Vorlesung

Ausgewählte Kapitel der Logik: Lokalität

Nicole Schweikardt
HU Berlin

Kapitel 0: Einleitung und Grundbegriffe

Stichworte:

- Wozu Lokalitätsresultate? — algorithmische Metatheoreme; Nicht-Ausdrückbarkeits-Resultate

- Dies ist eine forschungsorientierte VL — ich präsentiere die "Highlights" der in den letzten Jahren neu erzielten Lokalitätsresultate und deren Anwendungen.
  Vorsicht: Der Begriff "Highlights" ist hier höchst subjektiv.

Aufbau der VL: siehe Webseite:

www2.informatik.hu-berlin.de/logik/lehre/SS18/AKL

Im "Logbuch" gibt's jeweils Literaturhinweise.

Grundbegriffe

Ich setze voraus, dass Sie mit den Notationen und Resultaten meiner VL "Logik in der Informatik" vertraut sind — das zugehörige VL-Skript finden Sie unter
www2.informatik.hu-berlin.de/logik/lehre/WS17-18/Logik

Vereinbarungen speziell für die VL "Ausgewählte Kapitel der Logik: Lokalität":

- logische Strukturen sind stets endlich, d.h. ihr Universum ist endlich
- Signaturen σ sind stets endlich und relational, d.h. sie bestehen aus einer endlichen Menge von Relationssymbolen
- Manchmal betrachten wir Konstantensymbole $c_1, c_2, c_3, \ldots$. Für $k \in \mathbb{N}$ setzen wir
  $\sigma_k := \sigma \cup \{c_i : i \in [k]\}$
  Zur Erinnerung: $[n] \stackrel{\text{Def}}{=} \{j \in \mathbb{N} : 1 \leq j \leq n\}$
- Für $m, n \in \mathbb{N}$ ist
  - $[m,n] := \{j \in \mathbb{N} : m \leq j \leq n\}$
  - $[m,n) := [m,n] \setminus \{n\}$
  - $(m,n] := [m,n] \setminus \{m\}$

Definition FO+MOD

Die Logik FO+MOD ist die Erweiterung der Logik erster Stufe FO, bei der auch Quantoren der Form $\exists^{i \bmod m} y$ für $m \in \mathbb{N}_{\geq 1}$, $i \in [0,m)$ und $y \in \mathrm{VAR}$ benutzt werden können. Solche Quantoren heißen modulo-Zählquantoren.

Die Menge FO+MOD$[\sigma]$ aller Formeln der Logik erster Stufe mit modulo-Zählquantoren über der Signatur σ ist rekursiv auf die gleiche Art definiert wie die Menge FO$[\sigma]$, mit der zusätzlichen rekursiven Regel:

- Ist $\varphi \in$ FO+MOD$[\sigma]$, $y \in \mathrm{VAR}$, $m \in \mathbb{N}_{\geq 1}$, $i \in [0,m)$, so ist auch $\exists^{i \bmod m} y\, \varphi \in$ FO+MOD$[\sigma]$

Die Semantik von FO+MOD$[\sigma]$ ist analog zur Semantik von FO$[\sigma]$ definiert, wobei für alle σ-Interpretationen $\mathcal{I} = (\mathcal{A}, \beta)$ gilt:

$$[\![\exists^{i \bmod m} y\, \varphi]\!]^{\mathcal{I}} := \begin{cases} 1 & \text{wenn } |\{a \in A : \mathcal{I}\tfrac{a}{y} \models \varphi\}| \equiv i \bmod m \\ 0 & \text{sonst} \end{cases}$$

Die freien Variablen sind definiert als

$$\mathrm{frei}(\exists^{i \bmod m} y\, \varphi) := \mathrm{frei}(\varphi) \setminus \{y\}$$

Beispiel:

Sei $\sigma := \{E\}$ mit $ar(E) = 2$.

$\varphi := \exists^{0 \bmod 2} x \; x = x$ ist ein FO+MOD$[\sigma]$-Satz, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt: $\mathcal{A} \models \varphi \iff |A|$ ist gerade.

