Kapitel 2:
Logik zweiter Stufe und die Sätze von Büchi und Fagin

Notation:

- Wir nutzen an Stelle der kalligraphischen Buchstaben $\mathcal{A}, \mathcal{B}, \ldots$ auch Frakturbuchstaben $\mathfrak{A}, \mathfrak{B}, \ldots$ um σ-Strukturen zu bezeichnen.
  Deren Universen bezeichnen wir weiterhin mit den entsprechenden lateinischen Buchstaben $A, B, \ldots$
- Wir schreiben auch $\mathfrak{A}_w$, um die Wortstruktur $\mathcal{W}_w$ zu bezeichnen, die ein nicht-leeres Wort $w \in \Sigma^*$ repräsentiert.

Kapitel 2: Logik zweiter Stufe (SO)

2.1 Syntax und Semantik der Logik zweiter Stufe

<u>Idee:</u> Für jede Stelligkeit $k \geq 1$ gibt es abzählbar viele Relationsvariablen dieser Stelligkeit: $\mathrm{Var}_1^k, \mathrm{Var}_2^k, \mathrm{Var}_3^k, \ldots$

<u>Definition 2.1</u> (SO: Syntax)

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

(a) $\mathrm{Var}_2 := \{\mathrm{Var}_i^k : i, k \in \mathbb{N}_{\geq 1}\}$ ist die Menge aller <u>Variablen zweiter Stufe</u> (oder: <u>Relationsvariablen</u>).
Die Relationsvariable Var_i^k hat die Stelligkeit $ar(\mathrm{Var}_i^k) = k$.

$\mathrm{Var}_1 := \mathrm{Var} = \{\mathrm{var}_i : i \in \mathbb{N}_{\geq 1}\}$ ist die Menge aller <u>Variablen erster Stufe</u> (oder: <u>Individuenvariablen</u>)

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

atomare Formeln

(A1) $R(v_1, \ldots, v_k)$ gehört zu $SO[\sigma]$, für alle Relationssymbole $R \in \sigma$, $k := ar(R)$, $v_1, \ldots, v_k \in \mathrm{Var}_1 \cup \{c \in \sigma : c \text{ ist ein Konstantensymbol}\}$

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 ψ, ψ_1, ψ_2 Formeln in $SO[\sigma]$, so gehören auch die folgenden Formeln zu $SO[\sigma]$:

- $\neg \psi$
- $(\psi_1 \vee \psi_2)$
- $(\psi_1 \wedge \psi_2)$
- $(\psi_1 \rightarrow \psi_2)$
- $(\psi_1 \leftrightarrow \psi_2)$

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

- $\exists x \, \psi$
- $\forall x \, \psi$

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

- $\exists X \, \psi$
- $\forall X \, \psi$

(c) Die mit (A1), (A2) und (A3) gebildeten Formeln heißen <u>atomare σ-Formeln</u>

Definition 2.2

(a) Für $\varphi \in SO[\sigma]$ bezeichnet $qr(\varphi)$ 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 $X \in Var_2$
  $qr(X(v_1, \dots, v_k)) = 0$
- $\text{frei}(\neg\psi) = \text{frei}(\psi)$
  $qr(\neg\psi) = qr(\psi)$
- $\text{frei}((\varphi_1 * \varphi_2)) = \text{frei}(\varphi_1) \cup \text{frei}(\varphi_2)$, für $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
  $qr((\varphi_1 * \varphi_2)) = \max\{qr(\varphi_1), qr(\varphi_2)\}$
- $\text{frei}(Qx\varphi) = \text{frei}(\varphi) \setminus \{x\}$ 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.

<u>Beispiel</u>: 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 $X \in \mathrm{Var}_2$, $k = ar(X)$, $v_1, \dots, v_k \in \mathrm{Var}_1$, 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 $\text{frei}(\psi) \subseteq \{X, X_1, \dots, X_t, v_1, \dots, v_s\}$, wobei $X \in \mathrm{Var}_2$, 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:

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

<u>f.a.</u> $X^{\mathfrak{A}} \subseteq A^{ar(X)}$ 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:

