Logik II

Markus Lohrey

Universität Siegen

Sommersemester 2016

Organisatorisches zur Vorlesung

Informationen finden Sie unter

`http://www.eti.uni-siegen.de/ti/lehre/ss16/logikii/`

z. B.

- Aktuelle Version der Folien
- Übungsblätter

Literaturempfehlung:

- Schöning: Logik für Informatiker, Spektrum Akademischer Verlag
- Ebbinghaus, Flum, Thomas: Einfhrung in die mathematische Logik, Spektrum Akademischer Verlag

Die **Übungen** werden von Herrn Danny Hucke organisiert.

Wiederholung aus GTI

Definition (semi-entscheidbar)

Eine Sprache $L \subseteq \Sigma^*$ ist semi-entscheidbar, falls es gibt einen Algorithmus mit folgenden Eigenschaften gibt:

Für alle $x \in \Sigma^*$ gilt:

- Wenn $x \in L$, dann terminiert der Algorithmus bei Eingabe x.
- Wenn $x \notin L$, dann terminiert der Algorithmus bei Eingabe x nicht.

Äquivalenter Begriff: Rekursiv aufzählbar.

Definition (rekursiv aufzählbar)

Eine Sprache $L \subseteq \Sigma^*$ ist rekursiv aufzählbar, falls es gibt eine berechenbare totale Funktion $f : \mathbb{N} \to \Sigma^*$ gibt mit $L = \{f(i) \mid i \in \mathbb{N}\}$.

Wiederholung aus GTI

Definition (entscheidbar und unentscheidbar)

Eine Sprache $L \subseteq \Sigma^*$ ist entscheidbar, falls es gibt einen Algorithmus mit folgenden Eigenschaften gibt: Für alle $x \in \Sigma^*$ gilt:

- Wenn $x \in L$, dann terminiert der Algorithmus bei Eingabe x mit der Ausgabe "Ja".
- Wenn $x \notin L$, dann terminiert der Algorithmus bei Eingabe x mit der Ausgabe "Nein".

Eine Sprache $L \subseteq \Sigma^*$ ist unentscheidbar, falls sie nicht entscheidbar ist.

Satz

Eine Sprache $L \subseteq \Sigma^*$ ist entscheidbar genau dann, wenn L und $\Sigma^* \setminus L$ beide semi-entscheidbar sind.

Wiederholung aus Logik I

Eine prädikatenlogische Formel F ist:

- erfüllbar, falls es eine zu F passende Struktur $\mathcal{A}$ mit $\mathcal{A} \models F$ gibt (d.h. F ist wahr in der Struktur $\mathcal{A}$).
- gültig, falls $\mathcal{A} \models F$ für jede zu F passende Struktur $\mathcal{A}$ gilt.

Konsequenz aus dem Satz von Gilmore

Die Menge der unerfüllbaren prädikatenlogischen Formeln ist semi-entscheidbar.

Korollar

Die Menge der gültigen prädikatenlogischen Formeln ist semi-entscheidbar.

Beweis: F ist gültig, genau dann, wenn $\neg F$ unerfüllbar ist.

Unentscheidbarkeit der Prädikatenlogik

Wir wollen nun den folgenden zentralen Satz beweisen:

Satz von Church

Die Menge der gültigen prädikatenlogischen Formeln ist unentscheidbar.

Korollar

Die Menge der erfüllbaren prädikatenlogischen Formeln ist nicht semi-entscheidbar.

Beweis: Die Menge der unerfüllbaren Formeln ist semi-entscheidbar.

Wäre also die Menge der erfüllbaren Formeln semi-entscheidbar, so wäre sie entscheidbar.

Also wäre auch die Menge der unerfüllbaren Formeln und damit die Menge der gültigen Formeln entscheidbar. □

Registermaschinen

Wir beweisen den Satz von Church durch eine Reduktion vom Halteproblem für Registermachinenprogramme.

Seien $R_1, R_2, \ldots$ Bezeichner für Register.

Intuition: Jedes Register speichert eine natürliche Zahl ab.

Eine Registermachinenprogramm (kurz RMP) P besteht aus einer Folge $A_1; A_2; \ldots; A_l$ von Anweisungen, wobei A_l die Anweisung STOP ist, und für alle $1 \leq i \leq l-1$ die Anweisung A_i von einem der folgenden Typen ist:

- $R_j := R_j + 1$ für ein $1 \leq j \leq l$
- $R_j := R_j - 1$ für ein $1 \leq j \leq l$
- IF $R_j = 0$ THEN k_1 ELSE k_2 für $1 \leq j, k_1, k_2 \leq l$,

Eine Konfiguration von P ist ein Tupel $(i, n_1, \ldots, n_l) \in \mathbb{N}^{l+1}$ mit $1 \leq i \leq l$.

Intuition: i ist die Nummer der Anweisung, die als nächste ausgeführt wird, und n_j ist der aktuelle Inhalt von Register R_j.

Registermaschinen

Für Konfigurationen $(i, n_1, \ldots, n_l)$ und $(i', n'_1, \ldots, n'_l)$ schreiben wir

$$(i, n_1, \ldots, n_l) \to_P (i', n'_1, \ldots, n'_l)$$

genau dann, wenn $1 \leq i \leq l-1$ und einer der folgenden Fälle gilt:

- $A_i = (R_j := R_j + 1)$ für ein $1 \leq j \leq l$, $i' = i + 1$, $n'_j = n_j + 1$, $n'_k = n_k$ für $k \neq j$.
- $A_i = (R_j := R_j - 1)$ für ein $1 \leq j \leq l$, $i' = i + 1$, $n_j = n'_j = 0$ oder $(n_j > 0,\ n'_j = n_j - 1)$, und $n'_k = n_k$ für $k \neq j$.
- $A_i = (\text{IF } R_j = 0 \text{ THEN } k_1 \text{ ELSE } k_2)$ für ein $1 \leq j, k_1, k_2 \leq l$, $n'_k = n_k$ für alle $1 \leq k \leq l$, $i' = k_1$ falls $n_j = 0$, $i' = k_2$ falls $n_j > 0$.

Wir definieren

$$\begin{aligned}\text{HALT} = \{P \mid\ & P = A_1; A_2; \ldots; A_l \text{ ist ein RMP mit } l \text{ Anweisungen,} \\ & (1, 0, \ldots, 0) \to_P^* (l, n_1, \ldots, n_l) \text{ für } n_1, \ldots, n_l \geq 0\}\end{aligned}$$

Beweis des Satzes von Church

Registermachinenprogramme entsprechen genau den GOTO-Programmen aus der GTI.

Dort haben wir gezeigt, dass eine Turingmaschine durch ein GOTO-Programm simuliert werden kann (und umgekehrt).

Da das Halteproblem für Turingmaschinen auf dem leeren Band (Hält eine Turingmaschine, wenn Sie mit dem leeren Band gestartet wird?) unentscheidbar ist, erhalten wir:

Unentscheidbarkeit des Halteproblems für RMPs

Die Menge HALT ist unentscheidbar.

Bemerkung: HALT ist semi-entdscheidbar: Simuliere ein gegebenes RMP auf der Startkonfiguration $(1, 0, \ldots, 0)$ und stoppe, wenn das RMP bei der STOP-Anweisung ankommt.

Beweis des Satzes von Church

Wir beweisen den Satz von Church, indem wir jedem RMP P effektiv eine prädikatenlogischen Aussage F_P zuordnen, so dass gilt:

$$F_P \text{ ist gültig } \iff P \in \text{HALT}$$

Sei $P = A_1; A_2; \ldots; A_l$ ein RMP.

Wir fixieren folgende Symbole:

- $<$: 2-stelliges Prädikatensymbol
- c: Konstante
- f, g: 1-stellige Funktionssymbole
- R: $(l+2)$-stelliges Prädikatensymbol

Beweis des Satzes von Church

Wir definieren eine Struktur $\mathcal{A}_P$ durch Fallunterscheidung:

1. Fall: $P \notin$ HALT:

- Universum $U_{\mathcal{A}_P} = \mathbb{N}$
- $<^{\mathcal{A}_P} = \{(n, m) \mid n < m\}$ (gewöhnliche Ordnung auf $\mathbb{N}$)
- $c^{\mathcal{A}_P} = 0$
- $f^{\mathcal{A}_P}(n) = n + 1$, $g^{\mathcal{A}_P}(n + 1) = n$, $g^{\mathcal{A}_P}(0) = 0$
- $R^{\mathcal{A}_P} = \{(s, i, n_1, \ldots, n_l) \mid (1, 0, \ldots, 0) \to_P^s (i, n_1, \ldots, n_l)\}$

2. Fall: $P \in$ HALT:

Sei t so, dass $(1, 0, \ldots, 0) \to_P^t (l, n_1, \ldots, n_l)$ und $e = \max\{t, l\}$.

- Universum $U_{\mathcal{A}_P} = \{0, 1, \ldots, e\}$
- $<^{\mathcal{A}_P} = \{(n, m) \mid n < m\}$ (gewöhnliche Ordnung auf $\{0, 1, \ldots, e\}$)
- $c^{\mathcal{A}_P} = 0$
- $f^{\mathcal{A}_P}(n) = n + 1$ für $0 \leq n \leq e - 1$ und $f^{\mathcal{A}_P}(e) = e$.
- $g^{\mathcal{A}_P}(n + 1) = n$ für $0 \leq n \leq e - 1$ und $g^{\mathcal{A}_P}(0) = 0$.
- $R^{\mathcal{A}_P} = \{(s, i, n_1, \ldots, n_l) \mid 0 \leq s \leq t, (1, 0, \ldots, 0) \to_P^s (i, n_1, \ldots, n_l)\}$

Beweis des Satzes von Church

Im folgenden verwenden wir die Abkürzung $\overline{m}$ für den Term $f^m(c)$.

Wir definieren nun eine Aussage G_P (in der $<, c, f, g$ und R vorkommen) mit folgenden Eigenschaften:

(A) $\mathcal{A}_P \models G_P$

(B) Für jedes Modell $\mathcal{A}$ von G_P gilt Folgendes:

Wenn $(1, 0, \ldots, 0) \to_P^s (i, n_1, \ldots, n_l)$, dann:

$$\mathcal{A} \models R(\overline{s}, \overline{i}, \overline{n_1}, \ldots, \overline{n_l}) \wedge \bigwedge_{q=0}^{s-1} \overline{q} < \overline{q+1}.$$

Wir definieren

$$G_P = G_0 \wedge R(\overline{0}, \overline{1}, \overline{0}, \ldots, \overline{0}) \wedge G_1 \wedge \cdots \wedge G_{l-1}$$

wobei die Aussagen $G_0, G_1, \ldots, G_{l-1}$ wie folgt definiert sind.

Beweis des Satzes von Church

G_0 sagt aus:

- $<$ ist eine lineare Ordnung mit kleinstem Element c,
- $x \leq f(x)$ und $g(x) \leq x$ für alle x,
- für jedes x, das nicht das größte Element bzgl. $<$ ist, ist $f(x)$ der unmittelbare Nachfolger von x, und
- für jedes x, das nicht das kleinste Element c ist, ist $g(x)$ der unmittelbare Vorgänger von x.

$$\begin{aligned}\forall x, y, z\ & (\neg x < x) \wedge (x = y \vee x < y \vee y < x) \wedge ((x < y \wedge y < z) \rightarrow x < z) \\ & \wedge (x = c \vee c < x) \\ & \wedge (x = f(x) \vee x < f(x)) \\ & \wedge (x = g(x) \vee g(x) < x) \\ & \wedge \big(\exists u(x < u) \rightarrow (x < f(x) \wedge \forall u(x < u \rightarrow (u = f(x) \vee f(x) < u)))\big) \\ & \wedge \big(\exists u(u < x) \rightarrow (g(x) < x \wedge \forall u(u < x \rightarrow (u = g(x) \vee u < g(x))))\big)\end{aligned}$$

Beweis des Satzes von Church

Bemerkung: Für jedes Modell $\mathcal{A}$ von G_0 gilt:

- $\mathcal{A} \models g(c) = c$
- $\mathcal{A} \models \forall x \, (\exists u(x < u) \rightarrow g(f(x)) = x)$

Beweis des Satzes von Church

G_i für $1 \leq i \leq l-1$ beschreibt die Wirkung der Anweisung A_i.

1. Fall: $A_i = (R_j := R_j + 1)$. Dann sei

$$G_i = \forall x \forall x_1 \cdots \forall x_l \Big(R(x, \overline{i}, x_1, \ldots, x_l) \rightarrow (x < f(x) \wedge R(f(x), \overline{i+1}, x_1, \ldots, x_{j-1}, f(x_j), x_{j+1}, \ldots, x_l)) \Big)$$

2. Fall: $A_i = (R_j := R_j - 1)$. Dann sei

$$G_i = \forall x \forall x_1 \cdots \forall x_l \Big(R(x, \overline{i}, x_1, \ldots, x_l) \rightarrow (x < f(x) \wedge R(f(x), \overline{i+1}, x_1, \ldots, x_{j-1}, g(x_j), x_{j+1}, \ldots, x_l)) \Big)$$

Beweis des Satzes von Church

3. Fall: $A_i = (\text{IF } R_j = 0 \text{ THEN } k_1 \text{ ELSE } k_2)$ für ein $1 \leq j, k_1, k_2 \leq l$.
Dann sei

$$G_i = \forall x \forall x_1 \cdots \forall x_l \Big(R(x, \overline{i}, x_1, \ldots, x_l) \rightarrow (x < f(x) \wedge (x_j = c \wedge R(f(x), \overline{k_1}, x_1, \ldots, x_l)) \vee (x_j > c \wedge R(f(x), \overline{k_2}, x_1, \ldots, x_l))) \Big)$$

Aussage (A) folgt sofort aus der Definition von $\mathcal{A}_P$ und G_P.

Aussage (B) beweisen wir durch eine Induktion über s.

IA: $s = 0$. Gelte $(1, 0, \ldots, 0) \rightarrow_P^0 (i, n_1, \ldots, n_l)$, d.h. $i = 1$ und $n_1 = n_2 = \cdots = n_l = 0$.

Aus $\mathcal{A} \models G_P$ folgt $\mathcal{A} \models R(\overline{0}, \overline{1}, \overline{0}, \ldots, \overline{0})$, d. h. $\mathcal{A} \models R(\overline{s}, \overline{i}, \overline{n_1}, \ldots, \overline{n_l})$.

Beweis des Satzes von Church

IS: Sei nun $s > 0$ und gelte Aussage (B) für $s - 1$.

Sei $(1, 0, \ldots, 0) \to_P^s (i, n_1, \ldots, n_l)$.

Dann gibt es $j, m_1, \ldots, m_l$ mit

$$(1, 0, \ldots, 0) \to_P^{s-1} (j, m_1, \ldots, m_l) \to_P (i, n_1, \ldots, n_l)$$

Aus der IH folgt

$$\mathcal{A} \models R(\overline{s-1}, \bar{j}, \overline{m_1}, \ldots, \overline{m_l}) \wedge \bigwedge_{q=0}^{s-2} \overline{q} < \overline{q+1}.$$

Wir machen nun eine Fallunterscheidung bezüglich der Anweisung A_j, wobei wir nur den Fall betrachten, dass A_j von der Form $R_k := R_k - 1$ ist.

