Seminararbeit Theoretische Informatik

Erfassung deterministischer Polynomialzeit mittels kleinsten Fixpunktoperatoren

Markus Peschl
Matrikelnummer: 01609416
SS 2018

Betreuer: Prof. Stefan Hetzl

10. Juni 2018

Inhaltsverzeichnis

1 Einleitung **2**

2 Der Kleinste Fixpunkt Operator **2**

2.1 Existenz und Minimalität 2

2.2 $\mathbf{FO_{LFP} = P}$ 4

2.3 Die Tiefe von rekursiven Formeln 6

2.4 Ein Normalformensatz für R-positive Formeln 8

1 Einleitung

Will man die Komplexität diverser Berechnungen untersuchen, so stößt man beim Versuch diese Berechnungen mittels Ausdrücken der Prädikatenlogik erster Stufe zu beschreiben schnell an Grenzen. Es ist zum Beispiel generell nicht möglich, die transitive Hülle eines Graphen in erststufiger Logik auszudrücken (siehe [Lib04] Abschnitt 4.1). Ziel dieser Arbeit ist es, mittels induktiver Definitionen die Ausdrucksstärke der Logik erster Stufe zu erhöhen und zu zeigen, dass mithilfe jenen neuen Ausdrücken Entscheidungsprobleme in deterministischer Polynomialzeit erfasst werden.

2 Der Kleinste Fixpunkt Operator

2.1 Existenz und Minimalität

Wir illustrieren, wie man die transitive Hülle eines Graphen induktiv beschreiben kann. Sei dazu ein Graph $G = (V, E)$ gegeben, wobei V die Menge der Punkte und E eine zweistellige Relation auf V bezeichnet. Außerdem denotiere mit $dist(a, b)$ die Distanz zweier Knoten $a \in V$ und $b \in V$ als kleinste Zahl n, für die a und b mittels n Kanten verbunden werden können. Wenn es keine solchen Kanten gibt, so sei die Distanz auf ∞ gesetzt. Für ein zweistelliges Relationensymbol R definieren wir die Formel

$$\phi(R, x, y) \equiv x = y \ \vee \ \exists z(E(x, z) \wedge R(z, y)) \tag{2.1}$$

Diese Formel induziert eine Abbildung von der Menge aller zweistelligen Relationen des Graphen auf sich selbst:

$$\phi_G(R) = \{(a, b) \in V^2 \mid G \models \phi(R, a, b)\} \tag{2.2}$$

Nun wird ersichtlich, dass man durch wiederholtes anwenden dieser Abbildung auf die leere Menge die transitive Hülle von E erhält:

$$\begin{aligned}\phi_G(\emptyset) = \{(a, b) \in V^2 \mid dist(a, b) \leq 0\} \subseteq \{(a, b) \in V^2 \mid dist(a, b) \leq 1\} \subseteq \cdots \\ \cdots \subseteq \{(a, b) \in V^2 \mid dist(a, b) \leq k - 1\} = \phi_G^k(\emptyset)\end{aligned} \tag{2.3}$$

Falls $|V| = n$, so sieht man, dass diese Kette spätestens für $k = n$ nicht weiter wachsen kann. Wenn E^* die transitive Hülle on E bezeichnet, so gilt dann: $\phi_G^n(\emptyset) = E^* = \phi_G(E^*)$. Die Relation E^* ist also ein Fixpunkt der Abbildung ϕ_G. Dass mit diesem Verfahren ein Fixpunkt gewonnen werden kann, ist ein allgemeines Resultat:

Satz 2.1. *Sei R ein k-stelliges Relationensymbol, $\phi(R, x_1, \cdots, x_k)$ eine Formel erster Ordnung, deren induzierte Abbildung $\phi_\mathcal{A}$ für eine Struktur $\mathcal{A}$ monoton ist, das heißt es gelte $R \subseteq R' \implies \phi_\mathcal{A}(R) \subseteq \phi_\mathcal{A}(R')$. Wenn $\mathcal{A}$ endlich ist, so existiert ein kleinster Fixpunkt von $\phi_\mathcal{A}$. Dieser ist $\phi_\mathcal{A}^r$, wobei r die kleinste natürliche Zahl ist, für die $\phi_\mathcal{A}^r(\emptyset) = \phi_\mathcal{A}^{r+1}(\emptyset)$. Außerdem gilt $r \leq ||\mathcal{A}||^k$*

Beweis. Aufgrund der Monotonie können wir wie in (2.3) folgende Kette beobachten

$$\emptyset \subseteq \phi_\mathcal{A}(\emptyset) \subseteq \phi_\mathcal{A}^2(\emptyset) \subseteq \cdots \subseteq \phi_\mathcal{A}^i(\emptyset) \subseteq \cdots$$

Da die Struktur $\mathcal{A}$ nach Voraussetzung endlich ist und nur n^k verschiedene k- Tupel von $\mathcal{A}$ existieren, kann die Kette ab einem Index i nicht mehr strikt weiter wachsen. Wählen wir nun $r := \min\{i \in \mathbb{N} \mid \forall k \geq i : \ \phi_\mathcal{A}^i(\emptyset) = \phi_\mathcal{A}^k(\emptyset)\}$ so haben wir einen Fixpunkt der Abbildung gefunden. Um die Minimalität zu beweisen, sei F ein weiterer Fixpunkt der Abbildung.