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

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

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

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

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

(d) Ein $SO[\sigma]$-Satz, der besagt, dass ein Graph $G=(V,E)$ einen Hamiltonkreis enthält, d.h. 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 $(v_n, v_0) \in E$:

$$\Phi_{Ham} := \exists R_< \exists R_{succ} \exists z_0 \exists z_{max} \Big(E(z_{max}, z_0) \wedge \forall x \forall y \big(R_{succ}(x,y) \to E(x,y)\big) \wedge \underbrace{\varphi_{<,succ,0}(R_<, R_{succ}, z_0)} \wedge \forall x \underbrace{\big(R_<(x, z_{max}) \vee x = z_{max}\big)}$$

Die Formel aus dem Beweis des Satzes von Trakhtenbrot, die besagt, dass $R_<$ eine diskrete lineare Ordnung mit kleinstem Element z_0 und Nachfolger-Relation R_{succ} ist

z_{max} ist das größte Element bzgl. $R_<$

Definition 2.5

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

(b) Die existentielle Logik zweiter Stufe, $ESO[\sigma]$ (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: $\exists\mathrm{MSO}[\sigma]$, $\mathrm{mon}\,\Sigma_1^1[\sigma]$, $\mathrm{mon}\,\mathrm{NP}[\sigma]$
monadic $\Sigma_1^1[\sigma]$, monadic $\mathrm{NP}[\sigma]$)

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.

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

Beispiel 2.8

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

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

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

Definition 2.9

(a) Sei $L \subseteq \Sigma^*$ und sei φ ein MSO$[\sigma_\Sigma]$-Satz. Wir sagen: φ **beschreibt** 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 **MSO-definierbar** (bzw. EMSO-definierbar), falls es einen MSO$[\sigma_\Sigma]$-Satz (bzw. EMSO$[\sigma_\Sigma]$-Satz) gibt, der L 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} beschreiben:

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

mit

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

diese Abkürzungen werden wir 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 (d.h. wird von einem deterministischen endlichen Automaten erkannt)

(b) L ist EMSO-definierbar.

(c) L ist MSO-definierbar.

Beweis:

Wir beweisen die Richtung (a) $\Rightarrow$ (b) in folgendem Lemma:

Lemma 2.12

Jede reguläre Sprache $L \subseteq \Sigma^*$ ist EMSO-definierbar.

Beweis:

Sei $L \subseteq \Sigma^*$ regulär. D.h. L wird von einem deterministischen endlichen Automaten $\mathbb{A} = (Q, \Sigma, q_0, \delta, F)$ erkannt.

OBdA sei $Q = \{0, 1, \ldots, m\}$ für ein $m \in \mathbb{N}_{\geq 1}$,

$q_0 = 0$,

$F \subseteq Q$,

$\delta : Q \times \Sigma \to Q$.

Idee: Eingabewort: $w = w_1 \, w_2 \, w_3 \, w_4 \cdots w_n$

Lauf von $\mathbb{A}$: $q_0 \; q_1 \; q_2 \; q_3 \; q_4 \cdots q_n$

Für jeden Zustand $q \in Q$ "rate" die Menge Z_q der Positionen i von w, s.d. gilt: direkt nach dem Lesen des Buchstaben w_i ist $\mathbb{A}$ im Zustand q.

Wir konstruieren einen EMSO$[\tau_\Sigma]$-Satz $\Phi_{\mathbb{A}}$, s.d. f.a. $w \in \Sigma^*$ gilt: $\mathbb{A}$ akzeptiert $w \iff \mathfrak{A}_w \models \Phi_{\mathbb{A}}$.

Dann wählen wir $\Phi_{\mathcal{A}}$ wie folgt:

$$\Phi_{\mathcal{A}} := \exists Z_0 \cdots \exists Z_m \big(\varphi_{\text{Zustand}} \wedge \varphi_{\text{start}} \wedge \varphi_{\text{Schritt}} \wedge \varphi_{\text{akzeptiere}} \big)$$

mit

- $\underline{\varphi_{\text{Zustand}}}$: besagt, dass jede Position x zu genau <u>einer</u> der Mengen $Z_0, \dots, Z_m$ gehört:

$$\forall x \bigvee_{i=0}^{m} \Big(Z_i(x) \wedge \bigwedge_{j \neq i} \neg Z_j(x) \Big)$$

