4.4 Eine untere Schranke für Formeln in Gaifman-Normalform

Insbesondere angesichts der in Abschnitt 4.3 dargestellten algorithmischen Anwendungen des Satzes von Gaifman ist es natürlich interessant, zu wissen, wie effizient die laut Satz von Gaifman mögliche Umformung einer FO-Formel in eine äquivalente Formel in Gaifman-Normalform durchgeführt werden kann.

Eine Analyse des Algorithmus, der sich aus dem Beweis von Satz 4.11 ergibt, zeigt, dass die Laufzeit dieses Algorithmus verheerend ist: mit jedem Quantor, der in der Formel vorkommt, erhöht sich die Laufzeit um mindestens eine Zweierpotenz.

<u>Definition 4.21</u>

Die Funktion $\text{Turm}: \mathbb{N} \to \mathbb{N}$ ist induktiv definiert durch

$$\text{Turm}(0) :: 1 \quad \text{und}$$

$$\text{Turm}(k+1) :: 2^{\text{Turm}(k)} \qquad (\text{f.a. } k \in \mathbb{N}).$$

D.h.: $$\text{Turm}(k) = \left. 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \right\} k$$

Die Tatsache, dass der Algorithmus zur Transformation in GNF, den wir bisher kennengelernt haben, eine verheerende Laufzeit besitzt (nämlich: für eine Formel mit k ineinandergeschachtelten Quantoren ist die Laufzeit größer als Turm(k)), heißt natürlich noch nicht, dass die Transformation prinzipiell nicht effizienter bewerkstelligt werden kann.

Der folgende Satz zeigt allerdings, dass es in der Tat keinen wesentlich effizienteren Algorithmus zur Transformation in GNF geben kann, weil es FO-Sätze gibt, deren kürzeste äquivalente Sätze in GNF extrem lang sind:

<u>Satz 4.22</u> (Dawar, Grohe, Kreutzer, Schweikardt, 2007)

Für jedes $h \in \mathbb{N}_{\geq 1}$ gibt es einen $\text{FO}[\{E\}]$-Satz φ_h der Länge $\mathcal{O}(h^4)$, so dass jeder zu φ_h äquivalente $\text{FO}[\{E\}]$-Satz in Gaifman-Normalform mindestens die Länge $\text{Turm}(h)$ hat.

(hier ohne Beweis)

Kapitel 5: Der Satz von McNaughton und Papert

Der Satz von McNaughton und Papert (1971) besagt, dass die Logik erster Stufe genau die sternfreien regulären Wortsprachen beschreiben kann.

Sei $\Sigma := \{a_1, \ldots, a_\ell\}$ ein endliches Alphabet, das (für eine Zahl $\ell \in \mathbb{N}_{\geq 1}$) aus ℓ verschiedenen Buchstaben besteht.

Definition 5.1

(a) Sei σ_Σ die Signatur, die aus den folgenden Relationssymbolen besteht:

- σ_Σ enthält ein 2-stelliges Relationssymbol $\leq$
- für jeden Buchstaben $a \in \Sigma$ enthält σ_Σ ein 1-stelliges Relationssymbol P_a

(b) $\sigma_\Sigma' := \sigma_\Sigma \cup \{max\}$ sei die Signatur, die zusätzlich zu den Symbolen aus σ_Σ noch ein Konstantensymbol max enthält

<u>Definition 5.2</u>

Einem endlichen Wort $w = w_1 \cdots w_n$ der Länge $n \geq 1$ über dem Alphabet Σ ordnen wir die folgende σ_Σ-Struktur

$$\mathfrak{A}_w = \left(A_w, \leq^{\mathfrak{A}_w}, P_{a_1}^{\mathfrak{A}_w}, \ldots, P_{a_\ell}^{\mathfrak{A}_w} \right) \text{ zu:}$$

- $A_w := \{1, \ldots, n\}$
- $\leq^{\mathfrak{A}_w}$ ist die natürliche lineare Ordnung auf $\{1, \ldots, n\}$
- für jedes $a_j \in \Sigma$ ist
  $P_{a_j}^{\mathfrak{A}_w} := \{ i \in A_w : w_i = a_j \}$.

