge entlang der Nachfolger-Relation R_{succ} erhält, einen Hamiltonkreis bildet. Insgesamt gilt für jeden endlichen Graph G:

$$G \models \Phi_{\text{Ham}} \iff G \text{ hat einen Hamiltonkreis.}$$

2.1.2 Existentielle Logik zweiter Stufe und der Satz von Fagin

In diesem Abschnitt beweisen wir den Satz von Fagin, der besagt, dass die Komplexitätsklasse NP aus genau den Problemen besteht, die durch Formeln der *existentiellen Logik zweiter Stufe* beschrieben werden können.

2.6 Definition (Existentielle Logik zweiter Stufe ESO). Sei σ eine Signatur.
Die Formelmenge ESO$[\sigma]$ aller *existentiellen* SO$[\sigma]$*-Formeln* besteht aus allen SO$[\sigma]$-Formeln Φ, die von der Gestalt

$$\exists X_1 \exists X_2 \cdots \exists X_d\, \varphi$$

sind, wobei $d \geqslant 0$, $X_1, \ldots, X_d$ Relationsvariablen und φ eine FO$[\sigma \dot{\cup} \text{Var}_2]$-Formel ist.

2.7 Beispiele. Die SO$[E]$-Formeln $\Phi_{\text{3-col}}$ und Φ_{Ham} aus Beispiel 2.5 sind ESO$[E]$-Formeln. Die Formel Φ_{conn} aus Beispiel 2.5 ist keine ESO$[E]$-Formel.

2.8 Theorem (Satz von Fagin, 1974). ESO *beschreibt* NP *auf* Fin.

Beweis: Sei σ eine Signatur.

"$\subseteq$": Zunächst zeigen wir, dass für jeden ESO$[\sigma]$-Satz Φ gilt:

$$L_{\mathsf{Fin}}(\Phi) \;:=\; \{enc(\mathfrak{A}) \mid \mathfrak{A} \in \mathsf{Fin} \text{ und } \mathfrak{A} \models \Phi\} \;\in\; \text{NP},$$

d.h. wir müssen zeigen, dass das Problem

$\mathrm{Mod}_{\mathsf{Fin}}(\Phi)$:
Eingabe: Eine endliche Struktur $\mathfrak{A}$.
Frage: Gilt $\mathfrak{A} \models \Phi$?

durch eine nichtdeterministische Turing-Maschine lösbar ist, deren Zeitschranke polynomiell in der Größe des Universums der Eingabe-Struktur $\mathfrak{A}$ ist.
Sei dazu der gegebene ESO$[\sigma]$-Satz Φ von der Form

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

mit $d \geqslant 0$ und $\varphi \in$ FO$[\sigma \dot\cup \{X_1, .., X_d\}]$.
Aus Lemma 1.56 folgt, dass es eine deterministische Turing-Maschine M' gibt, die das Problem

$$L' := \{\mathit{enc}(\mathfrak{A}') \mid \mathfrak{A}' \text{ ist eine } (\sigma \dot\cup \{X_1, .., X_d\})\text{-Struktur mit } \mathfrak{A}' \models \varphi\}$$

löst und dabei nur Platz $\mathcal{O}(\log n)$ benutzt, wobei n die Größe des Universums von $\mathfrak{A}'$ bezeichnet. Aus Satz 1.25 folgt, dass es eine Konstante $d' \in \mathbb{N}$ gibt, so dass M' Zeitschranke $n^{d'}$ hat. Unter Verwendung von M' kann man leicht eine NTM M bauen, die dem folgenden (nichtdeterministischen) Algorithmus gemäß das Problem $\mathrm{Mod}_{\mathsf{Fin}}(\Phi)$ löst:

Eingabe: Eine endliche σ-Struktur $\mathfrak{A}$.
Frage: Gilt $\mathfrak{A} \models \Phi$?
Lösung:

1. Rate Belegungen $X_1^{\mathfrak{A}}, .., X_d^{\mathfrak{A}}$ für die Relationsvariablen $X_1, .., X_d$, d.h. rate (Kodierungen von) Relationen $X_i^{\mathfrak{A}} \subseteq A^{ar(X_i)}$, für $i = 1, .., d$.
2. Entscheide, ob
$$(\mathfrak{A}, X_1^{\mathfrak{A}}, .., X_d^{\mathfrak{A}}) \models \varphi,$$
indem die Turing-Maschine M' mit Eingabe $\mathit{enc}(\mathfrak{A}')$, für $\mathfrak{A}' := (\mathfrak{A}, X_1^{\mathfrak{A}}, .., X_d^{\mathfrak{A}})$ gestartet wird.

