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

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

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

$Eval_S(\varphi)$
Eingabe: Eine endliche Struktur $\mathfrak{A} \in S$
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

Eingabe: $\mathfrak{A} \in S$, $\mathfrak{A}$ eine σ-Struktur

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

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

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

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 $\mathfrak{A}$ als Eingabe einer Turingmaschine repräsentiert wird. Wir benutzen dazu die sog. <u>Standardkodierung</u>, die im Folgenden eingeführt wird.

<u>Definition 2.20</u>

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

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

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

Dh: $rg_<(a_i) = i$.

<u>(b)</u> Sei $r \in \mathbb{N}_{\geq 1}$. Die <u>lexikographische Ordnung</u> $<_{lex}$ 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 $enc_<(\mathfrak{A})$)

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

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

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

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

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

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

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

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

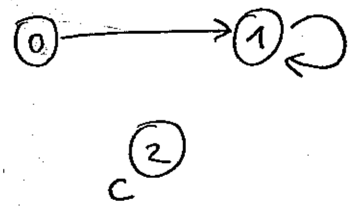
$$\mathrm{enc}_<(\mathfrak{A}) := \mathrm{enc}_<(|A|)\, \mathrm{enc}_<(R_1^{\mathfrak{A}}) \cdots \mathrm{enc}_<(R_l^{\mathfrak{A}})\, \mathrm{enc}_<(c_1^{\mathfrak{A}}) \cdots \mathrm{enc}_<(c_{l'}^{\mathfrak{A}})$$

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

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 $\mathfrak{A}$.

dann gilt: $r = 2$, $n = 3$, $n^r = 9$

$$enc_<(\mathfrak{A}) = \underbrace{111|000000}_{enc_<(|A|)}\ \underbrace{010|010|000}_{enc_<(E^{\mathfrak{A}})}\ \underbrace{001|000000}_{enc_<(c^{\mathfrak{A}})}$$

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 feste Signatur σ ist die Länge von $enc_<(\mathfrak{A})$ polynomiell in der Mächtigkeit $|A|$ der Struktur $\mathfrak{A}$.

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

Für ein Tupel $\bar{b} \in A^{r_j}$ 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 2.19 (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 zu NP gehört:

$\text{Eval}_{\text{FIN}}(\Phi)$
Eingabe: Eine endliche σ-Struktur $\mathfrak{A}$
Frage: Gilt $\mathfrak{A} \models \Phi$?

Ein nichtdeterministische 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 $X_1, \ldots, X_d$, d.h. rate Relationen $X_1^{\mathfrak{A}} \subseteq A^{ar(X_1)}, \ldots, X_d^{\mathfrak{A}} \subseteq A^{ar(X_d)}$

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

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

   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".