Gewichtete Endliche Automaten als Terminations-Zertifikate für String Rewriting

Dieter Hofbauer (Kassel)
Johannes Waldmann (HTWK Leipzig)

- Termination und monotone Interpretionen
- Matrizen (Automaten) über $(\mathbb{N}, +.\cdot)$
- relative Termination und Interpretationen
- Automaten in anderen Halbringen

Termination von SRS

SRS = string rewriting system =
(endliche) Regelmenge $R \subseteq \Sigma^* \times \Sigma^*$

Beispiel $R = \{ab \to bba\}$ über $\Sigma = \{a, b\}$.

induziert Ableitungsrelation $\to_R$ auf Σ^*

$$\to_R = \{(xly, xry) \mid x, y \in \Sigma^*, (l, r) \in R\}.$$

Ableitungen $ab^k \to_R^k b^{2k}a, \quad a^k b \to_R^{2^k-1} b^{2^k}a^k$

R terminiert := $\to_R$ ist wohlfundiert
(es gibt keine unendlichen $\to_R$-Ketten)

Monotone Interpretationen

[Lankford 1975, Manna und Ness 1970] Wenn zu einem SRS R über Σ eine wohlfundierte Menge $(M, >)$ existiert und eine Interpretation $i : \Sigma \to (M \to M)$ mit

- jedes i_a ist streng monoton: $\forall x > y : i_a(x) > i_a(y)$
- i ist kompatibel mit R:

$$\forall (l, r) \in R, x \in M : i_l(x) > i_r(x),$$

dann terminiert R.
Beweis: zu $w_0 \to_R w_1 \to \ldots$ gehört absteigende Kette $i_{w_0}(m) > i_{w_1}(m) > \ldots$, diese kann nicht unendlich sein.

Interpr. durch (lineare) Polynome

$R = \{ab \to bba\}$. Betrachte $(\mathbb{N} \setminus 0, >)$ und

$$i_a = (x \mapsto 3x), i_b = (x \mapsto 1 + x)$$

dann $i_{ab}(x) = 3x + 3 > 3x + 2 = i_{bba}(x)$.

$i_{abbaba}(1) = 3 \cdot (1 + (1 + (3 \cdot (1 + (3 \cdot 1))))) = 42$
$abb\underline{aba} \to_R abb\underline{bba}a$
$i_{abbbbaa}(1) = 3 \cdot (1 + (1 + (1 + (1 + (3 \cdot (3 \cdot 1)))))) = 39$
$\underline{ab}baba \to_R \underline{bba}baba$
$i_{bbababa}(1) = 1 + (1 + (3 \cdot (1 + (3 \cdot (1 + (3 \cdot 1)))))) = 41.$

Aufgaben: Interpretationen für $\{ab \to ba\}, \{aa \to aba\}$

Totale Termination

R ist total terminierend := R besitzt monotone Interpretation i in total geordnetes $(M, >)$.
dann $\forall c : i_c(x) \geq x$

$\{aa \to aba\}$ ist nicht total terminierend:
$i_a(i_a(x)) \leq i_a(i_b(i_a(x)))$
... aber terminierend:
betrachte Anzahl der Faktoren aa
... das ist aber keine Interpretation

liefert grundsätzliche Schranke für Beweiskraft von polynomiellen Interpretationen

Ableitungslängen

Wenn R eine polynomielle Interpretation i besitzt, dann hat R-Ableitung von w höchstens $i_w(0)$ Schritte.
$\Rightarrow$ Ableitungslängen sind primitiv rekursiv in $|w|$

$g :=$ höchster vorkommender Polynom-Grad
$i_w(0) \leq c^{g \cdot \cdots \cdot g} \Rightarrow i_w(0) \in 2^{2^{O(|w|)}}$
Ableitungslängen sind höchstens doppelt exponentiell

aber kurze Ableitungslängen sind nicht automatisch auch leicht zu beweisen!
$\{aba^k b \to (ba^k b)^2 a\}$ einfach exponentiell (?),
$\{a^2b^2 \to b^3a^3\}$ linear.

Interpretation durch Matrizen

$R = \{aa \to aba\}$ über $\Sigma = \{a, b\}$, $M = \mathbb{N}^2$,
Interpretation $i : \Sigma \to \mathbb{N}^{2\times 2} : a \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, b \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$

dann $i(aa) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} > \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} = i(aba)$
Ordnung $\geq$ punktweise, $(>) = (\geq) \setminus (=)$

Monotonie?
$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

$i : a \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, b \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, (aa - aba) \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$

betrachte Mengen N, M von Matrizen mit

- $N :=$ alle Koeffizienten ≥ 0,
- $P := N\cap$ wenigstens einer > 0,
- $M := N\cap$ in jeder Zeile wenigstens einer > 0.