Die σ'_Σ-Struktur $\mathfrak{A}'_w$ ist definiert durch

$$\mathfrak{A}'_w := \left(A_w, \leq^{\mathfrak{A}_w}, P_{a_1}^{\mathfrak{A}_w}, \ldots, P_{a_\ell}^{\mathfrak{A}_w}, \max^{\mathfrak{A}'_w} \right)$$

mit $\max^{\mathfrak{A}'_w} := n$.

Beispiel 5.3

Ist $\Sigma = \{a, b\}$ und $w = aaab$, so ist

$\mathfrak{M}_w$ die σ_Σ-Struktur mit

- Universum $\{1,2,3,4\}$
- $\leq^{\mathfrak{M}_w}$ = die lineare Ordnung auf $\{1,2,3,4\}$
- $P_a^{\mathfrak{M}_w} = \{1,2,3\}$
- $P_b^{\mathfrak{M}_w} = \{4\}$

$\mathfrak{M}'_w$ ist die σ'_Σ-Struktur, die mit $\mathfrak{M}_w$ auf σ_Σ übereinstimmt, und bei der $max^{\mathfrak{M}'_w} = 4$ ist.

Definition 5.4

(a) Sei $L \subseteq \Sigma^*$ und sei φ ein $FO[\sigma'_\Sigma]$-Satz.

Wir sagen: φ beschreibt L, falls für jedes nicht-leere Wort $w \in \Sigma^*$ gilt:

$$w \in L \iff \mathfrak{M}'_w \models \varphi.$$

(b) $L \subseteq \Sigma^*$ heißt FO-definierbar, falls es einen $FO[\sigma'_\Sigma]$-Satz φ gibt, der L beschreibt.

Beispiel 5.5

Für $\Sigma := \{a, b\}$ gilt:

Der $FO[\sigma_\Sigma']$ - Satz $\varphi :=$

$$\Big(P_b \max \wedge \exists x \forall y \big((y \le x \to P_a y) \wedge (x \le y \to (P_b y \vee y = x)) \big) \Big)$$

beschreibt die Sprache $L \subseteq \Sigma^*$, die durch den regulären Ausdruck $a^* a b^* b$ definiert wird.

Definition 5.6

(a) Die Klasse SFR_Σ aller sternfreien regulären Ausdrücke über Σ ist rekursiv wie folgt definiert:

- das Symbol $\emptyset$ gehört zu SFR_Σ
- für jedes $a \in \Sigma$ gehört das Symbol a zu SFR_Σ
- Sind $r \in SFR_\Sigma$ und $s \in SFR_\Sigma$, so gehören auch die folgenden Ausdrücke zu SFR_Σ:
  - $\overline{r}$
  - $(r | s)$
  - $(r \cdot s)$

(b) Jeder sternfreie reguläre Ausdruck r **beschreibt** eine Sprache $L(r) \subseteq \Sigma^*$, die wie folgt definiert ist:

- $L(\emptyset) = \emptyset$
- für jedes $a \in \Sigma$ ist $L(a) = \{a\}$
- für alle $r \in SFR_\Sigma$ und $s \in SFR_\Sigma$ ist
    - $L(\overline{r}) := \Sigma^* \setminus L(r)$
    - $L((r|s)) := L(r) \cup L(s)$
    - $L((r \cdot s)) := \{ wu : w \in L(r), u \in L(s)\}$

(c) Eine Sprache $L \subseteq \Sigma^*$ heißt **sternfrei regulär**, wenn es ein $r \in SFR_\Sigma$ mit $L(r) = r$ gibt.

Beispiel 5.7

Die durch den regulären Ausdruck $(a|b)^* a (a|b)^* b$ definierte Sprache wird durch den sternfreien regulären Ausdruck $((\overline{\emptyset} \cdot a) \cdot (\overline{\emptyset} \cdot b))$ beschreiben.

Satz 5.8 (Der Satz von McNaughton und Papert, 1971)

Für jede Sprache $L \subseteq \Sigma^*$ gilt:

L ist sternfrei regulär $\iff$ L ist FO-definierbar.

