Growth Functions for Ordered Monoids and Semi-rings

Johannes Waldmann, HTWK Leipzig, Germany

Motivation: Rewriting

alphabet Σ, rule $\Sigma^* \times \Sigma^*$,
rewriting system (semi-Thue system) R: set of rules,
rewrite relation on Σ^*: rule application in context

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

is (Turing complete) model of computation.

- termination (no infinite $\to_R$-chain)
- resource bounds (derivational complexity dc_R).
  $\mathrm{dh}_R(w) = \sup\{k \mid w \to_R^k w'\}$,
  $\mathrm{dc}_R(n) = \sup\{\mathrm{dh}_R(w) \mid n \geq |w|\}$.

Example: $R = \{ab \to ba\}$,
then $\underline{ab}ab \to_R ba\underline{ab} \to_R b\underline{ab}a \to_R bbaa$
$\mathrm{dh}_R(abab) = 3, \mathrm{dc}_R(n) = \lfloor n/2 \rfloor \cdot \lceil n/2 \rceil \in \Theta(n^2)$ (bubblesort)

Motivation: Monoids

Given rewriting system R over Σ,
find ordered monoid $(M, >)$ and morphism (interpretation) $i : \Sigma^* \to M$
such that $x \to_R y$ implies $i(x) > i(y)$.

deduce properties of $\to_R$ from properties of $(M, >)$.
(termination/well-foundedness, derivational complexity/height)

Motivation: Monoids

Given rewriting system R over Σ,
find ordered monoid $(M, >)$ and morphism (interpretation) $i : \Sigma^* \to M$
such that $x \to_R y$ implies $i(x) > i(y)$.

deduce properties of $\to_R$ from properties of $(M, >)$.
(termination/well-foundedness, derivational complexity/height)

special case: $M =$ the (matrix) monoid generated by a weighted automaton.

- suitable weight semiring
- suitable automaton

Strict partially ordered monoids

(cf. Fuchs: *Partially Ordered Algebraic Systems*, 1963)
If $(M, >)$ is strict p.o. ($a > b$ implies $ac > bc$ and $ca > cb$),
then $i(l) > i(r)$ for $(l, r) \in R$ implies $i(u) > i(v)$ for $u \to_R v$.

Strict partially ordered monoids

(cf. Fuchs: *Partially Ordered Algebraic Systems*, 1963)
If $(M, >)$ is strict p.o. ($a > b$ implies $ac > bc$ and $ca > cb$),
then $i(l) > i(r)$ for $(l, r) \in R$ implies $i(u) > i(v)$ for $u \to_R v$.

Example: $M = (\mathbb{N}, 0, +, >)$
$R = \{aba \to ab^3\}$, $i : a \mapsto 1, b \mapsto 0$

Strict partially ordered monoids

(cf. Fuchs: *Partially Ordered Algebraic Systems*, 1963)
If $(M, >)$ is strict p.o. ($a > b$ implies $ac > bc$ and $ca > cb$),
then $i(l) > i(r)$ for $(l, r) \in R$ implies $i(u) > i(v)$ for $u \to_R v$.

Example: $M = (\mathbb{N}, 0, +, >)$
$R = \{aba \to ab^3\}$, $i : a \mapsto 1, b \mapsto 0$

in general, M will not be commutative,
since order of letters matters in rewriting, e.g. $R = \{ab \to ba\}$

Strict partially ordered monoids

(cf. Fuchs: *Partially Ordered Algebraic Systems*, 1963)
If $(M, >)$ is strict p.o. ($a > b$ implies $ac > bc$ and $ca > cb$),
then $i(l) > i(r)$ for $(l, r) \in R$ implies $i(u) > i(v)$ for $u \to_R v$.

Example: $M = (\mathbb{N}, 0, +, >)$
$R = \{aba \to ab^3\}$, $i : a \mapsto 1, b \mapsto 0$

in general, M will not be commutative,
since order of letters matters in rewriting, e.g. $R = \{ab \to ba\}$

$$a \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, b \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, ab = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} > \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = ba,$$

$M = \begin{pmatrix} \geq 1 & * \\ * & \geq 1 \end{pmatrix}, (>) = \begin{pmatrix} \geq & > \\ \geq & \geq \end{pmatrix}$, this is a strict p.o.