- $\underline{\varphi_{\text{start}}}$: besagt, dass der Automat im Startzustand q_0 startet und dass an Position 1 der Zustand $\delta(q_0, w_1)$ steht (wobei w_1 der Buchstabe an Pos 1 ist)

$$\forall x \Big(\underbrace{\min(x)}_{\forall y\, x \leq y} \rightarrow \bigwedge_{a \in \Sigma} \big(P_a(x) \rightarrow Z_{\delta(q_0,a)}(x) \big) \Big)$$

- $\underline{\varphi_{\text{Schritt}}}$: besagt, dass von einem Schritt zum nächsten die Überführungsfunktion δ beachtet wird:

$$\forall x \forall y \Big(\mathrm{succ}(x,y) \rightarrow \bigwedge_{\substack{a \in \Sigma, \\ q \in Q}} \big((Z_q(x) \wedge P_a(y)) \rightarrow Z_{\delta(q,a)}(y) \big) \Big)$$

- $\underline{\varphi_{\text{akzeptiere}}}$ besagt, dass der letzte Zustand akzeptierend ist:

$$\forall x \Big(\max(x) \rightarrow \bigvee_{q \in F} Z_q(x) \Big).$$

Klar: Φ_A ist ein EMSO$[\sigma_\Sigma]$-Satz.

Man kann leicht nachprüfen, dass f.a. $w \in \Sigma^+$ gilt:

$$\mathfrak{A}_w \models \Phi_A \iff \mathbb{A} \text{ akzeptiert } w.$$

Somit gilt: Φ_A beschreibt die von $\mathbb{A}$ akzeptierte reguläre Sprache L.

$\square_{\text{Lemma 2.12}}$

Die Richtung (b) $\Rightarrow$ (c) von Theorem 2.11 gilt trivialerweise (da EMSO$[\sigma_\Sigma] \subseteq$ MSO$[\sigma_\Sigma]$).

Zum Beweis der Richtung (c) $\Rightarrow$ (a) von Theorem 2.11 bringen wir einen gegebenen MSO$[\sigma_\Sigma]$-Satz zunächst in eine für die Übersetzung in einen endlichen Automaten besonders geeignete Form.

Dazu nutzen wir die folgenden MSO$[\sigma_\Sigma]$-Formeln:

- $\text{singl}(X) := \exists y \,\big(X(y) \wedge \forall z \,(X(z) \to z = y)\big)$

  besagt: $|X| = 1$ ("X is a singleton set")

- $\text{le}(X,Y) := \forall x \forall y \,\big((X(x) \wedge Y(y)) \to x \leq y \big)$

  besagt: "Kein Element von Y liegt links von einem Element in X"

- $\text{sub}(X,Y) := \forall x \,(X(x) \to Y(x))$ besagt "$X \subseteq Y$"

- $\text{symb}_a(X) := \forall x \,(X(x) \to P_a(x))$, f.a. $a \in \Sigma$

  besagt: "alle Positionen in X tragen den Buchstaben a"

Eine gegebene $MSO[\sigma_\Sigma]$-Formel φ transformieren wir nun in eine "äquivalente" $MSO[\sigma_\Sigma]$-Formel φ^*, indem wir jede Individuenvariable x durch eine neue Mengenvariable V_x ersetzen und atomare Formeln durch geeignete Kombinationen der Formeln singl, le, sub, $symb_a$ ersetzen:

- Für $\varphi := x \leq y$ ist $\varphi^* := le(V_x, V_y)$
- Für $\varphi := x = y$ ist $\varphi^* := le(V_x, V_y) \land le(V_y, V_x)$
- Für $\varphi := P_a(x)$ ist $\varphi^* := symb_a(V_x)$
- Für $\varphi := Z(x)$ ist $\varphi^* := sub(V_x, Z)$
- Für $\varphi := \exists x\, \psi$ ist $\varphi^* := \exists V_x \big(singl(V_x) \land \psi^*\big)$
- Für $\varphi := \forall x\, \psi$ ist $\varphi^* := \forall V_x \big(singl(V_x) \to \psi^*\big)$
- Für $\varphi := \neg\psi$ ist $\varphi^* := \neg\psi^*$
- Für $\varphi := (\varphi_1 \square \varphi_2)$ mit $\square \in \{\land, \lor, \to, \leftrightarrow\}$ ist $\varphi^* := (\varphi_1^* \square \varphi_2^*)$
- Für $\varphi = QZ\psi$ mit $Q \in \{\exists, \forall\}$ und $Z \in Var_2$ ist $\varphi^* := QZ\psi^*$

<u>Lemma 2.13</u>

Für jeden $MSO[\sigma_\Sigma]$-Satz φ gilt: φ^* beschreibt dieselbe Sprache wie φ.