$\psi := \exists^{0 \bmod 2} x \; \exists^{1 \bmod 2} y \; E(x,y)$ ist ein FO+MOD$[\sigma]$-Satz, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt:

$\mathcal{A} \models \psi \iff |E^{\mathcal{A}}|$ ist gerade.

Übungsaufgabe:

Sei σ eine beliebige Signatur, $k \in \mathbb{N}$ mit $k \geq 2$, $\varphi(x_1, \dots, x_k)$ eine FO+MOD$[\sigma]$-Formel mit k freien Variablen $x_1, \dots, x_k$, sei $m \in \mathbb{N}_{\geq 1}$ und $i \in [0, m)$. Konstruieren Sie einen FO+MOD$[\sigma]$-Satz ψ, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt:

$$\mathcal{A} \models \psi \iff \left|\{(a_1, \dots, a_k) \in A^k : \mathcal{A} \models \varphi[a_1, \dots, a_k]\}\right| \equiv i \bmod m.$$

Manchmal wollen wir an Stelle von modulo-Zählquantoren auch andere "Zählquantoren" verwenden — z.B. solche, die Aussagen der Art: "die Anzahl der Belegungen für x, die φ erfüllen ist eine Primzahl".

Um dies zu ermöglichen, führen wir folgende Notationen ein.

<u>Definition Zählterm:</u>

Ist φ eine Formel einer Logik L und $\bar{y} = (y_1, \dots, y_k)$ ein Tupel von k verschiedenen Variablen, für $k \in \mathbb{N}_{\geq 1}$, so ist

$$\# \bar{y} . \varphi$$

ein <u>Zählterm</u> (über L) der <u>Weite</u> k.

<u>Semantik:</u> Für jede Interpretation $\mathcal{I} = (\mathcal{A}, \beta)$ einer zu φ passenden Signatur ist

$$[\![\# \bar{y} . \varphi]\!]^{\mathcal{I}} := \left| \left\{ (a_1, \dots, a_k) \in A^k : \mathcal{I}\tfrac{a_1 \dots a_k}{y_1 \dots y_k} \models \varphi \right\} \right|$$

Die freien Variablen sind definiert als

$$\text{frei}(\# \bar{y} . \varphi) := \text{frei}(\varphi) \setminus \{y_1, \dots, y_k\}$$

Definition $FO(\mathcal{P})$

Sei $\mathcal{P} \subseteq \mathcal{P}(\mathbb{Z})$ (zur Erinnerung: $\mathcal{P}(M)$ bezeichnet die Potenzmenge einer Menge M)

Die Logik $FO(\mathcal{P})$ ist die Erweiterung von FO um "unäre Zählquantoren aus $\mathcal{P}$": Rekursiv ist die Menge $FO(\mathcal{P})[\sigma]$ auf die gleiche Art wie $FO[\sigma]$ definiert, mit der zusätzlichen rekursiven Regel

- Ist $\varphi \in FO(\mathcal{P})[\sigma]$, $y \in VAR$ und $P \in \mathcal{P}$, so ist auch $P(\#(y).\varphi) \in FO(\mathcal{P})[\sigma]$.

Semantik: Für $I = (\mathcal{A}, \beta)$ ist

$$[\![P(\#(y).\varphi)]\!]^I := \begin{cases} 1 & \text{wenn } [\![\#(y).\varphi]\!]^I \in P \\ 0 & \text{sonst} \end{cases}$$

Beispiel: Sei $\sigma := \{E\}$ mit $ar(E) = 2$.
Sei $\mathcal{P} := \{PRIM\}$ mit $PRIM := \{n \in \mathbb{N} : n \text{ ist eine Primzahl}\}$
$\varphi := PRIM(\#(y).\, y=y)$ ist ein $FO(\mathcal{P})[\sigma]$-Satz, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt: $\mathcal{A} \models \varphi \iff |A|$ ist eine Primzahl.