Beweis:

"$\Longrightarrow$": Per Induktion über den Aufbau der sternfreien regulären Ausdrücke zeigt man, dass es für jedes $r \in SFR_\Sigma$ einen $FO[\sigma_\Sigma]$-Satz φ_r gibt, der die Sprache $L(r)$ beschreibt (beachte: $\sigma_\Sigma = \sigma'_\Sigma \setminus \{max\}$)

"$\Longleftarrow$": Wir benutzen das folgende Lemma:

Kompositionslemma:

Ist $m \in \mathbb{N}$ und sind $w, \tilde{w}, u, \tilde{u}$ nicht-leere Worte über dem Alphabet $\Sigma = \{a_1, \dots, a_\ell\}$, so dass

$\mathcal{A}'_w \approx_m \mathcal{A}'_{\tilde{w}}$ und $\mathcal{A}'_u \approx_m \mathcal{A}'_{\tilde{u}}$, so

gilt für $p := |w|$ und $\tilde{p} := |\tilde{w}|$, dass

$(\mathcal{A}'_{wu}, p) \approx_m (\mathcal{A}'_{\tilde{w}\tilde{u}}, \tilde{p})$, d.h.

Duplicator hat eine Gewinnstrategie im m-Runden EF-Spiel auf $(\mathcal{A}'_{wu}, p)$ und $(\mathcal{A}'_{\tilde{w}\tilde{u}}, \tilde{p})$.

<u>Beweis</u> des Kompositionslemmas: Übung.

Um die Richtung "$\Leftarrow$" von Satz 5.8 zu beweisen, gehen wir per Induktion über die Quantorentiefe m von $FO[\sigma'_\Sigma]$-Sätzen vor.

<u>Induktionsanfang: $m=0$</u>

Sei φ ein $FO[\sigma'_\Sigma]$-Satz der Quantorentiefe $m=0$

<u>Fall 1</u>: φ ist von der Form $P_a \max$ für ein $a \in \Sigma$.

Dann beschreibt φ dieselbe Sprache wie der sternfreie reguläre Ausdruck $(\overline{\emptyset} \cdot a)$.

<u>Fall 2</u>. φ ist von der Form $\max \leq \max$ oder von der Form $\max = \max$.

Dann beschreibt φ dieselbe Sprache wie der sternfreie reguläre Ausdruck $\overline{\emptyset}$.

Fall 3: φ ist von der Form $\neg\varphi_1$, wobei φ_1 ein $FO[\sigma_\Sigma']$-Satz der Quantorentiefe $m=0$ ist.

Per Induktion gibt es dann einen sternfreien regulären Ausdruck r, der dieselbe Sprache wie φ_1 beschreibt.

Der reguläre Ausdruck $\overline{r}$ beschreibt dann dieselbe Sprache wie φ.

Fall 4: φ ist von der Form $(\varphi_1 \vee \varphi_2)$, wobei φ_1 und φ_2 $FO[\sigma_\Sigma']$-Sätze der Quantorentiefe $m=0$ sind. Per Induktion gibt es dann r_1 und r_2 in SFR_Σ, die dieselben Sprachen wie φ_1 und φ_2 beschreiben.

Der reguläre Ausdruck $(r_1 | r_2)$ beschreibt dann dieselbe Sprache wie φ.

Fall 5: φ ist von der Form $(\varphi_1 \wedge \varphi_2)$ oder $(\varphi_1 \rightarrow \varphi_2)$ oder $(\varphi_1 \leftrightarrow \varphi_2)$:

Folgt durch eine Kombination der Fälle 3 und 4, da

$$
\begin{aligned}
(\varphi_1 \wedge \varphi_2) &\equiv \neg(\neg\varphi_1 \vee \neg\varphi_2) \\
(\varphi_1 \rightarrow \varphi_2) &\equiv (\neg\varphi_1 \vee \varphi_2) \\
(\varphi_1 \leftrightarrow \varphi_2) &\equiv ((\varphi_1 \rightarrow \varphi_2) \wedge (\varphi_2 \rightarrow \varphi_1))
\end{aligned}
$$

Induktionsschritt: $m \to m+1$: Sei $m \geq 0$.

Induktionsannahme: Für jeden $FO[\sigma_\Sigma^1]$-Satz ψ der Quantorentiefe $\leq m$ gibt es einen sternfreien regulären Ausdruck $r_\psi \in SFR_\Sigma$, der dieselbe Sprache wie ψ beschreibt.

Behauptung: Für jeden $FO[\sigma_\Sigma^1]$-Satz φ der Quantorentiefe $m+1$ gibt es einen sternfreien regulären Ausdruck $r_\varphi \in SFR_\Sigma$, der dieselbe Sprache wie φ beschreibt.