Es gilt dann $i = j + 1$, $n_1 = m_1, \ldots, n_{k-1} = m_{k-1}$, $n_{k+1} = m_{k+1}, \ldots, n_l = m_l$, ($n_k = m_k = 0$ oder $m_k > 0$ und $n_k = m_k - 1$).

Beweis des Satzes von Church

Wegen $\mathcal{A} \models G_j$ gilt:

$$\mathcal{A} \models \forall y, y_1, \ldots, y_l \Big(R(y, \bar{j}, y_1, \ldots, y_l) \rightarrow (y < f(y) \wedge R(f(y), \overline{j+1}, y_1, \ldots, y_{k-1}, g(y_k), y_{k+1}, \ldots, y_l)) \Big)$$

Wegen $\mathcal{A} \models R(\overline{s-1}, \bar{j}, \overline{m_1}, \ldots, \overline{m_l})$ folgt

$$\mathcal{A} \models \overline{s-1} < f(\overline{s-1}) \wedge R(f(\overline{s-1}), \overline{j+1}, \overline{m_1}, \ldots, \overline{m_{k-1}}, g(\overline{m_k}), \overline{m_{k+1}}, \ldots, \overline{m_l})$$

d.h.

$$\mathcal{A} \models \overline{s-1} < \bar{s} \wedge R(\bar{s}, \bar{i}, \overline{n_1}, \ldots, \overline{n_{k-1}}, g(\overline{m_k}), \overline{n_{k+1}}, \ldots, \overline{n_l})$$

Beweis des Satzes von Church

Wegen $\mathcal{A} \models \overline{s-1} < \overline{s}$ gilt

$$\mathcal{A} \models \bigwedge_{q=0}^{s-1} \overline{q} < \overline{q+1}.$$

Ausserdem folgt aus $\mathcal{A} \models G_0$, dass $\mathcal{A} \models g(\overline{m_k}) = \overline{n_k}$.

Also gilt auch $\mathcal{A} \models R(\overline{s}, \overline{i}, \overline{n_1}, \ldots, \overline{n_l})$.

Damit sind (A) und (B) gezeigt.

Beweis des Satzes von Church:

Setze $F_P = (G_P \to \exists x \exists x_1 \cdots \exists x_l R(x, \overline{l}, x_1, \ldots, x_l))$

Behauptung: F_P ist gültig $\iff P \in \mathrm{HALT}$.

Beweis des Satzes von Church

Ist F_P gültig, so gilt insbesondere $\mathcal{A}_P \models F_P$.

Wegen (A) gilt $\mathcal{A}_P \models \exists x \exists x_1 \cdots \exists x_l R(x, \overline{l}, x_1, \ldots, x_l)$.

Also gibt es $s, n_1, \ldots, n_l \geq 0$ mit $(s, l, n_1, \ldots, n_l) \in R^{\mathcal{A}_P}$.

Es folgt $P \in \mathrm{HALT}$.

Sein nun $P \in \mathrm{HALT}$ und gelte $(1, 0, \ldots, 0) \to_P^s (l, n_1, \ldots, n_l)$

Sei $\mathcal{A}$ eine Struktur mit $\mathcal{A} \models G_P$.

Aus (B) folgt $\mathcal{A} \models R(\overline{s}, \overline{l}, \overline{n_1}, \ldots, \overline{n_l})$.

Also ist F_P gültig. □

Der Satz von Trachtenbrot

Eine Formel F ist im Endlichen erfüllbar genau dann, wenn F ein Modell mit einem endlichen Universum hat, sonst ist F im Endlichen unerfüllbar.

Lemma

Die Menge der im Endlichen erfüllbaren Formeln ist semi-entscheidbar.

Beweis:

Sei $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \ldots$ eine systematische Auflistung aller endlichen zu F passenden Strukturen (o.B.d.A. ist $I_{\mathcal{A}_i}$ nur auf den in F vorkommenden Prädikaten- und Funktionssymbolen definiert).

Folgender Algorithmus terminiert genau dann, wenn F im endlichen erfüllbar ist:

$i := 1$;
while true do
    if $\mathcal{A}_i \models F$ **then STOP else** $i := i + 1$
end

□

Der Satz von Trachtenbrot

Eine Formel F ist im Endlichen gültig genau dann, wenn jede endliche zu F passende Struktur ein Modell von F ist.

Beispiel: Die Formel

$$\forall x \forall y (f(x) = f(y) \rightarrow x = y) \;\leftrightarrow\; \forall y \exists x (f(x) = y)$$

ist im Endlichen gültig, aber nicht (allgemein) gültig.

Satz von Trachtenbrot

Die Menge der im Endlichen erfüllbaren Formeln ist unentscheidbar.

Korollar

Die Menge der im Endlichen unerfüllbaren Formeln sowie die Menge der im Endlichen gültigen Formeln ist nicht semi-entscheidbar.

Der Satz von Trachtenbrot

Beweis des Satzes von Trachtenbrot:

Wir verwenden die Konstruktion aus dem Beweis des Satzes von Church.

Behauptung: G_P ist im Endlichen erfüllbar $\iff P \in \text{HALT}$.

(1) Gelte $P \in \text{HALT}$.

Dann ist $\mathcal{A}_P$ endlich und es gilt $\mathcal{A}_P \models G_P$ nach Aussage (A).

Also ist G_P im Endlichen erfüllbar.

Der Satz von Trachtenbrot

(2) Sei G_P im Endlichen erfüllbar.

Sei $\mathcal{A}$ eine endliche Struktur mit $\mathcal{A} \models G_P$.

Angenommen $P \notin \text{HALT}$ gilt.

Also gibt es für jede Zahl $s \geq 0$ Zahlen $i, n_1, \ldots, n_l$ mit $(1, 0, \ldots, 0) \to_P^s (i, n_1, \ldots, n_l)$.

Aussage (B) impliziert, dass $\mathcal{A} \models \bar{i} < \overline{i+1}$ für alle $i \geq 0$.

Da $<^{\mathcal{A}}$ eine lineare Ordnung ist (wegen $\mathcal{A} \models G_0$) ist die Menge $\{\mathcal{A}(\bar{i}) \mid i \geq 0\}$ unendlich, was ein Widerspruch ist. □

(Un)entscheidbare Theorien

Sei $\mathcal{A}$ eine Struktur, wobei der Definitionsbereich von $I_{\mathcal{A}}$ endlich sei und keine Variablen enthält.

Sei $f_1, \ldots, f_n, R_1, \ldots, R_m$ der Definitionsbereich von $I_{\mathcal{A}}$.

Wir identifizieren dann $\mathcal{A}$ mit dem Tupel $(U^{\mathcal{A}}, f_1^{\mathcal{A}}, \ldots, f_n^{\mathcal{A}}, R_1^{\mathcal{A}}, \ldots, R_m^{\mathcal{A}})$, wofür wir auch $(U^{\mathcal{A}}, f_1, \ldots, f_n, R_1, \ldots, R_m)$ schreiben.

Definition

Die Theorie von $\mathcal{A}$ ist die Menge von Formeln

$$\mathrm{Th}(\mathcal{A}) = \{F \mid F \text{ ist eine Aussage, } \mathcal{A} \text{ passt zu } F, \mathcal{A} \models F\}.$$

Wir interessieren uns für die Frage, ob eine Struktur eine entscheidbare Theorie hat.

(Un)entscheidbare Theorien

Satz

Sei $\mathcal{A}$ eine beliebige Struktur. Dann ist $\mathrm{Th}(\mathcal{A})$ *entscheidbar genau dann, wenn* $\mathrm{Th}(\mathcal{A})$ *semi-entscheidbar ist.*

Beweis: Sei $\mathrm{Th}(\mathcal{A})$ semi-entscheidbar und sei F eine beliebige Aussage.

Dann gilt entweder $F \in \mathrm{Th}(\mathcal{A})$ oder $\neg F \in \mathrm{Th}(\mathcal{A})$.

Wir können daher einen Semi-Entscheidungsalgorithmus für $\mathrm{Th}(\mathcal{A})$ mit Eingabe F und $\neg F$ parallel laufen lassen.

Einer der beiden Läufe wird irgendwann mit der Antwort terminieren. □

(Un)entscheidbare Theorien

Für die Frage nach der Entscheidbarkeit einer Struktur können wir uns auf sogenannte relationale Strukturen beschränken.

Eine Struktur $\mathcal{A} = (A, f_1, \ldots, f_n, R_1, \ldots, R_m)$ ist relational, falls $n = 0$ gilt.

Für eine beliebige Struktur $\mathcal{A} = (A, f_1, \ldots, f_n, R_1, \ldots, R_m)$ definieren wir

$$\mathcal{A}_{\text{rel}} = (A, P_1, \ldots, P_n, R_1, \ldots, R_m)$$

wobei

$$P_i = \{(a_1, \ldots, a_k, a) \mid f_i(a_1, \ldots, a_k) = a\}.$$

Lemma

$\text{Th}(\mathcal{A})$ *ist entscheidbar genau dann, wenn* $\text{Th}(\mathcal{A}_{rel})$ *entscheidbar ist.*

Beweis: Übung.

Unentscheidbarkeit der Arithmetik (nach Ebbinhaus,Flum,Thomas)

Satz (Gödel 1931)

$\mathrm{Th}(\mathbb{N}, +, \cdot)$ ist unentscheidbar.

Korollar

$\mathrm{Th}(\mathbb{N}, +, \cdot)$ ist nicht semi-entscheidbar, also nicht rekursiv aufzählbar.

Für den Beweis reduzieren wir die Menge HALT von terminierenden RMPs auf $\mathrm{Th}(\mathbb{N}, +, \cdot)$.

Um den Beweis etwas komfortabler zu machen, betrachten wir $\mathrm{Th}(\mathbb{N}, +, \cdot, s, 0)$ mit $s(n) = n + 1$.

Übung: $\mathrm{Th}(\mathbb{N}, +, \cdot, s, 0)$ ist unentscheidbar genau dann, wenn $\mathrm{Th}(\mathbb{N}, +, \cdot)$ unentscheidbar ist.

Unentscheidbarkeit der Arithmetik

Sei nun $P = A_1; A_2; \cdots ; A_l$ ein RMP, in dem die Register $R_1, \ldots, R_l$ verwendet werden.

Wir konstruieren eine arithmetische Formel F_P mit den freien Variablen $x, x_1, \ldots, x_l$, so dass für alle $1 \leq i \leq l$ und $n_1, \ldots, n_l \in \mathbb{N}$ folgende beiden Aussagen äquivalent sind:

- $(\mathbb{N}, +, \cdot, s, 0)_{[x/i,\ x_1/n_1, \ldots, x_l/n_l]} \models F_P$
- $(1, 0, \ldots, 0) \to_P^* (i, n_1, \ldots, n_l)$

Dann gilt $P \in \text{HALT} \iff (\mathbb{N}, +, \cdot, s, 0) \models \exists x_1 \cdots \exists x_l\ F_P[x/s^l(0)]$.

Unentscheidbarkeit der Arithmetik

Intuitiv sagt die Formel F_P Folgendes aus:

Es gibt ein $s \geq 0$ und Konfigurationen $C_0, C_1, \ldots, C_s$ mit:

- $C_0 = (1, 0, \ldots, 0)$
- $C_s = (x, x_1, \ldots, x_l)$
- $C_i \to_P C_{i+1}$ für alle $0 \leq i \leq s - 1$

Wir können die $(l+1)$-Tupel $C_0, C_1, \ldots, C_s$ durch ein $(s+1)(l+1)$-Tupel kodieren, und müssen dann Folgendes ausdrücken, wobei $k = l + 1$ sei.

Es gibt ein $s \geq 0$ und ein Tupel
$(y_0, y_1, \ldots, y_{k-1},\ y_k, y_{k+1}, \ldots, y_{2k-1}, \ldots, y_{sk}, y_{sk+1}, \ldots, y_{(s+1)k-1})$ mit:

- $y_0 = 1,\ y_1 = 0, \ldots, y_{k-1} = 0$
- $y_{sk} = x,\ y_{sk+1} = x_1, \ldots, y_{(s+1)k-1} = x_l$
- $(y_{ik}, \ldots, y_{(i+1)k-1}) \to_P (y_{(i+1)k}, \ldots, y_{(i+2)k-1})$ für alle $0 \leq i \leq s - 1$

Unentscheidbarkeit der Arithmetik

Will man dies durch eine arithmetische Formel ausdrücken, hat man das Problem, dass man nicht über Folgen von Zahlen quantifizieren kann ($\exists y \exists x_1 \cdots \exists x_y$ ist nicht zulässig).

Um trotzdem eine Quantifizierung über beliebig lange Folgen zu simulieren, benötigen wir Gödels β-Funktion.

Lemma

Es gibt eine Funktion $\beta : \mathbb{N}^3 \to \mathbb{N}$ mit:

- Für jede Folge $(a_0, \ldots, a_r)$ über $\mathbb{N}$ gibt es $t, p \in \mathbb{N}$, so dass $\beta(t, p, i) = a_i$ für alle $0 \leq i \leq r$
- Es gibt eine arithmetische Formel B mit freien Variablen v, x, y, z, so dass für alle $t, p, i, a \in \mathbb{N}$ gilt:

$$(\mathbb{N}, +, \cdot, s, 0)_{[v/t,\, x/p,\, y/i,\, z/a]} \models B \iff \beta(t, p, i) = a$$

Man sagt auch: β ist arithmetisch definierbar.

Unentscheidbarkeit der Arithmetik

Beweis des Lemmas:

Sei $(a_0, \ldots, a_r)$ eine beliebige Folge über $\mathbb{N}$.

Sei p eine Primzahl mit $p > r + 1$ und $p > a_i$ für alle i.

Sei weiter

$$t = 1p^0 + a_0p^1 + 2p^2 + a_1p^3 + \cdots + (i+1)p^{2i} + a_ip^{2i+1} + \cdots + (r+1)p^{2r} + a_rp^{2r+1}.$$

D.h. $(1, a_0, 2, a_1, \ldots, (i+1), a_i, \ldots, (r+1), a_r)$ ist die Darstellung von t zur Basis p.

Behauptung: Für alle $a \in \mathbb{N}$ und alle $0 \leq i \leq r$ gilt $a = a_i$ genau dann, wenn es $b_0, b_1, b_2 \in \mathbb{N}$ gibt mit:

(a) $t = b_0 + b_1((i+1) + ap + b_2p^2)$

(b) $a < p$

(c) $b_0 < b_1$

(d) Es gibt ein m mit $b_1 = p^{2m}$.