FRAGE: Gibt es auch einen $FO(\mathcal{P})[\sigma]$-Satz ψ, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt: $\mathcal{A} \models \psi \iff |E^{\mathcal{A}}|$ ist eine Primzahl?

Definition $\mathrm{FOC}(\mathbb{P})$

Sei $\mathbb{P} \subseteq \bigcup_{k \in \mathbb{N}_{\geq 1}} \mathcal{P}(\mathbb{Z}^k)$ (d.h. für jedes $P \in \mathbb{P}$ ex. eine Zahl $ar(P) \in \mathbb{N}_{\geq 1}$, s.d. $P \subseteq \mathbb{Z}^{ar(P)}$). Die Relationen $P \in \mathbb{P}$ werden auch numerische Prädikate genannt.

Die Logik $\mathrm{FOC}(\mathbb{P})$ ist die Erweiterung von FO um "verallgemeinerte Zählterme" und "numerische Prädikate aus $\mathbb{P}$". Rekursiv ist die Menge $\mathrm{FOC}(\mathbb{P})[\sigma]$ auf die gleiche Art wie $\mathrm{FO}[\sigma]$ definiert, mit den folgenden zusätzlichen Regeln:

- Jedes $i \in \mathbb{Z}$ ist ein verallgemeinerter Zählterm
- Für jede $\mathrm{FOC}(\mathbb{P})[\sigma]$-Formel φ, jedes $k \in \mathbb{N}_{\geq 1}$ und jedes Tupel $\bar{y} = (y_1, \dots, y_k)$ von k verschiedenen Variablen aus VAR ist $\#\bar{y}.\varphi$ ein verallgemeinerter Zählterm
- Sind t_1 und t_2 verallgemeinerte Zählterme, so ist auch $(t_1 + t_2)$ und $(t_1 \cdot t_2)$ ein verallgemeinerter Zählterm.
- Ist $P \in \mathbb{P}$, $k = ar(P)$ und sind $t_1, \dots, t_k$ verallgemeinerte Zählterme, so ist $P(t_1, \dots, t_k)$ eine $\mathrm{FOC}(\mathbb{P})[\sigma]$-Formel

<u>Semantik:</u> Für jede σ-Interpretation $\mathcal{I} = (\mathcal{A}, \beta)$ ist

- $[\![i]\!]^{\mathcal{I}} := i \in \mathbb{Z}$

- $[\![\#\overline{y}.\varphi]\!]^{\mathcal{I}} := \left| \left\{ (a_1,\dots,a_k) \in A^k : [\![\varphi]\!]^{\mathcal{I}\frac{a_1\dots a_k}{y_1\dots y_k}} = 1 \right\} \right|$

- $[\![(t_1 + t_2)]\!]^{\mathcal{I}} := [\![t_1]\!]^{\mathcal{I}} + [\![t_2]\!]^{\mathcal{I}} \in \mathbb{Z}$

  $[\![(t_1 \cdot t_2)]\!]^{\mathcal{I}} := [\![t_1]\!]^{\mathcal{I}} \cdot [\![t_2]\!]^{\mathcal{I}} \in \mathbb{Z}$

- $[\![P(t_1,\dots,t_k)]\!]^{\mathcal{I}} = \begin{cases} 1 & \text{falls } ([\![t_1]\!]^{\mathcal{I}},\dots,[\![t_k]\!]^{\mathcal{I}}) \in P \\ 0 & \text{sonst} \end{cases}$

<u>Notation:</u> Für verallgemeinerte Zählterme s und t schreiben wir $s-t$ um den verallgemeinerten Zählterm $(s + (-1 \cdot t))$ zu bezeichnen

<u>Beispiel:</u> Sei $\sigma := \{E\}$.

