Noncommutative rational Pólya series

Daniel Smertnig

University of Graz, Austria

joint work with **Jason Bell** (U. Waterloo, Canada)

doi:10.1007/s00029-021-00629-2

NCRA VII, Lens/Online, July 6, 2021

Motivation - A theorem of Pólya

Let K be a field and

$$S = \sum_{n=0}^{\infty} s_n x^n \in K[\![x]\!]$$

the (formal) power series expansion of a rational function

$$S = P(x)/Q(x) \qquad \text{with polynomials } P,\ Q \text{ and } Q(0) \neq 0.$$

Equivalently, the sequence s_n satisfies a linear recurrence relation.

Definition

S is a **Pólya series** if there exists a finitely generated subgroup G of $K^\times$, such that $s_n \in G_0 := G \cup \{0\}$ for all $n \geq 0$.

$K = \mathbb{Q}$: Equivalently, there are finitely many prime numbers p_1, $\dots$, p_r such that **every** nonzero coefficient is of the form

$$s_n = \pm p_1^{e_1} \cdots p_r^{e_r} \qquad (e_i \in \mathbb{Z}).$$

Example

1. Geometric series, e.g., $\frac{1}{1-2x} = \sum_{n=0}^{\infty} 2^n x^n$.
2. „Merges“ of geometric series, e.g.,

$$\sum_{n=0}^{\infty} 2^n x^{2n} + 5 \cdot \sum_{n=0}^{\infty} 3^n x^{2n+1}.$$

3. If S is a rational Pólya series, and P is a polynomial then $S + P$ is a rational Pólya series.

Pólya: All (univariate) rational Pólya series are essentially of this form (=merges of geometric series, plus a polynomial)!

Theorem (Pólya 1921; Benzaghou 1970; Bézivin 1987)

Let $S \in K[\![x]\!]$ be a rational series. Then S is a Pólya series if and only if there exist a polynomial $P \in K[x]$ such that

$$S(x) = \sum_{r=0}^{d-1} \frac{\alpha_r x^r}{1 - \beta_r x^d} + P(x) \qquad (d \geq 0,\ \alpha_r, \beta_r \in K).$$

(Noncommutative) rational series

Noncommutative (formal) power series

Let …

- K be a field;
- $A = \{a, b, c, \ldots\}$ a finite, non-empty set (**alphabet**);
- A^* the free monoid over A
  (E.g., if $A = \{a, b\}$, then $A^* = \{\varepsilon, a, b, ab, ba, a^2, b^2, a^3, \ldots\}$).

Let $K\langle\langle A\rangle\rangle$ be the algebra of formal, **noncommutative power series**:

$$S = \sum_{w \in A^*} \underbrace{S(w)}_{\in K} w.$$

$(S + T)(w) = S(w) + T(w)$ and $(S \cdot T)(w) = \sum_{\substack{u,v \in A^* \\ w = uv}} S(u)T(v)$.

Rational series

Definition

$S \in K\langle\langle A \rangle\rangle$ is **rational** if it can be obtained from noncommutative polynomials by the operations $+$, $\cdot$, and $*$, where

$$S^* = \frac{1}{1 - S} = \sum_{n=0}^{\infty} S^n \qquad (\text{if } S(\varepsilon) = 0).$$

- Subalgebra of $K\langle\langle A \rangle\rangle$.
- Univariate case ($A = \{x\}$) recovers "usual" rational series.

Schützenberger's Theorem

Theorem (Schützenberger)

For $S \in K\langle\langle A \rangle\rangle$ the following statements are equivalent.

1. S is rational.
2. There exists $d \geq 0$, a row vector $u \in K^{1\times d}$, column vector $v \in K^{d\times 1}$ and a monoid homomorphism $\mu\colon A^* \to K^{d\times d}$ such that
$$S(w) = u\mu(w)v.$$
3. S is recognized by a weighted finite automaton (WFA).