Unentscheidbarkeit der Arithmetik

$\Rightarrow$: Wenn $a = a_i$ dann können wir b_0, b_1, b_2 wie folgt wählen:

$$\begin{aligned} b_0 &= 1p^0 + a_0p^1 + 2p^2 + a_1p^3 + \cdots + ip^{2i-2} + a_{i-1}p^{2i-1} \\ b_1 &= p^{2i} \\ b_2 &= (i+2) + a_{i+1}p + \cdots + a_rp^{2(r-i)-1} \end{aligned}$$

$\Leftarrow$: Gelte (a)-(d), d.h.

$$\begin{aligned} t &= b_0 + b_1((i+1) + ap + b_2p^2) \\ &= b_0 + (i+1)p^{2m} + ap^{2m+1} + p^{2m+2}b_2. \end{aligned}$$

wobei $b_0 < b_1 = p^{2m}$, $a < p$ und $(i+1) < p$.

Ein Vergleich mit

$$t = 1p^0+a_0p^1+2p^2+a_1p^3+\cdots+(i+1)p^{2i}+a_ip^{2i+1}+\cdots+(r+1)p^{2r}+a_rp^{2r+1}$$

liefert $m = i$ und $a = a_i$.

Unentscheidbarkeit der Arithmetik

Da p eine Primzahl ist, ist (d) äquivalent zu: b_1 ist ein Quadrat, und für alle $d \geq 2$ mit $d|b_1$ gilt $p|d$.

Wir definieren nun für alle Zahlen $t, p, i \in \mathbb{N}$ die Zahl $\beta(t, p, i)$ als die kleinste Zahl a, so dass $b_0, b_1, b_2 \in \mathbb{N}$ existieren mit:

(a) $t = b_0 + b_1((i+1) + ap + b_2p^2)$,

(b) $a < p$,

(c) $b_0 < b_1$,

(d) b_1 ist ein Quadrat, und für alle $d \geq 2$ mit $d|b_1$ gilt $p|d$.

Sollten solche Zahlen $b_0, b_1, b_2 \in \mathbb{N}$ nicht existieren, so setzen wir $\beta(t, p, i) = 0$.

Aus der gerade gezeigten Behauptung folgt dann: Für jede Folge $(a_0, \ldots, a_r)$ über $\mathbb{N}$ gibt es $t, p \in \mathbb{N}$, so dass $\beta(t, p, i) = a_i$ für alle $0 \leq i \leq r$.

Außerdem ist β offensichtlich arithmetisch definierbar. □

Unentscheidbarkeit der Arithmetik

Wir können nun den Beweis für die Unentscheidbarkeit der Arithmetik beenden.

Wir müssen folgende Aussage durch eine arithmetische Formel (mit freien Variablen $x, x_1, \ldots, x_l$) ausdrücken:

Es gibt ein s und ein Tupel
$(y_0, y_1, \ldots, y_{k-1},\ y_k, y_{k+1}, \ldots, y_{2k-1}, \ldots, y_{sk}, y_{sk+1}, \ldots, y_{(s+1)k-1})$ mit:

- $y_0 = 1,\ y_1 = 0, \ldots, y_{k-1} = 0$
- $y_{sk} = x,\ y_{sk+1} = x_1, \ldots, y_{(s+1)k-1} = x_l$
- $(y_{ik}, \ldots, y_{(i+1)k-1}) \to_P (y_{(i+1)k}, \ldots, y_{(i+2)k-1})$ für alle $0 \leq i \leq s-1$

Beachte: $k = l + 1$ ist hierbei eine Konstante, die durch das RMP P festgelegt ist.

Unentscheidbarkeit der Arithmetik

Dies ist äquivalent zu: Es gibt s, t, p mit:

- $\beta(t, p, 0) = 1$, $\beta(t, p, 1) = 0$, $\ldots$, $\beta(t, p, k-1) = 0$
- $\beta(t, p, sk) = x$, $\beta(t, p, sk+1) = x_1, \ldots, \beta(t, p, (s+1)k-1) = x_l$
- Für alle $0 \leq i \leq s-1$ gilt:

$$\Big(\beta(t, p, ik), \ldots, \beta(t, p, (i+1)k-1)\Big) \to_P \Big(\beta(t, p, (i+1)k), \ldots, \beta(t, p, (i+2)k-1)\Big)$$

Eine arithmetische Formel für $(y, y_1, \ldots, y_l) \to_P (x, x_1, \ldots, x_l)$ ist einfach als Disjunktion über alle Anweisungen A_i des RMPs P anzugeben (Übung). □

Automatische Strukturen

Wir werden im folgenden automatische Strukturen einführen.

Die Hauptresultate zu automatische Strukturen, die wir beweisen, sind:

- Jede automatische Struktur hat eine entscheidbare Theorie.
- $(\mathbb{N}, +)$ ist automatisch.
- $(\mathbb{Q}, \leq)$ ist automatisch.

Konvolution von Wörtern

Sei $n \geq 1$. Sei Σ ein endliches Alphabet und sei $\# \notin \Sigma$.

Sei $\Sigma_\# = \Sigma \cup \{\#\}$ im Weiteren.

Seien $w_1, w_2 \ldots, w_n \in \Sigma^*$. Wir definieren die Konvolution

$$w_1 \otimes w_2 \otimes \cdots \otimes w_n \in \left(\Sigma_\#^n\right)^*$$

wie folgt:

- Sei $w_i = a_{i,1} a_{i,2} \cdots a_{i,\ell_i}$, d.h. $\ell_i = |w_i|$.
- Sei $\ell = \max\{\ell_1, \ldots, \ell_n\}$
- Für alle $1 \leq i \leq n$ und $\ell_i < j \leq \ell$ sei $a_{i,j} = \#$
- $w_1 \otimes w_2 \otimes \cdots \otimes w_n := (a_{1,1}, \ldots, a_{n,1})(a_{1,2}, \ldots, a_{n,2}) \cdots (a_{1,\ell}, \ldots, a_{n,\ell})$.

Beispiel: $abba \otimes babaaa = (a,b)(b,a)(b,b)(a,a)(\#,a)(\#,a)$

Synchrone Mehrbandautomaten

Ein synchroner n-Bandautomat A über dem Alphabet Σ ist ein gewöhnlicher endlicher Automat über dem Alphabet $\Sigma_{\#}^n$.

$\rightsquigarrow \; L(A) \subseteq \left(\Sigma_{\#}^n\right)^*$.

Es sei $K(A) = \{(w_1, \ldots, w_n) \mid w_1, \ldots, w_n \in \Sigma^*, w_1 \otimes \cdots \otimes w_n \in L(A)\}$.

Eine n-stellige Relation R über Σ^* ist synchron-rational, falls ein synchroner n-Bandautomat A mit $K(A) = R$ existiert.

Beachte: Elemente in $L(A)$ die nicht zu $\{w_1 \otimes \cdots \otimes w_n \mid w_1, \ldots, w_n \in \Sigma^*\}$ gehören, haben keinen Einfluss auf die Relation $K(A)$ (es handelt sich sozusagen um Müll).

Man kann aus A jedoch leicht einen synchronen n-Bandautomaten B mit $L(B) = L(A) \cap \{w_1 \otimes \cdots \otimes w_n \mid w_1, \ldots, w_n \in \Sigma^*\}$ konstruieren.

Beachte: $\{w_1 \otimes \cdots \otimes w_n \mid w_1, \ldots, w_n \in \Sigma^*\} \subseteq \left(\Sigma_{\#}^n\right)^*$ ist regulär.

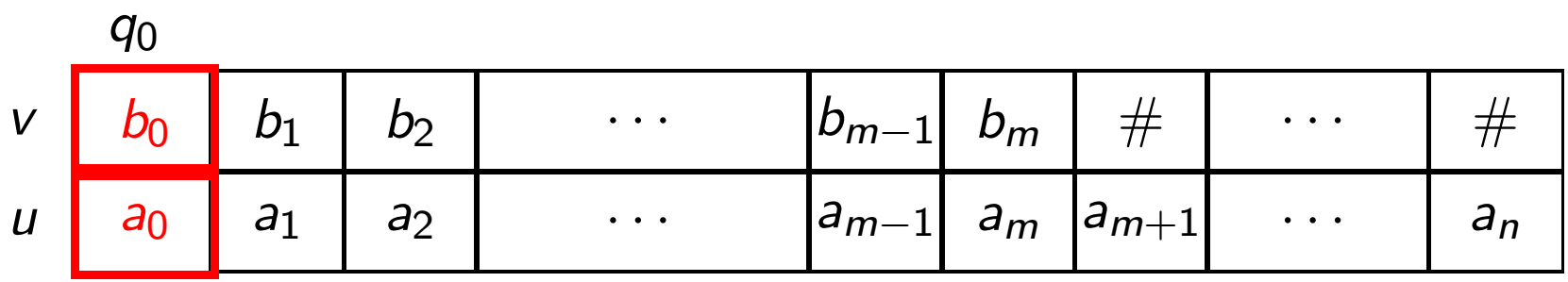
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:

v	b_0	b_1	b_2	$\cdots$	b_{m-1}	b_m	$\#$	$\cdots$	$\#$
u	a_0	a_1	a_2	$\cdots$	a_{m-1}	a_m	a_{m+1}	$\cdots$	a_n

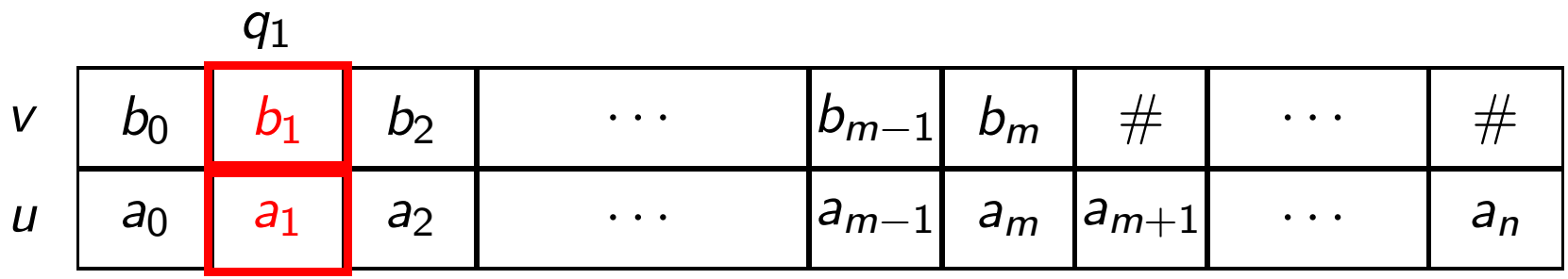
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



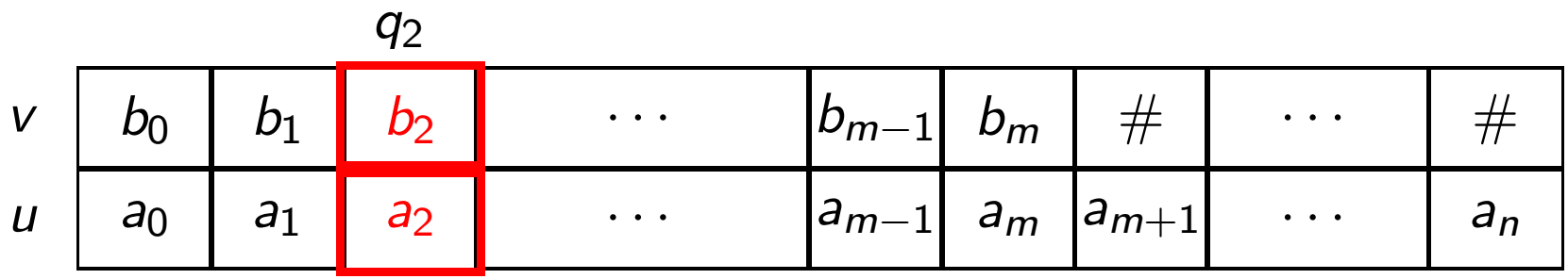
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



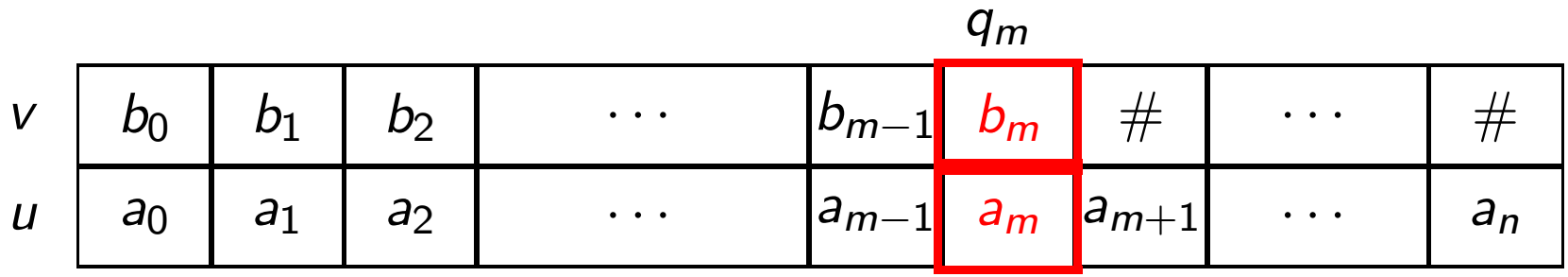
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



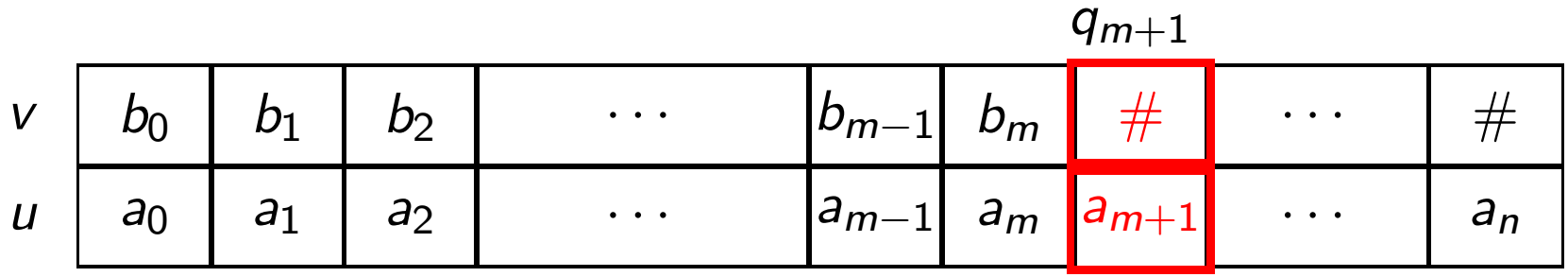
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



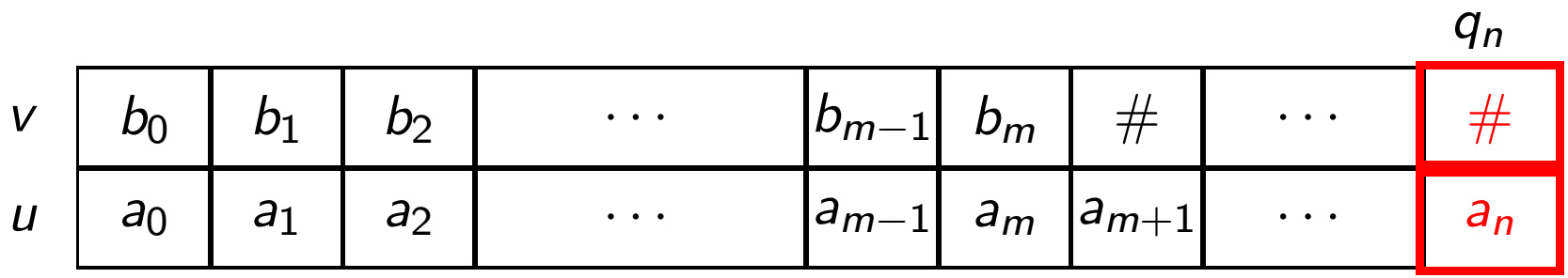
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



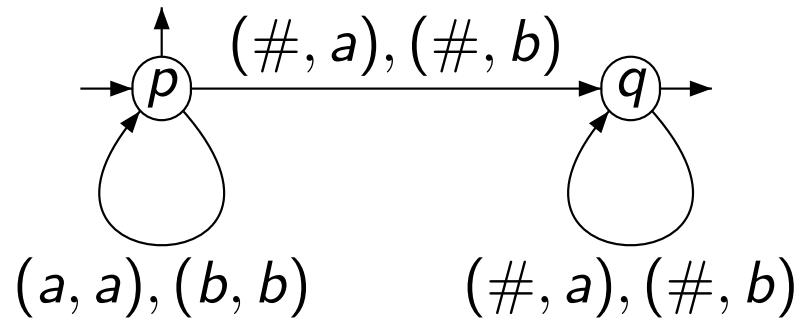
Synchrone Mehrbandautomaten

Veranschaulichung der Arbeitsweise eines synchronen Mehrbandautomaten:



Synchrone Mehrbandautomaten

Beispiel 1: Sei A der folgende synchrone 2-Bandautomat:



Es gilt $K(A) = \{(u, v) \mid u, v \in \{a, b\}^*, u \text{ ist Präfix von } v\}$.

