Termination of String Rewriting with Matrix Interpretations

Dieter Hofbauer, Kassel
Johannes Waldmann, HTWK Leipzig

Zantema's Problem : $a^2b^2 \to b^3a^3$

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

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

termination follows since all entries are ≥ 0
and marked entries are $\boxed{\geq 1}$.

Ring Interpretations

homomorphism: $\Sigma^* \to$ ordered ring $(D, +, \cdot, >)$

- multiplication ($\Rightarrow$ concatenation)
- addition/<u>subtraction</u> ($\Rightarrow$ rule application)

For step $xly \to_R xry$,

$i(xly) - i(xry) = i(x) \cdot \Big(i(l) - i(r)\Big) \cdot i(y).$

Proof obligation for termination of system R:

$$i(\Sigma^*) \cdot i(R) \cdot i(\Sigma^*) \in P$$

…where $(D, >)$ well-founded, $P := \{x \mid x > 0\}$,
$i(R) := \{i(l) - i(r) \mid (l \to r) \in R\}$

Admissable Differences

Given a set $A = i(\Sigma)$ of positive ring elements, define $\mathrm{core}(A) := \{d \mid A^* \cdot d \cdot A^* \subseteq P\}$.

Definition: $i : \Sigma^* \to D$ is an A-interpretation for R iff $i(\Sigma) \subseteq A$ and $i(R) \subseteq \mathrm{core}(A)$.

Theorem: For rewriting systems R and S over Σ: if i is A-interpretation for R with $i(S) \subseteq P \cup \{0\}$, then R terminates relative to S.

Illustration of Theorem

use $M := \{m \mid \forall i \exists j : m_{i,j} > 0\}$. (in each row, at least one positive entry). Then $\mathrm{core}(M) = M$.

$R = \{aa \to aba\}, S = \{b \to bb\}$.

M-interpretation $i : a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, b \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

$i(aa \to aba) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$

$i(b \to bb) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = 0$

R terminates relative to S.

More interesting matrix shapes

$E := \{m \mid \forall i : m_{i,i} > 0\}$. Then $\mathrm{core}(E) = P$.

$$\begin{pmatrix} * & \boxed{+} \\ * & * \end{pmatrix} \subseteq \mathrm{core}\begin{pmatrix} \boxed{+} & * \\ * & \boxed{+} \end{pmatrix}$$

also works for subsets of indices:
if $B = \begin{pmatrix} A & * \\ * & * \end{pmatrix}$, then $\begin{pmatrix} \mathrm{core}(A) & * \\ * & * \end{pmatrix} \subseteq \mathrm{core}(B)$.

proof of $a^2b^2 \to b^3a^3$ uses

$$\begin{pmatrix} \cdots & \boxed{+} \\ \vdots \ \ddots & \vdots \\ \cdots & \cdot \end{pmatrix} \subseteq \mathrm{core}\begin{pmatrix} \boxed{+} & \cdots & \cdot \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \boxed{+} \end{pmatrix}$$

Performance of Matrix Tools

(percentage of YES in 2006 SRS competition)

- MultumNonMulta (Dieter Hofbauer): uses only the matrix method: 51 %
- Matchbox/Satelite (J. W.): labelling, matrices, RFC match-bounds: 68 %
- Torpa (Hans Zantema): various techniques, including 3×3 matrices: 75 %
- Jambox (Jörg Endrullis): $\approx$ Matchbox + dependency pairs: 94 %

Implementation (1)

random guesses or complete enumeration:

Torpa uses matrix shape $\begin{pmatrix} 0 & * & + \\ 0 & * & * \\ 0 & 0 & 0 \end{pmatrix} \subseteq \mathrm{core}\begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & 0 & 1 \end{pmatrix}$

with $* \in \{0, 1, 4\}$, in 36% of its proofs, e.g. z007:

```
TORPA 1.6 is applied to
a b  -> b a , b a  -> a a c b ,
[A] Choose interpretation in NxN,
order :  (x,y) > (x',y') <==> x > x' & y >= y'
a : lambda (x,y) . (x+y,4y)
b : lambda (x,y) . (x,4y+1)
c : lambda (x,y) . (x,0)
remove: a b  -> b a
```