<u>Beweis:</u> Übung.

Als Nächstes konstruieren wir induktiv für jede Teilformel von φ^* einen "äquivalenten" endlichen Automaten. Formeln der Form

$\mathrm{singl}(X)$, $\mathrm{le}(X,Y)$, $\mathrm{sub}(X,Y)$, $\mathrm{symb}_a(X)$

behandeln wir dabei als "atomar".

Insbes: Die Teilformeln, die wir betrachten müssen, haben keine freien Individuenvariablen, wohl aber freie Mengenvariablen. Belegungen dieser Mengenvariablen repräsentieren wir durch ein größeres Alphabet:

Seien $X_1,\dots,X_k$ (mit $k\in\mathbb{N}$) die Mengenvariablen, die in φ^* vorkommen. Sei

$$\Sigma' := \Sigma \times \{0,1\}^k .$$

Ein Wort $w = w_1 \cdots w_n \in \Sigma^+$ (mit $w_i\in\Sigma$) und Belegungen $X_1^w,\dots,X_k^w \subseteq \{1,\dots,n\}$ der Mengenvariablen $X_1,\dots,X_k$ in w repräsentieren wir durch das Wort $u_{w,\overline{X}^w} = u_1 \cdots u_n \in (\Sigma')^+$ mit

$$u_i := (w_i, b_{1,i},\dots,b_{k,i}) \in \Sigma' \text{ mit}$$

$$b_{j,i} := \begin{cases} 1 & \text{falls } i\in X_j^w \\ 0 & \text{falls } i\notin X_j^w \end{cases} \qquad \text{f.a. } j\in\{1,\dots,k\} \text{ und } i\in\{1,\dots,n\}.$$

Umgekehrt repräsentiert jedes Wort

$$u = u_1 \cdots u_n \in (\Sigma')^+$$

ein Wort $w = w_1 \cdots w_n \in \Sigma^+$ und Belegungen $X_1^w, \ldots, X_n^w \subseteq \{1, \ldots, n\}$ wie folgt:

Ist, für $i \in \{1, \ldots, n\}$, $u_i = (\sigma_i, b_{i,1}, \ldots, b_{i,k})$, so ist $w_i = \sigma_i$ f.a. $i \in \{1 \ldots n\}$ und

$$X_j^w = \{ i \in \{1, \ldots, n\} : b_{i,j} = 1 \} \quad \text{f.a. } j \in \{1..k\}.$$

Setze $\mathcal{A}'_u := (\mathcal{A}_w, X_1^w, \ldots, X_k^w)$.

Eine Teilformel ψ von φ^* <u>definiert</u> die Sprache

$$L'(\psi) := \{ u \in (\Sigma')^+ : \mathcal{A}'_u \models \psi \}.$$

<u>Lemma 2.14</u>

Sei $k \in \mathbb{N}$, $\Sigma' := \Sigma \times \{0,1\}^k$, seien $i, j \in \{1, \ldots, k\}$, sei $a \in \Sigma$.

Es gibt nichtdeterministische endliche Automaten $\mathbb{A}_{sing(X_i)}$, $\mathbb{A}_{le(X_i, X_j)}$, $\mathbb{A}_{sub(X_i, X_j)}$, $\mathbb{A}_{symb_a(X_i)}$, so dass gilt:

<u>(a)</u> $\mathbb{A}_{sing(X_i)}$ erkennt die Sprache $L'(sing(X_i)) \subseteq (\Sigma')^+$

<u>(b)</u> $\mathbb{A}_{le(X_i, X_j)}$ erkennt die Sprache $L'(le(X_i, X_j)) \subseteq (\Sigma')^+$

<u>(c)</u> $\mathbb{A}_{sub(X_i, X_j)}$ erkennt die Sprache $L'(sub(X_i, X_j)) \subseteq (\Sigma')^+$

<u>(d)</u> $\mathbb{A}_{symb_a(X_i)}$ erkennt die Sprache $L'(symb_a(X_i)) \subseteq (\Sigma')^+$