Automatische Strukturen

Definition

Eine relationale Struktur $\mathcal{A} = (A, R_1, \ldots, R_m)$ (wobei R_i eine n_i-stellige Relation ist) ist automatisch, falls ein endliches Alphabet Σ, ein endlicher Automat B über dem Alphabet Σ und synchrone n_i-Bandautomaten B_i über dem Alphabet Σ $(1 \leq i \leq m)$ existieren mit:

- $L(B) = A$
- $K(B_i) = R_i$ für $1 \leq i \leq m$

Definition

Eine Struktur $\mathcal{A}$ ist automatisch präsentierbar, falls $\mathcal{A}$ isomorph zu einer automatischen Struktur ist.

$(\mathbb{N}, +)$ ist automatisch

Satz

$(\mathbb{N}, +)$ mit $+ = \{(a, b, c) \mid a + b = c\}$ ist automatisch präsentierbar.

Beweis: Sei A ein endlicher Automat mit $L(A) = \{0\} \cup \{0, 1\}^* 1$.

Dann ist die folgende Abbildung $h : L(A) \to \mathbb{N}$ eine Bijektion:

$$h(w) = \text{die durch } w \text{ repräsentierte Binärzahl, rückwärts gelesen}$$

Sei B_+ der synchrone 3-Bandautomat auf der nächsten Folie.

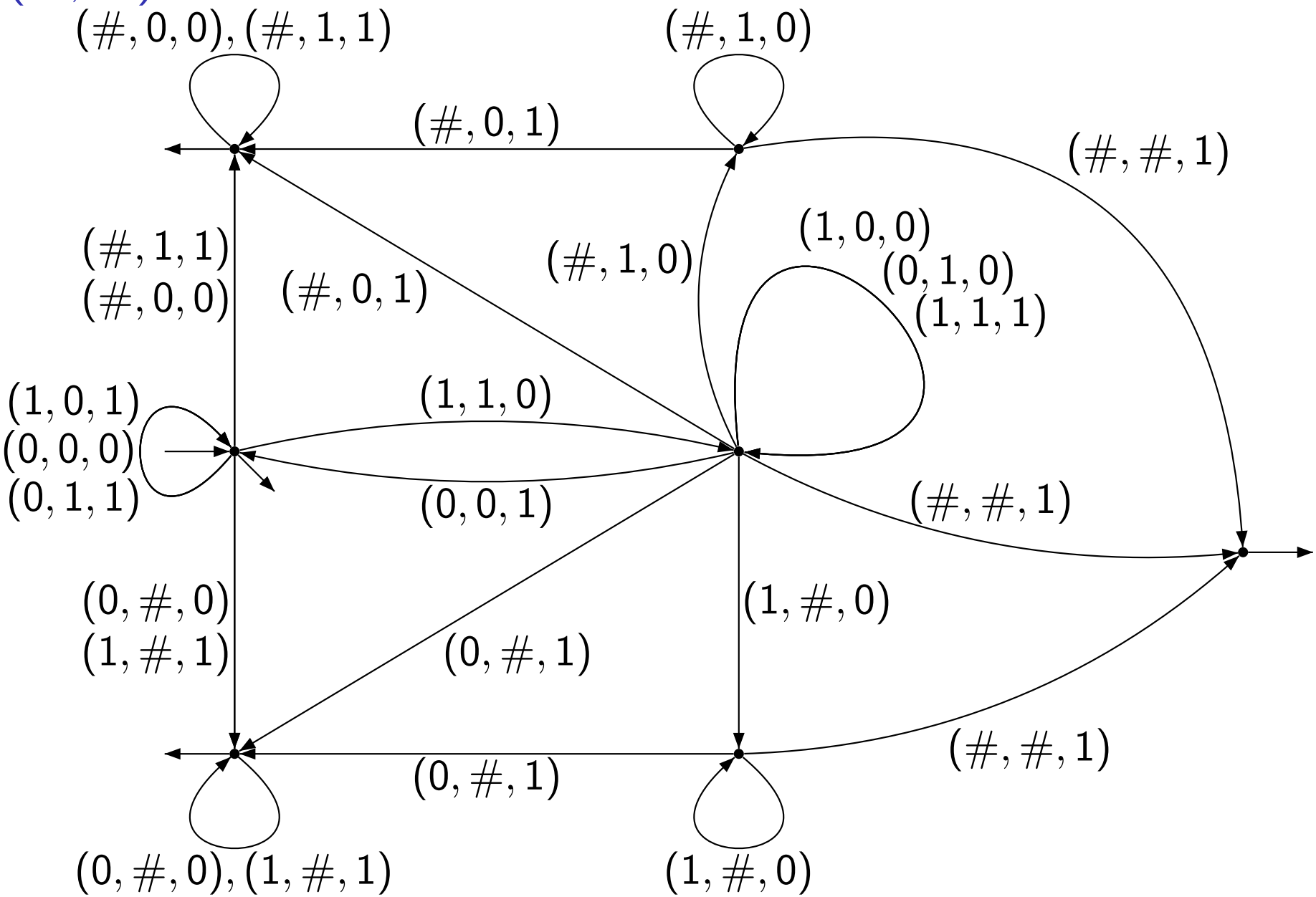
B_+ erkennt "fast" die Relation $\{(u, v, w) \in L(A)^3 \mid h(u) + h(v) = h(w)\}$, es gilt z. B. $(00, 0000, 0000) \in K(B_+)$.

Sei A_+ ein synchroner 3-Bandautomat mit

$$L(A_+) = L(B_+) \cap \{u \otimes v \otimes w \mid u, v, w \in L(A)\}.$$

Dann gilt $K(A_+) = \{(u, v, w) \in L(A)^3 \mid h(u) + h(v) = h(w)\}$. □

$(\mathbb{N}, +)$ ist automatisch



Weitere Beispiele

Man kann den vorherigen Satz noch erweitern: Sei $p > 1$ und $(\mathbb{N}, +, |_p)$, wobei $x |_p y$ genau dann, wenn $\exists n, k \in \mathbb{N} : x = p^n,\ y = k \cdot x$, ist automatisch präsentierbar.

Satz

$(\mathbb{Q}, \leq)$ ist automatisch präsentierbar.

Für den Beweis benutzen wir den Satz von Cantor.

Eine lineare Ordnung $(A, \leq)$ ist dicht falls gilt:

$$\forall x \forall y (x < y \rightarrow \exists z (x < z < y)).$$

Satz von Cantor

Seien $(A, \leq_A)$ und $(B, \leq_B)$ zwei abzählbare dichte lineare Ordnungen ohne kleinstes Element und ohne größtes Element. Dann sind $(A, \leq_A)$ und $(B, \leq_B)$ isomorph.

Satz von Cantor

Beweis des Satzes von Cantor:

Wir konstruieren Auflistungen

$$a_1, a_2, a_3, a_4, \ldots \text{ und } b_1, b_2, b_3, b_4, \ldots$$

mit folgenden Eigenschaften:

- $a_i \neq a_j$ und $b_i \neq b_j$ für $i \neq j$
- $A = \{a_i \mid i \geq 1\}$ und $B = \{b_i \mid i \geq 1\}$
- $a_i < a_j$ genau dann wenn $b_i < b_j$ für alle i, j.

Dann ist $f : A \to B$ mit $f(a_i) = b_i$ ein Isomorphismus.

Da A und B abzählbar unendlich sind, können wir beide Mengen auflisten:

$$A = \{x_1, x_2, x_3, \ldots\} \text{ und } B = \{y_1, y_2, y_3, \ldots\}$$

Der folgende "Algorithmus" konstruiert die Auflistungen:

Satz von Cantor

$L_A := [x_1, x_2, x_3, \ldots]$; $L_B := [y_1, y_2, y_3, \ldots]$
for all $i \geq 1$ **do** ($a_1, \ldots a_{i-1}$, $b_1, \ldots b_{i-1}$ sind bereits definiert)
  if i ist ungerade **then**
    sei x das erste Element aus L_A
    entferne x aus der Liste L_A
    sei y ein Element aus L_B mit folgender Eigenschaft:
    $\forall 1 \leq j \leq i-1 : a_j < x \longleftrightarrow b_j < y$
    entferne y aus der Liste L_B
    $a_i := x$; $b_i := y$
  else
    sei y das erste Element aus L_B
    entferne y aus der Liste L_B
    sei x ein Element aus L_A mit folgender Eigenschaft:
    $\forall 1 \leq j \leq i-1 : a_j < x \longleftrightarrow b_j < y$
    entferne x aus der Liste L_A
    $a_i := x$; $b_i := y$
endfor

$(\mathbb{Q}, \leq)$ ist automatisch

Beweis, dass $(\mathbb{Q}, \leq)$ automatisch ist:

Auf Grund des Satzes von Cantor genügt es, eine abzählbare dichte automatische lineare Ordnung ohne kleinstes und größtes Element anzugeben.

Sei hierzu $L = \{0,1\}^*1$.

Sei $\leq$ die lexikographische Ordnung auf L, d.h. für $x, y \in L$ gilt $x \leq y$ genau dann, wenn einer der folgenden Fälle gilt:

- Es gibt ein $u \in \{0,1\}^*$ mit $y = xu$ (x ist Anfangsstück von y)
- Es gibt $z, u, v \in \{0,1\}^*$ mit $x = z0u$ und $y = z1v$.

Offensichtlich ist $(L, \leq)$ eine lineare Ordnung.

- $(L, \leq)$ hat kein größtes Element:

  Sei $x \in L$ beliebig. Dann gilt $x < x1 \in L$

$(\mathbb{Q}, \leq)$ ist automatisch

- $(L, \leq)$ hat kein kleinstes Element:
  Sei $x = u1 \in L$ beliebig. Dann gilt $u01 < u1 = x$
- $(L, \leq)$ ist dicht:

  Seien $x, y \in L$ mit $x < y$ beliebig.

  1. Fall: $x = u1$, $y = u1v1$:

  Dann gilt: $x = u1 < u10^{|v|+1}1 < u1v1 = y$

  2. Fall: $x = u0v1$, $y = u1w$:

  Dann gilt: $x = u0v1 < u01^{|v|+2} < u1w = y$
- $(L, \leq)$ ist automatisch: Übung □

Nicht automatisch präsentierbare Strukturen

Von den folgenden Strukturen kann man zeigen, dass sie nicht automatisch sind:

- $(\mathbb{R}, +)$ (denn jede automatische Struktur ist abzählbar)
- jede Struktur mit einer unentscheidbaren Theorie (siehe nächste Folie).

  Beispiele hierfür:

  - $(\mathbb{N}, +, \cdot)$ (Satz von Gödel)
  - $(\Sigma^*, \circ)$ (das freie Monoid über Σ) falls $|\Sigma| > 1$ (Quine 1946)

- $(\mathbb{N}, \cdot)$ und $(\mathbb{N}, |)$
- $(\mathbb{Q}, +)$ (Tsankov 2009)

Theorie einer automatischen Struktur

Unser Hauptresultat über automatische Strukturen lautet:

Satz (Khoussainov, Nerode 1994)

Für jede automatisch präsentierbare Struktur $\mathcal{A}$ ist $\mathrm{Th}(\mathcal{A})$ entscheidbar.

Korollar (Presburger 1929)

$\mathrm{Th}(\mathbb{N}, +)$ ist entscheidbar.

Korollar

$\mathrm{Th}(\mathbb{Q}, \leq)$ ist entscheidbar.

Theorie einer automatischen Struktur

Beweis des Satzes von Khoussainov und Nerode:

Sei $\mathcal{A} = (L, R_1, \ldots, R_m)$ eine automatische Struktur mit $L \subseteq \Sigma^*$.

Für jede Formel F mit höchstens den freien Variablen $x_1, \ldots, x_n$ werden wir durch Induktion einen synchronen n-Bandautomaten B_F konstuieren, so dass gilt:

$$K(B_F) = \{(w_1, \ldots, w_n) \in L^n \mid \mathcal{A}_{[x_1/w_1]\cdots[x_n/w_n]} \models F\}.$$

Theorie einer automatischen Struktur

Fall 1: $F = R_i(x_{i_1}, \ldots, x_{i_k})$, wobei $1 \leq i_1, \ldots, i_k \leq n$:

Definiere den Homomorphismus $f : \left(\Sigma_\#^n\right)^* \to \left(\Sigma_\#^k\right)^*$ wie folgt, wobei $a_1, \ldots, a_n \in \Sigma_\#$:

$$f(a_1, \ldots, a_n) = \begin{cases} \varepsilon & \text{falls } a_{i_1} = \cdots = a_{i_k} = \# \\ (a_{i_1}, \ldots, a_{i_k}) & \text{sonst} \end{cases}$$

Beachte: $f(w_1 \otimes \cdots \otimes w_n) = w_{i_1} \otimes \cdots \otimes w_{i_k}$ für alle $w_1, \ldots, w_n \in \Sigma^*$.

Sei B_i der synchrone k-Bandautomat für R_i. Aus B_i konstruieren wir nun einen n-Bandautomaten B_F mit

$$L(B_F) = f^{-1}(L(B_i)) \cap \{w_1 \otimes \cdots \otimes w_n \mid w_1, \ldots, w_n \in L\}.$$

Beachte: Die regulären Sprachen sind unter inversen Homomorphismen abgeschlossen.