Wegen

$$\phi^0_{\mathcal{A}}(\emptyset) = \emptyset \subseteq F$$

folgt induktiv, mit der Annahme, dass $\phi^i_{\mathcal{A}}(\emptyset) \subseteq F$ und mit der Monotonie von $\phi_{\mathcal{A}}$:

$$\phi^{i+1}_{\mathcal{A}}(\emptyset) = \phi_{\mathcal{A}} \circ \phi^i_{\mathcal{A}}(\emptyset) \subseteq \phi_{\mathcal{A}}(F) = F$$

Also ist $\phi^i_{\mathcal{A}}(\emptyset) \subseteq F$ für alle $i \geq 0$. □

Ab sofort bezeichne $\mathbf{FO_{LFP}}$ die Sprache aller Formeln der Aussagenlogik, welche zusätzlich den Operator LFP enthalten können. LFP ordnet jeder Formel $\phi(R, x_1, \ldots, x_n)$ ihren kleinsten Fixpunkt nach Satz 2.1 zu. Man beachte, dass hier nur jene Formeln erlaubt sind, die die Voraussetzungen des Satzes 2.1 erfüllen. Ein induktiver Beweis zeigt aber, dass dies für Formeln $\phi(R, x_1, \ldots, x_n)$, in denen das Relationensymbol R nur innerhalb einer geraden Anzahl von Negationen vorkommt immer der Fall ist.

Satz 2.2. *Wenn eine Formel $\phi(R, x_1, \ldots, x_n)$ R-positiv ist (das bedeutet, dass R nur innerhalb einer geraden Anzahl von Negationen vorkommt), so ist die von einer Struktur $\mathcal{A}$ induzierte Abbildung $\phi_{\mathcal{A}}$ monoton.*

Beweis. Wir beweisen die Aussage per Induktion nach dem Aufbau der Formel. Der Induktionsanfang ist klar: Sei $\phi_0(R, \overline{x}) \equiv R(\overline{x})$, wobei $\overline{x}$ ein Tupel von Variablen bezeichnet. Offensichtlich folgt dann für $R \subseteq R'$

$$\mathcal{A} \models \phi_0(R, \overline{a}) \implies \mathcal{A} \models \phi_0(R', \overline{a}) \tag{2.4}$$

Im Induktionsschritt unterscheiden wir 2 Fälle:

- An eine R-positive Formel ϕ hängen wir mittels $\vee$ eine weitere R-positive Formel ψ: Wir beobachten, dass $\mathcal{A} \models (\phi \vee \psi)(R, \overline{a})$, wenn entweder $\mathcal{A} \models \phi(R, \overline{a})$ oder $\mathcal{A} \models \psi(R, \overline{a})$. Für $R \subseteq R'$ können wir wie in (2.4) die Implikation auf ϕ bzw. ψ anwenden, da nach Induktionsvoraussetzung beide Formeln monoton sind. Per Definition gilt dann aber auch $\mathcal{A} \models (\psi \vee \phi)(R', \overline{a})$. Analog beweist man den Fall für $\phi \wedge \psi$.

- Sei $\phi(R, \overline{x})$ eine nach Voraussetzung monotone Formel. Nun ist auch $\exists z(\phi(R, z, \overline{x}'))$ monoton: Per Definition gilt $\mathcal{A} \models \exists z(\phi(R, z, \overline{a}'))$, wenn für eine beliebige Interpretation ein $a \in |\mathcal{A}|$ existiert, sodass $(\mathcal{A}, i_{a/z}) \models \phi(R, z, \overline{x}')$, wobei $i_{a/x}$ die modifizierte Interpretation bezeichnet, welche $i_{a/x}(y) = a$ erfüllt für $y = x$ und ansonsten die gewöhnlichen Werte $i_{a/x}(y) = i(y)$ annimmt für $y \neq x$. Wegen der Monotonie von ϕ folgt daraus aber auch $(\mathcal{A}, i_{a/z}) \models \phi(R', z, \overline{x}')$ für $R \subseteq R'$. Wir haben also ein $a \in |\mathcal{A}|$ gefunden, und somit gilt auch $\mathcal{A} \models \exists z(\phi(R', z, \overline{x}'))$. Analog beweist man wieder den Fall für $\forall z(\phi(R, z, \overline{x}'))$.

□

Die Umkehrung des obigen Satzes gilt in der Regel nicht.Über endlichen Strukturen lassen sich nämlich Aussagen erster Ordnung konstruieren, welche zwar monoton in R sind, in denen aber R nicht notwendigerweise innerhalb einer geraden Anzahl von Negationen vorkommen muss.