Für Schritt 1 wird der Nicht-Determinismus genutzt. Da jede Relation $X_i^{\mathfrak{A}} \subseteq A^{ar(X_i)}$ durch ein 0-1-Wort der Länge $n^{ar(X_i)}$ kodiert werden kann, benötigt eine NTM für Schritt 1 nur polynomiell viele Schritte. Da die TM M' polynomiell zeitbeschränkt ist, reicht auch für Schritt 2 eine polynomielle Anzahl von Schritten aus.
Die so konstruierte NTM M löst also das Problem $L_{\mathsf{Fin}}(\Phi)$ und ist polynomiell zeitbeschränkt. Es gilt also: $L_{\mathsf{Fin}}(\Phi) \in$ NP.

"$\supseteq$": Sei C eine unter Isomorphie abgeschlossene Klasse endlicher σ-Strukturen, so dass

$$L_{\mathsf{C}} := \{\mathit{enc}(\mathfrak{A}) \mid \mathfrak{A} \in \mathsf{C}\} \in \mathrm{NP}.$$

D.h. es gibt eine NTM $M = (Q, \Sigma, \Gamma, \Delta, q_0, F)$ mit $F = F_{\text{akz}} \dot\cup F_{\text{verw}}$ und eine Konstante $k \in \mathbb{N}$, so dass M bei Eingabe (der Kodierung) einer endlichen σ-Struktur $\mathfrak{A}$ entscheidet, ob $\mathfrak{A} \in \mathsf{C}$ und dabei weniger als n^k Schritte macht. Mit n bezeichnen wir hierbei — und bis zum Ende dieses Beweises immer — die Größe des Universums der Eingabe-Struktur $\mathfrak{A}$. O.B.d.A. können wir annehmen, dass

- F_{akz} aus genau einem akzeptierenden Zustand q_{akz} besteht,
- jeder Lauf von M bei jeder Eingabe-Struktur $\mathfrak{A}$ mit $|A| \geqslant 2$ nach *genau* $n^k{-}1$ Schritten in einem (akzeptierenden oder verwerfenden) Endzustand endet und
- $n^k \geqslant |enc(\mathfrak{A})|$.

Unser Ziel ist, einen ESO$[\sigma]$-Satz Φ zu finden, so dass $\mathsf{C} = \mathrm{Mod}_{\mathsf{Fin}}(\Phi)$, d.h. für jede endliche σ-Struktur $\mathfrak{A}$ gilt:

$$\begin{aligned} \mathfrak{A} \models \Phi \quad &\iff \quad \mathfrak{A} \in \mathsf{C} \\ &\iff \quad M \text{ akzeptiert } \mathfrak{A} \\ &\iff \quad \text{es gibt einen Lauf von } M \text{ bei Eingabe } enc(\mathfrak{A}) \text{, der nach} \\ &\qquad\quad n^k{-}1 \text{ Schritten in Zustand } q_{\text{akz}} \text{ endet.} \end{aligned}$$

Idee zur Konstruktion von Φ: Ähnlich wie im Beweis des Satzes von Trachtenbrot. Jetzt wird aber jeder Zeitpunkt $t \in \{0,1,..,n^k{-}1\}$ durch das k-Tupel $\vec{t} := (t_1,..,t_k) \in \{0,..,n{-}1\}^k$ kodiert, für das gilt:

$$rg_{<_{lex}}(\vec{t}\,) \;=\; t.$$

Analog wird jede Bandposition $p \in \{0,1,..,n^k{-}1\}$ durch ein k-Tupel $\vec{p} := (p_1,..,p_k) \in \{0,..,n{-}1\}^k$ kodiert. Ein Lauf von M bei Eingabe $enc(\mathfrak{A})$ wird durch folgende Relationen repräsentiert:

- eine $2k$-stellige Relation $K^{\mathfrak{A}}$ mit der Bedeutung

  $(\vec{t},\vec{p}) \in K^{\mathfrak{A}} \iff$ der Schreib-/Lesekopf steht zum Zeitpunkt $\vec{t}$ auf Bandposition $\vec{p}$.

