Kapitel 2: Logik zweiter Stufe (SO)

2.1 Syntax und Semantik der Logik zweiter Stufe

Idee: Für jede Stelligkeit $k \geq 1$ gibt es abzählbar viele Relationsvariablen dieser Stelligkeit: $Var_1^k, Var_2^k, Var_3^k, \dots$

Definition 2.1 (SO: Syntax)

Sei $\sigma = \{R_1, \dots, R_\ell, c_1, \dots, c_m\}$ eine (endliche, funktionenfreie) Signatur.

(a) $Var_2 := \{ Var_i^k : i, k \in \mathbb{N}_{\geq 1} \}$ ist die Menge aller Variablen zweiter Stufe (oder: Relationsvariablen).
Die Relationsvariable Var_i^k hat die Stelligkeit $ar(Var_i^k) = k$.

(a') $Var_1 := Var = \{ var_i : i \in \mathbb{N}_{\geq 1} \}$ ist die Menge aller Variablen erster Stufe (oder: Individuenvariablen)

(b) Die Formelmenge $SO(\sigma)$ ist rekursiv wie folgt definiert:

atomare Formeln

(A1) $R(v_1, \dots, v_k)$ gehört zu $SO[\sigma]$, für alle Relationssymbole $R \in \sigma$, $k := ar(R)$, $v_1, \dots, v_k \in Var_1 \cup \{ c \in \sigma : c \text{ ist ein Konstantensymbol} \}$

atomare Formeln

(A2) $v = v'$ gehört zu $SO[\sigma]$, für alle $v, v' \in Var_1 \cup \{c \in \sigma : c \text{ ist Konstantensymbol}\}$

(A3) $X(v_1, \dots, v_k)$ gehört zu $SO[\sigma]$, für alle $X \in Var_2$, $k = ar(X)$, $v_1, \dots, v_k \in Var_1 \cup \{c \in \sigma : c \text{ ist Konstantensymbol}\}$

(BC) Sind $\varphi, \varphi_1, \varphi_2$ Formeln in $SO[\sigma]$, so gehören auch die folgenden Formeln zu $SO[\sigma]$:

- $\neg\varphi$
- $(\varphi_1 \vee \varphi_2)$
- $(\varphi_1 \wedge \varphi_2)$
- $(\varphi_1 \to \varphi_2)$
- $(\varphi_1 \leftrightarrow \varphi_2)$

(Q1) Ist φ eine Formel in $SO[\sigma]$ und $x \in Var_1$, so gehören auch folgende Formeln zu $SO[\sigma]$:

- $\exists x \varphi$
- $\forall x \varphi$

(Q2) Ist φ eine Formel in $SO[\sigma]$ und $X \in Var_2$, so gehören auch folgende Formeln zu $SO[\sigma]$:

- $\exists X \varphi$
- $\forall X \varphi$

(c) Die mit (A1), (A2) und (A3) gebildeten Formeln heißen **atomare σ-Formeln**

Definition 2.2

(a) Für $\varphi \in SO(\sigma)$ bezeichnet qr(φ) den Quantorenrang (bzw die Quantorentiefe von φ, d.h. die maximale Anzahl ineinander geschachtelter Quantoren in φ und frei(φ) die Menge aller Individuen- und Relationsvariablen, die frei in φ vorkommen. D.h.:

- $\text{frei}(R(v_1,\dots,v_k)) = \{v_1,\dots,v_k\} \cap Var_1$, für $R \in \sigma$
  $qr(R(v_1,\dots,v_k)) = 0$
- $\text{frei}(v = v') = \{v, v'\} \cap Var_1$
  $qr(v=v') = 0$
- $\text{frei}(X(v_1,\dots,v_k)) = \{X\} \cup (\{v_1,\dots,v_k\} \cap Var_1)$, für $X \in Var_2$
  $qr(X(v_1,\dots,v_k)) = 0$
- $\text{frei}(\neg\psi) = \text{frei}(\psi)$
  $qr(\neg\psi) = qr(\psi)$
- $\text{frei}((\psi_1 * \psi_2)) = \text{frei}(\psi_1) \cup \text{frei}(\psi_2)$, für $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
  $qr((\psi_1 * \psi_2)) = \max\{qr(\psi_1), qr(\psi_2)\}$
- $\text{frei}(Qx\,\varphi) = \text{frei}(\varphi) \setminus \{x\}$ für $Q \in \{\exists, \forall\}$ und $x \in Var_1 \cup Var_2$
  $qr(Qx\varphi) = 1 + qr(\varphi)$

Wir schreiben oft $\varphi(x_1,\dots,x_s, X_1,\dots,X_t)$ um anzudeuten, dass $\text{frei}(\varphi) = \{x_1,\dots,x_s, X_1,\dots,X_t\}$ ist.