2.2 $\mathbf{FO_{LFP}} = \mathbf{P}$

Es stellt sich heraus, dass mit der Hinzunahme von induktiven Definitionen, wie sie mittels dem kleinsten Fixpunkt Operator erzeugt werden können, genau jene Berechnungen, welche in der Komplexitätsklasse **P** liegen erfasst werden. Dazu zeigen wir zuerst folgendes Resultat:

Satz 2.3. *Die Sprache* $\mathbf{FO_{LFP}}$ *ist unter Reduktionen erster Stufe abgeschlossen.*

Beweis. Sei $I : \mathfrak{S}(\sigma) \to \mathfrak{S}(\tau)$ eine k-stellige Abfrage erster Stufe zwischen zwei abstrakten Strukturmengen, wobei σ und τ Vokabulare sind, die nur Relationen- und Konstantensymbole enthalten. Außerdem bezeichne $\hat{I} : \mathfrak{L}(\tau) \to \mathfrak{L}(\sigma)$ die dazugehörige duale Abbildung (siehe [Imm99] Definition 3.3). Die duale Abbildung von I erfüllt nach Konstruktion für jede Struktur $\mathcal{A} \in \mathfrak{S}(\sigma)$ und jede Formel $\tau \in \mathfrak{L}(\tau)$:

$$\mathcal{A} \models \hat{I}(\phi) \iff I(\mathcal{A}) \models \phi \tag{2.5}$$

Damit lässt sich zeigen, dass der Operator LFP mit Bildung von dualen Abbildungen verträglich ist. Es gilt nämlich für für R-positive $\phi \in \mathbf{FO_{LFP}}(\tau)$

$$\hat{I}(\mathrm{LFP}(\phi(R, x_1, \ldots, x_n))) \equiv \mathrm{LFP}(\hat{I}(\phi)(R_{nk}, x_1^1, \ldots x_1^k, \ldots, x_n^1, \ldots x_n^k)) \tag{2.6}$$

Um das einzusehen, betrachten wir die durch eine Struktur $A \in \mathfrak{S}(\sigma)$ induzierte Abbildung

$$\begin{aligned} \hat{I}(\phi)_{\mathcal{A}}(R_{nk}) &= \{(x_1^1, \ldots x_1^k, \ldots, x_n^1, \ldots x_n^k) \in A^{nk} \mid \mathcal{A} \models \hat{I}(\phi)(R_{nk}, x_1^1, \ldots x_1^k, \ldots, x_n^1, \ldots x_n^k)\} \\ &\cong \{(x_1, \ldots, x_n) \in |I(A)|^n \mid I(\mathcal{A}) \models \phi(R, x_1, \ldots, x_n)\} \\ &= \phi_{I(\mathcal{A})}(R) \end{aligned} \tag{2.7}$$

Wir haben also eine Isomorphie der Fixpunkte von $\hat{I}(\phi)$ und ϕ in den jeweiligen Strukturen $\mathcal{A}$ und $I(\mathcal{A})$ gegeben. Aus folgender Äquivalenzkette ergibt sich schießlich (2.6):

$$\begin{aligned} \mathcal{A} \models \mathrm{LFP}(\hat{I}(\phi)(R_{nk}, x_1^1, \ldots x_1^k, \ldots, x_n^1, \ldots x_n^k)) &\overset{(2.7)}{\iff} I(\mathcal{A}) \models \mathrm{LFP}(\phi(R, x_1, \ldots, x_n)) \\ &\overset{(2.5)}{\iff} \mathcal{A} \models \hat{I}(\mathrm{LFP}(\phi(R, x_1, \ldots, x_n))) \end{aligned} \tag{2.8}$$

Um schließlich die Abgeschlossenheitseigenschaft zu zeigen, seien also A und B zwei Entscheidungsprobleme, B durch eine Formel $\phi_B \in \mathbf{FO_{LFP}}$ formulierbar und $A \leq_{\mathrm{FO}} B$. Das heißt, dass eine Abbildung I existiert mit der Eigenschaft, dass für alle Strukturen gilt

$$S \in A \iff I(S) \in B$$

Die Äquivalenz in (2.6) besagt genau, dass für $\phi \in \mathbf{FO_{LFP}}$ auch $\hat{I}(\phi) \in \mathbf{FO_{LFP}}$. Wenden wir dies auf ϕ_B an, so sehen wir insgesamt (wieder mit (2.5)), dass

$$S \in A \iff I(S) \in B \iff S \models \hat{I}(\phi_B) \tag{2.9}$$

und somit A durch die Formel $\hat{I}(\phi_B) \in \mathbf{FO_{LFP}}$ ausgedrückt werden kann, woraus die Abgeschlossenheit folgt. □

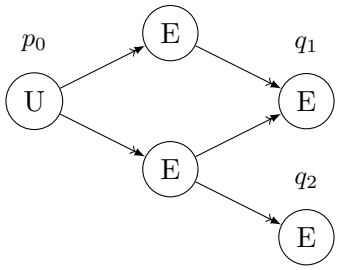

Abbildung 1: p_0 erreicht q_1, aber nicht q_2.