Theorie einer automatischen Struktur

Fall 2: $F = (x_i = x_j)$, wobei $1 \leq i, j \leq n$:

Analog zu Fall 1, da $\{(v, v) \mid v \in L\}$ synchron rational ist.

Fall 3: $F = \neg G$:

IH $\rightsquigarrow$ n-Bandautomat B_G für G

Wir wählen dann B_F so, dass gilt:

$$L(B_F) = \{w_1 \otimes \cdots \otimes w_n \mid w_1, \ldots, w_n \in L\} \setminus L(B_G)$$

Fall 4: $F = G \vee H$, wobei F höchstens freie Variablen $x_1, \ldots, x_n$ enthält:

IH $\rightsquigarrow$ n-Bandautomaten B_G, B_H für G und H

Wir wählen dann B_F so, dass gilt:

$$L(B_F) = L(B_G) \cup L(B_H)$$

Theorie einer automatischen Struktur

Fall 5: $F = \exists x_{n+1} : G(x_1, \ldots, x_n, x_{n+1})$:

IH $\rightsquigarrow$ $(n+1)$-Bandautomat B_G für G

Definiere den Homomorphismus $f : \left(\Sigma_{\#}^{n+1}\right)^* \to \left(\Sigma_{\#}^{n}\right)^*$ wie folgt, wobei $a_1, \ldots, a_n, a_{n+1} \in \Sigma_{\#}$:

$$f(a_1, \ldots, a_n, a_{n+1}) = \begin{cases} \varepsilon & \text{falls } a_1 = \cdots = a_n = \# \\ (a_1, \ldots, a_n) & \text{sonst} \end{cases}$$

Beachte: $f(w_1 \otimes \cdots \otimes w_n \otimes w_{n+1}) = w_1 \otimes \cdots \otimes w_n$ für alle $w_1, \ldots, w_{n+1} \in \Sigma^*$.

Dann wählen wir für B_F einen n-Bandautomaten mit $L(B_F) = f(L(B_G))$.

Beachte: Die regulären Sprachen sind unter Homomorphismen abgeschlossen.

Dies beendet die Konstruktion von B_F.

Theorie einer automatischen Struktur

Sei nun F eine Aussage (keine freien Variablen).

O.B.d.A. können wir davon ausgehen, dass F von der Form $F = \exists x\, G(x)$ ist (wir können immer einen Dummy-$\exists$-Quantor hinzufügen).

Dann gilt: $\mathcal{A} \models F \iff L(B_G) \neq \emptyset$.

Letzteres ist entscheidbar, da Leerheit der von einem endlichen Automaten akzeptierten Sprache entscheidbar ist. $\square$

Theorie einer automatischen Struktur

Bemerkungen zur Komplexität:

Unser Algorithmus, der $F \in \mathrm{Th}(\mathcal{A})$ entscheidet, ist nicht sehr effzient.

Grund: Für jede Negation $\neg$ in F müssen wir einen Automaten komplementieren. Dies verursacht einen exponentiellen Blow-Up in der Automatengröße.

Die Laufzeit unseres Algorithmus ist deshalb in etwa $f_{|F|}(O(1))$, wobei $f_0(n) = n$ und $f_{i+1}(n) = 2^{f_i(n)}$ für $i \geq 0$.

Dies ist jedoch auch nicht vermeidbar:

Sei $T_2 = (\{0,1\}^*, S_0, S_1, \leq)$ wobei:

- $S_0 = \{(w, w0) \mid w \in \{0,1\}^*\}$
- $S_1 = \{(w, w1) \mid w \in \{0,1\}^*\}$
- $\leq = \{(w, wu) \mid w, u \in \{0,1\}^*\}$

Beachte: T_2 ist eine automatische Struktur.

Theorie einer automatischen Struktur

Meyer 1974

Es gibt kein $i \in \mathbb{N}$ und einen Algorithmus, der $\mathrm{Th}(T_2)$ korrekt entscheidet und dessen Laufzeit durch $f_i(n)$ (bei einer Eingabeformel der Länge n) beschränkt ist.

Man sagt auch: Es existiert kein elementarer Algorithmus für $\mathrm{Th}(T_2)$.

Es gibt jedoch viele Spezialfälle von automatischen Strukturen, für die ein elementarer Algorithmus zur Entscheidung der Theorie existiert.

Hier sind zwei Beispiele:

Oppen 1978

Es existiert ein Algorithmus, der $\mathrm{Th}(\mathbb{N}, +)$ in Zeit $2^{2^{2^{O(n)}}}$ entscheidet.

Entscheidbarkeit der reellen Arithmetik

Satz (Tarski 1948)

$\mathrm{Th}(\mathbb{R}, +, \cdot)$ ist entscheidbar.

Beweis:

Zunächst betrachten wir anstatt $\mathrm{Th}(\mathbb{R}, +, \cdot)$ die Theorie $\mathrm{Th}(\mathbb{R}, +, \cdot, <, 0, 1, -1)$.

Wir schreiben im Folgenden $\mathbb{R}$ für $(\mathbb{R}, +, \cdot, <, 0, 1, -1)$.

Quantorenelimination: Sei F eine prädikatenlogischen Formel mit den freien Variablen $y_0, \ldots, y_n$.
Wir konstruieren eine quantorenfreie Formel F' mit den freien Variablen $y_0, \ldots, y_n$, so dass gilt:

$$\forall a_0, \ldots, a_n \in \mathbb{R} : \mathbb{R}_{[y_0/a_0, \ldots, y_n/a_n]} \models F \iff \mathbb{R}_{[y_0/a_0, \ldots, y_n/a_n]} \models F'$$

Es genügt, dies für eine Formel $F = \exists x\, G$ zu zeigen, wobei G quantorenfrei ist.

Entscheidbarkeit der reellen Arithmetik

Außerdem können wir annehmen, dass G folgende Gestalt hat:

$$G \;=\; s(x, y_0, \ldots, y_n) = 0 \wedge \bigwedge_{i=1}^{m} t_i(x, y_0, \ldots, y_n) > 0,$$

wobei $s, t_1, \ldots, t_m \in \mathbb{Z}[x, y_0, \ldots, y_n]$.

Beachte hierzu:

- $\exists x(G_1 \vee G_2) \equiv (\exists x G_1) \vee (\exists x G_2)$
- $s_1 = s_2 \iff s_1 - s_2 = 0$
- $s_1 < s_2 \iff s_2 - s_1 > 0$
- $\neg(s = 0) \iff (s > 0 \vee -s > 0)$
- $\neg(s > 0) \iff (s = 0 \vee -s > 0)$
- $\bigwedge_{i=1}^{k} s_i = 0 \iff \sum_{i=1}^{k} s_i^2 = 0$

Entscheidbarkeit der reellen Arithmetik

Jedes der Polynome $s, t_1, \ldots, t_m$ können wir eindeutig schreiben als Summe

$$\sum_{i=0}^{d} p_i \cdot x^{a_i}$$

mit $a_0 < a_1 < \cdots < a_d$ und $p_1, \ldots, p_d \in \mathbb{Z}[y_0, \ldots, y_n]$.

Wir können nun jedes Koeffizientenpolynom p_i durch eine neue Variable z_i ersetzen, die in der Formel nur einmal verwendet wird.

Ist für die resultierende Formel eine quantorenfreie Formel konstruiert, so kann in dieser jede Variable z_i wieder durch das ursprüngliche Polynom p_i ersetzt werden.

Beispiel: $\exists x : z_0 + z_1 x^2 + z_2 x^3 = 0 \wedge z_3 x + z_4 x^2 > 0 \wedge z_5 + z_6 x^3 > 0$

Entscheidbarkeit der reellen Arithmetik

Seien $z_0, \ldots, z_n$ alle Koeffizientenvariablen in der Formel G.

Wir müssen für die z_i nur Werte $\neq 0$ betrachten:

Ersetze hierzu $\exists x\, G$ durch die Formel

$$\bigwedge_{I \subseteq \{0,\ldots,n\}} \left(\bigwedge_{i \in I} z_i = 0 \wedge \bigwedge_{i \notin I} z_i \neq 0 \;\rightarrow\; \exists x\, G_I \right)$$

Hier ist G_I die Formel die aus G entsteht, indem für alle $i \in I$ die Variable z_i (und damit das Monom $z_i x^a$) durch 0 ersetzt wird.

Angenommen, wir haben für jede Formel $F_I := \exists x\, G_I$ eine quantorenfreie Formel F_I' konstruiert mit:

$$\forall a_0, \ldots, a_n \in \mathbb{R} \setminus \{0\} : \mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models F_I \iff \mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models F_I'$$

Entscheidbarkeit der reellen Arithmetik

Dann sind für alle $a_0, \ldots, a_n \in \mathbb{R}$ folgende Aussagen äquivalent:

- $\mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models \exists x\, G$
- $\mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models \bigwedge_{I\subseteq\{0,\ldots,n\}} \left(\bigwedge_{i\in I} z_i = 0 \wedge \bigwedge_{i\notin I} z_i \neq 0 \;\rightarrow\; \exists x\, G_I \right)$
- $\mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models \bigwedge_{I\subseteq\{0,\ldots,n\}} \left(\bigwedge_{i\in I} z_i = 0 \wedge \bigwedge_{i\notin I} z_i \neq 0 \;\rightarrow\; F'_I \right)$

Zwischenstand: Für ein Formel $F = \exists x : s = 0 \wedge \bigwedge_{i=1}^{m} t_i > 0$ müssen wir eine quantorenfreie Formel F' konstruieren mit:

$$\forall a_0, \ldots, a_n \in \mathbb{R} \setminus \{0\} : \mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models F \iff \mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models F'$$

Dabei sind $s, t_1, \ldots, t_m$ Polynome in der Variablen x, und die Koeffizienten sind Parameter $z_0, \ldots, z_m$ die nur mit Werten $\neq 0$ belegt werden. Jeder Parameter z_i kommt in F nur einmal vor.

Ausserdem können wir voraussetzen: $t_i \neq 0$ für alle $1 \leq i \leq m$ und ($s = 0$ oder x kommt in s vor).

Entscheidbarkeit der reellen Arithmetik

Wir unterscheiden nun 3 Fälle:

- Fall 1: x kommt in s vor und $m = 1$
- Fall 2: x kommt in s vor und $m > 1$
- Fall 3: $s = 0$.

Fall 1: $G = (s = 0 \wedge t > 0)$, wobei x in s vorkommt.

Notation: Für $k \geq 0$ sei $(\#x : G) = k$ eine neue Formel mit:
Für alle $a_0, \ldots, a_n \in \mathbb{R} \setminus \{0\}$ gilt $\mathbb{R}_{[z_0/a_0,\ldots,z_n/a_n]} \models (\#x : G) = k$ g.d.w.

$$|\{a \in \mathbb{R} \mid \mathbb{R}_{[x/a,z_0/a_0,\ldots,z_n/a_n]} \models G\}| = k.$$

Beachte: Ist $d \geq 1$ der x-Grad von s, so ist $\exists x\, G$ in $\mathbb{R}$ äquivalent zu

$$(\#x : G) = 1 \vee (\#x : G) = 2 \vee \cdots \vee (\#x : G) = d$$

Neues Ziel: Finde eine quantorenfreie Formel, welche in $\mathbb{R}$ äquivalent ist zu $(\#x : G) = k$.

Entscheidbarkeit der reellen Arithmetik

Unser Hilfsmittel sind sogenannte Sturmfolgen.

Für $\overline{a} = (a_1, \ldots, a_n) \in (\mathbb{R} \setminus \{0\})^n$ sei

$$\mathrm{Var}(\overline{a}) = |\{i < n \mid a_i a_{i+1} < 0\}|$$

(Anzahl der Vorzeichenwechsel).

Für $\overline{a} \in \mathbb{R}^n$ sei $\mathrm{Var}(\overline{a}) = \mathrm{Var}(\overline{b})$, wobei $\overline{b}$ aus $\overline{a}$ durch Löschen aller Nullen entsteht.

Für $\overline{f} = (f_1, \ldots, f_n) \in (\mathbb{R}[x])^n$ und $a \in \mathbb{R}$ sei

$$\mathrm{Var}_a(\overline{f}) = \mathrm{Var}(f_1(a), \ldots, f_n(a)).$$

Entscheidbarkeit der reellen Arithmetik

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$. Definiere die Polynome $h_0(x), \ldots, h_n(x)$ eindeutig wie folgt (Euklidischer Algorithmus):

$$\begin{aligned}
h_0(x) &= f(x), \qquad h_1(x) = g(x) \\
h_0(x) &= q_1(x)h_1(x) - h_2(x) \qquad \deg(h_2) < \deg(h_1) \\
h_1(x) &= q_2(x)h_2(x) - h_3(x) \qquad \deg(h_3) < \deg(h_2) \\
&\vdots \\
h_{n-1}(x) &= q_n(x)h_n(x)
\end{aligned}$$

Dann gilt:

- $h_n(x) = \mathrm{ggT}(f, g)$
- Für alle $0 \leq i \leq n$ ist das Polynom $h_n(x)$ ein Teiler von $h_i(x)$.

Dann ist $[f, g] = (h_0(x), h_1(x), \ldots, h_n(x))$ die Sturmfolge von f und g.

Entscheidbarkeit der reellen Arithmetik

Die gekürzte Sturmfolge von f und g ist

$$\left(\frac{h_0(x)}{h_n(x)}, \frac{h_1(x)}{h_n(x)}, \ldots, \frac{h_{n-1}(x)}{h_n(x)}, 1\right).$$

Für eine quantorenfreie Formel H mit der einzigen freien Variablen x und $a, b \in \mathbb{R}$ mit $a < b$ sei

$$(\#x : H)_a^b = |\{c \in (a, b) \mid \mathbb{R}_{[x/c]} \models H\}|.$$

Mit $f'(x)$ bezeichnen wir die formale Ableitung des Polynoms $f(x) \in \mathbb{R}[x]$.

Satz von Sturm und Tarski

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$, $f' \neq 0$, $\mathrm{ggT}(f, g) = \mathrm{ggT}(f, f') = 1$, $a, b \in \mathbb{R}$, $a < b$, $f(a) \neq 0 \neq f(b)$. Dann gilt

$$(\#x : f(x) = 0 \wedge g(x) > 0)_a^b - (\#x : f(x) = 0 \wedge g(x) < 0)_a^b = \mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]).$$

Entscheidbarkeit der reellen Arithmetik

Für den Beweis des Satzes von Sturm und Tarski benötigen wir zwei Lemmata.

Lemma A

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$, $a, b \in \mathbb{R}$, $a < b$, und $\forall c \in [a, b] : f(c) \neq 0$. Dann gilt $\mathrm{Var}_a([f, g]) = \mathrm{Var}_b([f, g])$.

Beweis von Lemma A: Sei

$$[f, g] = S = (h_0, h_1, \ldots, h_s)$$

und sei

$$\tilde{S} = (\tilde{h}_0, \tilde{h}_1, \ldots, \tilde{h}_s)$$

die gekürzte Sturmfolge, d.h. $\tilde{h}_s = 1$ und $\tilde{h}_i = \frac{h_i}{h_s}$.