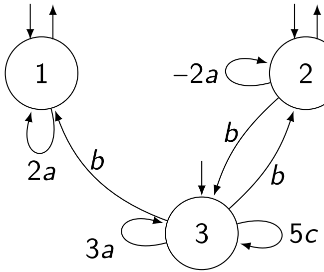
Note: Many different linear representations/WFAs give rise to the same series!

Example

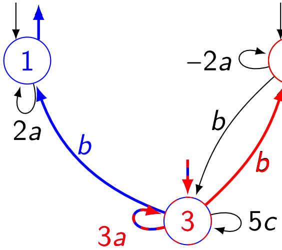
$A = \{a, b, c\},\ K = \mathbb{Q}$

$$u = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \qquad v = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}^T$$

$$\mu(a) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \mu(b) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \quad \mu(c) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$



Example



- For $w \in A^*$, find all accepting paths (from initial to terminal state) labeled by w.
- For each path form the product of all weights along the path.
- $S(w)$ is the sum of all these products.

$$S(a^2b) = 3 \cdot 3 \cdot 1 + 3 \cdot 3 \cdot 1 = 18.$$

$$S = 2 + 2b + 8a^2 + 10cb + 6ab + \cdots + 18a^2b + \cdots \in \mathbb{Q}\langle\langle a, b, c\rangle\rangle$$

Pólya series

Pólya series

Definition

$S \in K\langle\langle A \rangle\rangle$ is a **Pólya series** if there exists a finitely generated subgroup G of $K^\times$, such that $S(w) \in G_0 := G \cup \{0\}$ for all words $w \in A^*$.

Reutenauer (1979): Conjecture characterizing noncommutative rational Pólya series.

Pólya's Theorem for noncommutative series

Theorem (Bell-S., '19)

Let $S \in K\langle\langle A \rangle\rangle$ be a rational series. TFAE.

1. S is a Pólya series.
2. S is an **unambiguous** rational series.
3. S is recognized by an **unambiguous** WFA.
4. There exist $\lambda_1, \dots, \lambda_k \in K^\times$, linearly bounded rational series $a_1, \dots, a_k \in \mathbb{Z}\langle\langle A \rangle\rangle$, and a regular language $\mathcal{L} \subseteq A^*$ such that $\operatorname{supp}(a_i) \subseteq \mathcal{L}$ for all $i \in [1, k]$ and
$$S(w) = \begin{cases} \lambda_1^{a_1(w)} \cdots \lambda_k^{a_k(w)} & \text{if } w \in \mathcal{L}, \\ 0 & \text{if } w \notin \mathcal{L}. \end{cases}$$
5. S is Hadamard sub-invertible ($\sum_{w \in \operatorname{supp}(S)} S(w)^{-1} w$ is rational).

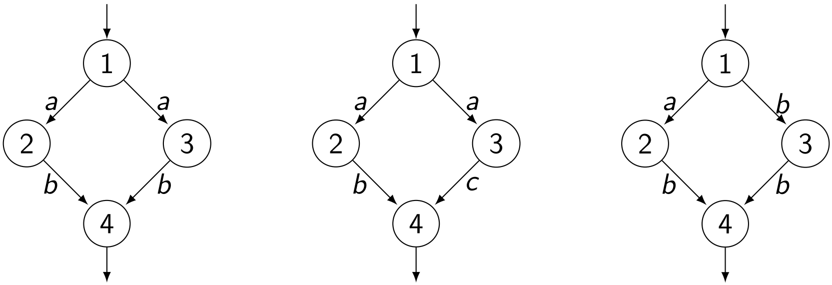
Also works over completely integrally closed domains (e.g. $\mathbb{Z}$).

