Polynomial functions and sequential products

Jean-Éric Pin[1]

based on results with Christophe Reutenauer[2]

[1]IRIF, CNRS et Université de Paris

[2]Mathématiques, Université du Québec à Montréal, Montréal, CP 8888, succ. Centre Ville, Canada H3C 3P8.

WATA, April 2021

Polynomial functions from $\mathbb{N}$ to $\mathbb{Z}$

A polynomial function $f = \mathbb{N} \to \mathbb{Z}$ is defined by a polynomial. For instance

$$f(n) = 3n^2 - 4n + 1$$
$$f(n) = (n+3)^3$$

are polynomial functions.

Is there a noncommutative version of this notion?

More precisely, let G be a group and let $f : A^* \to G$ be a function. When should f be called a polynomial function?

Polynomial functions and Taylor series

Let $f : \mathbb{R} \to \mathbb{R}$ be an analytic function on a neighborhood of 0.

Proposition

The following conditions are equivalent:

(1) f *is a polynomial function,*

(2) *there is a* $d \geqslant 0$ *such that, for all* $n > d$, $f^{(n)} = \mathbf{0}$,

(3) *there is a* $d \geqslant 0$ *such that, for all* $n > d$, $f^{(n)}(0) = 0$.

Is there a discrete version of this result?

The difference operator Δ

The difference operator associates to each function $f = \mathbb{N} \to \mathbb{Z}$ the function $\Delta f : \mathbb{N} \to \mathbb{Z}$ defined by

$$\Delta f(n) = f(n+1) - f(n)$$

Thus

$$(\Delta^2 f)(n) = f(n+2) - 2f(n+1) + f(n)$$

$$(\Delta^k f)(n) = \sum_{0 \leqslant r \leqslant k} (-1)^r \binom{k}{r} f(n+r)$$

By convention

$$(\Delta^0 f)(n) = f(n)$$

Two examples

Let $f(n) = r^n$. Then

$$\Delta f(n) = r^{n+1} - r^n = r^n(r-1)$$

$$\Delta^2 f(n) = (r^{n+2} - r^{n+1}) - (r^{n+1} - r^n) = r^n(r-1)^2$$

$$\Delta^k f(n) = r^n(r-1)^k$$

Let f be the parity function

$$f(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$$

$$\Delta^k f(n) = \begin{cases} (-1)^{k-1}2^{k-1} & \text{if } n \text{ is even} \\ (-1)^k 2^{k-1} & \text{if } n \text{ is odd} \end{cases}$$

Polynomial functions and difference operator

Let $f : \mathbb{N} \to \mathbb{Z}$ be a function. For each $n \geqslant 0$, set

$$\delta_n f = (\Delta^n f)(0).$$

Proposition

The following conditions are equivalent:

(1) f *is a polynomial function,*

(2) *there is a* $d \geqslant 0$ *such that, for all* $n > d$, $\Delta^n f = \mathbf{0}$,

(3) *there is a* $d \geqslant 0$ *such that, for all* $n > d$, $\delta_n f = 0$.

Noncommutative extensions

$\mathbb{N} \to A^*$, the free monoid on the alphabet A.

$\mathbb{Z} \to F(B)$, the free group on B.

Can one define polynomial functions from A^* to a group G?

At first sight, it seems to be doomed to failure, since the definition of a polynomial function requires the two operations of the ring $\mathbb{Z}$, when there is only one operation in a group.

However, one can try to extend the previous proposition to a noncommutative setting.

Difference operator

Let G be a group and let $f : A^* \to G$ be a function. For each letter a, the difference operator Δ^a is the function $\Delta^a f : A^* \to G$ defined by

$$\Delta^a f(u) = f(u)^{-1} f(ua).$$

If $w = a_1 \cdots a_n$, then

$$\Delta^w f = \Delta^{a_1}(\Delta^{a_2}(\cdots \Delta^{a_n} f) \cdots)).$$

Finally, we set $\delta_w f = \Delta^w f(1)$.

Notation: 1 is the empty word, that is, the identity of A^*.