Sei $N = \{c \in [a, b] \mid \exists 0 \leq i \leq s : \tilde{h}_i(c) = 0\}$.

Dann ist N endlich.

Sei $[a', b'] \subseteq [a, b]$ ein Intervall mit $|N \cap [a', b']| \leq 1$.

Entscheidbarkeit der reellen Arithmetik

Es genügt folgende Behauptung zu zeigen:

$$\mathrm{Var}_{a'}([f,g]) = \mathrm{Var}_{b'}([f,g]).$$

Fall 1: Kein $\tilde{h}_i$ hat eine Nullstelle in $[a', b']$.

Nach dem Zwischenwertsatz gilt $\tilde{h}_i(a') \cdot \tilde{h}_i(b') > 0$ für alle $0 \leq i \leq s$.

Also gilt $\mathrm{Var}_{a'}(S') = \mathrm{Var}_{b'}(S')$.

Wegen $h_s(a') \neq 0 \neq h_s(b')$ (denn $f(a') \neq 0 \neq f(b')$ und $h_s = \mathrm{ggT}(f,g)$ ist Teiler von f) folgt

$$\mathrm{Var}_{a'}(S) = \mathrm{Var}_{a'}(S') = \mathrm{Var}_{b'}(S') = \mathrm{Var}_{b'}(S).$$

Entscheidbarkeit der reellen Arithmetik

Fall 2: Mindestens ein $\tilde{h}_i$ hat eine Nullstelle $c \in [a', b']$, d.h. $N \cap [a', b'] = \{c\}$.

Wegen $\tilde{h}_s = 1$ und der Annahme, dass $f = h_0$ keine Nullstelle in $[a, b]$ hat (damit hat auch $\tilde{h}_0$ keine Nullstelle in $[a, b]$) gilt $1 \leq i \leq s - 1$.

Es gilt $\tilde{h}_{i-1}(c) = q_i(c)\tilde{h}_i(c) - \tilde{h}_{i+1}(c) = -\tilde{h}_{i+1}(c)$.

Würde $\tilde{h}_{i+1}(c) = 0 = \tilde{h}_i(c)$ gelten, so wäre $\tilde{h}_j(c) = 0$ für alle $j \geq i$, was $\tilde{h}_s = 1$ widerspricht.

Also gilt $\tilde{h}_{i+1}(c) \neq 0$ und damit

$$\tilde{h}_{i-1}(c)\tilde{h}_{i+1}(c) = -(\tilde{h}_{i+1}(c))^2 < 0,$$

d.h. $\tilde{h}_{i-1}(c)$ und $\tilde{h}_{i+1}(c)$ haben verschiedene Vorzeichen.

Da $\tilde{h}_{i-1}$ und $\tilde{h}_{i+1}$ keine Nullstelle in $[a', b']$ haben, gilt

$$\tilde{h}_{i-1}(a')\tilde{h}_{i+1}(a') < 0 \quad \text{und} \quad \tilde{h}_{i-1}(b')\tilde{h}_{i+1}(b') < 0.$$

Entscheidbarkeit der reellen Arithmetik

Es folgt:

$$\begin{aligned}
\mathrm{Var}_{a'}(S') &= \mathrm{Var}(\tilde{h}_0(a'), \ldots, \tilde{h}_{i-1}(a'), \tilde{h}_i(a'), \tilde{h}_{i+1}(a'), \ldots, \tilde{h}_s(a')) \\
&= \mathrm{Var}(\tilde{h}_0(a'), \ldots, \tilde{h}_{i-1}(a'), \tilde{h}_{i+1}(a'), \ldots, \tilde{h}_s(a')) \\
\mathrm{Var}_{b'}(S') &= \mathrm{Var}(\tilde{h}_0(b'), \ldots, \tilde{h}_{i-1}(b'), \tilde{h}_i(b'), \tilde{h}_{i+1}(b'), \ldots, \tilde{h}_s(b')) \\
&= \mathrm{Var}(\tilde{h}_0(b'), \ldots, \tilde{h}_{i-1}(b'), \tilde{h}_{i+1}(b'), \ldots, \tilde{h}_s(b'))
\end{aligned}$$

Auf diese Weise können wir für alle j mit $\tilde{h}_j(c) = 0$ die Einträge $\tilde{h}_j(a')$ und $\tilde{h}_j(b')$ eliminieren.

Wir erhalten somit

$$\begin{aligned}
\mathrm{Var}_{a'}(S') &= \mathrm{Var}(g_0(a'), \ldots, g_t(a')) \\
\mathrm{Var}_{b'}(S') &= \mathrm{Var}(g_0(b'), \ldots, g_t(b'))
\end{aligned}$$

wobei die Polynome $g_0, \ldots, g_t$ keine Nullstelle in $[a', b']$ haben.

Entscheidbarkeit der reellen Arithmetik

Also gilt:

$$\begin{aligned} \mathrm{Var}_{a'}(S) = \mathrm{Var}_{a'}(S') &= \mathrm{Var}(g_0(a'), \ldots, g_t(a')) \\ &= \mathrm{Var}(g_0(b'), \ldots, g_t(b')) = \mathrm{Var}_{b'}(S') = \mathrm{Var}_{b'}(S) \end{aligned}$$

□

Lemma B

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$, $f' \neq 0$, $\mathrm{ggT}(f, g) = \mathrm{ggT}(f, f') = 1$, $a, b, c \in \mathbb{R}$, $a < c < b$, $f(c) = 0$, $\forall d \in [a, b] \setminus \{c\} : f(d) \neq 0$. Dann gilt

$$\mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]) = \begin{cases} 1 & \text{falls } g(c) > 0 \\ -1 & \text{falls } g(c) < 0 \end{cases}$$

Entscheidbarkeit der reellen Arithmetik

Beweis von Lemma B:

Wegen $\mathrm{ggT}(f, g) = \mathrm{ggT}(f, f') = 1$ haben f und g keine gemeinsamen Nullstellen, und f hat keine mehrfache Nullstelle.

Insbesondere gilt $g(c) \neq 0$ und es gibt ein Polynom $h(x)$ mit $f(x) = (x - c) \cdot h(x)$, $h(c) \neq 0$.

Also gilt $f\, f'\, g = (x - c) \cdot \underbrace{(h^2 g + (x - c)\, h\, h'\, g)}_{u(x)}$.

Sei $[f, f'g] = (f, f'g, h_2, \ldots, h_s)$ mit $s \geq 1$.

Gelte $g(c) > 0$ (der Fall $g(c) < 0$ kann analog analysiert werden).

Es gilt $u(c) = (h(c))^2 g(c) > 0$ und $f'g(c) \neq 0$.

Also gibt es $a' < b'$ mit $a \leq a' < c$, $c < b' \leq b$ und $\forall x \in [a', b'] : u(x) > 0$ und $f'g(x) \neq 0$.

Es folgt $f(a') \cdot f'g(a') < 0$ und $f(b') \cdot f'g(b') > 0$.

Entscheidbarkeit der reellen Arithmetik

Wir erhalten damit im Fall $s \geq 2$:

$$\begin{aligned}
\mathrm{Var}_a([f, f'g]) &\overset{\text{Lemma A}}{=} \mathrm{Var}_{a'}([f, f'g]) \\
&= 1 + \mathrm{Var}_{a'}([f'g, h_2]) \\
&\overset{\text{Lemma A}}{=} 1 + \mathrm{Var}_{b'}([f'g, h_2]) \\
&= 1 + \mathrm{Var}_{b'}([f, f'g]) \\
&\overset{\text{Lemma A}}{=} 1 + \mathrm{Var}_{b}([f, f'g])
\end{aligned}$$

Im Fall $s = 1$ (d.h. $[f, f'g] = (f, f'g)$) gilt

$$\begin{aligned}
\mathrm{Var}_a([f, f'g]) &\overset{\text{Lemma A}}{=} \mathrm{Var}_{a'}([f, f'g]) \\
&= 1 \\
&= 1 + \mathrm{Var}_{b'}([f, f'g]) \\
&\overset{\text{Lemma A}}{=} 1 + \mathrm{Var}_{b}([f, f'g])
\end{aligned}$$

Entscheidbarkeit der reellen Arithmetik

Beweis des Satzes von Tarski und Sturm:

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$, $f' \neq 0$, $\mathrm{ggT}(f, g) = \mathrm{ggT}(f, f') = 1$, $a, b \in \mathbb{R}$, $a < b$, $f(a) \neq 0 \neq f(b)$.

Sei $N = \{c \in (a, b) \mid f(c) = 0\}$ (endlich).

Falls $N = \emptyset$ gilt wegen Lemma A:

$$(\#x : f(x) = 0 \wedge g(x) > 0)_a^b - (\#x : f(x) = 0 \wedge g(x) < 0)_a^b = 0 = \mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]).$$

Sei nun $N = \{c_1, c_2, \ldots, c_n\}$ mit $n \geq 1$.

Wähle Punkte $a = a_0 < c_1 < a_1 < c_2 < a_2 < \cdots < a_{n-1} < c_n < a_n = b$.

Entscheidbarkeit der reellen Arithmetik

Dann gilt wegen Lemma B für alle $1 \leq i \leq n$:

$$\mathrm{Var}_{a_{i-1}}([f, f'g]) - \mathrm{Var}_{a_i}([f, f'g]) = \begin{cases} 1 & \text{falls } g(c_i) > 0 \\ -1 & \text{falls } g(c_i) < 0 \end{cases}$$

Aufsummieren ergibt

$$\mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]) =$$
$$(\#x : f(x) = 0 \wedge g(x) > 0)_a^b - (\#x : f(x) = 0 \wedge g(x) < 0)_a^b$$

Dies beendet den Beweis des Satzes von Tarski und Sturm. □

Entscheidbarkeit der reellen Arithmetik

Korollar aus dem Satz von Tarski und Sturm

Seien $f, g \in \mathbb{R}[x] \setminus \{0\}$, $f' \neq 0$, $\mathrm{ggT}(f, g) = \mathrm{ggT}(f, f') = 1$, $a, b \in \mathbb{R}$, $a < b$, $f(a) \neq 0 \neq f(b)$. Dann gilt

$$\begin{aligned} &\#x(f(x) = 0 \wedge g(x) > 0)_a^b \\ &= \frac{1}{2}(\mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]) + \mathrm{Var}_a([f, f']) - \mathrm{Var}_b([f, f'])). \end{aligned}$$

Beweis: Nach dem Satz von Tarski und Sturm gilt:

$$\begin{aligned} &(\#x : f(x) = 0 \wedge g(x) > 0)_a^b - (\#x : f(x) = 0 \wedge g(x) < 0)_a^b \\ &= \mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]). \end{aligned}$$

Entscheidbarkeit der reellen Arithmetik

sowie (da f und g keine gemeinsame Nullstelle haben)

$$\begin{aligned}
&(\#x : f(x) = 0 \wedge g(x) > 0)_a^b + (\#x : f(x) = 0 \wedge g(x) < 0)_a^b \\
&= (\#x : f(x) = 0)_a^b = \\
&= (\#x : f(x) = 0 \wedge 1 > 0)_a^b - (\#x : f(x) = 0 \wedge 1 < 0)_a^b \\
&= \mathrm{Var}_a([f, f']) - \mathrm{Var}_b([f, f']).
\end{aligned}$$

Addieren der beiden Gleichungen ergibt:

$$\begin{aligned}
&2 \cdot \#x(f(x) = 0 \wedge g(x) > 0)_a^b \\
&= \mathrm{Var}_a([f, f'g]) - \mathrm{Var}_b([f, f'g]) + \mathrm{Var}_a([f, f']) - \mathrm{Var}_b([f, f'])
\end{aligned}$$

□

Entscheidbarkeit der reellen Arithmetik

Wir brauchen auch noch Cauchys Schranke für die Nullstellen eines Polynoms.

Lemma (Cauchys Schranke für Nullstellen eines Polynoms)

Sei $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$, $a_m \neq 0$. Dann liegen alle Nullstellen von f im Intervall $(-c, c)$ mit

$$c = 1 + \frac{\max\{|a_0|, \ldots, |a_{m-1}|\}}{|a_m|}.$$

Beweis:

Indem wir $f(x)$ durch das Polynom $x^m + \frac{a_{m-1}}{a_m} x^{m-1} + \cdots + \frac{a_1}{a_m} x + \frac{a_0}{a_m}$ ersetzen, genügt es, Cauchys Schranke für den Fall $a_m = 1$ zu zeigen.

Entscheidbarkeit der reellen Arithmetik

Sei also $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ und

$$h = \max\{|a_i| \mid 0 \leq i \leq m-1\}.$$

Gelte $f(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$, d.h.

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha - a_0.$$

Zu zeigen: $|\alpha| < 1 + h$.

Wenn $|\alpha| \leq 1$ gilt, gilt auch $|\alpha| < 1 + h$ (falls $h = 0$ muss $\alpha = 0$ gelten).

Gelte also $|\alpha| > 1$.

Entscheidbarkeit der reellen Arithmetik

Es folgt:

$$\begin{aligned} |\alpha|^m &\leq |a_{m-1}| \cdot |\alpha|^{m-1} + \cdots + |a_1| \cdot |\alpha| + |a_0| \\ &\leq h \cdot (|\alpha|^{m-1} + \cdots + |\alpha| + 1) \\ &= h \cdot \frac{|\alpha|^m - 1}{|\alpha| - 1} \end{aligned}$$

Da $|\alpha| > 1$ gilt, folgt:

$$|\alpha| - 1 \leq h \cdot \frac{|\alpha|^m - 1}{|\alpha|^m} < h$$

□

Entscheidbarkeit der reellen Arithmetik

Wir kommen nun zurück zu Fall 1.

Erinnerung: Wir müssen eine quantorenfreie arithmetische Formel für $(\#x : s = 0 \wedge t > 0) = k$ finden, wobei $s \neq 0 \neq t$ und (o.B.d.A.) $s = z_0 + z_1 x + \cdots z_{m-1} x^m$, $t = z_{m+1} + z_{m+2} x + \cdots z_n x^{n-m-1}$ $m \geq 1$.

Wegen Cauchys Schranke genügt es für $(\#x : s = 0 \wedge t > 0)_y^z = k$ eine quantorenfreie Formel in den freien Variablen $y, z, z_0, \ldots, z_n$ zu finden.

In dieser Formel können wir dann y durch $-\frac{|z_m| + \max\{|z_0|,\ldots,|z_{m-1}|\}}{|z_m|}$ und z durch $\frac{|z_m| + \max\{|z_0|,\ldots,|z_{m-1}|\}}{|z_m|}$ ersetzen.

Beachte: Wir "wissen", dass $z_m \neq 0$ gilt.

Anwendungen von $|\cdot|$ und max können mittels einer Fallunterscheidung (ähnlich zu Folie 63 eliminiert werden.

Anwendungen von $\frac{\cdot}{|z_m|}$ (im Fall $z_m \neq 0$) können durch Multiplizieren mit genügend großen Potenzen von z_m eliminiert werden.

