

Vorlesung

Ausgewählte Kapitel der Logik:
Lokalität

Nicole Schweikardt
HU Berlin

Kapitel 0: Einleitung und Grundbegriffe

Stichworte:

• Worum Lokalitätsresultate?
 $\swarrow$ algorithmische Metatheoreme
 $\searrow$ Nicht-Ausdrückbarkeits-Resultate

• Dies ist eine besuchungsorientierte VL — ich präsentiere die "Highlights" der in den letzten Jahren neu erhaltenen 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 $c_1, c_2, c_3, \dots$. 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 $F_0 + MOD$

Die Logik $F_0 + MOD$ ist die Erweiterung der Logik erster Stufe F_0 , bei der auch Quantoren der Form $\exists^{i \bmod m} y$ für $m \in \mathbb{N}_{\geq 1}$, $i \in [0, m)$ und $y \in VAR$ benutzt werden können. Solche Quantoren heißen modulo-Zählquantoren.

Die Menge $F_0 + MOD[\sigma]$ aller Formeln der Logik erster Stufe mit modulo-Zählquantoren über der Signatur σ ist rekursiv auf die gleiche Art definiert wie die Menge $F_0[\sigma]$, mit der zusätzlichen rekursiven Regel:

- Ist $\varphi \in F_0 + MOD[\sigma]$, $y \in VAR$, $m \in \mathbb{N}_{\geq 1}$, $i \in [0, m)$, so ist auch $\exists^{i \bmod m} y \varphi \in F_0 + MOD[\sigma]$

Die Semantik von $F_0 + MOD[\sigma]$ ist analog zur Semantik von $F_0[\sigma]$ definiert, wobei für alle σ -Interpretationen

$\mathcal{I} = (A, \beta)$ gilt:

$$\llbracket \exists^{i \bmod m} y \varphi \rrbracket^{\mathcal{I}} = \begin{cases} 1 & \text{wenn } |\{a \in A : \mathcal{I}_y^a \models \varphi\}| \equiv i \bmod m \\ 0 & \text{sonst} \end{cases}$$

Die freien Variablen sind definiert als

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

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 A gilt: $A \models \varphi \iff |A|$ 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 A gilt:

$A \models \psi \iff |E^A|$ 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 A gilt:

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

0.5

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.

Definition Zählterm:

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 Zählterm (über L) der Weite k .

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

$$\llbracket \# \bar{y}. \varphi \rrbracket^I := \left| \left\{ (a_1, \dots, a_k) \in A^k : \mathbb{I} \frac{a_1 \dots a_k}{y_1 \dots y_k} \models \varphi \right\} \right|$$

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

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

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

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

Sei $\mathcal{P} := \{\text{PRIM}\}$ mit $\text{PRIM} := \{n \in \mathbb{N} : n \text{ ist eine Primzahl}\}$

$\varphi := \text{PRIM}(\#(y). y=y)$ ist ein $FO(\mathcal{P})[\sigma]$ -Satz, s.d. f.a.

σ -Strukturen $\mathcal{U}$ gilt: $\mathcal{U} \models \varphi \Leftrightarrow |A|$ ist eine Primzahl.

FRAGE: Gibt es auch einen $FO(\mathcal{P})[\sigma]$ -Satz ψ , s.d. f.a.

σ -Strukturen $\mathcal{U}$ gilt: $\mathcal{U} \models \psi \Leftrightarrow |E^{\mathcal{U}}|$ ist eine Primzahl?

Definition $\text{FOC}(\mathcal{P})$

Sei $\mathcal{P} \subseteq \bigcup_{k \in \mathbb{N}_{\geq 1}} \mathcal{P}(\mathbb{Z}^k)$ (d.h. für jedes $P \in \mathcal{P}$

ex. die Zahl $\text{ar}(P) \in \mathbb{N}_{\geq 1}$, s.d. $P \subseteq \mathbb{Z}^{\text{ar}(P)}$). Die Relationen $P \in \mathcal{P}$ werden auch numerische Prädikate genannt.

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

- Jedes $i \in \mathbb{Z}$ ist ein verallgemeinerter Zählterm
- Für jede $\text{FOC}(\mathcal{P})[\sigma]$ -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 $\# \bar{y} \cdot \varphi$ 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 $P \in \mathcal{P}$, $k = \text{ar}(P)$ und sind $t_1, \dots, t_k$ verallgemeinerte Zählterme, so ist $P(t_1, \dots, t_k)$ eine $\text{FOC}(\mathcal{P})[\sigma]$ -Formel.