Example 1: the inversion function

The iterated commutator of n elements of a group is defined by $[x_1] = x_1$, $[x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$ and, for $n \geqslant 2$, $[x_1, x_2, \ldots, x_n] = [x_1, [x_2, x_3, \ldots, x_n]]$.

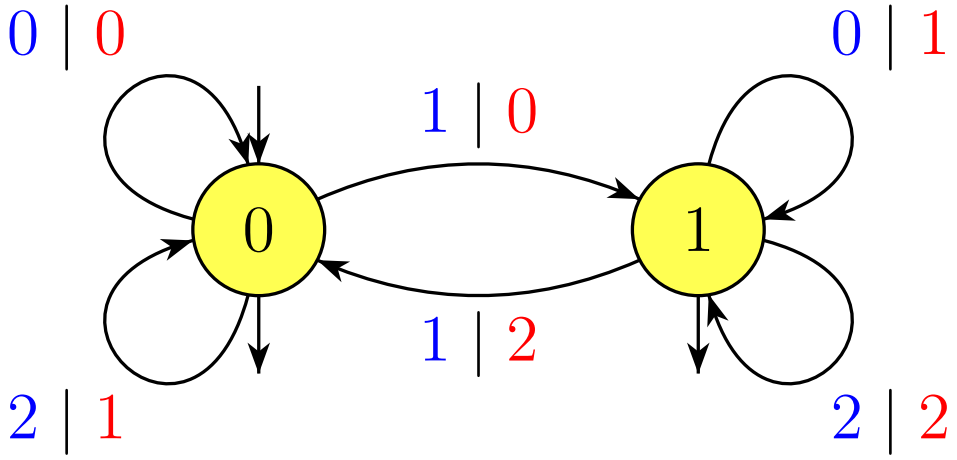
Proposition

Let $f : A^* \to F(A)$ be defined by $f(x) = x^{-1}$. Then

$$\Delta^{a_1 a_2 \cdots a_n} f(x) = x[a_1, a_2, \ldots, a_n]^{-1} x^{-1}.$$

Example 2: Division by 2 in base 3

Let $f : \{0,1,2\}^* \to \{0,1,2\}^*$ be the function which associates to a word $u \in \{0,1,2\}^*$ representing n in base 3, the unique word v of the same length as u representing the quotient of the division of n by 2.



$f(1212) = 0221$ and $f(12121) = 02210$

Example 2: Division by 2 in base 3

Let $f : \{0,1,2\}^* \to \{0,1,2\}^*$ be the function which associates to a word $u \in \{0,1,2\}^*$ representing n in base 3, the unique word v of the same length as u representing the quotient of the division of n by 2.

Example:

$$f(1212) = 0221 \quad \text{and} \quad f(12121) = 02210$$

since

$$50 = \overline{1212}^3 \quad \text{and} \quad 50/2 = 25 = \overline{0221}^3,$$
$$151 = \overline{12121}^3 \quad \text{and} \quad 151/2 = 75 = \overline{02210}^3.$$

The functions $\Delta^a f$ for $a \in \{0,1,2\}$

$$\Delta^a f(u) = \begin{cases} \text{if } a=0 & \begin{cases} 0 & \text{if } \overline{u}^3 \text{ is even} \\ 1 & \text{if } \overline{u}^3 \text{ is odd} \end{cases} \\ \text{if } a=1 & \begin{cases} 0 & \text{if } \overline{u}^3 \text{ is even} \\ 2 & \text{if } \overline{u}^3 \text{ is odd} \end{cases} \\ \text{if } a=2 & \begin{cases} 1 & \text{if } \overline{u}^3 \text{ is even} \\ 2 & \text{if } \overline{u}^3 \text{ is odd} \end{cases} \end{cases}$$

Notation. Since the alphabet is $\{0,1,2\}$, 0, 1, and 2 are letters and $\Delta^1 f(u) = f(u)^{-1} f(u1)$. For instance $\Delta^1 f(1212) = f(1212)^{-1} f(12121) = (0221)^{-1}02210 = 0$.

