A Mahler's theorem for functions from words to integers

Jean-Éric Pin[1] Pedro V. Silva[2]

[1]LIAFA, CNRS and University Paris Diderot

[2]Centro de Matemática, Faculdade de Ciências, Universidade do Porto, R. Campo Alegre 687, 4169-007 Porto, Portugal.

Novembre 2010, LIPN

supported by the ESF (European Science Foundation) network AutoMathA

Outline

(1) Mahler's expansions
(2) The p-adic norm
(3) Mahler's theorem
(4) Extension to words
(5) The p-adic and pro-p topologies
(6) An extension of Mahler's theorem
(7) Real motivations

Part I

Mahler's expansion

Mahler's theorem is the dream of math students:
A function is equal to the sum of its Newton series iff it is uniformly continuous.

http://en.wikipedia.org/wiki/Mahler's_theorem

Log in / create account
article | discussion | edit this page | history

Mahler's theorem

From Wikipedia, the free encyclopedia

In mathematics, **Mahler's theorem**, named after Kurt Mahler (1903–1988), identifies one of various respects in which analysis is simpler with p-adic numbers than with real numbers.

In any field, one has the following result. Let

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

be the forward difference operator. Then for polynomial functions *f* we have the Newton series:

$$f(x) = \sum_{k=0}^{\infty} (\Delta^k f)(0) \binom{x}{k},$$

where

$$\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$$

is the *k*th binomial coefficient polynomial.

Over the field of real numbers, the assumption that the function *f* is a polynomial can be weakened, but it cannot be weakened all the way down to mere continuity.

Mahler's theorem states that if *f* is a continuous p-adic-valued function on the *p*-adic integers then the same identity holds.

The relationship between the operator Δ and this polynomial sequence is much like that between differentiation and the sequence whose *k*th term is x^k.

It is remarkable that as weak an assumption as continuity is enough; by contrast, Newton series on the complex number field are far more tightly constrained, and require Carlson's theorem to hold.

It is a fact of algebra that if *f* is a polynomial function with coefficients in any field of

navigation
- Main page
- Contents
- Featured content
- Current events
- Random article

search

Go Search

interaction
- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox
- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page

Two basic definitions

Binomial coefficients

$$\binom{n}{k} = \begin{cases} \frac{n(n-1)\ \cdots\ (n-k+1)}{k!} & \text{if } 0 \leqslant k \leqslant n \\ 0 & \text{otherwise} \end{cases}$$

Difference operator

Let $f : \mathbb{N} \to \mathbb{Z}$ be a function. We set

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

Note that

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

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

Mahler's expansions

For each function $f : \mathbb{N} \to \mathbb{Z}$, there exists a unique family a_k of integers such that, for all $n \in \mathbb{N}$,

$$f(n) = \sum_{k=0}^{\infty} a_k \binom{n}{k}$$

This family is given by

$$a_k = (\Delta^k f)(0)$$

where Δ is the difference operator, defined by

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

Examples

Fibonacci sequence: $f(0) = f(1) = 1$ and $f(n) = f(n-1) + f(n-2)$ for $(n \geqslant 2)$. Then

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

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

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

Examples (2)

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

$$\text{then } f(n) = \sum_{k>0}^{\infty} (-2)^{k-1} \binom{n}{k}$$

$$\text{Factorial} \quad n! = \sum_{k=0}^{\infty} a_k \binom{n}{k}$$

where the a_k are derangements: number of permutations of k elements with no fixed points: $1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961$.

The p-adic valuation

Let p be a prime number. The p-adic valuation of a non-zero integer n is

$$\nu_p(n) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divides } n\right\}$$

By convention, $\nu_p(0) = +\infty$. The p-adic norm of n is the real number

$$|n|_p = p^{-\nu_p(n)}$$

Finally, the metric d_p can be defined by

$$d_p(u, v) = |u - v|_p$$

Examples

Let $n = 1200 = 2^4 \times 3 \times 5^2$

$|n|_2 = 2^{-4}$ $\quad$ $|n|_3 = 3^{-1}$ $\quad$ $|n|_5 = 5^{-2}$ $\quad$ $|n|_7 = 1$