Um die Gleichheit $\mathbf{P} = \mathbf{FO_{LFP}}$ zu zeigen, werden wir ausnützen, dass ein $\mathbf{P}$ vollständiges Problem existiert, welches in $\mathbf{FO_{LFP}}$ liegt. Es handelt sich hier um das Erreichbarkeitsproblem in alternierenden Graphen: Sei $G = (V, E, U, p_0, q)$ ein gerichteter Graph mit Start- und Endpunkt p_0 und q, wessen Knoten noch in zwei Typen, Existenz- und Universalknoten unterteilt sind. $U \subseteq V$ sei die Menge der Universalknoten. Das Konzept ist ähnlich zu alternierenden Turing Maschinen: Wir sagen, dass von einem Universalknoten u ein Knoten k erreicht wird, wenn alle Kanten, die von u weg gehen (sofern welche existieren), zu einem anderen Knoten gehen, der selbst k erreicht. Ein Existenzknoten e erreicht einen Knoten k im alternierenden Sinn, sobald eine einzige Kante zu einem Knoten geht, der k erreicht. Abbildung 1 illustriert einen alternierenden Graphen als Beispiel.

Wir können nun mit dem kleinsten Fixpunktoperator dieses Erreicharkeitsproblem logisch ausdrücken: Sei

$$\phi_a(R, x, y) \equiv (x = y) \vee \left[\exists z(E(x, z) \wedge R(z, y)) \wedge (A(x) \implies \forall z(E(x, z) \implies R(z, y)))\right] \tag{2.10}$$

Der erste Teil der Formel ist analog zu verstehen wie in Formel (2.1) und die rechte Seite der Konjunktion stellt sicher, dass alle von Universalknoten entspringenden Kanten den Zielpunkt erreichen. Wie bei der transitiven Hülle, können wir nun die Menge aller alternierenden Graphen G, bei denen p vom Start q_0 erreicht wird als $\mathrm{LFP}(\phi_a(R, x, y))(q_0, p)$ ausdrücken. Somit gilt für das Entscheidungsproblem

$$\textsc{Reach}_a = \{G = (V, E, U, p_0, q) \mid G \text{ alternierender Graph} \wedge \mathrm{LFP}(\phi_a(E, x, y))(q_0, p)\} \in \mathbf{FO_{LFP}} \tag{2.11}$$

Wir erhalten nun folgendes Resultat:

Satz 2.4. *Für endliche und geordnete Strukturen gilt*

$$\mathbf{FO_{LFP}} = \mathbf{P} \tag{2.12}$$

Beweis. Wir zeigen Teilmengeninklusion in beide Richtungen.

($\mathbf{FO_{LFP}} \subseteq \mathbf{P}$) : Sei $\mathcal{A}$ eine beliebige endliche Struktur, das heißt für die Grundmenge A von $\mathcal{A}$ gilt $|A| = n < \infty$. Sei weiters $\mathrm{LFP}(\phi(R, x_1, \ldots, x_k)) \in \mathbf{FO_{LFP}}$ beliebig. Satz 2.1 gibt uns eine Darstellung des kleinsten Fixpunktes von ϕ, nämlich $\phi^r_{\mathcal{A}}(\emptyset)$, wobei $r \leq n^k$. Das heißt die Formel ϕ muss höchstens n^k mal ausgewertet werden. Das Auswerten von Formeln erster Stufe erfolgt aber in deterministischer Polynomialzeit (siehe [Imm99] Satz 3.1; Auswertung erfolgt sogar in $\mathbf{L}$), daher ist $\mathrm{LFP}(\phi(R, x_1, \ldots, x_k)) \in \mathbf{P}$.

($\mathbf{P} \subseteq \mathbf{FO_{LFP}}$) : Im obigen Abschnitt wurde schon erwähnt, dass $\text{REACH}_a \in \mathbf{FO_{LFP}}$. Nun gilt aber, dass REACH_a vollständig ist in $\mathbf{P}$ bezüglich Reduktionen erster Stufe (siehe [Imm99] Satz (3.26)). Nach Satz 2.3 ist $\mathbf{FO_{LFP}}$ abgeschlossen unter solchen Reduktionen, also folgt daraus, dass jedes Entscheidungsproblem aus $\mathbf{P}$ auch in $\mathbf{FO_{LFP}}$ liegen muss. □

Bemerkung: Der obige Satz gibt uns eine logische Beschreibung der Komplexitätsklasse $\mathbf{P}$, die ohne Turing Maschinen und Laufzeit auskommt. Obwohl die Voraussetzung der Ordnung nicht direkt im Beweis eingeht, wird sie benötigt um die Vollständigkeit von REACH_a zu beweisen.