- für jedes Symbol $\gamma \in \Gamma$ eine $2k$-stellige Relation $B_\gamma^{\mathfrak{A}}$ mit der Bedeutung

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

- für jeden Zustand $q \in Q$ eine k-stellige Relation $Z_q^{\mathfrak{A}}$ mit der Bedeutung

  $\vec{t} \in Z_q^{\mathfrak{A}} \iff M$ ist zum Zeitpunkt $\vec{t}$ in Zustand q.

Damit k-Tupel $\vec{t} \in A^k$ bzw. $\vec{p} \in A^k$ überhaupt mit Tupeln aus $\{0,..,n{-}1\}^k$, und somit mit Zahlen aus $\{0,1,..,n^k{-}1\}$ identifiziert werden können, benötigen wir außerdem eine lineare Ordnung $<^{\mathfrak{A}}$ auf dem Universum A von $\mathfrak{A}$, deren Nachfolger-Relation $succ^{\mathfrak{A}}$, sowie Elemente $z_0^{\mathfrak{A}}$ und $z_{max}^{\mathfrak{A}}$ für das kleinste und das größte Element in A bzgl. der Ordnung $<^{\mathfrak{A}}$.

Der ESO$[\sigma]$-Satz Φ, der in jeder Struktur $\mathfrak{A}$ die Berechnung von M bei Eingabe $enc(\mathfrak{A})$ beschreibt, wird nun folgendermaßen gewählt:

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

wobei $\varphi_{<,succ,0,max}(R_<, R_{succ}, z_0, z_{max})$ die bereits in Beispiel 2.5(c) benutzte FO-Formel ist, die in ihren Modellen erzwingt, dass $R_<$ mit einer linearen Ordnung, R_{succ} mit deren Nachfolger-Relation und z_0 bzw. z_{max} mit deren kleinstem bzw. größtem Element belegt wird. Die FO-Formeln der letzten Zeile von Φ sind wie folgt gewählt:

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

$$\varphi_{Band} \ := \ \forall x_1 \cdots \forall x_k \, \forall y_1 \cdots \forall y_k \ \bigvee_{\gamma\in\Gamma} \Big(B_\gamma(\vec{x},\vec{y}) \ \wedge \ \bigwedge_{\substack{\gamma'\in\Gamma\\ \gamma'\neq\gamma}} \neg B_{\gamma'}(\vec{x},\vec{y}) \Big).$$

φ_{Kopf} besagt, dass zu jedem Zeitpunkt der Schreib-/Lesekopf auf genau einer Bandposition steht:

$$\varphi_{Kopf} \ := \ \forall x_1 \cdots \forall x_k \, \exists y_1 \cdots \exists y_k \ \Big(K(\vec{x},\vec{y}) \ \wedge \ \forall y'_1 \cdots \forall y'_k \ \big(K(\vec{x},\vec{y}\,') \leftrightarrow \bigwedge_{i=1}^{k} y_i = y'_i \big) \Big).$$

$\varphi_{Zustand}$ besagt, dass die Maschine zu jedem Zeitpunkt in genau einem Zustand aus der Zustandsmenge Q ist:

$$\varphi_{Zustand} \ := \ \forall x_1 \cdots \forall x_k \ \bigvee_{q\in Q} \Big(Z_q(\vec{x}) \ \wedge \ \bigwedge_{\substack{q'\in Q\\ q'\neq q}} \neg Z_{q'}(\vec{x}) \Big).$$

$\varphi_{Akzeptiere}$ besagt, dass M zum Zeitpunkt $n^k{-}1$, der durch das k-Tupel $(z_{max},\ldots,z_{max})$ repräsentiert wird, in dem *akzeptierenden* Zustand q_{akz} ist:

$$\varphi_{Akzeptiere} \ := \ Z_{q_{\text{akz}}}(\underbrace{z_{max},\ldots,z_{max}}_{k}).$$