Beweis: Per Induktion nach dem Aufbau von $FO[\sigma_\Sigma^1]$-Sätzen der Quantorentiefe $m+1$.

Fall 1: φ ist von der Form $\exists x\, \psi(x)$, wobei $\psi(x)$ eine $FO[\sigma_\Sigma^1]$-Formel der Quantorentiefe m mit $frei(\psi) = \{x\}$ ist.

Wir betrachten die Menge

$$m\text{-Typen}_0 := \left\{ \varphi_{\mathcal{A}}^m : \begin{array}{l} \mathcal{A} \text{ ist eine} \\ \sigma_\Sigma^1\text{-Struktur} \end{array} \right\}$$

aller m-Isomorphietypen von σ_Σ^1-Strukturen.

Von Bemerkung 3.20 wissen wir, dass

m-Typen_0 eine <u>endliche</u> Menge von $FO[\sigma'_\Sigma]$-Sätzen

der Quantorentiefe $\leq m$ ist.

Sei S_ψ die folgendermaßen definierte Menge

aller Paare (τ, τ') von Elementen aus m-Typen_0:

$S_\psi := \{ (\tau, \tau') :$ $\tau, \tau' \in m$-Typen_0,

es gibt nicht-leere Worte

$\tilde{w} \in \Sigma^*$ und $\tilde{u} \in \Sigma^*$, so dass für

$\tilde{p} := |\tilde{w}|$ gilt:

- $\mathfrak{A}'_{\tilde{w}\tilde{u}} \models \psi[\tilde{p}]$ und
- $\mathfrak{A}'_{\tilde{w}} \models \tau$ und
- $\mathfrak{A}'_{\tilde{u}} \models \tau'$ $\}$.

<u>Beachte:</u> S_ψ ist endlich, da m-Typen_0 endlich ist.

Behauptung ⊛:

Für alle nicht-leeren Worte $v \in \Sigma^*$ gilt:

$$\mathfrak{A}'_v \models \exists x\, \psi(x)$$

$\iff$ $\mathfrak{A}'_v \models \psi\frac{max}{x}$ oder

es gibt eine Position $p \in \{1, \dots, |v|-1\}$ und ein Paar $(\tau, \tau') \in S_\psi$, so dass für die nicht-leeren Worte w und u mit $v = wu$ und $|w| = p$ gilt:

$$\mathfrak{A}'_w \models \tau \quad \text{und} \quad \mathfrak{A}'_u \models \tau'$$

(d.h. τ und τ' sind die m-Isomorphietypen von w und u)

Beweis von Behauptung ⊛:

"$\Longrightarrow$": Folgt direkt aus der Definition der Menge S_ψ.

"$\Longleftarrow$": klar: Falls $\mathfrak{A}'_v \models \psi\frac{max}{x}$, so gilt: $\mathfrak{A}'_v \models \exists x\, \psi(x)$.

Sei also $p \in \{1, \dots, |v|-1\}$ und sei $(\tau, \tau') \in S_\psi$, so dass für die nicht-leeren Worte w und u mit $v = wu$ und $|w| = p$ gilt:

(1) $\tau = \varphi^m_{\mathfrak{A}'_w}$ und $\tau' = \varphi^m_{\mathfrak{A}'_u}$.

Wir müssen zeigen, dass dann auch $\mathfrak{A}'_{wu} \models \exists x \psi(x)$ gilt.

Wegen $(\tau, \tau') \in S_\psi$ muss es gemäß der Definition der Menge S_ψ nicht-leere Worte $\tilde{w} \in \Sigma^*$ und $\tilde{u} \in \Sigma^*$ geben, so dass für $\tilde{p} := |\tilde{w}|$ gilt:

$\underline{(2)}$ $\mathfrak{A}'_{\tilde{w}\tilde{u}} \models \psi[\tilde{p}]$ und $\mathfrak{A}'_{\tilde{w}} \models \tau$ und $\mathfrak{A}'_{\tilde{u}} \models \tau'$.