Als Folgerung der letzten beiden Sätze können wir noch einen Normalformensatz für induktive Formeln beweisen. Im allgemeinen könnte es ja passieren, dass Formeln $\phi \in \mathbf{FO_{LFP}}$ sehr kompliziert aussehen, da es erlaubt ist mehrere kleinste Fixpunkte ineinander zu schachteln, sowie diese zu quantifizieren. Glücklicherweise kann aber jede Formel so umgeschrieben werden, dass nur ein einziges mal der kleinste Fixpunktoperator darin vorkommt:

Satz 2.5. *Für eine beliebige Formel $\phi \in \mathbf{FO_{LFP}}$ existiert eine Formel ψ erster Stufe, sowie ein Konstantentupel c, sodass in endlichen und geordneten Strukturen gilt:*

$$\phi \equiv \text{LFP}(\psi)(c) \tag{2.13}$$

Beweis. Fassen wir REACH_a als Entscheidungsproblem auf, so haben wir oben schon gesehen dass wir dieses mithilfe der Formel ϕ_a ausdrücken können, also

$$\text{REACH}_a = \text{FP}(\phi_a(R, x, y))(p_0, q) \tag{2.14}$$

Da REACH_a vollständig in $\mathbf{P}$ bezüglich Reduktionen erster Stufe ist, existiert für jedes Problem $A \in \mathbf{P}$ eine k-stellige Abbildung $I_A : \mathfrak{S}(\sigma) \to \mathfrak{S}(\tau)$, für die (2.9) gilt(wobei B durch REACH_a zu ersetzen ist). Das bedeutet aber, dass sich jedes Problem A aus $\mathbf{P}$ als $\hat{I}_A(\text{REACH}_a)$ schreiben lässt. Wenden wir die Gleichheit (2.14) an und nutzen die Verträglichkeit des Fixpunktoperators mit dualen Abbildungen aus (siehe (2.6)), so sieht man, dass

$$\hat{I}_A(\text{REACH}_a) = \text{LFP}(\hat{I}_A(\phi_a))(\hat{I}_A(p_0, q)) \tag{2.15}$$

Das Resultat folgt, da $\hat{I}_A$ die Konstantensymbole p_0 und q wieder mit den Konstantensymbolen 0 und *max* ersetzt, was aus [Imm99] Satz 3.26 hervorgeht. □

2.3 Die Tiefe von rekursiven Formeln

Die Tiefe einer induktiven Definition ist in der Komplexitätstheorie von großer Bedeutung. Offensichtlich macht es auch in der praktischen Anwendung einen großen Unterschied, wie oft ein rekursiver Algorithmus die Rekursion durchlaufen muss um zum Stillstand zu kommen. Für eine beliebige Struktur $\mathcal{A}$ und eine induktive Formel ϕ definieren wir die zu $\mathcal{A}$ relative Tiefe $|\phi_\mathcal{A}|$ der Formel ϕ als kleinste Zahl $r \in \mathbb{N}$, sodass für die von $\mathcal{A}$ induzierte Abbildung $\phi_\mathcal{A}$ (siehe Satz 2.1) gilt:

$$\phi_\mathcal{A}^r(\emptyset) = \phi_\mathcal{A}^{r+1}(\emptyset) \tag{2.16}$$

Satz 2.1 gibt uns die Existenz eines solchen r, sowie eine obere Schranke, welche von der Mächtigkeit der Grundmenge von $\mathcal{A}$ abhängt. Meistens ist es interessanter die Tiefe einer Formel unabhängig von einer bestimmten Struktur zu betrachten. Wir nehmen daher für die Tiefe $|\phi|(n)$von ϕ in Strukturen der Mächtigkeit n das Maximum über alle relativen Tiefen:

$$|\phi|(n) := \max_{|\mathcal{A}|=n} |\phi_{\mathcal{A}}| \tag{2.17}$$

Betrachten wir die Formel $\phi(R, x, y)$ aus (2.1), so lässt sich aus den Mengeninklusionen in (2.3) schnell einsehen, dass $|\phi|(n) = n$ gilt. Natürlich ist $\phi(R, x, y)$ nicht die einzige Formel, dessen Fixpunkt die transitive Hülle einses Graphen ausdrücken kann. Wir könnten zum Beispiel auch durch die Formel

$$\psi(R, x, y) \equiv x = y \vee E(x, y) \vee \exists z(R(x, z) \wedge R(z, y)) \tag{2.18}$$

das selbe erreichen, wobei nun $|\psi|(n) = \lceil \log n \rceil + 1$, also hat ψ generell eine eindeutig geringere Tiefe als ϕ. Es bezeichne ab sofort $\mathbf{IND}[f(n)] \subseteq \mathbf{FO_{LFP}}$ die Sprache aller Formeln ϕ für die $|\phi|(n) = \mathcal{O}(f(n))$ gilt (wobei natürlich nur Formeln zugelassen werden, die einen kleinsten Fixpunkt besitzen). Mit dieser Definition können wir $\mathbf{FO_{LFP}}$ auch anschreiben als