Die Formel $\varphi_{Schritt}$ besagt für jeden Zeitpunkt $\vec{t}$: Falls $\vec{t}$ nicht das Ende der Berechnung ist, so ist M im Zeitpunkt $\vec{t}\,' := \vec{t}+1$ in einem laut Übergangsrelation Δ zulässigen Zustand q' und hat das entsprechende Symbol auf's Band geschrieben, den Kopf an die richtige Stelle bewegt und die Beschriftung aller anderen Bandpositionen nicht verändert.
Die Formel $\varphi_{Schritt}$ benutzt die FO-Formel

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

sowie eine FO-Formel

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

die besagt, dass das k-Tupel $\vec{y}$ mit dem unmittelbaren Nachfolger (bzgl. der aus $R_<$ gebildeten lexikographischen Ordnung) des Tupels $\vec{x}$ belegt ist (genaue Konstruktion der Formel $\mathit{succ}_{<_{lex}}(\vec{x}, \vec{y})$: *Übung*).
Zur besseren Lesbarkeit schreiben wir in der folgenden Formel

$$\exists \vec{t} \qquad \text{bzw.} \qquad \forall \vec{p}$$

als Abkürzung für die Quantifizierungen

$$\exists t_1 \cdots \exists t_k \qquad \text{bzw.} \qquad \forall p_1 \cdots \forall p_k\,.$$

$$\begin{aligned}
&\varphi_{\mathit{Schritt}} \;:= \\
&\forall \vec{t}\, \forall \vec{p} \bigwedge_{q \in Q \setminus F} \bigwedge_{\gamma \in \Gamma} \Big(\Big(K(\vec{t}, \vec{p}) \;\wedge\; Z_q(\vec{t}) \;\wedge\; B_\gamma(\vec{t}, \vec{p}) \Big) \;\rightarrow \\
&\qquad \Big(\exists \vec{t}\,' \exists \vec{p}\,' \; \big(\mathit{succ}_{<_{lex}}(\vec{t}, \vec{t}\,') \;\wedge\; K(\vec{t}\,', \vec{p}\,') \;\wedge \\
&\qquad\qquad \big(\forall \vec{p}\,'' \; (\mathit{equal}(\vec{p}\,'', \vec{p}) \;\vee \bigwedge_{\gamma'' \in \Gamma} (B_{\gamma''}(\vec{t}\,', \vec{p}\,'') \leftrightarrow B_{\gamma''}(\vec{t}, \vec{p}\,''))\,)\,\big) \;\wedge \\
&\qquad\qquad \bigvee_{\substack{q', \gamma', m \,:\\ (q, \gamma, q', \gamma', m) \in \Delta}} (\, Z_{q'}(\vec{t}\,') \;\wedge\; B_{\gamma'}(\vec{t}\,', \vec{p}) \;\wedge\; \chi_m(\vec{p}, \vec{p}\,')\,)\,\big)\Big)\Big),
\end{aligned}$$

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

$$\begin{aligned}
\chi_1(\vec{p}, \vec{p}\,') &:= \mathit{succ}_{<_{lex}}(\vec{p}, \vec{p}\,'), \\
\chi_{-1}(\vec{p}, \vec{p}\,') &:= \mathit{succ}_{<_{lex}}(\vec{p}\,', \vec{p}), \\
\chi_0(\vec{p}, \vec{p}\,') &:= \mathit{equal}(\vec{p}, \vec{p}\,').
\end{aligned}$$

Nun fehlt nur noch die Formel φ_{Start}, die besagt, dass M zum Zeitpunkt 0 (der durch das k-Tupel $\vec{z}_0 := (z_0, \dots, z_0)$ kodiert wird) in der Anfangskonfiguration bei Eingabe des Worts $\mathit{enc}(\mathfrak{A})$ ist, d.h. M ist im Startzustand q_0, der Schreib-/Lesekopf steht auf Bandposition 0 (die durch das k-Tupel $\vec{z}_0 := (z_0, \dots, z_0)$ kodiert wird), und für jedes $\vec{p} \in \{0, \dots, n{-}1\}^k$ gilt: Auf Bandposition $i := \mathit{rg}_{<_{lex}}(\vec{p}) \in \{0, 1, \dots, n^k{-}1\}$ steht

- das Symbol 0, falls an der i-ten Position des Worts $\mathit{enc}(\mathfrak{A})$ eine 0 steht,
- das Symbol 1, falls an der i-ten Position des Worts $\mathit{enc}(\mathfrak{A})$ eine 1 steht,
- das Blank-Symbol $\Box$, falls $i \geqslant |\mathit{enc}(\mathfrak{A})|$.