Growth of Semigroups

(cf. Okninski: *Semigroups of Matrices*, Singapore, 1998)
Let M be generated by a finite set V.
Define $V^{\leq m} := \{v_1 \cdot \ldots \cdot v_k \mid k \leq m, v_i \in V\}$.
$d_V(m) := |V^{\leq m}|$

Gelfand-Kirillov dimension GK$(M) := \limsup \log_m d_V(m)$.
(dimension $< \infty \Rightarrow$ polynomial growth)

Growth of Semigroups

(cf. Okninski: *Semigroups of Matrices*, Singapore, 1998)
Let M be generated by a finite set V.
Define $V^{\leq m} := \{v_1 \cdot \ldots \cdot v_k \mid k \leq m, v_i \in V\}$.
$d_V(m) := |V^{\leq m}|$

Gelfand-Kirillov dimension GK$(M) := \limsup \log_m d_V(m)$.
(dimension $< \infty \Rightarrow$ polynomial growth)

If R is not length-increasing,
and $(M, >)$ is strict p.o. with $i(\to_R) \subseteq >$,
then $\mathrm{dc}_R(n) \leq d_{i(\Sigma)}(n)$.

Growth of Semigroups

(cf. Okninski: *Semigroups of Matrices*, Singapore, 1998)
Let M be generated by a finite set V.
Define $V^{\leq m} := \{v_1 \cdot \ldots \cdot v_k \mid k \leq m, v_i \in V\}$.
$d_V(m) := |V^{\leq m}|$

Gelfand-Kirillov dimension GK$(M) := \limsup \log_m d_V(m)$.
(dimension $< \infty \Rightarrow$ polynomial growth)

If R is not length-increasing,
and $(M, >)$ is strict p.o. with $i(\to_R) \subseteq >$,
then $\mathrm{dc}_R(n) \leq d_{i(\Sigma)}(n)$.

but most “interesting” R will have some length-increasing rules, e.g. $a^2b^2 \to b^3a^3$.

Heights

need to consider longest descending chain *starting* in $V^{\leq m}$
$h_V(m) = \sup\{k \mid x_0 \in V^{\leq m}, x_0 > \ldots > x_k, x_i \in M\}$
examples:

- $(\mathbb{N}, +, >)$: linear
- $(\mathbb{N}, \cdot, >)$: exponential

Heights

need to consider longest descending chain *starting* in $V^{\leq m}$
$h_V(m) = \sup\{k \mid x_0 \in V^{\leq m}, x_0 > \ldots > x_k, x_i \in M\}$
examples:

- $(\mathbb{N}, +, >)$: linear
- $(\mathbb{N}, \cdot, >)$: exponential

…and staying in $V^* = \bigcup_{m \geq 0} V^m \subseteq M$:
$h_V(m) = \sup\{k \mid x_0 \in V^{\leq m}, x_0 > \ldots > x_k, x_i \in V^*\}$

- $(\mathbb{N}, \cdot, >)$: polynomial (for finite V)

since $\log x_i$ is non-negative integer linear combination of $\{\log v \mid v \in V\}$

Controlled Heights

more detailed analysis:
in each rewrite step, length increase is bounded.

$$h'_{V,B}(m) = \sup\{k \mid x_0 \in V^m, x_0 > \ldots > x_k, x_i \in V^{m+iB}\}$$

(cf. “controlled” bad sequences in constructive proofs of Higman’s theorem, see papers by Cichon and Weiermann)

Weighted Automata

$A = (\Sigma, W, Q, \lambda, \mu, \gamma)$ with alphabet Σ, weight semiring W, set of states Q, initial weights $\lambda : Q \times 1 \to W$, transitions $\mu : \Sigma \to (Q^2 \to W)$, final weights $\gamma : 1 \times \Sigma \to W$.
$A(w) = \lambda \cdot \mu(w) \cdot \gamma$.
$\mu(\Sigma)$ generates a (matrix) monoid M.
To get strict p.o. on M, need

- multiplication on W: strict (e.g., plus, times)
- addition on W:
  - strict (plus),
  - half strict (min, max):
    $a > b \wedge c > d \Rightarrow (a + c) > (b + d)$

(cf. Waldmann: WATA06, JALC07)
Note: M must be free of zero divisors.