The functions $\Delta^w f$, for $w \in \{0,1,2\}^*$

For each $n > 0$,

$$\Delta^{1^n 0} f(u) = (0^{-1}1)^{2^{n-1}(-1)^{n-1+\overline{u}^3}}$$
$$\Delta^{1^n 1} f(u) = (0^{-1}2)^{2^{n-1}(-1)^{n-1+\overline{u}^3}}$$
$$\Delta^{1^n 2} f(u) = (1^{-1}2)^{2^{n-1}(-1)^{n-1+\overline{u}^3}}$$

and, for any other word w, $\Delta^w f$ is the constant function to the identity of $F(\{0,1,2\})$.

The functions $\Delta^w f$ are constant functions, and if w is not of the form $1^n a$, this constant is the identity.

Polynomial functions

Definition

A function $f : A^* \to G$ is a polynomial function if $\Delta^w f = \mathbf{1}$ for almost all[1] words $w \in A^*$.

The degree of f is the smallest d such that $\Delta^w f = \mathbf{1}$ for all words w of length $> d$.

[1] Almost all = all but a finite number

An equivalent definition

Definition

A function $f : A^* \to G$ is a polynomial function if $\Delta^w f = \mathbf{1}$ for almost all words $w \in A^*$. The degree of f is the smallest d such that $\Delta^w f = \mathbf{1}$ for all words w of length $> d$.

Proposition

A function $f : A^* \to G$ is a polynomial function if and only if $\delta_w f = 1$ for almost all words $w \in A^*$.

The degree of f is the smallest d such that $\delta_w f = 1$ for all words w of length $> d$.

Examples of polynomial functions

$\deg(f) = -1$ iff $f = \mathbf{1}$.

$\deg(f) = 0$ iff f is a constant function $\neq \mathbf{1}$.

$\deg(f) \leqslant 1$ iff f is an affine function, that is,
$f = f(1)h$ for some monoid morphism $h\colon A^* \to G$.

A polynomial function of degree 2:

$$f(a_1 \cdots a_n) = a_1(a_1a_2)(a_1a_2a_3) \ \cdots \ (a_1 \cdots a_n)$$

The integration problem

Integration problem

Given an element g of G and a family $(f_a)_{a \in A}$ of functions from A^* to G, find a function f such that $f(1) = g$ and $\Delta^a f = f_a$ for all $a \in A$.

A functional equation

The functions f and $\Delta^a f$, for $a \in A$, are related by the functional equation:

$$f(a_1 \cdots a_n) = f(1) \prod_{1 \leqslant i \leqslant n} \Delta^{a_i} f(a_1 \cdots a_{i-1})$$

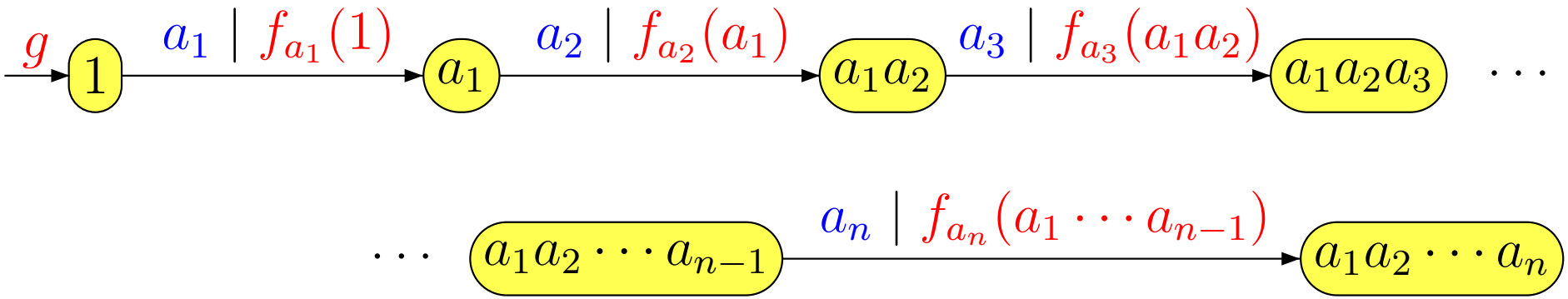
For instance,

$$\begin{aligned} & f(1)\, \Delta^a f(1)\, \Delta^b f(a)\, \Delta^c f(ab) \\ = {} & f(1)\, [f(1)^{-1} f(a)]\, [f(a)^{-1} f(ab)]\, [f(ab)^{-1} f(abc)] \\ = {} & f(abc) \end{aligned}$$