Implementation (2)

MultumNonMulta:
GNU Linear Programming Kit for shape $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$
and “sophisticated guesses” for larger dimensions,
e. g. r10: $\{ba^2b \to a^4, ab^2a \to b^4\}/\{b \to b^3\}$

```
a: | 1 0 1 0 0 0 0 0 0 0 0 0 0 0 |      b: | 1 0 0 0 0 0 0 0 1 0 0 0 0 0 |
   | 0 1 0 0 0 0 0 0 0 0 0 0 0 0 |         | 0 1 0 0 0 0 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |         | 0 0 0 1 0 1 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |         | 0 0 0 0 1 0 0 0 0 0 0 0 0 0 |
   | 0 1 0 0 0 0 0 0 1 0 0 0 0 0 |         | 0 0 0 0 0 1 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 1 0 0 0 0 0 0 0 |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 1 0 0 0 0 0 0 |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |
   | 0 0 1 0 0 0 0 0 0 0 0 0 0 0 |         | 0 1 0 0 0 0 0 0 0 0 0 1 0 1 |
   | 0 0 0 0 0 0 0 0 0 1 0 0 0 0 |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 0 0 0 1 0 0 0 |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 0 0 0 0 1 0 0 |         | 0 0 1 0 1 0 0 0 0 0 0 0 0 0 |
   | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |         | 0 0 0 0 0 0 0 0 1 0 0 0 1 0 |
   | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 1 |
   | 0 0 0 0 0 1 0 0 0 0 0 0 0 0 |         | 0 0 0 0 0 0 0 0 1 0 0 0 0 0 |
```

(found in 250 seconds)

Implementation (3)

- fix dimension, say 5. $\Rightarrow$ constraint system with $|\Sigma| \cdot d^2$ unknowns (entries in interpretation) and $|R| \cdot d^2$ constraints (entries in differences)
- fix maximal value for entries, say 7. $\Rightarrow$ finite domain constraint system
- represent unknowns in binary $\Rightarrow$ boolean satisfiability problem, (15.000 variables, 90.000 clauses, 300.000 literals) $\Rightarrow$ solve by SAT solver (SateliteGTI) (z001 takes 7 seconds)
- Jambox: linear programming $+$ SAT solving, Matchbox: likewise, but . . .

Implementation (4)

. . . Matchbox uses only one bit per matrix entry (computation in $\{0, 1\} \subset \mathbb{N}$, so $1 + 1$ is “forbidden”)

Limits (I): Growth

Entries in powers of a fixed matrix are bounded by an exponential function of the exponent.

There can be no strictly monotone matrix interpretation for a rewriting system with longer than exponential derivations.

But there could be matrix proof by step-wise removal of rules.

It cannot, for systems with long derivations where each rule occurs (roughly) equally often, e.g. $\{ab \to bca, cb \to bbc\}$ (z018, z020)

Limits (II): Dimension

Matrix rings obey certain polynomial identities, e.g.

- dim 1, $[A, B] = 0$. No one-dimensional termination proof for $\{ab \to ba\}$
- dim 2, $[[A, B]^2, C] = 0$. No 2-dim proof for $\{abcbc \to cbcba, acbcb \to bcbca, bccba \to abccb, cbbca \to acbbc\}$.

(Notation uses commutator $[A, B] := AB - BA$)
Consider SRS hierarchy defined by “minimal matrix proof dimension”:

- is every level inhabited?
- what levels are decidable?

Zantema’s “other” Problem

$\{a^2 \to bc, b^2 \to ac, c^2 \to ab\}$ = RTALOOP 104 = z086 , solved by strictly monotone interpretation

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

This interpretation grows exponentially (see $\boxed{}$).
Exact complexity of z086 is open.
suggest RTALOOP $104'$: is it polynomial?