General Value Bounds

…for weighted automata

- arctic $(\mathbb{N} \cup \{-\infty\}, \max, +)$: linear
- tropical $(\mathbb{N} \cup \{+\infty\}, \min, +)$: linear
- standard $(\mathbb{N}, +, \cdot)$: exponential

General Value Bounds

. . . for weighted automata

- arctic $(\mathbb{N} \cup \{-\infty\}, \max, +)$: linear
- tropical $(\mathbb{N} \cup \{+\infty\}, \min, +)$: linear
- standard $(\mathbb{N}, +, \cdot)$: exponential

get polynomial bounds by restricting shapes
(e.g., upper triangular, with $\{0, 1\}$ on main diagonal)

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

this is an instance of a more general result

Bounds, Growth and Ambiguity

(Schützenberger 1962, Jacob 1978) It is decidable whether a $\mathbb{Z}$-rational series is

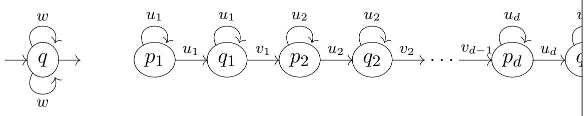
- bounded
- polynomially growing

Bounds, Growth and Ambiguity

(Schützenberger 1962, Jacob 1978) It is decidable whether a $\mathbb{Z}$-rational series is

- bounded
- polynomially growing

restrict to non-negative numbers: $(\mathbb{N}, +, \cdot)$-automata:
measure the ambiguity of classical automata;
detect polynomially, exponentially growing ambiguity
(cf. Weber and Seidl, 1991, conditions EDA, IDA$_d$)

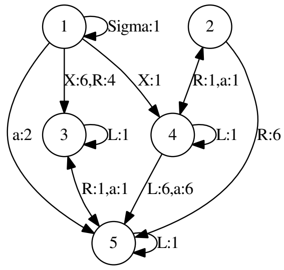


Bounds, Growth and Ambiguity

polynomial growth as constraint system:

- SCCs must have weights 1 and be unambigious,
- height of SCC decomposition gives degree bound)

combined with constraints for $i(l) > i(r)$ (Waldmann, RTA10)



Question

what ordered weight semiring W with

- strict multiplication (except at 0)
- and strict or half-strict addition

gives a quadratic (polynomial) general bound for height of finitely generated matrix monoids (= weights computed by W-automata)?

recall:

- half-strict: arctic (max,plus), tropical (min,plus): linear
- strict: standard (plus,times): exponential

Half-Strict and Linear

Arctic semiring (max,plus)

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

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

monoid $M = \begin{pmatrix} \neq -\infty & * \\ * & * \end{pmatrix}$, ordered by $\begin{pmatrix} >_0 & >_0 \\ >_0 & >_0 \end{pmatrix}$,
where $x >_0 y := (x = -\infty = y) \vee (x > y)$

Half-Strict and Quadratic

Gaubert suggested:

- $G = -\infty \cup \{(x, y) \mid x \geq y \geq 0\}$,
- $(x_1, y_1) \otimes (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$,
- $\oplus$ = lexicographic max.

Half-Strict and Quadratic

Gaubert suggested:

- $G = -\infty \cup \{(x, y) \mid x \geq y \geq 0\}$,
- $(x_1, y_1) \otimes (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$,
- $\oplus$ = lexicographic max.

Cannot find G-matrices A, B with $AB > BA$.
Some axiom missing?

Half-Strict and Quadratic

Gaubert suggested:

- $G = -\infty \cup \{(x, y) \mid x \geq y \geq 0\}$,
- $(x_1, y_1) \otimes (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$,
- $\oplus$ = lexicographic max.

Cannot find G-matrices A, B with $AB > BA$.
Some axiom missing?

Test case: prove "automatically" the quadratic derivational complexity for $\{a^2 \to bc, b^2 \to ac, c^2 \to ab\}$

open since 2006, solved "manually" by Adian 2009.