$$\mathbf{FO_{LFP}} = \bigcup_{k=1}^{\infty} \mathbf{IND}[n^k] \tag{2.19}$$

Als Anwendung zeigen wir, dass die numerische Relation $\text{BIT}(i, j)$, welche wahr ist wenn in der Binärdarstellung von i das j-te Bit gleich 1 ist, in $\mathbf{IND}[\log n]$ enthalten ist. Das bedeutet, dass wir BIT als kleinsten Fixpunkt darstellen können, wobei die resultierende Tiefe der Formel durch $\log n$ beschränkt ist. Da durch die Existenz der numerischen Relationen $\text{PLUS}(i, j, k)$, welche für $i + j = k$ wahr ist und durch $\text{TIMES}(i, j, k)$, welche für $i * j = k$ wahr ist, in einem Vokabular (inklusive Ordnung) schon folgt, dass BIT in Logik erster Stufe definierbar ist (siehe [Imm99] Satz 1.17), reicht es $\mathbf{IND}[\log n]$ Definitionen für PLUS und TIMES zu finden:

Satz 2.6. *Die numerischen Relationen* PLUS *und* TIMES *sind in* $\mathbf{IND}[\log n]$ *enthalten.*

Beweis. Es denotiere SUCC die Nachfolger-Relation, sowie 0 das minimale Element bezüglich SUCC (Die Existenz dieser Relation und dieses Konstantensymbols sei vorausgesetzt). Wir finden zuerst eine Formel $\nu_+(x, y, z)$, welche genau die Relation $x + y = z$ beschreibt. Dazu sei

$$\begin{aligned}\phi_+(R, x, y, z) \equiv &(x = 0 \wedge z = y) \vee \exists u, v[\text{SUCC}(u, 0) \wedge \text{SUCC}(v, y) \wedge x = u \wedge z = v] \vee \\ &\exists z_1, z_2, z_3, z_4, \alpha, \beta[R(\alpha, \beta, x) \wedge R(\alpha, z_1, z_2) \wedge R(\beta, z_3, z_4) \wedge \\ &R(z_1, z_3, y) \wedge R(z_2, z_4, z)]\end{aligned} \tag{2.20}$$

Die erste Zeile gibt uns den Anfang der induktiven Definition: Entweder wir haben ein paar $(0, y)$, so gilt natürlich $0 + y = z$, mit $z = y$. Damit erfassen wir alle Tripel, welche eine Null in der ersten Koordinate haben. Ansonsten haben wir ein Tripel $(1, y, z)$ vorliegen, für das $1 + y = z$, indem wir z als Nachfolger von y dekodieren und $x = 1$ voraussetzen. Im Induktionsschritt seien schon alle Tripel von (x, y, z) gegeben, mit $x \leq k$, für die $x + y = z$ gilt. Nun schließen wir aus dem Bekannten auf alle neuen Summentripel (x', y', z'), für die $x' \leq 2k$ ist. Dies funktioniert, indem wir $\alpha \leq k$ und $\beta \leq k$ mit $\alpha + \beta = x'$ finden, sowie z_1, z_2, z_3, z_4 mit $\alpha + z_1 = z_2$ und $\beta + z_3 = z_4$. Addieren wir die Tripel (α, z_1, z_2) und (β, z_3, z_4) auf (das heißt wir addieren die zwei Gleichungen), so erhalten wir die Vorschrift $(\alpha + \beta) + (z_1 + z_3) = (z_2 + z_4)$, das heißt $z_1 + z_3 = y$ und $z_2 + z_4 = z$ müssen erfüllt werden. Dieses Verfahren funktioniert wirklich, da man natürlich jede natürliche Zahl n zum

Beispiel in $1 + (n-1)$ aufpsalten kann. Damit wird auch $R(z_1, z_3, y)$, sowie $R(z_2, z_4, z)$ wirklich erfüllt. Wir finden immer eine Zerlegung von y, sodass z_1 und z_3 kleiner oder gleich k sind. Wir setzen nun

$$\nu_+(i,j,k) = \mathrm{LFP}(\phi_+(R,x,y,z))(i,j,k) \tag{2.21}$$

Nach Konstruktion bricht diese Fixpunktiteration nach spätestens $\lceil \log n \rceil + 1$ Schritten ab. Also gilt PLUS $\in$ **IND**$[\log n]$. Für TIMES ist das Vorgehen ähnlich: Sei

$$\begin{aligned}\phi_\times(R,x,y,z) \equiv &(x = 0 \wedge z = 0) \vee \exists u(\textsc{Succ}(u,x) \wedge x = 0 \wedge z = y) \vee \\ &\exists \alpha,\beta,\gamma,\delta,z_1,z_2,z_3,z_4,z_{12},z_{34}(\phi_+(\alpha,\beta,x) \wedge \phi_+(\gamma,\delta,y) \wedge R(\alpha,\gamma,z_1) \wedge \\ &R(\alpha,\delta,z_2) \wedge R(\beta,\gamma,z_3) \wedge R(\beta,\delta,z_4) \wedge \phi_+(z_1,z_2,z_{12}) \wedge \phi_+(z_3,z_4,z_{34}) \wedge \\ &\phi_+(z_{12},z_{34},z))\end{aligned} \tag{2.22}$$