Dies wird durch die FO-Formel

$$\varphi_{\mathit{Start}} \;:=\; Z_{q_0}(\vec{z}_0) \,\wedge\, K(\vec{z}_0,\vec{z}_0) \,\wedge\, \forall y_1\cdots\forall y_k \Big(\big(B_0(\vec{z}_0,\vec{y}) \leftrightarrow \zeta_0(\vec{y})\big) \wedge \big(B_1(\vec{z}_0,\vec{y}) \leftrightarrow \zeta_1(\vec{y})\big) \wedge \big(B_{\Box}(\vec{z}_0,\vec{y}) \leftrightarrow \neg(\zeta_0(\vec{y}) \vee \zeta_1(\vec{y}))\big) \Big)$$

ausgedrückt, wobei $\zeta_0(\vec{y})$ und $\zeta_1(\vec{y})$ geeignete FO-Formeln sind, die ausdücken, dass in dem 0-1-Wort $\mathit{enc}(\mathfrak{A})$ an Position $\mathit{rg}_{<_{\mathit{lex}}}(\vec{y})$ eine 0 bzw. eine 1 steht. Im Folgenden werden die Formeln ζ_0 und ζ_1 für den speziellen Fall angegeben, dass die Signatur σ aus einem 2-stelligen Relationssymbol R_1 und einem Konstantensymbol c_1 besteht. Der allgemeine Fall, in dem σ aus mehreren Relationssymbolen verschiedener Stelligkeiten und mehreren Konstantensymbolen besteht, kann ganz analog behandelt werden.

Ist $\sigma = \{R_1, c_1\}$ (für ein 2-stelliges Relationssymbol R_1 und ein Konstantensymbol c_1), so gilt für jede σ-Struktur $\mathfrak{A}$, dass das Wort $\mathit{enc}(\mathfrak{A})$ die Länge $3n^2$ hat, wobei $n := |A|$ ist und $\mathit{enc}(\mathfrak{A})$ von der Form

$$\mathit{enc}(\mathfrak{A}) \;=\; \underbrace{1^n 0^{n^2-n}}_{\text{Länge } n^2}\; \underbrace{\mathit{enc}(R_1^{\mathfrak{A}})}_{\text{Länge } n^2}\; \underbrace{\mathit{enc}(c_1^{\mathfrak{A}})}_{\text{Länge } n^2} \;\in\; \{0,1\}^{3n^2}.$$

Die Positionen $0,..,3n^2{-}1$ des Worts $\mathit{enc}(\mathfrak{A})$ werden durch genau diejenigen k-Tupel $\vec{p} = (p_1,..,p_k) \in \{0,..,n{-}1\}^k$ kodiert, für die gilt:

$$p_1 = \cdots = p_{k-3} = 0, \quad p_{k-2} \in \{0,1,2\} \quad \text{und} \quad p_{k-1}, p_k \in \{0,..,n{-}1\}.$$

Daher erzwingen die folgenden Formeln $\zeta_1(\vec{y})$ und $\zeta_0(\vec{y})$, dass in ihren Modellen die Variablen $\vec{y}$ mit Werten belegt sind, die Positionen kodieren, an denen in $\mathit{enc}(\mathfrak{A})$ eine 1 bzw. eine 0 steht:

$$\begin{aligned}
\zeta_1(y_1,..,y_k) \;:=&\\
&\bigwedge_{i=1}^{k-3} y_i = z_0 \,\wedge\, \Big(\big(y_{k-2} = z_0 \,\wedge\, y_{k-1} = z_0\big) && \text{(Anfangsblock } 1^n0^{n^2-n}\text{)}\\
&\qquad \vee \big(R_{\mathit{succ}}(z_0, y_{k-2}) \,\wedge\, R_1(y_{k-1}, y_k)\big) && \text{(Teilstück } \mathit{enc}(R_1^{\mathfrak{A}})\text{)}\\
&\qquad \vee \big(\text{“}y_{k-2} = 2\text{”} \,\wedge\, y_{k-1} = z_0 \,\wedge\, y_k = c_1\big) \Big) && \text{(Teilstück } \mathit{enc}(c_1^{\mathfrak{A}})\text{)}
\end{aligned}$$

$$\begin{aligned}
\zeta_0(y_1,..,y_k) \;:=&\\
&\bigwedge_{i=1}^{k-3} y_i = z_0 \,\wedge\, \Big(y_{k-2} = z_0 \,\vee\, R_{\mathit{succ}}(z_0, y_{k-2}) \,\vee\, \text{“}y_{k-2} = 2\text{”}\Big) \,\wedge\, \neg\, \zeta_1(y_1,..,y_k),
\end{aligned}$$

wobei “$y_{k-2} = 2$” für die Formel $\exists x\big(R_{\mathit{succ}}(z_0, x) \wedge R_{\mathit{succ}}(x, y_{k-2})\big)$ steht.

Insgesamt sind wir nun fertig mit der Konstruktion der ESO-Formel Φ. Man kann leicht nachprüfen (per Induktion nach den Zeitpunkten $0, 1, . . , n^k-1$), dass für jede endliche σ-Struktur $\mathfrak{A}$ gilt:

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

Da M genau die σ-Strukturen akzeptiert, die in C liegen, gilt demnach:
$\mathfrak{A} \models \Phi \iff \mathfrak{A} \in \mathsf{C}$. Somit sind wir fertig mit dem Beweis von Theorem 2.8. □

Unter Verwendung des Satzes von Fagin erhält man relativ leicht einen Beweis für das folgende Resultat (das allerdings bereits vor dem Satz von Fagin bekannt war):

2.9 Theorem (Satz von Cook, 1971). *Das aussagenlogische Erfüllbarkeitsproblem*

SAT:
Eingabe: Eine aussagenlogische Formel α.
Frage: Gibt es eine Variablenbelegung, die α erfüllt?

ist NP*-vollständig.*

Beweis: SAT $\in$ NP, denn man kann leicht einen nichtdeterministischen Polynomialzeit-Algorithmus angeben, der bei Eingabe einer aussagenlogischen Formel α zunächst eine Belegung der in α vorkommenden 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 von L auf SAT gibt. Jedes Problem L kann man, für eine geeignete Signatur σ, mit einer Klasse C endlicher σ-Strukturen identifizieren, so dass $L = L_{\mathsf{C}}$ ist. Da nach Voraussetzung $L \in$ NP ist, liefert der Satz von Fagin (Theorem 2.8), dass es einen ESO$[\sigma]$-Satz Φ gibt, so dass für jede endliche σ-Struktur $\mathfrak{A}$ gilt: $\mathfrak{A} \in \mathsf{C} \iff \mathfrak{A} \models \Phi$.
Der Satz Φ sei von der Form

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

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

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

$$\mathfrak{A} \models \Phi \iff \alpha_{\Phi,\mathfrak{A}} \text{ hat eine erfüllende Belegung.}$$

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

$$V \;:=\; \{\, v_{X_i,\vec{a}} \;\mid\; i \in \{1, . . , d\} \text{ und } \vec{a} \in A^{ar(X_i)} \,\}.$$

Die Idee dabei ist, dass eine Belegung, die der Variablen $v_{X_i,\vec{a}}$ den Wahrheitswert 1 zuordnet, kodiert, dass das Tupel $\vec{a}$ in der Relation X_i liegt. Somit entspricht eine Belegung der aussagenlogischen Variablen aus V mit Werten aus $\{0, 1\}$ gerade einer Belegung der Relationsvariablen $X_1, . . , X_d$ mit Relationen über dem Universum von $\mathfrak{A}$.

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

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

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

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

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

5. Ersetze jedes "Atom" der Form $R(\vec{a})$ (für $R \in \sigma$ und $\vec{a} \in A^{ar(R)}$) durch den Wahrheitswert 1, falls $\vec{a} \in R^{\mathfrak{A}}$, und durch den Wahrheitswert 0, falls $\vec{a} \notin R^{\mathfrak{A}}$.