Examples

Let $n = 1200 = 2^4 \times 3 \times 5^2$

$|n|_2 = 2^{-4}$ $\quad |n|_3 = 3^{-1}$ $\quad |n|_5 = 5^{-2}$ $\quad |n|_7 = 1$

Let $u = 512$ and $v = 12$. Then $u - v = 500 = 2^2 \times 5^3$. Thus

$d_2(u, v) = 2^{-2}$ $\quad d_5(u, v) = 5^{-3}$

$d_p(u, v) = p^0 = 1$ for $p \neq 2, 5$

Mahler's theorem

Theorem (Mahler)

Let $f(n) = \sum_{k=0}^{\infty} a_k \binom{n}{k}$ *be the* *Mahler's expansion* *of a function* $f : \mathbb{N} \to \mathbb{Z}$. *TFCAE:*

(1) f *is uniformly continuous for the* p*-adic norm,*

(2) *the polynomial functions* $n \to \sum_{k=0}^{m} a_k \binom{n}{k}$ *converge uniformly to* f*,*

(3) $\lim_{k\to\infty} |a_k|_p = 0$.

(2) means that $\lim_{m\to\infty} \sup_{n\in\mathbb{N}} \left|\sum_{k=m}^{\infty} a_k \binom{n}{k}\right|_p = 0$.

Mahler's theorem (2)

Theorem (Mahler)

f is uniformly continuous iff its Mahler's expansion converges uniformly to f.

The most remarkable part of the theorem is the fact that any uniformly continuous function can be approximated by polynomial functions, in contrast to Stone-Weierstrass approximation theorem, which requires much stronger conditions.

Examples

• The Fibonacci function is not uniformly continuous (for any p).

• The factorial function is not uniformly continuous (for any p).

• The function $f(n) = r^n$ is uniformly continuous iff $p \mid r - 1$ since $f(n) = \sum_{k=0}^{\infty} (r-1)^k \binom{n}{k}$.

• If $f(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$ then $f(n) = \sum_{k>0}^{\infty} (-2)^{k-1} \binom{n}{k}$ and hence f is uniformly continuous for the p-adic norm iff $p = 2$.

Part II

Extension to words

Is it possible to obtain similar results for functions from A^* to $\mathbb{Z}$?

Questions to be solved:

(1) Extend binomial coefficients to words and difference operators to word functions.

(2) Find a Mahler expansion for functions from A^* to $\mathbb{Z}$.

(3) Find a metric on A^* which generalizes d_p.

(4) Extend Mahler's theorem.

The free monoid A^*

An alphabet is a finite set whose elements are letters ($A = \{a, b, c\}$, $A = \{0, 1\}$).
Words are finite sequences of letters. The empty word 1 has no letter. Thus 1, a, bab, $aaababb$ are words on the alphabet $\{a, b\}$. The set of all words on the alphabet A is denoted by A^*.

Words can be concatenated

$$abraca \quad dabra \rightarrow abracadabra$$

The concatenation product is associative. Further, for any word u, $1u = u1 = u$. Thus A^* is a monoid, in fact the free monoid on A.

Subwords

Let $u = a_1 \cdots a_n$ and v be two words of A^*. Then u is a subword of v if there exist $v_0, \ldots, v_n \in A^*$ such that $v = v_0 a_1 v_1 \ldots a_n v_n$.

For instance, $aaba$ is a subword of $aacbdcac$.

Binomial coefficients (see Eilenberg or Lothaire)

Given two words $u = a_1 a_2 \cdots a_n$ and v, the binomial coefficient $\binom{v}{u}$ is the number of times that u appears as a subword of v. That is,

$$\binom{v}{u} = |\{(v_0, \ldots, v_n) \mid v = v_0 a_1 v_1 \ldots a_n v_n\}|$$

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

$$\binom{v}{u} = \binom{m}{n}$$

Pascal triangle

Let $u, v \in A^*$ and $a, b \in A$. Then

(1) $\binom{u}{1} = 1$,

(2) $\binom{u}{v} = 0$ if $|u| \leqslant |v|$ and $u \neq v$,

(3) $\binom{ua}{vb} = \begin{cases} \binom{u}{vb} & \text{if } a \neq b \\ \binom{u}{vb} + \binom{u}{v} & \text{if } a = b \end{cases}$