In der ersten Zeile dieser Formel wird wieder der Induktionsanfang ausgedrückt. Entweder man hat ein Tripel $(0,y,z)$ vorliegen oder ein Tripel der Form $(1,y,z)$. In diesen Fällen muss natürlich $z = 0$ oder $z = y$ sein. Im Induktionsschritt wollen wir wieder von allen Tripel (x,y,z) mit $x \leq k$ auf alle Tripel (x',y',z') mit $x' \leq 2k$ schließen. Dazu zerlegen wir jeweils x' und y' in eine Summe und wir überprüfen, ob $(\alpha+\beta) * (\gamma+\delta) = z'$ gilt. Durch Ausmultiplizieren erhält man eine Summe aus vier Summanden, in denen jeweils eine Multiplikation vorkommt mit Zahlengrößen, deren Multiplikationsergebnis bereits nach Induktionsvoraussetzung bekannt ist. Gesamt erhalten wir auch hier mit

$$\nu_\times(i,j,k) = \mathrm{LFP}(\phi_\times(R,x,y,z))(i,k,k) \tag{2.23}$$

einen induktiven Algorithmus für die Multiplikation, der nach $\lceil \log n \rceil + 1$ Schritten abbricht. □

2.4 Ein Normalformensatz für R-positive Formeln

In Satz 2.5 ging es darum, mehrfache geschachtelte Fixpunktoperatoren in einen einzelnen umzuschreiben. Im folgenden Normalformensatz wird gezeigt, dass man R-positive Formeln $\phi(R,x_1,\ldots,x_n)$ in eine Form umschreiben kann, in der die Relation R nur einmal nach einem Block von Quantoren vorkommt:

Satz 2.7. *Sei $\phi(R,x_1,\ldots,x_n)$ R-positiv. Dann gibt es Quantoren $Q_1,\ldots,Q_r$ und quantorenfreie Ausdrücke $M_1,\ldots,M_r$, in denen R nicht vorkommt, sodass*

$$\phi(R,x_1,\ldots,x_n) \equiv (Q_1 z_1 : M_1)(Q_2 z_2 : M_2)\ldots(Q_r z_r : M_r)(\exists x_1,\ldots,x_n : M_{r+1})R(x_1,\ldots,x_n) \tag{2.24}$$

wobei $(Q_i z_i : M_i)(\psi)$ für den Ausdruck $Q_i z_i (M \implies \psi)$ steht.

Beweis. Der Beweis verläuft induktiv nach dem Aufbau der Formel. Für den Induktionsanfang sei also $\phi_0(R,y_1,\ldots,y_n) \equiv R(y_1,\ldots,y_n)$. Wir setzen $M_1 \equiv (x_1 = y_1,\ldots,x_n = y_n)$ und erhalten

$$\phi_0 \equiv (\exists x_1,\ldots x_k : M_1)R(x_1,\ldots,x_n) \tag{2.25}$$

Ansonsten sei ϕ_0 eine Formel in der R nicht vorkommt, sowie keine Quantoren. Dann gilt

$$\phi_0 \equiv (\forall z : \neg\phi_0)(\exists x_1,\ldots,x_n : \textsc{false})R(x_1,\ldots,x_n) \tag{2.26}$$

weil $(\neg\phi_0 \implies \text{FALSE}) \equiv (\phi_0 \wedge \text{FALSE})$ und offensichtlich ist $(\phi_0 \wedge \text{FALSE}) \equiv \phi_0$. Im Induktionsschritt sind eigentlich nur die Fällle $(\phi \wedge \psi)$ bzw. $(\phi \vee \psi)$ interessant. Die Hinzunahme eines weiteren Quantoren Q kann direkt links an eine Formel, welche sich schon in der Normalform aus (2.24) befindet, gehängt werden und man erhält wieder eine Formel in der gewünschten Form. Wir betrachten nun den Fall $\nu = (\phi \vee \psi)$, wobei ψ und ν schon in Normalformen gegeben sind:

$$\phi \equiv (Q_1 y_1 : N_1) \dots (Q_r y_r : N_r)(\exists x_1, \dots, x_n : N_{r+1}) R(x_1, \dots, x_n)$$
$$\psi \equiv (Q'_1 z_1 : M_1) \dots (Q'_s z_s : M_s)(\exists x_1, \dots, x_n : M_{s+1}) R(x_1, \dots, x_n)$$