M ist abgeschlossen unter Multiplikation (P nicht.)
es folgt: $\forall x, y \in \Sigma^* : i(x) \cdot (i(aa - aba)) \cdot i(y) \in M \subseteq P$

also $u \to_R v \Rightarrow i(u) \begin{pmatrix} 1 \\ 1 \end{pmatrix} > i(v) \begin{pmatrix} 1 \\ 1 \end{pmatrix} \Rightarrow$ Termination.

Für jedes SRS R über Σ: falls existiert $i : \Sigma \to \mathbb{N}^{k\times k}$ mit

$$\forall x, y \in \Sigma^*, (l, r) \in R : i(x) \cdot i(l - r) \cdot i(y) > 0,$$

dann terminiert R.
Spezialisierungen:

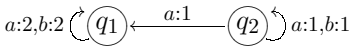
- $i(\Sigma) \subseteq M, i(l - r) \subseteq M$ (vorige Folie)
- $i(\Sigma) \subseteq D, i(l - r) \subseteq P$, wobei $D = N\cap$ Diagonale > 0

$i(a) = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, i(b) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, i(ab - ba) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$

Interpretationen und Automaten

Interpretation $i : \Sigma \to \mathbb{N}^{k\times k}$ entspricht
Übergangsrelation eines $\mathbb{N}$-gewichteten Automaten

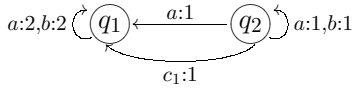
$$R = \{ab \to ba\}, i(a) = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, i(b) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$



$i(l) > i(r)$ bedeutet
$\forall p, q \in Q(A) : A(p, l, q) \geq A(p, r, q)$
und $\exists p, q \in Q(A) : A(p, l, q) > A(p, r, q)$.

Ein Kriterium

Automat A': für jede Regel $(l_j \to r_j) \in R$ einen neuen Buchstaben c_j mit Interpretation $i(c_j) = i(l_j) - i(r_j)$



$\forall x, y \in \Sigma^*, (l, r) \in R : i(x) \cdot i(l - r) \cdot i(y) > 0$
$\approx \forall w \in \Sigma^* \cdot \{c_1, \ldots, c_n\} \cdot \Sigma^* : \exists p, q : A(p, w, q) > 0.$

Benutze Hom. $h : \{0, 1, 2, \ldots\} \to \{0, 1, 1 \ldots\}$
von $(\mathbb{N}, +, \cdot)$ nach $(\{0, 1\}, +, \cdot) =$ Boolean

teste $\Sigma^* \cdot \{c_1, \ldots, c_n\} \cdot \Sigma^* \subseteq h(A')$
Inklusion für klassische Automaten

Beispiel (I)

System $\{aaab \to aabbaba\}$ hat Interpretation in $\mathbb{N}^3$:

$$a \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in M, b \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \in M$$

$$l \mapsto \begin{pmatrix} 2 & 4 & 0 \\ 4 & 6 & 0 \\ 3 & 4 & 0 \end{pmatrix}, r \mapsto \begin{pmatrix} 0 & 3 & 0 \\ 0 & 6 & 0 \\ 0 & 4 & 0 \end{pmatrix}, i(l) - i(r) \in M$$

aber keine in $\mathbb{N}^2$ (?)

Beispiel (II)

System $\{bbb \to abbabb\}$ hat Interpretation

$$a \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, b \mapsto \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$i(l) = \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}, i(r) = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix}$$

aber keine in M oder E (?)

trotzdem Termination? Immerhin $i(l) - i(r) \geq \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

Ableitungstypen, -längen

monotone Matrix-Interpretationen auch für nicht total terminierende Systeme ($\{aa \to aba\}$),
denn Ordnung $>$ auf $\mathbb{N}$-Vektoren ist wohlfundiert, aber nicht total.

Matrix-Koeffizienten ergeben sich durch fortgesetzte Multiplikation $\Rightarrow$ Ableitungslängen sind einfach exponentiell beschränkt.