Unambiguous rational series

A rational series S is **unambiguous** if it can be constructed from noncommutative polynomials using **unambiguous** operations:

- $T + T'$ if $\mathrm{supp}(T) \cap \mathrm{supp}(T') = \varnothing$.
- TT' if for every $w \in \mathrm{supp}(T)\,\mathrm{supp}(T')$ there exist **unique** $u \in \mathrm{supp}(T)$, $v \in \mathrm{supp}(T')$ with $w = uv$.
- T^* if $\mathrm{supp}(T)$ is a code (=the basis of a free monoid)

Unambiguous/sequential WFAs



ambiguous *unambiguous* *sequential*

unambiguous: at most one accepting path for each word
sequential: reading a word left to right, at each step there is at most one branch to follow

sequential ⇒ unambiguous

Ingredients of the proof

Linear Zariski topology

Definition

$K^{1\times d} \supseteq X$ is **closed** if it is a finite union of vector subspaces.

Let (u, μ, v) be a minimal linear representation for a rational Pólya series S (+suitable change of basis).

Definition

The **(left) linear hull** of (u, μ, v) is the closure $\overline{\Omega}$ of

$$\Omega = \{ u\mu(w) : w \in A^* \} \subseteq K^{1\times d}.$$

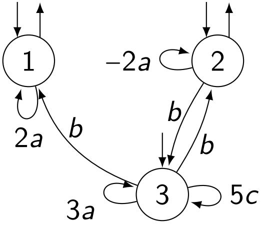
Irreducible components:

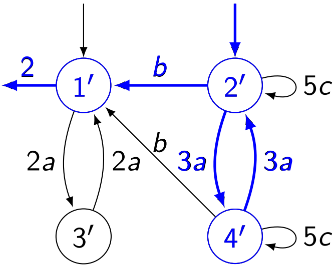
$$\overline{\Omega} = V_1 \cup \cdots \cup V_l.$$

New linear representation (u', μ', v') of S on

$$V_1 \oplus \cdots \oplus V_l.$$

Example





Linear hull:

$\langle e_1 + e_2, e_3 \rangle \cup \langle e_1 - e_2, e_3 \rangle \subseteq K^{1\times 3}$.

$S(a^2 b) = 3 \cdot 3 \cdot 1 \cdot 2 = 18.$

$$\mu'(a) = \left[\begin{array}{cc:cc} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ \hdashline 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \end{array}\right] \quad \mu'(b) = \left[\begin{array}{cc:cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array}\right] \quad \mu'(c) = \left[\begin{array}{cc:cc} 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 \end{array}\right]$$

$$u' = (1, 1, 0, 0), \qquad v' = (2, 0, 0, 0)^T$$

Unit equations

Suppose K has **characteristic** 0.

A solution $(y_1 : \ldots : y_n) \in \mathbb{P}^{n-1}(K)$ of

$$X_1 + \cdots + X_n = 0 \tag{1}$$

is **non-degenerate** if, for all $\varnothing \neq I \subsetneq [1, n]$ one has $\sum_{i \in I} y_i \neq 0$.

Theorem (Evertse 1984; van der Poorten-Schlickewei 1982)

Let $G \leq K^{\times}$ be a finitely generated subgroup. There exist only finitely many non-degenerate solutions $(y_1 : \ldots : y_n) \in \mathbb{P}^{n-1}(K)$ of (1) with $y_1, \ldots, y_n \in G$.

Unit equations - The key lemma

$\Omega \cap V_i$ is dense in V_i.

Lemma

Let $\operatorname{char} K = 0$, $G \leq K^\times$ finitely generated.

Let V be a vector space with basis $e_1, \ldots, e_n$, and suppose

$$\Omega \subseteq G_0 e_1 + \cdots + G_0 e_n$$

with $\overline{\Omega} = V$.

Then, if $\varphi \in \operatorname{Hom}_K(V, K)$ with $\varphi(\Omega) \subseteq G_0$, there exists at most one $i \in [1, n]$ with $\varphi(e_i) \neq 0$.

Positive characteristic: similar idea but harder; using a theorem of **Derksen–Masser 2012**.

Summary

- Noncommutative rational Pólya series admit a natural structural characterization (resolving a conjecture of Reutenauer from 1979).

- Proof mixes elements from algebra, automata theory, and number theory.