Entscheidbarkeit der reellen Arithmetik

Wir konstruieren eine quantorenfreie arithmetische Formel in den freien Variablen $y, z, z_0, \ldots, z_n$ für $(\#x : s = 0 \wedge t > 0)_y^z = k$ mittels des Satzes von Sturm und Tarski (Korollar hiervon).

Beachte: Es gilt $s \neq 0 \neq t$ und $s' \neq 0$ (da der x-Grad von s mindestens 1 ist).

Problem: Wie stellen wir die Vorbedingung $\mathrm{ggT}(s, t) = \mathrm{ggT}(s, s') = 1$ sicher?

Beachte hierzu:

- $(\#x : s = 0 \wedge t > 0)_y^z = k$ gdw. $(\#x : s/\mathrm{ggT}(s, t) = 0 \wedge t > 0)_y^z = k$.
- $(\#x : s = 0 \wedge t > 0)_y^z = k$ gdw. $(\#x : s/\mathrm{ggT}(s, s') = 0 \wedge t > 0)_y^z = k$.

Entscheidbarkeit der reellen Arithmetik

Wir können daher s zunächst durch $r = s/\mathrm{ggT}(s,t)$ ersetzen, und dann r durch $r/\mathrm{ggT}(r,r')$ ersetzen.

Betrachten wir die Berechnung von $s/\mathrm{ggT}(s,t)$ genauer.

Die Koeffizienten der x-Polynome s und t sind die Parameter $z_i \neq 0$.

Wir lassen den Euklidischen Algorithmus symbolisch mit $s = z_0 + z_1 x + \cdots z_{m-1} x^m$ und $t = z_{m+1} + z_{m+2} x + \cdots z_n x^{n-m-1}$ laufen.

Entscheidbarkeit der reellen Arithmetik

Besipiel: $m = 2$, $n = 4$, d.h.

$$s(x) = z_0 + z_1 x + z_2 x^2 \text{ und } t(x) = z_3 + z_4 x$$

Dann gilt $(\#x : s = 0 \wedge t > 0)_y^z = k$ g.d.w. $(\#x : z_4^2 \cdot s = 0 \wedge t > 0)_y^z = k$.

Division mit Rest:

$$\begin{array}{l} (z_2 z_4^2 x^2 + z_1 z_4^2 x + z_0 z_4^2) : (z_4 x + z_3) = z_2 z_4 x + (z_1 z_4 - z_2 z_3) \\ \underline{-(z_2 z_4^2 x^2 + z_2 z_4 z_3 x)} \\ ((z_1 z_4^2 - z_2 z_4 z_3) x + z_0 z_4^2) \\ \underline{-((z_1 z_4^2 - z_2 z_4 z_3) x + (z_1 z_4 z_3 - z_2 z_3^2))} \\ z_0 z_4^2 - z_1 z_4 z_3 + z_2 z_3^2 \text{ (Rest)} \end{array}$$

Entscheidbarkeit der reellen Arithmetik

Also:

- Wenn $z_0 z_4^2 - z_1 z_4 z_3 + z_2 z_3^2 \neq 0$, dann gilt $\mathrm{ggT}(z_4^2 s, t) = 1$ und wir machen mit der symbolischen Berechnung von $\mathrm{ggT}(z_4^2 s, z_4^2 s')$ weiter.
- Wenn $z_0 z_4^2 - z_1 z_4 z_3 + z_2 z_3^2 = 0$, dann gilt $\mathrm{ggT}(z_4^2 s, t) = t = (z_4 x + z_3)$ und $\frac{z_4^2 s}{t} = z_2 z_4 x + (z_1 z_4 - z_2 z_3)$.

  Ausserdem gilt $(\#x : z_4^2 \cdot s = 0 \wedge t > 0)_y^z = k$ g.d.w.

  $$(\#x : z_2 z_4 x + z_1 z_4 - z_2 z_3 = 0 \wedge t > 0)_y^z = k.$$

  sowie $\mathrm{ggT}(z_2 z_4 x + z_1 z_4 - z_2 z_3, t) = 1$.

Auf die gleiche Weise kann die Voraussetzung $\mathrm{ggT}(s, s') = 1$ sichergestellt werden.

Entscheidbarkeit der reellen Arithmetik

Unter der Voraussetzung $\mathrm{ggT}(s,t) = \mathrm{ggT}(s,s') = 1$ (und $s(y) \neq 0 \neq s(z)$) ist $(\#x : s = 0 \wedge t > 0)_y^z = k$ äquivalent zu

$$\mathrm{Var}_y([s, s't]) - \mathrm{Var}_z([s, s't]) + \mathrm{Var}_y([s, s']) - \mathrm{Var}_z([s, s']) = 2k$$

Dies kann als eine Boolesche Kombination von Aussagen der Gestalt $\mathrm{Var}_y([s, s't]) = i_1$, $\mathrm{Var}_z([s, s't]) = i_2$, $\mathrm{Var}_y([s, s']) = i_3$ und $\mathrm{Var}_z([s, s']) = i_4$ geschrieben werden.

Eine Aussage $\mathrm{Var}_y([s, s't]) = i$ (analog für die anderen Polynome) kann schließlich durch eine quantorenfreie Formel ausgedrückt werden.

Hierzu lassen wir wieder symbolisch den Euklidischen Algorithmus für s und $s't$ laufen und berechnen so die Sturmfolge symbolisch.

Dies beendet die Behandlung von Fall 1.

Entscheidbarkeit der reellen Arithmetik

Fall 2: $G = (s = 0 \wedge \bigwedge_{i=1}^{m} t_i > 0)$, $m \geq 1$, und x kommt in s vor.

Induktion über m:

IA: $m = 1$. Siehe Fall 1.

IS: $m \geq 2$.

Sei $G' = (s = 0 \wedge \bigwedge_{i=1}^{m-2} t_i > 0)$.

$$\begin{aligned} &\#x(G' \wedge t_{m-1} > 0 \wedge t_m > 0) + \\ &\#x(G' \wedge t_{m-1} > 0 \wedge t_m < 0) \quad = \quad \#x(G' \wedge t_{m-1} t_m^2 > 0) \end{aligned} \tag{1}$$

$$\begin{aligned} &\#x(G' \wedge t_{m-1} > 0 \wedge t_m > 0) + \\ &\#x(G' \wedge t_{m-1} < 0 \wedge t_m > 0) \quad = \quad \#x(G' \wedge t_{m-1}^2 t_m > 0) \end{aligned} \tag{2}$$

$$\begin{aligned} &\#x(G' \wedge t_{m-1} > 0 \wedge t_m < 0) + \\ &\#x(G' \wedge t_{m-1} < 0 \wedge t_m > 0) \quad = \quad \#x(G' \wedge t_{m-1} t_m < 0) \end{aligned} \tag{3}$$

Entscheidbarkeit der reellen Arithmetik

(1) + (2) - (3) ergibt:

$$\begin{aligned} 2 \cdot \#xG &= 2 \cdot \#x \cdot (G' \wedge t_{m-1} > 0 \wedge t_m > 0) \\ &= \#x(G' \wedge t_{m-1} t_m^2 > 0) \; + \\ &\quad \#x(G' \wedge t_{m-1}^2 t_m > 0) \; - \\ &\quad \#x(G' \wedge -t_{m-1} t_m > 0) \end{aligned}$$

Fall 3: $s = 0$, d.h. $G = \bigwedge_{i=1}^{m} t_i > 0$ mit $t_i \neq 0$.

Sei $t = t_1 t_2 \cdots t_m$.

Behauptung: $\exists x \; G$ ist äquivalent in $\mathbb{R}$ zu

$$\exists x_0 \forall x \leq x_0 : G \;\vee\; \exists x_0 \forall x \geq x_0 : G \;\vee\; \exists x \, (t'(x) = 0 \wedge G). \qquad (4)$$

Die Implikation (4) $\Rightarrow \exists x \; G$ ist klar.

Entscheidbarkeit der reellen Arithmetik

Gelte nun $\mathbb{R} \models \exists x\ G$.

Hieraus folgt:

$$\begin{aligned}\mathbb{R} \models\ & \exists x_0 \forall x \leq x_0 : G \ \vee\ \exists x_0 \forall x \geq x_0 : G \ \vee \\ & \exists x_1\ \exists x\ \exists x_2\ (x_1 < x < x_2\ \wedge\ \neg G[x/x_1] \wedge G \wedge \neg G[x/x_2])\end{aligned}$$

Angenommen es gilt

$$\mathbb{R} \models \exists x_1\ \exists x\ \exists x_2\ (x_1 < x < x_2\ \wedge\ \neg G[x/x_1] \wedge G \wedge \neg G[x/x_2])$$

Dann gibt es $x_1' < x_2'$ mit $t(x_1') = 0 = t(x_2')$ und $t_i(y) > 0$ für alle $y \in (x_1', x_2')$ und $1 \leq i \leq m$ (insbesondere $t(y) > 0$ für alle $y \in (x_1', x_2')$).

Aus dem Satz von Rolle folgt, dass ein x existiert mit $t'(x) = 0$ und $t_i(x) > 0$ für alle $1 \leq i \leq m$, d.h.

$$\mathbb{R} \models \exists x_0 \forall x \leq x_0 : G \ \vee\ \exists x_0 \forall x \geq x_0 : G \ \vee\ \exists x\ (t'(x) = 0 \wedge G).$$

Dies zeigt die Behauptung.

Entscheidbarkeit der reellen Arithmetik

Es genügt also, eine quantorenfreie Formel für

$$\exists x_0 \forall x \leq x_0 : G \ \vee \ \exists x_0 \forall x \geq x_0 : G \ \vee \ \exists x \, (t'(x) = 0 \wedge G)$$

anzugeben.

Für die Formeln $\exists x_0 \forall x \leq x_0 \; G$ und $\exists x_0 \forall x \geq x_0 \; G$ kann man leicht quantorenfreie Formeln angeben.

Beachte hierzu: Für ein Polynom $a_n x^n + \cdots + a_1 x + a_0$ mit $a_n \neq 0$ gilt $\exists x_0 \forall x \leq x_0 \; (a_n x^n + \cdots + a_1 x + a_0 > 0)$ genau dann, wenn einer der beiden folgenden Fälle gilt:

- n gerade und $a_n > 0$
- n ungerade und $a_n < 0$

Entscheidbarkeit der reellen Arithmetik

Die Formel $\exists x\,(t'(x) = 0 \wedge G)$ kann über Fall 1 bzw. 2 behandelt werden, falls x in $t'(x)$ vorkommt.

Beachte: Kommt x in $t'(x)$ nicht vor, so hat $t(x) = t_1(x) \cdots t_m(x)$ einen x-Grad von höchstens 1.

Dies bedeutet, dass x in höchstens einem t_i vorkommt; sei dies o.B.d.A. t_1.

Ausserdem hat $t_1(x)$ einen x-Grad von höchstens 1, d.h. (o.B.d.A.) $t_1 = z_1 \cdot x + z_0$, $t_i = z_i$ für $2 \leq i \leq m$.

Dann ist $\exists x \bigwedge_{i=1}^{m} t_i > 0$ äquivalent zu $\bigwedge_{i=2}^{m} t_i > 0$

Dies beendet den Beweis des Satzes von Tarski. □

Entscheidbarkeit der reellen Arithmetik

Aus dem Satz von Tarski folgt sofort, dass es keine arithmetische Formel $\varphi(x)$ mit der einzigen freien Variablen x gibt, so dass für alle $r \in \mathbb{R}$ gilt:

$$(\mathbb{R}, +, \cdot)_{[x/r]} \models \varphi(x) \;\Leftrightarrow\; r \in \mathbb{N}$$

Denn gäbe es solch ein Formel $\varphi(x)$ so würde mit Gödels Satz ($\mathrm{Th}(\mathbb{N}, +, \cdot)$ unentscheidbar) sofort die Unentscheidbarkeit von $\mathrm{Th}(\mathbb{R}, +, \cdot)$ folgen.

Erstaunlicherweise hat Julia Robinsion 1949 solch ein Formel für $\mathbb{Q}$ anstatt $\mathbb{R}$ angegeben.

Satz (Robinson 1949)

Es existiert eine arithmetische Formel $\varphi(x)$ mit der einzigen freien Variablen x gibt, so dass für alle rationalen Zahlen $r \in \mathbb{Q}$ gilt:

$$(\mathbb{Q}, +, \cdot)_{[x/r]} \models \varphi(x) \;\Leftrightarrow\; r \in \mathbb{N}$$

Konsequenz: $\mathrm{Th}(\mathbb{Q}, +, \cdot)$ ist unentscheidbar.

Monadische Logik 2. Stufe

Monadische Logik 2. Stufe (kurz MSO für monadic second order) ist eine Erweiterung der Prädikatenlogik (welche auch als Logik 1. Stufe bezeichnet wird), bei der über Teilmengen des Universums quantifiziert werden darf.

Wir fixieren hierzu zwei Mengen von Variablen:

- Variablen 1. Stufe: $\mathrm{Var}_1 = \{x_1, x_2, x_3, \ldots\}$
- Variablen 2. Stufe: $\mathrm{Var}_2 = \{X_1, X_2, X_3, \ldots\}$

Es gelte $\mathrm{Var}_1 \cap \mathrm{Var}_2 = \emptyset$.

Variablen aus Var_1 bezeichnen wir im folgenden mit $x, y, z, x', x_0, \ldots$, während wir Variablen aus Var_2 mit $X, Y, Z, X', X_0, \ldots$ bezeichnen.

Wie in der Prädikatenlogik haben wir Prädikatensymbole P_i^k (k-stellig) und Funktionssymbole f_i^k (k-stellig).

Terme sind dann wieder genau wie in der Prädikatenlogik definiert.

Monadische Logik 2. Stufe

Die Menge MSO aller MSO-Formeln ist die kleinste Menge mit:

- Wenn t_1, t_2 Terme sind und $X \in \mathrm{Var}_2$, dann sind $(t_1 = t_2), (t_1 \in X) \in \mathrm{MSO}$.
- Wenn $t_1, t_2, \ldots, t_k$ Terme sind, und P ein k-stelliges Prädikatensymbol ist, dann ist, dann ist $P(t_1, \ldots, t_k) \in \mathrm{MSO}$.
- Wenn $F, G \in \mathrm{MSO}$, dann auch $\neg F,\ F \wedge G,\ F \vee G \in \mathrm{MSO}$.
- Wenn $F \in \mathrm{MSO}$ und $x \in \mathrm{Var}_1, X \in \mathrm{Var}_2$ dann $\exists x F,\ \exists X F,\ \forall x F,\ \forall X F \in \mathrm{MSO}$.

Die Menge $\mathrm{free}(F) \subseteq \mathrm{Var}_1 \cup \mathrm{Var}_2$ aller in $F \in \mathrm{MSO}$ freien Variablen ist definiert wie üblich.

Für $F \in \mathrm{MSO}$ schreiben wir auch $F(x_1, \ldots, x_n, X_1, \ldots, X_m)$ um $\mathrm{free}(F) = \{x_1, \ldots, x_n, X_1, \ldots, X_m\}$ auszudrücken.