Aus $(\underline{1})$ und $(\underline{2})$ folgt gemäß dem Satz von Ehrenfeucht (Satz 3.21), dass

$$\mathfrak{A}'_w \approx_m \mathfrak{A}'_{\tilde{w}} \quad \text{und} \quad \mathfrak{A}'_u \approx_m \mathfrak{A}'_{\tilde{u}}.$$

Das Kompositionslemma liefert dann, dass auch gilt:

$$(\mathfrak{A}'_{wu}, p) \approx_m (\mathfrak{A}'_{\tilde{w}\tilde{u}}, \tilde{p})$$

Wegen $m = qr(\psi)$ und $\mathfrak{A}'_{\tilde{w}\tilde{u}} \models \psi[\tilde{p}]$ (gemäß $(\underline{2})$), liefert der Satz von Ehrenfeucht (Satz 3.21) daher, dass auch $\mathfrak{A}'_{wu} \models \psi[p]$ gilt.

Somit gilt: $\mathfrak{A}'_{wu} \models \exists x \psi(x)$.

$\Box$ Behauptung (*)

Für den Satz $\varphi = \exists x\, \psi(x)$ liefert Behauptung ⊛, dass die von φ beschriebene Sprache folgendermaßen aussieht:

$$\{ v \in \Sigma^* : v \text{ ist nicht-leer und } \mathfrak{A}'_v \models \varphi \}$$

$$\underset{\text{Beh}⊛}{=} \{ v \in \Sigma^* : v \text{ ist nicht-leer und } \mathfrak{A}'_v \models \psi\tfrac{\max}{x} \}$$

$$\cup \bigcup_{(\tau,\tau') \in S_\psi} L_{(\tau,\tau')} ,$$

wobei $L_{(\tau,\tau')} := \{ wu : w \in \Sigma^* \text{ und } u \in \Sigma^*, w \text{ und } u \text{ sind nicht-leer und } \mathfrak{A}'_w \models \tau \text{ und } \mathfrak{A}'_u \models \tau' \}$.

Da τ und τ' $\mathrm{FO}[\sigma'_\Sigma]$-Sätze der Quantorentiefe $\leq m$ sind, gibt es laut Induktionsannahme sternfreie reguläre Ausdrücke r_τ und $r_{\tau'}$, die dieselben Sprachen wie τ und τ' beschreiben.

Daher gilt: $L_{(\tau,\tau')} = L\big((r_\tau \cdot r_{\tau'}) \big)$.

Außerdem ist $\psi\frac{\max}{x}$ ein $\mathrm{FO}[\sigma'_\Sigma]$-Satz der Quantorentiefe m. Laut Induktionsannahme gibt es daher einen sternfreien regulären Ausdruck

$r_{\psi^{\max}_{x}}$, der dieselbe Sprache wie $\psi^{\max}_{x}$ beschreibt.

Insgesamt gilt: Ist $(\tau_1, \tau_1'), \dots, (\tau_t, \tau_t')$ eine Liste aller Elemente in der Menge S_ψ, so beschreibt der sternfreie reguläre Ausdruck

$$r_\varphi := \left(r_{\psi^{\max}_{x}} \;\middle|\; \left((r_{\tau_1} \cdot r_{\tau_1'}) \;|\; \cdots \;|\; (r_{\tau_t} \cdot r_{\tau_t'}) \right) \right)$$

dieselbe Sprache wie der $FO[\sigma_\Sigma']$-Satz φ.

Somit ist der Beweis von Fall 1 des Induktionsschritts abgeschlossen.

<u>Fall 2:</u> φ ist von der Form $\forall x\, \psi$:

Beachte, dass $\varphi \equiv \neg \exists x \neg \psi$.

Gemäß Fall 1 gibt es einen sternfreien regulären Ausdruck r, der dieselbe Sprache wie der Satz $\exists x \neg \psi$ beschreibt.

Klar: Der sternfreie reguläre Ausdruck $\overline{r}$ beschreibt dieselbe Sprache wie φ.

Fall 3: φ ist von der Form $\neg\varphi_1$ oder von der Form $(\varphi_1 * \varphi_2)$ mit $* \in \{\vee, \wedge, \rightarrow, \leftrightarrow\}$, wobei φ_1 und φ_2 $FO[\sigma_\Sigma]$-Sätze der Quantorentiefe $m+1$ sind:

Analog zu Fall 3, Fall 4 und Fall 5 des Induktionsanfangs.

Insgesamt ist damit der Beweis von Satz 5.8 abgeschlossen.

$\square$