Für $\mathbb{P} = \{\text{PRIM}, \text{GLEICH}\}$ mit

$\text{PRIM} := \{n \in \mathbb{N} : n \text{ ist eine Primzahl}\}$ und

$\text{GLEICH} := \{(n,n) : n \in \mathbb{Z}\}$ ist

$$\varphi_1 := \text{PRIM}\big(\#(x).x{=}x + \#(x,y).E(x,y) \big)$$

ein $\text{FOC}(\mathbb{P})[\sigma]$-Satz, s.d. f.a. σ-Strukturen $\mathcal{A}$ gilt:

$\mathcal{A} \models \varphi_1 \iff |A| + |E^{\mathcal{A}}|$ ist eine Primzahl.

Der $\text{FOC}(\mathbb{P})[\sigma]$-Satz

$$\varphi_2 := \exists x\ \text{PRIM}\big(\#(y).\ \text{GLEICH}\big(\underbrace{\#(z).E(x,z)}_{\hat{=}\ \text{Aus-Grad}(x)}, \underbrace{\#(z).E(y,z)}_{\hat{=}\ \text{Aus-Grad}(y)} \big) \big)$$

wird von genau den σ-Strukturen $\mathcal{A}$ erfüllt, für die gilt: Es gibt eine Zahl d, so dass die Anzahl der Knoten vom Aus-Grad d in $\mathcal{A}$ eine Primzahl ist.

Weitere Grundbegriffe

- Der Gaifman-Graph $G_{\mathcal{A}}$ einer σ-Struktur $\mathcal{A}$ ist der ungerichtete Graph mit Knotenmenge A, s.d. f.a. $a, b \in A$ gilt:

  In $G_{\mathcal{A}}$ gibt es eine Kante zwischen a und b

  $:\iff$ $a \neq b$ und es gibt ein $R \in \sigma$ und ein Tupel $(t_1, \dots, t_{ar(R)}) \in R^{\mathcal{A}}$ s.d. $a, b \in \{t_1, \dots, t_{ar(R)}\}$.

- Der <u>Grad</u> von $\mathcal{A}$ ist definiert als der Grad von $G_{\mathcal{A}}$.
- $\mathcal{A}$ heißt <u>zusammenhängend</u> $:\iff$ $G_{\mathcal{A}}$ ist zusammenhängend

- Die Zusammenhangskomponenten von $\mathcal{A}$ sind definiert als die Zusammenhangskomponenten von $G_{\mathcal{A}}$

- $dist^{\mathcal{A}}(a,b) := dist^{G_{\mathcal{A}}}(a,b)$, wobei die Distanz $dist^{G}(a,b)$ von zwei Knoten in einem ungerichteten Graphen G definiert ist als die Länge (= Anzahl Kanten) eines kürzesten Weges zwischen a und b in G (bzw "∞", falls es in G keinen Weg zwischen a und b gibt).

- Für einen ungerichteten Graphen $G = (V, E)$ und eine Menge $W \subseteq V$ ist $G[W]$ definiert als der von W induzierte Teilgraph von G.
  D.h.: $G[W]$ hat Knotenmenge W, und für $u, v \in W$ gibt es in $G[W]$ eine Kante zwischen u und v genau dann, wenn es in G eine Kante zwischen u und v gibt.

- Analog ist für eine σ-Struktur $\mathcal{A}$ und eine Menge $B \subseteq A$ die von B <u>induzierte Substruktur</u> von $\mathcal{A}$ definiert als die σ-Struktur $\mathcal{A}[B]$ mit Universum B und
  $$R^{\mathcal{A}[B]} := R^{\mathcal{A}} \cap B^{ar(R)} \qquad \text{f.a. } R \in \sigma$$

<u>Nachbarschaften</u>

- Für $r \in \mathbb{N}$, $a \in A$ ist
  $$N_r^{\mathcal{A}}(a) := \{ b \in A : dist^{\mathcal{A}}(a, b) \leq r \}.$$

- Für $\bar{a} = (a_1, \ldots, a_k) \in A^k$ ist
  $$N_r^{\mathcal{A}}(\bar{a}) := \bigcup_{i=1}^{k} N_r^{\mathcal{A}}(a_i)$$

- $\mathcal{W}_r^{\mathcal{A}}(\bar{a}) := \mathcal{A}[N_r^{\mathcal{A}}(\bar{a})]$ ist eine σ-Struktur und wird „die r-Nachbarschaft von $\bar{a}$ in $\mathcal{A}$" genannt.