6. Ersetze jede Gleichung der Form $a = b$ (für $a, b \in A$) durch den Wahrheitswert 1, falls $a = b$ ist, und durch den Wahrheitswert 0, falls $a \neq b$ ist.

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

- $\mathfrak{A} \models \Phi \iff \alpha_{\Phi,\mathfrak{A}}$ ist erfüllbar,
- Bei Eingabe der Struktur $\mathfrak{A}$ kann man in polynomieller Zeit (also 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 die Formel $\alpha_{\Phi,\mathfrak{A}}$ zuordnet, eine Polynomialzeit-Reduktion von dem Problem L auf das aussagenlogische Erfüllbarkeitsproblem SAT.
Insgesamt haben wir also gezeigt, dass das Problem SAT NP-vollständig ist. □

2.1.3 Logische Charakterisierung der Polynomialzeit-Hierarchie

Die folgenden Fragmente der Logik zweiter Stufe stehen in einem wichtigen Zusammenhang zur den Stufen der Polynomialzeit-Hierarchie:

2.10 Definition (Σ^1_k und Π^1_k).
Für jedes $k \in \mathbb{N}$ definieren wir induktiv die Formelklassen Σ^1_k und Π^1_k folgendermaßen:

- $\Sigma^1_0 \ := \ \Pi^1_0 \ := \ \text{FO}.$
- $\Sigma^1_{k+1} \ := \ \{\, \exists X_1 \cdots \exists X_\ell\, \varphi \ \mid \ \ell \geqslant 0,\ X_1, .., X_\ell$ sind Relationsvariablen und $\varphi \in \Pi^1_k \,\}$
- $\Pi^1_{k+1} \ := \ \{\, \forall X_1 \cdots \forall X_\ell\, \varphi \ \mid \ \ell \geqslant 0,\ X_1, .., X_\ell$ sind Relationsvariablen und $\varphi \in \Sigma^1_k \,\}$.

2.11 Bemerkungen.

(a) Man beachte, dass $\Sigma^1_1 = \text{ESO}$, und für alle $k \in \mathbb{N}$ gilt:

$$\text{FO} \ \subseteq \ \Sigma_k \ \subseteq \ \Pi_{k+1} \ \subseteq \ \Sigma_{k+2} \ \subseteq \ \text{SO}.$$

(b) Σ_k^1-Formeln sind von der Gestalt

$$\exists \vec{Y}_1 \, \forall \vec{Y}_2 \cdots Q \, \vec{Y}_k \, \varphi,$$

wobei φ eine FO-Formel, jedes $\vec{Y}_i$ ein Tupel von Relationsvariablen und

$$Q = \begin{cases} \forall\,, & \text{falls } k \text{ gerade} \\ \exists\,, & \text{falls } k \text{ ungerade.} \end{cases}$$

Die einzelnen Tupel $\vec{Y}_i$ heißen (existentielle bzw. universelle) *Quantorenblöcke*.

(c) Man kann leicht sehen, dass es für jede SO-Formel Φ eine Zahl k und eine Formel $\Psi \in \Sigma_k^1$ gibt, so dass Ψ äquivalent zu Φ ist.
Somit ist jede SO-Formel äquivalent zu einer Formel in $\bigcup_{k \in \mathbb{N}} \Sigma_k^1$.

Aus dem Satz von Fagin erhält man leicht die folgende Charakterisierung der Polynomialzeit-Hierarchie:

2.12 Korollar.

(a) Für jedes $k \in \mathbb{N}_{\geqslant 1}$ gilt: Σ_k^1 beschreibt Σ_k^p auf Fin.

D.h. ein Problem gehört genau dann zur k-ten Stufe Σ_k^p der Polynomialzeit-Hierarchie, wenn es durch einen Σ_k^1-Satz beschrieben werden kann.

(b) Für jedes $k \in \mathbb{N}_{\geqslant 1}$ gilt: Π_k^1 beschreibt Π_k^p auf Fin.

(c) SO *beschreibt* PH *auf* Fin.

Beweis: Übung. □