Monotone Interpretationen (Wdhlg.)

bisher: streng monotone Interpretation $\Rightarrow$ Termination.
$R = \{ab \to bba, ac \to ca, bc \to ccb\}$
hat lange Ableitungen: $ab^k \to^* b^{2k}a,\ a^kb \to^* b^{2^k}a^k$
$\underline{a^k}bc \to^* b^{2^k}\underline{a^kc} \to^* \underline{b^{2^k}c}a^k \to^* c^{2^{2^k}}b^{2^k}a^k$
doppelt exponentiell $\Rightarrow$ keine lineare Interpretation

$R = \{ab \to bba, ac \to ca, bc \to ccb\}$ hat Interpretation

$$i_a = (x \mapsto 3x), i_b = (x \mapsto x+1), i_c = (x \mapsto x)$$

mit Eigenschaften

- $\forall s \in \Sigma, x > y > 0 : i_s(x) > i_s(y)$
- $\forall x > 0 : i_{ab}(x) > i_{bba}(x)$
- $\forall x > 0 : i_{ac}(x) = i_{ca}(x), i_{cb}(x) = i_{bcc}(x)$

in jeder $\to_R$-Ableitung gibt es nur endlich viele $(ab \to bba)$-Schritte $\Rightarrow$ Termination von $\{ac \to ca, cb \to bcc\}$ impliziert Termination von R.

$\mathrm{SN}(R)$: SRS R terminiert (is *strongly normalising*)
$\mathrm{SN}(R/S)$: SRS R terminiert *relativ zu* SRS S,
wenn jede $(\to_R \cup \to_S)$-Ableitung
nur endlich viele $\to_R$-Schritte enthält.

Satz. $\mathrm{SN}(R/S) \wedge \mathrm{SN}(S) \Rightarrow \mathrm{SN}(R \cup S)$.

Satz. Falls Interpretation $i : \Sigma \to (M \to M)$ existiert mit

- $\forall s \in \Sigma, x, y \in M : x > y \Rightarrow i_s(x) > i_s(y)$,
- $\forall (l \to r) \in R, x \in M : i_l(x) > i_r(x)$,
- $\forall (l \to r) \in S, x \in M : i_l(x) \geq i_r(x)$,

dann $\mathrm{SN}(R/S)$.

. . . und Anwendungen

relative Termination ermöglicht das Entfernen von Regeln und damit *modulare* Terminations-Beweise.

Beweiskraft wird dadurch erhöht:
$R = \{ab \to bba, ac \to ca, bc \to ccb\}$ hat keine lineare Interpretation, aber modularer Beweis verwendet *Folge* von linearen Interpretationen

- $i_a = (x \mapsto 3x), i_b = (x \mapsto x+1), i_c = (x \mapsto x)$ entfernt $ab \to bba$
- $i_a = (x \mapsto x), i_b = (x \mapsto 3x), i_c = (x \mapsto x+1)$ entfernt $bc \to ccb$
- $i_a = (x \mapsto 2x), i_c = (x \mapsto x+1)$ entfernt $ac \to ca$

Zertifikate erzeugen

experimentell: Interpretation würfeln und verbessern (evolutionär). Benutze dabei

- spezielle Matrizen M, E, P
- oder allgemeine Matrizen und (teuren) Automaten-Test

Was ist geeignetes Maß für Fitness?
Welche Mutationen? Rekombinationen?

Direkte Konstruktion — durch Hinzufügen von Knoten und Kanten? Zu jedem Redukt-Pfad muß ein Redex-Pfad (mit höherem Gewicht) existieren. (Ungewöhnliche Richtung für eine Vervollständigung!)

Der $(\min, +)$-Halbring

bisher: $(\mathbb{N}, +, \cdot, 0, 1)$, jetzt: $(\mathbb{N} \cup \infty, \min, +, \infty, 0)$.

$$i(a) = \begin{pmatrix} 3 & 1 & \infty & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \\ 1 & 1 & \infty & 0 & \infty \\ \infty & \infty & \infty & \infty & \infty \\ \infty & 0 & \infty & \infty & \infty \end{pmatrix}, i(b) = \begin{pmatrix} 3 & \infty & \infty & \infty & \infty \\ \infty & \infty & 1 & \infty & \infty \\ \infty & \infty & \infty & \infty & 0 \\ \infty & \infty & \infty & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \end{pmatrix}$$

$$i(aa) = \begin{pmatrix} 6 & 4 & \infty & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \\ 4 & 2 & \infty & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \\ \infty & \infty & \infty & \infty & \infty \end{pmatrix} > \begin{pmatrix} 3 & 3 & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & \infty \\ 3 & 0 & \infty & 2 & \infty \\ \infty & \infty & \infty & \infty & \infty \\ 2 & 2 & \infty & 1 & \infty \end{pmatrix} = i(aba)$$

folgt daraus Termination von $\{aa \to aba\}$?