Ohne Beschränkung der Allgemeinheit können wir annehmen, dass die y von den z verschieden sind (ansonsten tausche man die betroffenen gebundenen Variablen aus). Wir setzen nun

$$N'_i \equiv N_i \vee b = 1$$
$$M'_i \equiv M_i \vee b = 0$$

und modifizieren die Quantorenblöcke von den beiden Formeln:

$$Q_\phi \equiv (Q_1 y_1 : N'_1) \dots (Q_r y_r : N'_r)$$
$$Q_\psi \equiv (Q'_1 z_1 : M'_1) \dots (Q'_s z_s : M'_s)$$

Dies ermöglicht uns, sobald beide Quantorenblöcke hintereinander in einer Formel stehen, sich jeweils nur einen der beiden Blöcke auszusuchen und diesen einzeln auszuwerten. Schließlich definieren wir

$$S \equiv (b = 0 \wedge N_{r+1}(\overline{u}/\overline{x})) \vee (b = 1 \wedge M_{s+1}(\overline{u}/\overline{x}))$$
$$T \equiv (u_1 = x_1 \wedge \dots \wedge u_n = x_n)$$

wobei die Notation $N(\overline{u}/\overline{x})$ die Formel N meint, in der das Variablentupel $\overline{x}$ durch das Tupel $\overline{u}$ ersetzt wurde. In S und in T kommen weder Quantoren noch R vor, da N_{r+1} und M_{s+1} nach Voraussetzung keines der beiden enthalten. Nun gilt

$$\nu \equiv (\exists b : [b = 0 \vee b = 1])(Q_\phi)(Q_\psi)(\exists u_1, \dots, u_n : S)(\exists x_1, \dots, x_n : T) R(x_1, \dots, x_n) \tag{2.27}$$

□

Als Beispiel betrachten wir nochmals die Formel aus (2.1):

$$\phi(R, x, y) \equiv x = y \vee \exists z (E(x, z) \wedge R(z, y))$$

Wir können mithilfe des eben bewiesenen Satzes eine Normalform finden. Zuerst setzen wir

$$\phi(R, x, y) \equiv (\forall z : \neg(x = y))(\exists z)(E(x, z) \wedge R(z, y))$$

Nun muss nur noch der letzte Block umgeschrieben werden. Analog wie im Beweis des Satzes erhalten wir

$$\begin{aligned}\phi(R, x, y) \equiv (\forall z : \neg(x = y))(\exists z)(\forall b : (b = 0 \ \vee \ b = 1))(\forall \alpha(\neg E(x, z) \ \vee \ b = 1)) \\ (\exists z_1, z_2 : (z_1 = \alpha \wedge z_2 = y) \vee b = 0)(\exists u_1, u_2 : (b = 0 \ \wedge \ u_1 = z_1 \wedge u_2 = z_2)) \\ (\exists x_1, x_2 : (u_1 = x_1 \ \wedge \ u_2 = x_2)) R(x_1, x_2)\end{aligned} \tag{2.28}$$

Diese Normalform von R-positiven Formeln, gibt uns eine praktische Beschreibung des kleinsten Fixpunktes. Wir denotieren mit Q_ϕ den Block der alle Quantoren enthält, also die komplette Formel bis auf das Relationensymbol $R(x_1, x_2)$. Wendet man die von ϕ induzierte Abbildung $\phi_\mathcal{A}$ n-Mal auf eine Relation R an, so bedeutet das im Wesentlichen, dass man den Block Q_ϕ n-Mal hintereinander schreibt und als Formel anwendet:

$$\phi^n_\mathcal{A}(R) = \{(x_1, x_2) \in |\mathcal{A}|^2 \mid \mathcal{A} \models (Q_\phi)^n R(x_1, x_2)\} \tag{2.29}$$

Insbesondere bedeutet das, da in unserem Beispiel $|\phi|(n) = n$, dass für $\mathcal{A}$ mit Mächtigkeit n gilt:

$$\mathcal{A} \models \mathrm{LFP}(\phi(R, x_1, x_2)) \iff \mathcal{A} \models (Q_\phi)^n \textsc{false}(x_1, x_2) \tag{2.30}$$

Bezeichnen wir nun allgemein $\mathbf{FO}[f(n)]$ als die Menge aller Strukturmengen, welche durch $f(n)$-malige Iteration von Quantorenblöcke beschrieben werden können (wobei n wieder die Mächtigkeit der Strukturgrundmenge bezeichnet), so sehen wir mithilfe der obigen Überlegungen, dass für beliebige Funktionen $f(n)$ (und über endliche Strukturen) gilt:

$$\mathbf{IND}[f(n)] \subseteq \mathbf{FO}[f(n)] \tag{2.31}$$

Literatur

[Imm99] Neil Immerman. *Descriptive complexity*. New York: Springer, 1999. ISBN: 978-0-387-98600-5.

[Lib04] Leonid Libkin. *Elements Of Finite Model Theory (Texts in Theoretical Computer Science. An Eatcs Series)*. SpringerVerlag, 2004. ISBN: 3540212027.