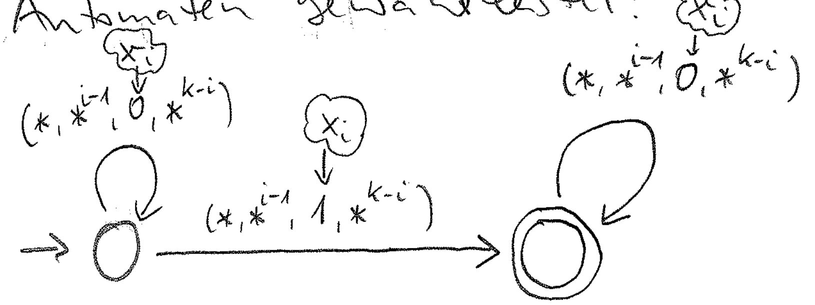
Beweis:

(a) Der Automat $\mathcal{A}_{\mathrm{sing}(X_i)}$ soll ein Wort $u = u_1 \cdots u_n \in (\Sigma')^+$ genau dann akzeptieren, wenn gilt: "es gibt genau eine Position $p \in \{1, \ldots, n\}$, so dass der Buchstabe

$$u_p = (w_p, b_{p,1}, \ldots, b_{p,k}) \in \Sigma \times \{0,1\}^k$$

an der zu X_i gehörigen Komponente $b_{p,i}$ eine 1 hat.

Dies wird durch den folgenden nichtdeterministischen Automaten gewährleistet:

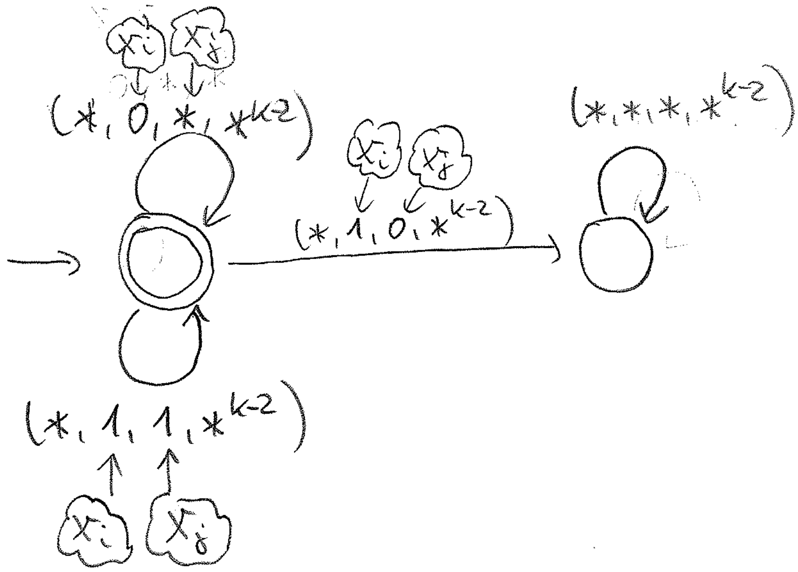


wobei ein "$*$" bedeutet, dass in der entsprechenden Komponente jeder mögliche Wert stehen kann.

(b) Übung

(c) $\mathcal{A}_{\mathrm{sub}(X_i, X_j)}$ soll ein Wort genau dann akzeptieren, wenn an jeder Position p für den dortigen Buchstaben $u_p = (w_p, b_{p,1}, \ldots, b_{p,k}) \in \Sigma \times \{0,1\}^k$ gilt: Falls $b_{p,i} = 1$, so auch $b_{p,j} = 1$

Dies wird durch den folgenden Automaten gewährleistet: OBdA betrachten wir nur den Fall, dass $i=1$ und $j=2$ ist:



<u>(d)</u> Übung.

$\square$

<u>Lemma 2.15</u>

Sei φ ein $MSO[\sigma_\Sigma]$-Satz, seien $X_1, \dots, X_k$ die in φ^* vorkommenden Mengenvariablen und sei $\Sigma' := \Sigma \times \{0,1\}^k$.