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

$$\bullet \llbracket i \rrbracket^I := i \in \mathbb{Z}$$

$$\bullet \llbracket \# \bar{y} \cdot \varphi \rrbracket^I := \left| \{ (a_1, \dots, a_k) \in A^k : \llbracket \varphi \rrbracket^I \frac{a_1 \dots a_k}{y_1 \dots y_k} = 1 \} \right|$$

$$\bullet \llbracket (t_1 + t_2) \rrbracket^I := \llbracket t_1 \rrbracket^I + \llbracket t_2 \rrbracket^I \in \mathbb{Z}$$

$$\llbracket (t_1 \cdot t_2) \rrbracket^I := \llbracket t_1 \rrbracket^I \cdot \llbracket t_2 \rrbracket^I \in \mathbb{Z}$$

$$\bullet \llbracket P(t_1, \dots, t_k) \rrbracket^I = \begin{cases} 1 & \text{falls } (\llbracket t_1 \rrbracket^I, \dots, \llbracket t_k \rrbracket^I) \in P \\ 0 & \text{sonst} \end{cases}$$

Notation: Für verallgemeinerte Zählerterme s und t schreiben wir $s-t$ um den verallgemeinerten Zählerterm $(s + (-1 \cdot t))$ zu bezeichnen

Beispiel: Sei $\sigma = \{E\}$.

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

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

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

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

ein $\text{FOC}(\mathcal{P})[\sigma]$ -Satz, s.d. f.a. σ -Strukturen $\mathcal{A}$ gilt:
 $\mathcal{A} \models \varphi_1 \iff |\mathcal{A}| + |E^{\mathcal{A}}| \text{ ist eine Primzahl.}$

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

$$\varphi_2 := \exists x \text{ PRIM} \left(\#(y). \underbrace{\text{GLEICH}(\#(z). E(x, z))}_{\equiv \text{Ans-Grad}(x)}, \underbrace{\#(z). E(y, z)}_{\equiv \text{Ans-Grad}(y)} \right)$$

wird von genau den σ -Strukturen $\mathcal{A}$ erfüllt, für die gilt:

Es gibt eine Zahl d , so dass die Anzahl der Knoten vom Ans-Grad d in $\mathcal{A}$ eine Primzahl ist.

Weitere Grundbegriffe

- Der Gaufman-Graph G_U einer σ -Struktur U ist der ungerichtete Graph mit Knotenmenge A , s.d. f.a. $a, b \in A$ gilt:

In G_U gibt es eine Kante zwischen a und b $\Leftrightarrow a \neq b$ und es gibt ein $R \in \sigma$ und ein Tupel $(t_1, \dots, t_{\text{ar}(R)}) \in R^U$ s.d. $a, b \in \{t_1, \dots, t_{\text{ar}(R)}\}$.

- Der Grad von U ist definiert als der Grad von G_U .

- U heißt zusammenhängend $\Leftrightarrow G_U$ ist zusammenhängend

- Die Zusammenhangskomponenten von U sind definiert als die Zusammenhangskomponenten von G_U .

- $\text{dist}^U(a, b) := \text{dist}^{G_U}(a, b)$, wobei die Distanz $\text{dist}^G(a, b)$ 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 induzierte Substruktur von $\mathcal{A}$ definiert als die σ -Struktur $\mathcal{A}[B]$ mit Universum B und

$$R^{\mathcal{A}[B]} := R^{\mathcal{A}} \cap B^{\text{ar}(R)} \quad \text{f.ä. } R \in \sigma$$

Nachbarschaften

- Für $r \in \mathbb{N}$, $a \in A$ ist

$$N_r^{\mathcal{A}}(a) := \{b \in A : \text{dist}^{\mathcal{A}}(a,b) \leq r\}.$$
- Für $\vec{a} = (a_1, \dots, a_k) \in A^k$ ist

$$N_r^{\mathcal{A}}(\vec{a}) := \bigcup_{i=1}^k N_r^{\mathcal{A}}(a_i)$$
- $W_r^{\mathcal{A}}(\vec{a}) := \mathcal{A}[N_r^{\mathcal{A}}(\vec{a})]$ ist eine σ -Struktur und wird "die r -Nachbarschaft von $\vec{a}$ in $\mathcal{A}$ " genannt.