(b) Eine $SO[\sigma]$-Formel φ heißt <u>Satz</u>, falls $\text{frei}(\varphi) = \emptyset$ ist.

Beispiel: für $\varphi = \exists X \forall Y (\exists z \exists Z\, Z(z) \vee \forall u (Y(u) \vee u = z))$

gilt $qr(\varphi) = 4$

Definition 2.3 (SO: Semantik)

Die Semantik von SO[σ] ist auf die offensichtliche Weise definiert, (als Erweiterung der Semantik von FO[σ].). D.h:

(A3): Ist φ eine SO[σ]-Formel der Form $X(v_1 \dots v_k)$ mit $X \in Var_2$, $k = ar(X)$, $v_1 \dots v_k \in Var_1$, ist $\mathfrak{A}$ eine σ-Struktur und sind $X^{\mathfrak{A}} \subseteq A^k$ und $a_1, \dots, a_k \in A$, so gilt:

$$(\mathfrak{A}, X^{\mathfrak{A}}, a_1, \dots, a_k) \models \varphi \iff (a_1, \dots, a_k) \in X^{\mathfrak{A}}$$

(Q2): Ist φ eine SO[σ]-Formel der Form $\exists X \psi$ mit $frei(\psi) \subseteq \{X, X_1, \dots, X_t, v_1, \dots, v_s\}$, wobei $X \in Var_2$), ist $\mathfrak{A}$ eine σ-Struktur und sind $X_1^{\mathfrak{A}} \subseteq A^{ar(X_1)}, \dots, X_t^{\mathfrak{A}} \subseteq A^{ar(X_t)}$, $a_1, \dots, a_s \in A$, so gilt:

$$(\mathfrak{A}, X_1^{\mathfrak{A}}, \dots, X_t^{\mathfrak{A}}, a_1, \dots, a_s) \models \exists X \psi \iff$$

es gibt (mind.) eine Relation $X^{\mathfrak{A}} \subseteq A^{ar(X)}$ s.d. $(\mathfrak{A}, X^{\mathfrak{A}}, X_1^{\mathfrak{A}}, \dots, X_t^{\mathfrak{A}}, a_1, \dots, a_s) \models \psi$.

Analog: Semantik von "$\forall X \psi$" definiert via:
$(\mathfrak{A}, X_1^{\mathfrak{A}}, \dots, X_t^{\mathfrak{A}}, a_1, \dots, a_s) \models \forall X \psi \iff$
f.a. $X^{\mathfrak{A}} \subseteq A^{ar(X)}$ gilt: $(\mathfrak{A}, X^{\mathfrak{A}}, X_1^{\mathfrak{A}}, \dots, X_t^{\mathfrak{A}}, a_1, \dots, a_s) \models \psi$.

Beispiele 2.4

Sei $\sigma := \{E\}$ die Signatur für Graphen, d.h.: E ist ein 2-stelliges Relationssymbol.

(a) Ein $SO[\sigma]$-Satz, der genau dann für einen Graphen $G = (V, E)$ gilt, wenn G 3-färbbar ist:

$$\Phi_{3\text{-col}} := \exists R \exists G \exists B \Big(\forall x \, (R(x) \vee G(x) \vee B(x)) \wedge \forall x \forall y \, \big(E(x,y) \rightarrow \neg\big((R(x) \wedge R(y)) \vee (G(x) \wedge G(y)) \vee (B(x) \wedge B(y))\big)\big)\Big)$$

(b) Ein $SO[\sigma]$-Satz, der besagt, dass ein Graph symmetrisch und nicht zusammenhängend ist:

$$\Phi_{\text{non-conn}} := \Big(\exists X \big(\exists x \, X(x) \wedge \exists y \, \neg X(y) \wedge \neg \exists u \exists v \, (E(u,v) \wedge X(u) \wedge \neg X(v))\big) \wedge \forall u \forall v \, (E(u,v) \leftrightarrow E(v,u)) \Big)$$