Sequential products

Given an element g of a group G and a family $(f_a)_{a\in A}$ of functions from A^* to G, the sequential product of g and $(f_a)_{a\in A}$ is the function $f\colon A^* \to G$ defined by

$$f(a_1\cdots a_n) = g\prod_{1\leqslant i\leqslant n} f_{a_i}(a_1\cdots a_{i-1}).$$



The integration problem

Integration problem

Given an element g of G and a family $(f_a)_{a \in A}$ of functions from A^* to G, find a function f such that $f(1) = g$ and $\Delta^a f = f_a$ for all $a \in A$.

Proposition

The sequential product of $f(1)$ and $(f_a)_{a \in A}$ is the unique function f such that $f_a = \Delta^a f$ for all $a \in A$.

Generating the polynomial functions

Theorem

The set of polynomial functions from A^* to G is the smallest set of functions containing the constant functions and closed under sequential product.

For instance,

$$f(a_1 \cdots a_n) = a_1(a_1a_2)(a_1a_2a_3) \ \cdots \ (a_1 \cdots a_n)$$

is the sequential product $\mathrm{Seq}(1, (f_a)_{a\in A})$ where each f_a is the affine morphism defined by $f_a(u) = ua$.

Languages

A language L is recognised by a monoid M if there exists a monoid morphism $\varphi : A^* \to M$ and a subset P of M such that $L = \varphi^{-1}(P)$.

Let p be a prime number. A p-group is a group in which the order of every element is a power of p. A finite group G is a p-group iff $|G|$ is a power of p.

A language is p-recognisable is it is recognised by a finite p-group.

Binomial coefficients (see Eilenberg or Lothaire)

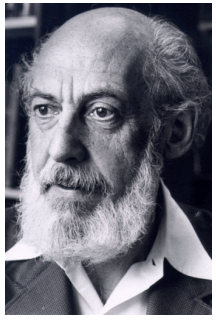
Let u and $v = a_1 \cdots a_n$ be two words of A^*. Then v is a subword of u if there exist $u_0, \ldots, u_n \in A^*$ such that $u = u_0 a_1 u_1 \cdots u_{n-1} a_n u_n$ (the u_i's might be empty words).

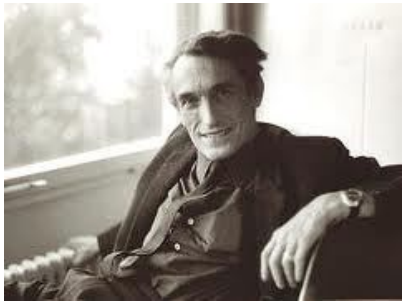
The binomial coefficient $\binom{u}{v}$ is the number of times that v appears as a subword of u.

$$abab, abab, abab. \text{ Thus } \binom{abab}{ab} = 3.$$

If $u = a^n$ and $v = a^m$, then $\binom{u}{v} = \binom{n}{m}$.

p-recognisable languages





Theorem (Eilenberg-Schützenberger 1976)

A language is p-recognisable iff it is a finite Boolean combination of the languages

$$L(x,r,p) = \left\{ u \in A^* \mid \binom{u}{x} \equiv r \bmod p \right\},$$

for $0 \leqslant r < p$ and $x \in A^*$.