Ein Formel $F \in \mathrm{MSO}$ ist ein MSO-Satz, falls $\mathrm{free}(F) = \emptyset$ gilt.

Monadische Logik 2. Stufe

Eine Struktur ist nun ein Paar $\mathcal{A} = (U_\mathcal{A}, I_\mathcal{A})$, wobei $U_\mathcal{A}$ eine nicht-leere Menge (das Universum) ist und $I_\mathcal{A}$ eine partiell definierte Abbildung, die

- jedem k–stelligen Prädikatensymbol P aus dem Definitionsbereich von $I_\mathcal{A}$ eine k–stellige Relation $I_\mathcal{A}(P) \subseteq U_\mathcal{A}^k$ zuordnet,
- jedem k–stelligen Funktionssymbol f aus dem Definitionsbereich von $I_\mathcal{A}$ eine k–stellige Funktion $I_\mathcal{A}(f) : U_\mathcal{A}^k \to U_\mathcal{A}$ zuordnet,
- jeder Variablen $x \in \mathrm{Var}_1$ aus dem Definitionsbereich von $I_\mathcal{A}$ ein Element $I_\mathcal{A}(x) \in U_\mathcal{A}$ zuordnet, und
- jeder Variablen $X \in \mathrm{Var}_2$ aus dem Definitionsbereich von $I_\mathcal{A}$ eine Teilmenge $I_\mathcal{A}(X) \subseteq U_\mathcal{A}$ zuordnet.

Die Struktur $\mathcal{A}$ heißt passend zur Formel $F \in \mathrm{MSO}$, falls $I_\mathcal{A}$ auf allen in F vorkommenden Prädikatsymbolen, Funktionssymbolen und freien Variablen definiert ist.

Monadische Logik 2. Stufe

Wenn $\mathcal{A}$ passend zu F ist, schreiben wir $\mathcal{A} \models F$ genau dann, wenn einer der folgenden Fälle gilt:

- $F = (t_1 = t_2)$ und $\mathcal{A}(t_1) = \mathcal{A}(t_2)$
- $F = (t \in X)$ und $\mathcal{A}(t) \in I_{\mathcal{A}}(X)$
- $F = P(t_1, \ldots, t_k)$ und $(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_k)) \in I_{\mathcal{A}}(P)$
- $F = \neg G$ und $\mathcal{A} \not\models G$
- $F = G \wedge H$ und ($\mathcal{A} \models G$ und $\mathcal{A} \models H$)
- $F = G \vee H$ und ($\mathcal{A} \models G$ oder $\mathcal{A} \models H$)
- $F = \exists x\ G$ und es gibt ein $a \in U_{\mathcal{A}}$ mit $\mathcal{A}_{[x/a]} \models G$
- $F = \forall x\ G$ und für alle $a \in U_{\mathcal{A}}$ gilt $\mathcal{A}_{[x/a]} \models G$
- $F = \exists X\ G$ und es gibt ein $B \subseteq U_{\mathcal{A}}$ mit $\mathcal{A}_{[X/B]} \models G$
- $F = \forall X\ G$ und für alle $B \subseteq U_{\mathcal{A}}$ gilt $\mathcal{A}_{[X/B]} \models G$.

Monadische Logik 2. Stufe

Konventionen:

- Im folgenden bezeichen wir die Interpretation $I_{\mathcal{A}}(P)$ eines Symbols P ebenfalls mit dem Symbol P.
- Eine Struktur $\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}})$ mit $\mathrm{dom}(I_{\mathcal{A}}) = \{P_1, \ldots, P_n, f_1, \ldots, f_m\}$ schreiben wir auch als $(U_{\mathcal{A}}, I_{\mathcal{A}}(P_1), \ldots, I_{\mathcal{A}}(P_n), I_{\mathcal{A}}(f_1), \ldots, I_{\mathcal{A}}(f_m))$ oder kurz $(U_{\mathcal{A}}, P_1, \ldots, P_n, f_1, \ldots, f_m)$.
- Für eine MSO-Formel $F = F(x_1, \ldots, x_n, X_1, \ldots, X_m)$ und $a_1, \ldots, a_n \in U_{\mathcal{A}}$, $A_1, \ldots, A_m \subseteq U_{\mathcal{A}}$ schreiben wir auch $\mathcal{A} \models F(a_1, \ldots, a_n, A_1, \ldots, A_m)$ anstatt $\mathcal{A}_{[x_1/a_1,\ldots,x_n/a_n,X_1/A_1,\ldots,X_m/A_m]} \models F$.

Die MSO-Theorie einer Struktur $\mathcal{A}$ ist die Menge aller MSO-Sätze F mit $\mathcal{A} \models F$.

Monadische Logik 2. Stufe: Beispiel

Ein Beispiel für eine nützliche MSO-Formel:

Sei $\theta(x, y)$ eine MSO-Formel.

Die folgende Formel $\text{reach}_\theta(x, y)$ drückt aus, dass in der durch $\theta(x, y)$ definierten binären Relation ein Pfad von x nach y existiert:

$$\text{reach}_\theta(x, y) = \forall X \Big(\big(x \in X \wedge \forall y \forall z(\theta(y, z) \wedge y \in X \ \rightarrow z \in X)\big) \rightarrow y \in X \Big)$$

In Worten: Es gibt einen θ-Pfad von x nach y genau dann, wenn jede Teilmenge X, die x enthält und unter der durch θ definierten Relation abgeschlossen ist ($\forall y \forall z(\theta(y, z) \wedge y \in X \ \rightarrow z \in X)$), auch y enthält.

MSO-definierbare Sprachen

Wir wollen MSO-Sätze benutzen, um (formale) Sprachen zu definieren.

Hierzu müssen wir zunächst Wörter als Strukturen repräsentieren.

Sei Σ ein endliches Alphabet im folgenden.

Ein nicht-leeres Wort $w = a_1 a_2 \cdots a_n$ ($n \geq 1$, $a_i \in \Sigma$) identifizieren wir mit der Struktur

$$\mathcal{A}_w = (\{1, 2, \ldots, n\}, <, (P_a)_{a \in \Sigma}),$$

wobei gilt:

- $<$ ist die gewöhnliche Ordnung auf $\{1, 2, \ldots, n\}$
- P_a ist die einstellige Relation $P_a = \{i \mid 1 \leq i \leq n, a_i = a\}$

Im folgenden schreiben wir einfach w für $\mathcal{A}_w$.

Eine Sprache $L \subseteq \Sigma^+$ ist MSO-definierbar, falls ein MSO-Satz F existiert mit $L = \{w \in \Sigma^+ \mid w \models F\}$.

MSO-definierbare Sprachen

Für die folgenden Beispiele sei das Alphabet $\Sigma = \{a, b\}$.

Beispiel 1: Der MSO-Satz

$$\exists x \exists y \exists z (\forall u (x \leq u \wedge u \leq z) \wedge P_a(x) \wedge P_b(y) \wedge P_a(z))$$

definiert die Sprache $a\Sigma^* b\Sigma^* a$.

Hier ist $x \leq u$ eine Abkürzung für $x < u \vee x = u$.

Beispiel 2: Der MSO-Satz

$$\begin{aligned} \exists X \, (&\exists x \exists y (\forall u (x \leq u \wedge u \leq y) \wedge x \in X \wedge \neg y \in X) \wedge \\ &\forall x \forall y (y = x + 1 \rightarrow (x \in X \leftrightarrow y \notin X))) \end{aligned}$$

definiert die Sprache $\{w \in \{a, b\}^* \mid |w| \text{ ist gerade}\}$.

Hier ist $y = x + 1$ eine Abkürzung für die Formel
$x < y \wedge \forall z (x \leq z \leq y \rightarrow (x = z \vee y = z))$.

Der Satz von Büchi

Satz (Büchi, Elgot 1958 und Trachtenbrot 1958)

Eine Sprache L ist MSO-definierbar genau dann, wenn sie regulär ist.

Beweis:

1. Sei $L \subseteq \Sigma^*$ regulär. Wir zeigen, dass L MSO-definierbar ist.

Sei $A = (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat mit $L(A) = L$, wobei

- Q die endliche Menge der Zustände ist,
- $\delta : Q \times \Sigma \to Q$ die Überführungsfunktion ist,
- $q_0 \in Q$ der Anfangszustand ist, und
- $F \subseteq Q$ die Menge der Endzustände ist.

Der Satz von Büchi

O.B.d.A. sei $Q = \{1, \ldots, n\}$.

Dann definiert der folgende MSO-Satz die Sprache $L = L(A)$:

$$\exists X_1 \exists X_2 \cdots \exists X_n$$
$$\bigwedge_{p \neq q} X_p \cap X_q = \emptyset \ \wedge \ \forall x \bigvee_{q \in Q} x \in X_q \ \wedge$$
$$\exists x(\forall y(x \leq y) \wedge \bigvee_{a \in \Sigma} (P_a(x) \wedge x \in X_{\delta(q_0,a)})) \wedge$$
$$\exists x(\forall y(y \leq x) \wedge \bigvee_{q \in F} x \in X_q) \wedge$$
$$\forall x \forall y(y = x + 1 \rightarrow \bigvee_{q \in Q} \bigvee_{a \in \Sigma} (x \in X_q \wedge P_a(y) \wedge y \in X_{\delta(q,a)}))$$

Hierbei ist $X_p \cap X_q = \emptyset$ eine Abkürzung für $\neg \exists x(x \in X_p \wedge x \in X_q)$.

Der Satz von Büchi

2. Sei $L \subseteq \Sigma^*$ MSO-definierbar. Wir zeigen, dass L regulär ist.

Sei $V \subseteq \mathrm{Var}_1 \cup \mathrm{Var}_2$ eine endliche Menge von Variablen.

Ein nicht-leeres Wort

$$w = (a_1, V_1)(a_2, V_2) \cdots (a_k, V_k) \in (\Sigma \times 2^V)^*$$

$(k \geq 1,\ a_i \in \Sigma,\ V_k \subseteq V)$ nennen wir gültig falls es für jede Variable $x \in V \cap \mathrm{Var}_1$ genau ein $1 \leq i \leq k$ mit $x \in V_i$ gibt.

Für solch ein gültiges Wort w definieren wir die Abbildung $f_w : V \to \{1, \ldots, k\} \cup 2^{\{1,\ldots,k\}}$ durch:

- $f_w(x) = i$ falls $x \in V_i \cap \mathrm{Var}_1$.
- $f_w(X) = \{i \mid X \in V_i\}$ für $X \in V \cap \mathrm{Var}_2$.

Der Satz von Büchi

Weiter identifizieren wir ein gültiges Wort $w = (a_1, V_1)(a_2, V_2) \cdots (a_k, V_k)$ mit der Struktur $\mathcal{A}_w = (\{1, \ldots, k\}, I_w)$, wobei

- $I_w(x) = f_w(x)$ für $x \in V \cap \mathrm{Var}_1$,
- $I_w(X) = f_w(X)$, für $X \in V \cap \mathrm{Var}_2$,
- und I_w auf den Symbolen $<$, P_a $(a \in \Sigma)$ genau so definiert ist wie die Struktur $\mathcal{A}_v$ für $v = a_1 a_2 \cdots a_k$.

Für eine MSO-Formel F mit $\mathrm{free}(F)$ sei $L(F)$ die Menge aller nicht-leeren gültigen Wörter w über dem Alphabet $\Sigma \times 2^{\mathrm{free}(F)}$ mit $w \models F$.

Beweisstrategie: Wir konstruieren für jede Formel F durch Induktion über den Aufbau von F einen endlichen Automaten A_F für die Sprache $L(F)$.

Der Satz von Büchi

Zunächst kann man für jede endliche Variablenmenge $V \subseteq \mathrm{Var}_1 \cup \mathrm{Var}_2$ einen Automaten A_V konstruieren, der genau die gültigen Wörter aus $(\Sigma \times 2^V)^*$ akzeptiert.

1. Fall: $F = (x = y)$. Konstruiere A_F so, dass

$$L(A_F) = (\Sigma \times \{\emptyset\})^*(\Sigma \times \{x, y\})(\Sigma \times \{\emptyset\})^*.$$

2. Fall: $F = (x < y)$. Konstruiere A_F so, dass

$$L(A_F) = (\Sigma \times \{\emptyset\})^*(\Sigma \times \{x\})(\Sigma \times \{\emptyset\})^*(\Sigma \times \{y\})(\Sigma \times \{\emptyset\})^*.$$

3. Fall: $F = P_a(x)$. Konstruiere A_F so, dass

$$L(A_F) = (\Sigma \times \{\emptyset\})^*(a, \{x\})(\Sigma \times \{\emptyset\})^*.$$

4. Fall: $F = (x \in X)$. Konstruiere A_F so, dass

$$L(A_F) = (\Sigma \times \{\emptyset, \{X\}\})^*(\Sigma \times \{x, X\})(\Sigma \times \{\emptyset, \{X\}\})^*.$$

Der Satz von Büchi

5. Fall: $F = \neg G$. Sei $V = \text{free}(G)$. Konstruiere A_F so, dass

$$L(A_F) = L(A_V) \setminus L(A_G).$$

6. Fall: $F = G \vee H$.

Sei $V_G = \text{free}(G)$, $V_H = \text{free}(H)$ und $V = \text{free}(F) = V_G \cup V_H$.

Definiere Homomorphismen $g : (\Sigma \times 2^V)^* \to (\Sigma \times 2^{V_G})^*$ und $h : (\Sigma \times 2^V)^* \to (\Sigma \times 2^{V_H})^*$ durch

$$\begin{aligned} g(a, S) &= (a, S \cap V_G), \\ h(a, S) &= (a, S \cap V_H). \end{aligned}$$

Konstruiere nun Automaten A'_G und A'_H, so dass

$$\begin{aligned} L(A'_G) &= L(A_V) \cap g^{-1}(L(A_G)), \\ L(A'_H) &= L(A_V) \cap h^{-1}(L(A_H)). \end{aligned}$$

Der Automat A_F wird dann so konstruiert, dass $L(A_F) = L(A'_G) \cup L(A'_H)$.

Der Satz von Büchi

7. Fall: $F = \exists x\ G$.

Sei $V = \text{free}(G)$ und damit $\text{free}(F) = V \setminus \{x\}$.

Definiere den Homomorphismen $f : (\Sigma \times 2^V)^* \to (\Sigma \times 2^{V \setminus \{x\}})^*$ durch

$$f(a, S) = (a, S \setminus \{x\}).$$

Konstruiere dann den Automaten A_F so, dass $L(A_F) = f(L(A_G))$.

8. Fall: $F = \exists X\ G$.

Sei $V = \text{free}(G)$ und damit $\text{free}(F) = V \setminus \{X\}$.

Definiere den Homomorphismen $f : (\Sigma \times 2^V)^* \to (\Sigma \times 2^{V \setminus \{X\}})^*$ durch

$$f(a, S) = (a, S \setminus \{X\}).$$

Konstruiere dann den Automaten A_F so, dass $L(A_F) = f(L(A_G))$.

Dies beendet den Beweis des Satzes von Büchi. □