Für jede Teilformel ψ von φ^* (wobei Formeln der Form $Sing(X_i)$, $le(X_i, X_j)$, $suc(X_i, X_j)$, $symb_a(X_i)$ als "atomar" betrachtet werden) gibt es einen nichtdeterministischen endlichen Automaten A_ψ, so dass gilt:

A_ψ erkennt die Sprache $L'(\psi) \subseteq (\Sigma')^+$.

Beweis:

Per Induktion nach dem Aufbau von φ.
Der Induktionsanfang für "atomares" φ wird durch Lemma 2.14 gewährleistet.

Induktionsschritt:

Fall 1: $\varphi = \neg \chi$

Gemäß Induktionsannahme gibt es einen Automaten $\mathbb{A}_\chi$, der die Sprache $L'(\chi)$ erkennt.
klar: $L'(\varphi) = \{ u \in (\Sigma')^+ : u \notin L'(\chi)\}$, dh
$u \in L'(\varphi) \iff u \notin L'(\chi)$, f.a. $u \in (\Sigma')^+$
Dh wir erhalten den gesuchten Automaten $\mathbb{A}_\varphi$, indem wir $\mathbb{A}_\chi$ zunächst deterministisch machen (↗ Potenzmengenkonstruktion) und dann akzeptierende Zustände zu nichtakzeptierenden Zuständen machen und umgekehrt.

Fall 2: $\varphi = (\varphi_1 \vee \varphi_2)$

Gemäß Induktionsannahme gibt es Automaten $\mathbb{A}_{\varphi_1}$ und $\mathbb{A}_{\varphi_2}$, die die Sprachen $L'(\varphi_1)$ und $L'(\varphi_2)$ erkennen. OBdA sind deren Zustandsmengen disjunkt. Den nichtdeterministischen Automaten $\mathbb{A}_\varphi$ erhalten wir, indem wir die Automaten $\mathbb{A}_{\varphi_1}$ und $\mathbb{A}_{\varphi_2}$ vereinigen und deren Startzustände miteinander identifizieren.

D.h.: Ist $A_{\psi_i} = (Q_i, \Sigma', q_{0,i}, \Delta_i, F_i)$ mit

$\Delta_i \subseteq Q_i \times \Sigma_i \times Q_i$ und $Q_1 \cap Q_2 = \emptyset$,

So ist $A_\psi = (Q, \Sigma', q_0, \Delta, F)$ mit

- $Q = Q_1 \dot\cup Q_2 \dot\cup \{q_0\}$
- $F = F_1 \cup F_2 \cup M$ mit $M = \begin{cases} \{q_0\} & \text{falls } q_{0,1} \in F_1 \text{ oder } q_{0,2} \in F_2 \\ \emptyset & \text{sonst} \end{cases}$
- $\Delta = \Delta_1 \cup \Delta_2 \cup \{ (q_0, \sigma', q) : (q_{0,1}, \sigma', q) \in \Delta_1$ oder $(q_{0,2}, \sigma', q) \in \Delta_2 \}$

Fall 3: $\psi = (\psi_1 \Box \psi_2)$ mit $\Box \in \{\wedge, \rightarrow, \leftrightarrow\}$:

Durch geeignete Kombination der Fälle 1 und 2
(da z.B. $(\psi_1 \rightarrow \psi_2)$ äquivalent ist zu $(\neg\psi_1 \vee \psi_2)$).

Fall 4: $\psi = \exists X_i \chi$ mit $i \in \{1, \dots, k\}$

Gemäß Induktionsannahme gibt es bereits einen Automaten A_χ, der die Sprache $L'(\chi)$ erkennt.

Klar: Für jedes $u = u_1 \cdots u_n \in (\Sigma')^+$ mit

$u_p = (w_p, b_{p,1}, \dots, b_{p,k}) \in \Sigma \times \{0,1\}^k$ f.a. $p \in \{1 \dots n\}$

gilt:

Δ $\begin{cases} u \in L'(\psi) \iff \text{Es gibt Werte } \tilde{b}_1 \cdots \tilde{b}_n \in \{0,1\}^n \text{, die} \\ \text{für die "}X_i\text{"-Komponente eingesetzt werden können, s.d. für} \\ \tilde{u} = \tilde{u}_1 \cdots \tilde{u}_n \text{ mit } \tilde{u}_p = (w_p, b_{p,1}, \dots, b_{p,i-1}, \tilde{b}_p, b_{p,i+1}, \dots, b_{p,m}) \text{ f.a.} \end{cases}$