Computing the subword function

Let $a_1a_2\cdots a_n$ be a word. The function τ from A^* to $\mathcal{M}_{n+1}(\mathbb{Z})$ defined by

$$\tau(u) = \begin{pmatrix} 1 & \binom{u}{a_1} & \binom{u}{a_1a_2} & \binom{u}{a_1a_2a_3} & \cdots & \binom{u}{a_1a_2\cdots a_n} \\ 0 & 1 & \binom{u}{a_2} & \binom{u}{a_2a_3} & \cdots & \binom{u}{a_2\cdots a_n} \\ 0 & 0 & 1 & \binom{u}{a_3} & \cdots & \binom{u}{a_3\cdots a_n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \binom{u}{a_n} \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is a monoid morphism.

Computing binomial coefficients modulo p

The function $\tau_p : A^* \to \mathcal{M}_{n+1}(\mathbb{Z}/p\mathbb{Z})$ defined by

$$\tau_p(u) = \tau(u) \bmod p$$

is a monoid morphism.

Furthermore, the unitriangular $n \times n$ matrices with entries in $\mathbb{Z}/p\mathbb{Z}$ form a p-group.

$\mathcal{V}$-preserving functions

Let $\mathbf{V}$ be a variety of finite monoids and let $\mathcal{V}$ be the corresponding variety of languages. A function $f : A^* \to B^*$ is $\mathcal{V}$-preserving if, for each language L in $\mathcal{V}(B^*)$, the language $f^{-1}(L)$ belongs to $\mathcal{V}(A^*)$.

if $\mathbf{V}$ is the variety

- $\mathbf{M}$ (all finite monoids) $\longrightarrow$ regularity-preserving functions;
- $\mathbf{A}$ (all aperiodic monoids) $\longrightarrow$ star-free preserving functions;
- $\mathbf{G}_p$ (all p-groups) $\longrightarrow$ p-preserving functions.

Wreath products

The wreath product $M \circ N$ of two monoids M and N is the monoid with support $M^N \times N$ and product defined, for all $(f_0, u_0), (f_1, u_1) \in M^N \times N$ by

$$(f_0, n_0)(f_1, n_1) = (f, n_0 n_1) \text{ where, for all } n \in N,$$
$$f(n) = f_0(n) f_1(n n_0)$$

The varieties $\mathbf{M}$, $\mathbf{A}$ and $\mathbf{G}_p$ are closed under wreath product.

$\mathcal{V}$-preserving functions

Theorem

If $\mathbf{V}$ *is closed under wreath product, then every sequential product of* $\mathcal{V}$*-preserving functions is* $\mathcal{V}$*-preserving.*

Corollary

If $\mathbf{V}$ *is closed under wreath product, then every polynomial function is* $\mathcal{V}$*-preserving.*

In particular $a_1(a_1a_2)(a_1a_2a_3)\ \cdots\ (a_1\cdots a_n)$ is regularity-, star-free and p-preserving.

Sketch of the proof

Let $n \in B^*$, let $(f_a)_{a \in A} : A^* \to B^*$ be a family of $\mathcal{V}$-preserving functions and let

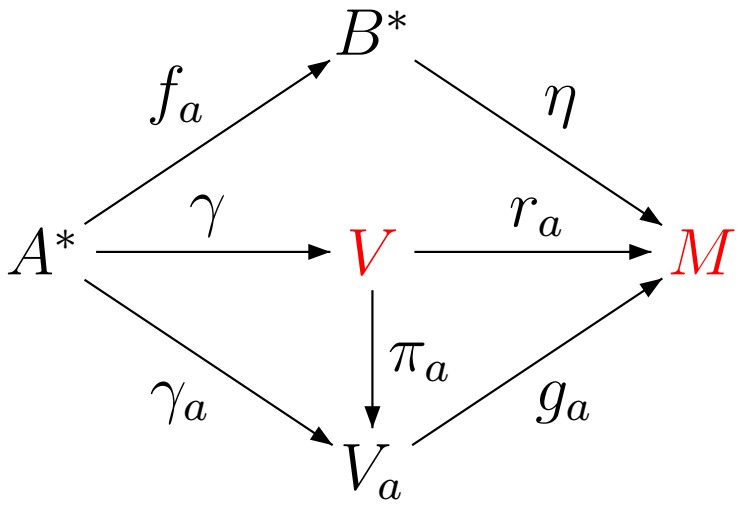
$$f = \mathrm{Seq}(n, (f_a)_{a \in A})$$

Let $L \in \mathcal{V}(B^*)$ and let $\eta : B^* \to M \in \mathbf{V}$ be its syntactic morphism. For each $m \in M$, let $L_m = \eta^{-1}(m) \in \mathcal{V}(B^*)$.