Typen

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

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

- Sei $\tau = (B, b_1, \dots, b_k)$ ein r -Typ mit k Zentren, sei $\mathcal{A}$ eine σ -Struktur und sei $\bar{a} = (a_1, \dots, a_k) \in \mathcal{A}^k$.
Wir sagen: " $\bar{a}$ ist von (bzw. realisiert den) r -Typ τ in $\mathcal{A}$ ",

wenn gilt: $(N_r^{\mathcal{A}}(\bar{a}), a_1, \dots, a_k) \cong \tau$

— d.h. es gibt einen Isomorphismus π von der σ -Struktur $N_r^{\mathcal{A}}(\bar{a})$ zur σ -Struktur B mit $\pi(a_i) = b_i$ f.a. $i \in [k]$.

Beachte:

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 .

Lemma 0.1 (Beweis: Übung)

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

(a) Es gibt eine $\mathcal{F}_0[\sigma]$ -Formel $\text{dist}_{\leq r}(x, y)$, s.d.
f.a. σ -Strukturen $\mathcal{A}$ und alle $a, b \in A$ gilt:

$$\mathcal{A} \models \text{dist}_{\leq r}[a, b] \quad (\Leftrightarrow) \quad \text{dist}^{\mathcal{A}}(a, b) \leq r$$

(b) 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

$\mathcal{F}_0[\sigma]$ -Formel $\text{sph}_{\tau, R}(x_1, \dots, x_k)$

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

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

$$(\Rightarrow) \left(\bigvee_R^{\mathcal{A}} (a_1, \dots, a_k), a_1, \dots, a_k \right) \cong \tau.$$

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:

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

Insb. gilt: $d=0 \Rightarrow v_d(r) = 1$

$$d=1 \Rightarrow v_d(r) \leq 2$$

$$d=2 \Rightarrow v_d(r) = 2r+1$$

$$d \geq 3 \Rightarrow v_d(r) \leq d^{r+1}$$

$$\stackrel{\leq}{(d-1)^r}$$

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 von 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:

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

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

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

~~(c) $W_r^u(a_1, a_2)$ ist genau dann zusammenhängend, wenn $\text{dist}^u(a_1, a_2) \leq 2r+1$ ist~~

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

$$N_r^u(\bar{a}) \subseteq N_{r+(k-1)(2r+1)}^u(a_i)$$

(e) Sei B eine σ -Struktur von $\text{Grad} \leq d$ und sei $\bar{b} = (b_1, \dots, b_k) \in B^k$.

Bei Eingabe von $A, \bar{a}, B, \bar{b}$ können wir in Zeit $O((k \cdot v_d(r))^{O(\|K\| + k \cdot v_d(r))}) \leq 2^{O(\|K\| k^2 v_d(r)^2)} \leq 2^{O(\|K\| k^2 d^{2r})}$

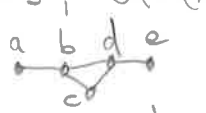
testen, ob $(W_r^u(\bar{a}), a_1, \dots, a_k) \cong (W_r^B(\bar{b}), b_1, \dots, b_k)$ gilt.

(c)(i) $W_r^u(a_1, a_2)$ zusammenhängend $\Rightarrow \text{dist}^u(a_1, a_2) \leq 2r+1$

(ii) Falls ex $E \in \sigma$ mit $\text{ar}(E)=2$ und $E^u \subseteq \{(a_1, a_2) \in A^2 : \{a_1, a_2\} \text{ ist eine Kante im Gaifman-Graph } G_A\}$, so gilt:

$$W_r^u(a_1, a_2) \text{ zusammenhängend} \Leftrightarrow \text{dist}^u(a_1, a_2) \leq 2r+1$$

Gegenbeispiel zu " $\Leftarrow$ " bei c)(i) [Charlotte Lenz, Masterarbeit, 2025]:

$\sigma = \{R\}$ mit $\text{ar}(R)=3$; $\mathcal{A} = (A, R^A)$ mit $A = \{a, b, c, d, e\}$, $R^A = \{(a, b, c), (b, c, d), (d, e, c)\}$.
Dann ist G_A : , $\text{dist}^u(a, e) = 3 = 2 \cdot 1 + 1$, aber $N_1^u(a, e) = \{a, b, d, e\}$ und $N_1^u(a, e) = B = (B, R^B)$ mit $B = \{a, b, d, e\}$, $R^B = \{(a, b, d), (d, e, e)\}$ und G_B : , Also ist $W_1^u(a, e)$ nicht zusammenhängend.

Lemma 0.4 (Beweis: 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 $2^{(k \cdot \text{vd}(r))^{O(\|\sigma\|)}}$.

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

Vereinbarung:

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.