$p \in \{1,\dots,n\}$ gilt: $\tilde{u} \in L'(\chi)$ (d.h.: $\tilde{u}$ wird von A_χ akzeptiert)

Somit wird die Sprache $L'(\varphi)$ durch den nichtdeterministischen Automaten A_φ erkannt, der aus A_χ entsteht, indem in der Beschriftung jedes Pfeils der graphischen Darstellung von A_χ die X_i-Komponente durch das "Wildcard"-Symbol $*$ ersetzt wird. D.h.: Ist

$$A_\chi = (Q, \Sigma', q_0, \Delta, F), \text{ so ist}$$

$$A_\varphi = (Q, \Sigma', q_0, \tilde{\Delta}, F) \text{ mit}$$

$\tilde{\Delta} = \{ (q, \tilde{\sigma}, q') :$ $(q, \sigma, q') \in \Delta$ und $\tilde{\sigma} = (\tilde{a}, \tilde{b}_1, \dots, \tilde{b}_k) \in \Sigma \times \{0,1\}^k$ entsteht aus $\sigma = (a, b_1, \dots, b_k) \in \Sigma \times \{0,1\}^k$ indem der Wert b_i durch einen beliebigen Wert $\tilde{b}_i \in \{0,1\}$ ersetzt wird $\}$

Man kann leicht nachprüfen, dass für alle Worte $u \in (\Sigma')^+$ gilt: A_φ akzeptiert $u \iff$ (△) gilt.

<u>Fall 5</u>: $\varphi = \forall X_i\, \chi$ mit $i \in \{1,\dots,k\}$:
Durch Kombination der Fälle 4 und 1, da $\forall X_i \chi$ äquivalent ist zu $\neg \exists X_i \neg \chi$.

Beachte: Dies sind alle Fälle, die auftreten können.

$\square$ Lemma 2.1?

Wir können nun die Richtung (c) $\Rightarrow$ (a) von Theorem 2.11 beweisen:

Lemma 2.16:

Für jeden $MSO[\sigma_\Sigma]$-Satz φ gibt es einen nichtdeterministischen endlichen Automaten A_φ, der die von φ beschriebene Sprache erkennt.

Beweis:

Wir nutzen Lemma 2.13 und 2.15, um die Formel φ^* und den Automaten A_{φ^*} zu konstruieren, der die Sprache $L'(\varphi^*) \subseteq (\Sigma')^+$ erkennt, wobei $\Sigma' = \Sigma \times \{0,1\}^k$ ist und k so gewählt ist, dass $X_1, \dots, X_k$ die in φ^* vorkommenden Mengenvariablen sind.

Dh: A_{φ^*} akzeptiert ein Wort $u = u_1 \cdots u_n \in (\Sigma')^+$ genau dann, wenn $\mathfrak{A}'_u = (\mathfrak{A}_w, X_1^w, \dots, X_k^w)$ die Formel φ^* erfüllt. Da φ^* keine freien Variablen hat, gilt: $\mathfrak{A}'_u \models \varphi^* \iff \mathfrak{A}_w \models \varphi^*$ (dh: die jeweilige Belegung der Mengenvariablen $X_1, \dots, X_k$ ist irrelevant).

Somit erhalten wir einen nichtdeterministischen Automaten A_φ, der genau diejenigen Worte $w \in \Sigma^+$ akzeptiert, für die $\mathfrak{A}_w \models \varphi^*$ gilt, indem wir in der graphischen Darstellung von $\mathcal{A}_{\varphi^*}$ in der Beschriftung jedes Pfeils die Komponenten für $X_1, \dots, X_k$ weglassen. D.h.:

Ist $\mathcal{A}_{\varphi^*} = (Q, \Sigma', q_0, \Delta, F)$, so ist

$$\mathcal{A}_{\varphi} = (Q, \Sigma, q_0, \tilde{\Delta}, F) \quad \text{mit}$$

$$\tilde{\Delta} = \{ (q, \sigma, q') : \text{ es gibt } b_1, \dots, b_k \in \{0,1\}, \text{ s.d. } (q, (\sigma, b_1 \dots b_k), q') \in \Delta \}$$

Man kann leicht nachprüfen, dass für alle Worte $w \in \Sigma^+$ gilt: $\mathcal{A}_\varphi$ akzeptiert $w \iff \mathfrak{A}_w \models \varphi$.