Since f_a is $\mathcal{V}$-preserving, each language $f_a^{-1}(L_m)$ belongs to $\mathcal{V}(A^*)$ and there is a surjective morphism $\gamma_a : A^* \to V_a \in \mathbf{V}$ recognising simultaneously the languages $f_a^{-1}(L_m)$.

Sketch of the proof (2)

Let $\gamma : A^* \to \prod_{a \in A} V_a$ and let $V = \gamma(A^*)$. Then $V \in \mathbf{V}$. One gets the following commutative diagram, where Greek letters are morphisms:



Then $f^{-1}(L)$ is recognised by $M \circ V$.

Synthesis problem

Describe the set of all $\mathcal{V}$-preserving functions, in particular, the sets of

(1) regularity-preserving functions,

(2) star-free preserving functions,

(3) p-preserving functions.

Pro-p metric on $F(A)$

Let A be a finite alphabet and let $u, v \in F(A)$.
Define a metric d_p on $F(A)$ by setting

$$d_p(u,v) = p^{-r_p(u,v)}$$

where

$$r_p(u,v) = \min\{n \mid G \text{ is a } p\text{-group of order } p^{n+1} \text{ that separates } u \text{ and } v\}$$

with the usual convention $\min \emptyset = -\infty$ and $p^{-\infty} = 0$.

An equivalent metric using binomial coefficients

Let A be a finite alphabet and let $u, v \in A^*$. Set

$$d'_p(u,v) = p^{-r'_p(u,v)}$$

where

$$r'_p(u,v) = \min\left\{|x| \;\middle|\; \binom{u}{x} \not\equiv \binom{v}{x} \bmod p\right\}$$

Proposition

On A^*, the metric d'_p is uniformly equivalent to d_p.

Uniform convergence

A sequence of functions $f_n : A^* \to B^*$ converges uniformly to a function $f : A^* \to B^*$ if, for all $k \geqslant 0$, there exists $N > 0$ such that, for all $n \geqslant N$, for all words x such that $|x| \leqslant k$,

$$\binom{f(u)}{x} \equiv \binom{f_n(u)}{x} \bmod p$$

The synthesis problem for p-preserving functions

Theorem (Pin-Reutenauer ICALP 2019)

A function is p-preserving iff it is the uniform limit of a sequence of polynomial functions.

Corollary

The class of p-preserving functions is the smallest set containing the constant functions and is closed under taking sequential products and uniform limits.

Contains some non recursively enumerable functions.

Other known results

$\mathcal{V}$-preserving functions are the uniformly continuous functions with respect to the pro-$\mathbf{V}$ metric.
However, this does not solve the synthesis problem.

[Reutenauer-Schützenberger, 1995] characterized the star-free preserving sequential functions.

[Cadilhac-Carton-Paperman 2017] characterized the regular-preserving functions that are p-preserving using profinite equations. However, a p-preserving function is not necessarily regular-preserving.

An example

Let $f : \mathbb{N} \to \mathbb{N}$ be the function defined as follows: $f(0) = 0$ and if $n > 0$, the binary representation of $f(n)$ is obtained from that of n by replacing the rightmost bit 1 by 0.

For instance, since $26 = \overline{11010}^2$, then $f(26) = \overline{11000}^2$, and hence $f(26) = 24$.

Then f is uniformly continuous for d_2 and 2-preserving. But it is not regularity-preserving: $\{0\}$ is a regular language, but $f^{-1}(0) = \{0\} \cup \{2^n \mid n \geqslant 0\}$ is not regular.