Typen

Sei $r \in \mathbb{N}$, $k \in \mathbb{N}_{\geq 1}$.

- Ein <u>r-Typ mit k Zentren über σ</u> ist von der Form $\tau = (\mathcal{B}, b_1, \ldots, b_k)$, wobei $\mathcal{B}$ eine σ-Struktur ist, $\bar{b} = (b_1, \ldots, b_k) \in B^k$ und $B = N_r^{\mathcal{B}}(\bar{b})$. Die Elemente $b_1, \ldots, b_k$ heißen "Zentren" von τ.

- Sei $\tau = (\mathcal{B}, b_1, \ldots, b_k)$ ein r-Typ mit k Zentren, sei $\mathcal{A}$ eine σ-Struktur und sei $\bar{a} = (a_1, \ldots, a_k) \in A^k$.
  Wir sagen: "$\bar{a}$ ist vom (bzw. realisiert den) r-Typ τ in $\mathcal{A}$",
  wenn gilt: $\left(\mathcal{N}_r^{\mathcal{A}}(\bar{a}), a_1, \ldots, a_k\right) \cong \tau$
  — d.h. es gibt einen Isomorphismus π von der σ-Struktur $\mathcal{N}_r^{\mathcal{A}}(\bar{a})$ zur σ-Struktur $\mathcal{B}$ mit $\pi(a_i) = b_i$ f.a. $i \in [k]$.

<u>Beachte:</u>
Wenn τ ein r-Typ mit k Zentren über σ ist, dann ist τ auch für jedes $R \geq r$ ein R-Typ mit k Zentren über σ.

<u>Lemma 0.1</u> (Beweis: Übung)

Sei σ eine Signatur und sei $r \in \mathbb{N}$.

<u>(a)</u> Es gibt eine $\mathrm{FO}[\sigma]$-Formel $\mathrm{dist}_{\leq r}(x,y)$, s.d. f.a. σ-Strukturen $\mathcal{A}$ und alle $a,b \in A$ gilt:

$$\mathcal{A} \models \mathrm{dist}_{\leq}[a,b] \iff \mathrm{dist}^{\mathcal{A}}(a,b) \leq r$$

<u>(b)</u> Sei $k \in \mathbb{N}_{\geq 1}$ und sei τ ein r-Typ mit k Zentren. Für jedes $R \in \mathbb{N}$ mit $R \geq r$ gibt es eine $\mathrm{FO}[\sigma]$-Formel

$$\mathrm{sph}_{\tau,R}(x_1,\dots,x_k)$$

s.d. f.a. σ-Strukturen $\mathcal{A}$ und alle $a_1,\dots,a_k \in A$ gilt:

$$\mathcal{A} \models \mathrm{sph}_{\tau,R}[a_1,\dots,a_k]$$

$$\iff \left(\mathcal{N}^{\mathcal{A}}_R(a_1,\dots,a_k),\ a_1,\dots,a_k\right) \cong \tau .$$

Lemma 0.2 (Beweis: Übung)

Für jedes $d \in \mathbb{N}$, jede σ-Struktur $\mathcal{A}$ von Grad $\leq d$, jedes $r \in \mathbb{N}$ und jedes $a \in A$ gilt:

$$|N_r^{\mathcal{A}}(a)| \leq 1 + d \cdot \sum_{i=0}^{r-1} (d-1)^i =: \nu_d(r).$$

Insbes. gilt:

$$d=0 \Rightarrow \nu_d(r) = 1$$
$$d=1 \Rightarrow \nu_d(r) \leq 2$$
$$d=2 \Rightarrow \nu_d(r) = 2r+1$$
$$d \geq 3 \Rightarrow \nu_d(r) \leq d^{r+1}$$

$$\leq (d-1)^r$$

Weitere einfache Beobachtungen zu Typen und Nachbarschaften

Notation: $\|\sigma\| := \sum_{R \in \sigma} ar(R)$

Lemma 0.3 (Beweis: Übung)