Examples

$\binom{abab}{a} = 2 \quad \binom{abab}{ab} = 3 \quad \binom{abab}{ba} = 1$

An exercise

Verify that, for every word u, v,

$$\begin{pmatrix} 1 & \binom{u}{a} & \binom{u}{ab} \\ 0 & 1 & \binom{u}{b} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \binom{v}{a} & \binom{v}{ab} \\ 0 & 1 & \binom{v}{b} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \binom{uv}{a} & \binom{uv}{ab} \\ 0 & 1 & \binom{uv}{b} \\ 0 & 0 & 1 \end{pmatrix}$$

Computing the Pascal triangle

Let $a_1 a_2 \cdots a_n$ be a word. The function $\tau : A^* \to \mathcal{M}_{n+1}(\mathbb{Z})$ defined by

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

is a morphism of monoids.

Computing the Pascal triangle modulo p

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

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

is a morphism of monoids.

Further, the unitriangular $n \times n$ matrices with entries in $\mathbb{Z}/p\mathbb{Z}$ form a p-group, that is, a finite group whose number of elements is a power of p.

Difference operator

Let $f : A^* \to \mathbb{Z}$ be a function. For each letter a, we define the difference operator Δ^a by

$$(\Delta^a f)(u) = f(ua) - f(u)$$

One can now define inductively an operator Δ^w for each word $w \in A^*$ by setting $(\Delta^1 f)(u) = f(u)$, and for each letter $a \in A$,

$$(\Delta^{aw} f)(u) = (\Delta^a(\Delta^w f))(u)$$

Direct definition of Δ^w

$$\Delta^w f(u) = \sum_{0 \leqslant |x| \leqslant |w|} (-1)^{|w|+|x|} \binom{w}{x} f(ux)$$

Example

$$\begin{aligned}\Delta^{aab} f(u) = &-f(u) + 2f(ua) + f(ub) \\ &-f(uaa) - 2f(uab) + f(uaab)\end{aligned}$$

Mahler's expansion of word functions

Theorem (cf. Lothaire)

For each function $f : A^* \to \mathbb{Z}$, there exists a unique family $\langle f, v\rangle_{v\in A^*}$ of integers such that, for all $u \in A^*$,

$$f(u) = \sum_{v\in A^*} \langle f, v\rangle \binom{u}{v}$$

This family is given by

$$\langle f, v\rangle = (\Delta^v f)(1) = \sum_{0\leqslant |x|\leqslant |v|} (-1)^{|v|+|x|} \binom{v}{x} f(x)$$

An example

Let $f : \{0,1\}^* \to \mathbb{N}$ the function mapping a binary word onto its value: $f(010111) = f(10111) = 23$.

$$(\Delta^v f) = \begin{cases} f+1 & \text{if the first letter of } v \text{ is } 1 \\ f & \text{otherwise} \end{cases}$$

$$(\Delta^v f)(\varepsilon) = \begin{cases} 1 & \text{if the first letter of } v \text{ is } 1 \\ 0 & \text{otherwise} \end{cases}$$

Thus, if $u = 01001$, then
$f(u) = \binom{u}{1} + \binom{u}{10} + \binom{u}{11} + \binom{u}{100} + \binom{u}{101} + \binom{u}{1001} =$
$2 + 2 + 1 + 1 + 2 + 1 = 9$.

Mahler's expansion of the product of two functions

An interesting question is to compute the Mahler's expansion of the product of two functions.

Mahler's expansion of the product of two functions

An interesting question is to compute the Mahler's expansion of the product of two functions.

Proposition

Let f and g be two word functions. The coefficients of the Mahler's expansion of fg are given by

$$\langle fg, x\rangle = \sum_{v_1, v_2 \in A^*} \langle f, v_1\rangle \langle g, v_2\rangle \langle v_1 \uparrow v_2, x\rangle$$

where $v_1 \uparrow v_2$ denotes the infiltration product.