Insbes.: Die von φ beschriebene Sprache ist regulär.

$\square$ Lemma 2.16

Dies beendet den Beweis des Satzes von Büchi

$\square$ Theorem 2.11

<u>Beachte</u>: Der Satz von Büchi besagt insbesondere, dass <u>existentielle</u> monadische Logik zweiter Stufe auf <u>Worten</u> dieselbe Ausdrucksstärke besitzt wie die "volle" monadische Logik zweiter Stufe (und genau die regulären Sprachen beschreiben kann).

Aus dem Gebiet der "formalen Sprachen" sind viele Methoden bekannt, mit denen man nachweisen kann, dass bestimmte Sprachen <u>nicht</u> regulär sind (z.B.: Pumping-Lemma, Satz von Myhill und Nerode, Abschlusseigenschaften..., siehe einführende Vorlesungen in Theoretische Informatik, formale Sprachen bzw Automatentheorie).
Insbes. wissen wir, dass die Sprache

$$L_{a^nb^n} := \{ a^n b^n : n \in \mathbb{N}_{\geq 1} \}$$

<u>nicht</u> regulär ist.

Gemäß Satz von Büchi kann $L_{a^nb^n}$ also auch <u>nicht</u> durch einen MSO-Satz beschrieben werden. Durch Anwenden einer "logischen Reduktion" können wir daraus folgern, dass z.B. bestimmte Graphen-Eigenschaften nicht in MSO beschrieben werden können:

<u>Satz 2.17</u> ("Hamiltonkreis ist <u>nicht</u> MSO-definierbar")
Sei $\sigma_{Graph} = \{E\}$ für ein 2-stelliges Relationssymbol E.
Es gibt keinen MSO$[\sigma_{Graph}]$-Satz φ, so dass für jeden endlichen Graphen G gilt:

$G \models \varphi \iff G$ besitzt einen Hamiltonkreis.

Beweis: Durch Widerspruch.

Angenommen, φ_{Ham} ist ein $MSO[\sigma_{Graph}]$-Satz, s.d. für jeden endlichen Graphen G gilt:

$G \models \varphi_{Ham} \iff G$ besitzt einen Hamiltonkreis.

Ziel: Modifiziere φ_{Ham} zu einem $MSO[\sigma_\Sigma]$-Satz $\varphi_{a^n b^n}$ (für $\Sigma = \{a,b\}$), der die Sprache $L_{a^n b^n} = \{ a^n b^n : n \geq 1\}$ beschreibt.

Idee: Einem Wort $w \in \{a,b\}^+$ ordnen wir den Graphen $G_w = (V_w, E_w)$ zu mit

- Knotenmenge V_w: die Menge der Positionen des Worts w
- Kantenmenge E_w: zwischen zwei Positionen x und y gibt es genau dann eine Kante, wenn die beiden Positionen unterschiedliche Buchstaben tragen. D.h.:

$$E(x,y) \iff \big(P_a(x) \wedge P_b(y)\big) \vee \big(P_b(x) \wedge P_a(y)\big)$$

Beachte: G_w ist ein vollständiger bipartiter Graph, dessen Knotenmenge in $P_a^w \,\dot\cup\, P_b^w$ partitioniert ist.

Insbes.: G_w besitzt einen Hamiltonkreis

$\iff$ $|P_a^w| = |P_b^w|$, dh w besitzt genau so viele a's wie b's.

Daher wird $L_{a^nb^n}$ durch folgenden MSO$[\sigma_2]$-Satz $\varphi_{a^nb^n}$ beschreiben:

$$\varphi_{a^nb^n} := \forall x \forall y \Big(\big(P_a(x) \land P_b(y) \big) \to x \leq y \Big) \land \varphi'_{Ham},$$

wobei φ'_{Ham} aus φ_{Ham} entsteht, indem jedes Atom der Form $E(x,y)$ ersetzt wird durch die Formel $\Big(\big(P_a(x) \land P_b(y) \big) \lor \big(P_b(x) \land P_a(y) \big) \Big)$.

Dies ist ein Widerspruch, da gemäß Satz von Büchi dann $L_{a^nb^n}$ regulär sein müsste.

$\square$