Gleichungen und Ungleichungen in nichtkommutativen Ringen

Johannes Waldmann (HTWK Leipzig)
Dieter Hofbauer (Kassel)

Modelle für Gleichungen

- *Gleichungssystem* := Menge von formalen Polynomen mit Unbestimmten aus $V = \{a, b, \ldots\}$ und Koeffizienten in $\mathbb{Z}$
  Beispiel $G = \{ab - ba\}$, Schreibweise: $\{ab = ba\}$.
- *Ring* $(M, 0, 1, +, \cdot)$
  $(M, 0, +)$ ist kommutative Gruppe, $(M, 1, \cdot)$ ist (nicht notw. komm.) Monoid, $+$ und $\cdot$ sind verträglich
- *Interpretation* (Belegung der Variablen) $i : V \to M$, fortgesetzt zu Int. auf Monomen und Polynomen
- Interpretation i heißt *Modell* für G, falls $\forall g \in G : i(g) = 0$. Bsp.: $M = \mathbb{Z}, i : a \mapsto 3, b \mapsto 5$

Modelle für Ungleichungen (Ansatz)

- *geordneter* Ring: $(M, <)$,
  Halbordnung $<$ verträglich mit $+$ und $\cdot$, d. h.
  $a < b \Rightarrow a + c < b + c$, $a < b \wedge 0 < c \Rightarrow ac < bc \wedge ca < cb$
  Positivbereich $M_+ := \{m \mid m \in M, m \geq 0\}$.
- *Ungleichungssystem* := Menge von formalen Polynomen mit Unbestimmten aus $V = \{a, b, \ldots\}$ und Koeffizienten in $\mathbb{Z}$
  Beispiel $U = \{ab - ba\}$, Schreibweise: $\{ab > ba\}$.
- Interpretation $i : V \to M_+$ heißt *Modell* für U, falls $\forall u \in U : i(u) > 0$.

Beispiel $ab > ba$ hat nur nichtkommutative Modelle

Der geordnete Matrizenring

- $M = \mathbb{Z}^{d \times d}$ mit üblichem $+$ und $\cdot$
- Ordnung *komponentenweise*:
  - $A \geq B \iff \forall j, k : A_{jk} \geq B_{jk}$
  - $A > B \iff A \geq B \wedge B \not\geq A$.
- Positivbereich ist $\mathbb{N}^{d \times d}$.

Beispiel: $M = \mathbb{Z}^{2 \times 2}, i : a \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, b \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
$i(ab) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} > \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = i(ba)$.
ist Modell für $ab > ba$, aber auch für $ab > b^2a^2$.
ist nicht *stabil*, denn $i(b \cdot ab) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = i(b \cdot ba)$

Stabile Modelle für Ungleichungen

- Interpretation $i : V \to M_+$ heißt *stabiles Modell* für U, falls $\forall x \in V^*, u \in U, y \in V^* : i(x \cdot u \cdot y) > 0$.

Beispiel für $U = \{ab - ba\}$:

- Interpretation: $i(a) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, i(b) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
- ist Modell: $i(ab) = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, i(ba) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$
- ist stabil: $i(a), i(b) \geq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i(ab - ba) \geq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$
  $\Rightarrow i(x \cdot u \cdot y) \geq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} > 0$.

Wohlfundierte stabile Modelle

- Relation $>$ heißt *wohlfundiert* (terminierend), falls es keine unendlich langen echt absteigenden Ketten $m_0 > m_1 > \ldots$ gibt.
- *Satz*: Wortersetzungssystem R terminiert $\iff$ ensprechendes Ungleichungssystem $U(R)$ besitzt stabiles Modell M mit wohlfundiertem Positivbereich.
- Beweis: ($\Leftarrow$): klar, ($\Rightarrow$): M der freie Halbgruppenring über dem Alphabet (Linearkombinationen von Wörtern), $>$ erzeugt durch Ersetzungsrelation $\to_R^+$.

Anwendung: $\{a^2b^2 > b^3a^3\}$

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

$$a^2b^2 = \begin{pmatrix} 1 & \boxed{4} & 4 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 0 \\ 0 & 4 & 4 & 2 & 0 \end{pmatrix}, b^3a^3 = \begin{pmatrix} 1 & \boxed{0} & 4 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 0 & 0 \\ 0 & 4 & 1 & 2 & 0 \end{pmatrix}$$

ist stabiles Modell, denn $0 < \{a, b\}^* \cdot (a^2b^2 - b^3a^3) \cdot \{a, b\}^*$

Anwendung: $\{a^2 > bc, b^2 > ac, c^2 > ab\}$

(RTA List of Open Problems # 104)

$$a = \begin{pmatrix} 1 & 1 & 4 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 \\ 0 & 2 & 2 & 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, c = \begin{pmatrix} 1 & 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 4 & 2 & 1 & 0 \end{pmatrix}$$

Stabile Matrix-Interpretation ist bis heute die einzige Methode, die für dieses System Termination zeigt.