Infiltration product (Chen, Fox, Lyndon)

Intuitively, the coefficient $\langle u \uparrow v, x \rangle$ is the number of pairs of subsequences of x which are respectively equal to u and v and whose union gives the whole sequence x. For instance,

$$ab \uparrow ab = ab + 2aab + 2abb + 4aabb + 2abab$$

($4aabb$ since $aabb = aabb = aabb = aabb = aabb$)

$$ab \uparrow ba = aba + bab + abab + 2abba + 2baab + baba$$

Infiltration product (2)

The infiltration product on $\mathbb{Z}\langle\langle A\rangle\rangle$, denoted by $\uparrow$, is defined inductively by ($u, v \in A^*$ and $a, b \in A$)

$$u \uparrow 1 = 1 \uparrow u = u,$$

$$ua \uparrow bv = \begin{cases} (u \uparrow vb)a + (ua \uparrow v)b + (u \uparrow v)a & \text{if } a = b \\ (u \uparrow vb)a + (ua \uparrow v)b & \text{if } a \neq b \end{cases}$$

for all $s, t \in \mathbb{Z}\langle\langle A\rangle\rangle$,

$$s \uparrow t = \sum_{u,v \in A^*} \langle s, u\rangle\langle t, v\rangle(u \uparrow v)$$

Mahler polynomials

A function $f : A^* \to \mathbb{Z}$ is a Mahler polynomial if its Mahler's expansion has finite support, that is, if the number of nonzero coefficients $\langle f, v \rangle$ is finite.

Proposition

Mahler polynomials form a subring of the ring of all functions from A^* to $\mathbb{Z}$ for addition and multiplication.

Part III

The pro-p metric

p-groups

Let p be a prime number. A p-group is a finite group whose order is a power of p.

Let u and v be two words of A^*. A p-group G separates u and v if there is a monoid morphism from A^* onto G such that $\varphi(u) \neq \varphi(v)$.

Proposition

Any pair of distinct words can be separated by a p-group.

Pro-p metrics

Let u and v be two words. Put

$$r_p(u,v) = \min\{|G| \mid G \text{ is a } p\text{-group that separates } u \text{ and } v\}$$

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

with the usual convention $\min\emptyset = -\infty$ and $p^{-\infty} = 0$. Then d_p is an ultrametric:

(1) $d_p(u,v) = 0$ if and only if $u = v$,

(2) $d_p(u,v) = d_p(v,u)$,

(3) $d_p(u,v) \leqslant \max(d_p(u,w), d_p(w,v))$

An equivalent metric

Let us set

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

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

Proposition (Pin 1993)

d'_p is an ultrametric uniformly equivalent to d_p.

Mahler's theorem for word functions

Theorem (Main result)

Let $f(u) = \sum_{v \in A^*} \langle f, v \rangle \binom{u}{v}$ *be the Mahler's expansion of a function* $f : A^* \to \mathbb{Z}$. *TFCAE:*

(1) f *is uniformly continuous for* d_p,

(2) *the partial sums* $\sum_{0 \leqslant |v| \leqslant n} \langle f, v \rangle \binom{u}{v}$ *converge uniformly to* f,

(3) $\lim_{|v| \to \infty} |\langle f, v \rangle|_p = 0$.

Part IV

Real motivations

First motivation

Study of regularity-preserving functions $f : A^* \to B^*$: if X is a regular language of B^*, then $f^{-1}(X)$ is a regular language of A^*.

More generally, we are interested in functions preserving a given variety of languages $\mathcal{V}$: if X is a language of $\mathcal{V}$, then $f^{-1}(X)$ is also a language of $\mathcal{V}$.

For instance, Reutenauer and Schützenberger characterized in 1995 the sequential functions preserving star-free languages.

Second motivation: continuous reductions

A fundamental idea of descriptive set theory is to use continuous reductions to classify topological spaces: given two sets X and Y, Y reduces to X if there exists a continuous function f such that $X = f^{-1}(Y)$.

Our idea was to consider similar reductions for regular languages. Let us call p-reduction a uniformly continuous function between the metric spaces (A^*, d_p) and (B^*, d_p). These p-reductions define a hierarchy similar to the Wadge hierarchy that we would like to explore.

Languages recognized by a p-group

A language recognized by a p-group is called a p-group language.

Theorem (Eilenberg-Schützenberger 1976)

A language of A^* is a p-group language iff it is a Boolean combination of the languages

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

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

Uniformly continuous functions

Theorem

A function $f : A^* \to B^*$ is uniformly continuous for d_p iff, for every p-group language L of A^*, $f^{-1}(L)$ is also a p-group language.

Thus our two motivations are strongly related...