$(\min, +)$, Teil 2

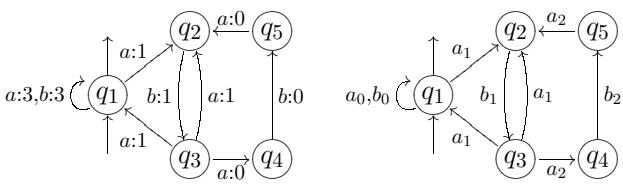
. . . ja. Betrachte Automat mit Übergangstabelle i und Finalvektor $v = (1, \infty, \infty, \infty, \infty)$, Initialvektor v^T, erzeugt Bewertung $A(w) = v \cdot i(w) \cdot v^T$.
Es gilt

- $\forall w \in \Sigma^* : A(w) < \infty$
- und $\forall p, q : \infty > A(p, l, q) \Rightarrow A(p, l, q) > A(p, r, q)$.

Wenn $xly \to_R xry$, dann
$A(xly) = \min_{i \in I, p, q \in Q, f \in F} A(i, x, p) + A(p, l, q) + A(q, y, f) >$
$A(xry) = \min_{i \in I, p, q \in Q, f \in F} A(i, x, p) + A(p, r, q) + A(q, y, f)$,
denn es genügt Minimum über (p, q) mit $A(p, l, q) < \infty$.

Match bounded rewriting

Das ist der gewichtete Automat zu i (links) . . .



. . . und rechts steht der Zertifikat-Automat dafür, daß $\{aa \to aba\}$ match-bounded durch 2 ist!
Die Gewichte $g : *_0 \mapsto 3, *_1 \mapsto 1, *_2 \mapsto 0$ beweisen Termination von $\mathrm{match}(R)$:

Der $(\min, \max)$-Halbring

$(\mathbb{N} \cup \infty, \min, +, \infty, 0)$ $(\mathbb{N} \cup \infty, \min, \max, \infty, 0)$.
der *richtige* Halbring für match-bounded rewriting?

$$\mathrm{match}(R) = \left\{ (l' \to r') \mid \begin{array}{l} (\mathrm{base}\, l' \to \mathrm{base}\, r') \in R, \\ \max \mathrm{height}\, l' < \max \mathrm{height}\, r' \end{array} \right\}$$

durch Spiegeln (Vorzeichenumkehr und Verschieben) der Höhen entsteht
$\forall (l, r) \in R, p, q \in A : \infty > A(p, l, q) \Rightarrow A(p, l, q) > A(p, r, q)$

das gilt lokal, aber wo ist die monotone globale Bewertung? $A(p, w, q)$ ist hier sogar beschränkt, das

- $(\mathbb{N}, +, \cdot, 0, 1)$,
- $(\mathbb{N} \cup \infty, \min, +, \infty, 0)$,
- $(\mathbb{N} \cup \infty, \min, \max, \infty, 0)$.

Monotonie für $f : M^2 \to M$: $\forall x > x', y > y'$ gilt

- unabhängig (?) monoton:
  $f(x, y) > f(x', y) \wedge f(x, y) > f(x', y)$
  Beispiele: $(+)$, $(\cdot)$ auf $\mathbb{N} \setminus 0$
- abhängig (?) monoton: $f(x, y) > f(x', y')$
  Beispiele: $\min, \max$

- Ring-Addition
  - unabhängig monoton: für jede Regel genügt *ein* absteigendes Redex-Redukt-Paar (die anderen dürfen gleiche Gewichte haben)
  - nur abhängig monoton: für jede Regel müssen *alle* Paare absteigen
- Ring-Multiplikation
  - unabhängig monoton:
    Automat liefert monotone Interpretation
  - nur abhängig monoton: ??
    (Automat liefert gar keine sinnvolle Interpretation)

Vergleich der Halbringe: Ordnungen

- Ring-0 $<$ andere Elemente, Beispiel: $(+, \cdot)$:

  jedes *Redukt* muß überdeckt werden,
  aber nicht jeder Redex benötigt ein Redukt

  Vervollständigung *rückwärts*
- Ring-0 $>$ andere Elemente,
  Beispiel $(\min, +), (\min, \max)$

  jeder *Redex* muß überdeckt werden,
  nicht jedes Redukt benötigt einen Redex

  Vervollständigung *vorwärts*,
  vgl. deleting/matchbounded rewriting

Vergleich der Halbringe: Schranken

Schranke für Koeffizienten in einem Produkt von n Matrizen aus einer festen Menge
(d. h. Interpretation eines Wortes der Länge n):

- $(+, \cdot)$: exponentiell in n
- $(\min, +)$: linear in n
- $(\min, \max)$: konstant

Ziel: match-bounded Techniken aus $(\min, \max)$ (Automaten-Vervollständigung exakt oder approximiert) in $(+, \cdot)$ anwenden.