Eine Hierarchie

- Die *Dimension* eines Ungleichungssystems U über einem Ring M ist die kleinste Zahl d, so daß es stabile U-Interpretation in $M^{d\times d}$ gibt.
- $\{a^2 > bc, b^2 > ac, c^2 > ab\}$ hat Dimension ≤ 5 über $\mathbb{Z}$.
- Ist diese Dimensions-Hierarchie *echt*?
- in Matrixringen gelten polynomielle Identitäten: in $M^{2\times 2}$ gilt $[[a,b]^2, c] = 0$ mit $[x,y] := xy - yx$.
- also hat $\{ababc > cbaba, babac > cabab, cabba > abbac, cbaab > baabc\}$ nicht die Dimension 2.

Grenzen des Wachstums

Gegeben ein stabiles Modell (Menge von Matrizen) i für Ungleichungssystem U zu Ersetzungssystem R.
Wachstumsfunktion $w : n \mapsto \max\{i(x)_{j,k} \mid x, j, k\}$.
Das System R hat Ableitungskomplexität $O(w)$.
Triviale obere Schranke ist exponentiell.
Beispiele für $ab > ba$:

- $i(a) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, i(b) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ exponentiell
- $i(a) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, i(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ quadratisch

(obere Dreiecksmatrizen mit Diagonal-Einträgen ≤ 1)

Grenzen des Wachstums (II)

- Welche Wachstumsfunktionen sind *darstellbar*?
- Gilt ein *gap theorem* (nur polynomielles und exponentielles Wachstum)?
- Kann man den Grad des Polynoms berechnen?
- . . . oder entscheiden, ob er $\le d$ ist?

Grenzen des Wachstums (III)

Vergleiche entscheidbare Fragen zu

- *Wachstum von D0L-Folgen*
  Bsp: $\phi^n(a)$ für $\phi : a \mapsto abc, b \mapsto ac, c \mapsto a$,
  entspr $\{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}\}$),
- *Dichtefunktionen* von regulären Sprachen
  $d_L : n \mapsto \#\{w \mid w \in \Sigma^* \cap L\}$.
  Bsp: $d_{a^*b^*c^*} = \Theta(n^2)$.

Schrittweise Konstruktion von Modellen

vgl. relative Termination

- Wenn $i_1 : V \to M_1$ ein Modell für das Ungleichungssystem U_1 und ein (Quasi-)Modell für das Gleichungssystem U_2 ist
- und $i_2 : V \to M_2$ ein Modell für das Ungleichungssystem U_2,
- dann ist das *lexikografische Produkt* $i : V \mapsto M_1 \times M_2 : a \mapsto (i_1(a), i_2(a))$ ein Modell für das Ungleichungssytem $U_1 \cup U_2$.

$M_1 \times M_2$ ist geordneter Ring: Operationen unabhängig komponentenweise, Ordnung lexikografisch

Schrittweise Konstruktion (Beispiel)

- $U = \{as > sa, babs > absa, bab^2 > abab, aba^2 > baba\}$
- $U_1 = \{as > sa, babs > absa\}$ und Interpretation

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

$$as - sa = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, babs - absa = \begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix} - \begin{pmatrix} 1 & 5 \\ 0 & 2 \end{pmatrix},$$

$$bab^2 - abab = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, aba^2 - baba = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$$

- bleibt $U_2 = \{bab^2 > abab, aba^2 > baba\}$

Schrittweise Konstruktion (Beispiel cont.)

$U_2 = \{bab^2 > abab, aba^2 > baba\}$

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

$$bab^2 - abab = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & 1 & 0 & 5 \\ 2 & 0 & 0 & 2 \\ 6 & 0 & 0 & 4 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$aba^2 - baba = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 2 & 0 \\ 6 & 0 & 4 & 0 \\ 2 & 0 & 2 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 0 & 2 & 0 \end{pmatrix}$$

Bestimmung der Matrixeinträge

- Einträge als Unbekannte über $\mathbb{N}$, gibt System von Ungleichungen zwischen Polynomen.
- Exakte Lösung praktisch nicht möglich (Grad ist > 1).
- Iterative Lösung (diskrete Optimierung, z. B. genetische Algorithmen).
- nach Festhalten von Dimension und maximaler Höhe der Einträge ergibt sich ein endliches Problem, das kann im Prinzip durch *finite domain constraint solver* behandelt werden.

Bestimmung der Matrixeinträge (II)

- Unbekannte als Binärzahlen ansetzen,
- dann Constraints als logische Schaltung (aussagenlogische Formel) kodieren, (benötigt viele viele Hilfsvariablen: Matrixprodukte, Skalarprodukte, Summation, Multiplikation)
- dann dafür erfüllende Belegung suchen.
- benutzen SateliteGTI, Gewinner der SAT competition 2005.
- dieses Verfahren allein löst ca. 95 von 125 Problemen aus der Termination Problen Data Base