(c) Eine $SO[\sigma]$-Formel $\Phi_{\text{reach}}(x,y)$, die besagt, dass es einen Weg von Knoten x zu Knoten y gibt:

$$\Phi_{\text{reach}}(x,y) := \forall X \Big(\big(X(x) \wedge \forall z \forall z' \, ((E(z,z') \wedge X(z)) \rightarrow X(z'))\big) \rightarrow X(y) \Big)$$

(d) Ein $SO[\sigma]$-Satz, der besagt, dass ein Graph $G=(V,E)$ einen <u>Hamiltonkreis</u> enthält, dh es gibt eine Folge $v_0, \dots, v_n$ von Knoten, s.d. $V=\{v_0,\dots,v_n\}$ und $(v_i, v_{i+1}) \in E$ f.a. $i<n$ und $(v_n, v_0) \in E$:

$$\Phi_{Ham} := \exists R_< \, \exists R_{succ} \, \exists z_0 \, \exists z_{max} \Big(E(z_{max}, z_0) \wedge \forall x \forall y \big(R_{succ}(x,y) \rightarrow E(x,y) \big) \wedge \underbrace{\varphi_{<,succ,0}(R_<, R_{succ}, z_0)}_{\text{Die Formel aus dem Beweis des Satzes von Trakhtenbrot, die besagt, dass } R_< \text{ eine diskrete lineare Ordnung mit kleinstem Element } z_0 \text{ und Nachfolger-Relation } R_{succ} \text{ ist}} \wedge \forall x \underbrace{\big(R_<(x, z_{max}) \vee x = z_{max} \big)}_{z_{max} \text{ ist das größte Element bzgl } R_<} \Big)$$

Definition 2.5

(a) Die <u>monadische Logik zweiter Stufe</u>, $MSO[\sigma]$, ist die Klasse aller $SO[\sigma]$-Formeln φ, s.d. alle in φ vorkommenden Relationsvariablen die Stelligkeit 1 besitzen (solche Relationsvariablen werden auch <u>Mengenvariablen</u> genannt).

(b) Die <u>existentielle Logik zweiter Stufe</u>, $ESO[\sigma]$ (auch: $\exists SO[\sigma]$, $\Sigma_1^1[\sigma]$) ist die Klasse aller $SO[\sigma]$-Formeln der Form

$\exists X_1 \cdots \exists X_d \ \varphi$, wobei

$d \in \mathbb{N}$, $X_1, \dots, X_d$ sind Relationsvariablen und
$\varphi \in \mathrm{FO}[\sigma \cup \mathrm{Var}_2]$.

(c) Die <u>monadische existentielle Logik zweiter Stufe</u>,
$\mathrm{EMSO}[\sigma]$ (auch: $\exists\mathrm{MSO}[\sigma]$, $\mathrm{mon}\Sigma_1^1[\sigma]$, $\mathrm{monNP}[\sigma]$, monadic $\Sigma_1^1[\sigma]$, monadicNP$[\sigma]$)

ist die Klasse aller $\mathrm{MSO}[\sigma]$-Formeln, die zugleich auch $\mathrm{ESO}[\sigma]$-Formeln sind, d.h. aller $\mathrm{SO}[\sigma]$-Formeln der Form $\exists X_1 \cdots \exists X_d \ \varphi$, wobei
$d \in \mathbb{N}$, $X_1, \dots, X_d$ sind Mengenvariablen und
$\varphi \in \mathrm{FO}[\sigma \cup \mathrm{Var}_2]$.

<u>Beispiele 2.6</u>

Betrachte die Formeln aus Bsp 2.4:

- $\Phi_{3\text{-col}}$ gehört zu $\mathrm{MSO}[\sigma]$, $\mathrm{ESO}[\sigma]$, $\mathrm{EMSO}[\sigma]$
- $\Phi_{\text{non-conn}}$ gehört zu " " "
- $\Phi_{\text{reach}}(x,y)$ gehört zu $\mathrm{MSO}[\sigma]$, aber <u>nicht</u> zu $\mathrm{ESO}[\sigma]$ und <u>nicht</u> zu $\mathrm{EMSO}[\sigma]$
- Φ_{Ham} gehört zu $\mathrm{ESO}[\sigma]$, aber <u>nicht</u> zu $\mathrm{MSO}[\sigma]$ und <u>nicht</u> zu $\mathrm{EMSO}[\sigma]$.