Sei $d \in \mathbb{N}$ mit $d \geq 2$. Sei $\mathcal{A}$ eine σ-Struktur vom Grad $\leq d$. Sei $r \in \mathbb{N}$, $k \in \mathbb{N}_{\geq 1}$, $\bar{a} = (a_1, \dots, a_k) \in A^k$. Dann gilt:

(a) $|N_r^{\mathcal{A}}(\bar{a})| \leq k \cdot \nu_d(r) \leq k \cdot d^{r+1}$.

(b) Bei Eingabe von $\mathcal{A}$ und $\bar{a}$ können wir den r-Typ $(\mathcal{N}_r^{\mathcal{A}}(\bar{a}), a_1, \dots, a_k)$ in Zeit

$$(k \cdot \nu_d(r))^{O(\|\sigma\|)} \leq (k \cdot d^{r+1})^{O(\|\sigma\|)}$$ berechnen

(c) $W_r^{\mathcal{A}}(a_1, a_2)$ ist genau dann zusammenhängend, wenn $\mathrm{dist}^{\mathcal{A}}(a_1, a_2) \leq 2r+1$ ist

(d) Wenn $W_r^{\mathcal{A}}(\bar{a})$ zusammenhängend ist, dann gilt für jedes $i \in [k]$:

$$N_r^{\mathcal{A}}(\bar{a}) \subseteq N^{\mathcal{A}}_{r+(k-1)(2r+1)}(a_i)$$

(e) Sei $\mathcal{B}$ eine σ-Struktur vom Grad $\leq d$ und sei $\bar{b} = (b_1, \ldots, b_k) \in B^k$.
Bei Eingabe von $\mathcal{A}, \bar{a}, \mathcal{B}, \bar{b}$ können wir in Zeit

$$\left(k \cdot v_d(r)\right)^{O(\|\sigma\| + k \cdot v_d(r))} \leq 2^{O(\|\sigma\| k^2 v_d(r)^2)} \leq 2^{O(\|\sigma\| k^2 d^{2r \cdots})}$$

testen, ob $\left(W_r^{\mathcal{A}}(\bar{a}), a_1, \ldots, a_k\right) \cong \left(W_r^{\mathcal{B}}(\bar{b}), b_1, \ldots, b_k\right)$ gilt.

<u>Lemma 0.4</u> (<u>Beweis</u>: Übung)

Es gibt einen Algorithmus, der bei Eingabe einer Signatur σ und Zahlen $d \geq 2$, $r \geq 0$, $k \geq 1$ eine Liste

$$\mathcal{L}_r^{\sigma,d}(k) = \tau_1, \dots, \tau_\ell$$

(für eine geeignete Zahl $\ell \geq 1$) von r-Typen mit k Zentren vom Grad $\leq d$ über σ berechnet, so dass für jeden r-Typen τ mit k Zentren vom Grad $\leq d$ über σ gilt:

es gibt genau ein $i \in [\ell]$ s.d. $\tau \cong \tau_i$.

Die Laufzeit des Algorithmus ist $2^{(k \cdot \nu_d(r))^{O(\|\sigma\|)}}$.

Außerdem können wir bei Eingabe von τ in Zeit $2^{(k \cdot \nu_d(r))^{O(\|\sigma\|)}}$ die Zahl $i \in [\ell]$ berechnen, für die $\tau \cong \tau_i$ gilt.

<u>Vereinbarung</u>:

Ab jetzt wird $\mathcal{L}_r^{\sigma,d}(k)$ die Liste bezeichnen, die vom Algorithmus aus Lemma 0.4 erzeugt wird.
Wir schreiben "$\tau \in \mathcal{L}_r^{\sigma,d}(k)$" um auszudrücken, dass $\tau \in \{\tau_1, \dots, \tau_\ell\}$ ist.