2.2 MSO und der Satz von Büchi

Der Satz von Büchi besagt, dass die regulären Sprachen genau diejenigen Sprachen sind, die in MSO (bzw in EMSO) beschrieben werden können.

Sei $\Sigma = \{a_1, \dots, a_\ell\}$ ein endliches (nicht-leeres) Alphabet. Nicht-leere Worte $w \in \Sigma^+$ repräsentieren wir durch Strukturen wie folgt (siehe das Kapitel über den Satz von McNaughton und Papert in der Vorlesung "Logik in der Informatik – Einführung in die formale Logik"):

Definition 2.7

(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) Einem endlichen Wort $w = w_1 \cdots w_n \in \Sigma^+$ der Länge $n \geq 1$ (mit $w_i \in \Sigma$ f.a. $i \in \{1, \dots, n\}$) ordnen wir die folgende σ_Σ-Struktur $\mathfrak{A}_w = (A_w, \leq^{\mathfrak{A}_w}, P_{a_1}^{\mathfrak{A}_w}, \dots, P_{a_\ell}^{\mathfrak{A}_w})$ zu:

- $A_w = \{1, \dots, n\}$ ist die Menge aller Positionen in w
- $\leq^{\mathfrak{A}_w}$ ist die natürliche lineare Ordnung auf A_w
- Für jedes $a \in \Sigma$ ist $P_a^{\mathfrak{A}_w} := \{ i \in A_w : w_i = a \}$ die Menge aller Positionen in w, an denen der Buchstabe a steht

<u>Beispiel 2.8</u>

$\Sigma = \{a, b\}$, $w = aaab$ $\Rightarrow$

$\mathfrak{A}_w = (A_w, \leq^{\mathfrak{A}_w}, P_a^{\mathfrak{A}_w}, P_b^{\mathfrak{A}_w})$ mit

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

<u>Definition 2.9</u>

(a) Sei $L \subseteq \Sigma^*$ und sei φ ein $MSO[\sigma_\Sigma]$-Satz.
Wir sagen: φ <u>beschreibt</u> L, falls für jedes nicht-leere Wort $w \in \Sigma^+$ gilt:

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

(b) $L \subseteq \Sigma^*$ heißt <u>MSO-definierbar</u> (bzw EMSO-definierbar), falls es einen $MSO[\sigma_\Sigma]$-Satz (bzw $EMSO[\sigma_\Sigma]$-Satz) gibt, der φ beschreibt.

Beispiel 2.10

Sei $\Sigma = \{a,b\}$. Die Sprache

$$L_{even} := \{ w \in \{a,b\}^* : |w| \text{ ist gerade} \}$$

wird durch folgenden EMSO$[\sigma_\Sigma]$-Satz φ_{even} beschrieben:

$$\varphi_{even} := \exists X \Big(\forall x \, (\min(x) \to \neg X(x)) \wedge \forall x \, (\max(x) \to X(x)) \wedge \forall x \forall y \, \big(\mathrm{succ}(x,y) \to (X(x) \leftrightarrow \neg X(y))\big)\Big)$$

mit

$$\begin{cases} \min(x) := \forall z \; x \le z \\ \max(x) := \forall z \; z \le x \\ \mathrm{succ}(x,y) := x \le y \wedge \neg x = y \wedge \forall z \, (z \le x \vee y \le z) \end{cases}$$

diese Abkürzungen werden wir oft später immer wieder nutzen.

(Idee: "X enthält genau die "geraden" Positionen eines Worts, in dem die Formel ausgewertet wird, und die letzte Position des Worts gehört zu X").

Theorem 2.11 (Der Satz von Büchi)

Sei Σ ein endliches (nicht-leeres) Alphabet und sei $L \subseteq \Sigma^*$. Die folgenden Aussagen sind äquivalent:

(a) L ist regulär (dh wird von einem deterministischen endlichen Automaten erkannt)

(b) L ist EMSO-definierbar

(c) L ist MSO-definierbar