



# **A Mahler's Theorem for Word Functions**

Jean-Eric Pin, Christophe Reutenauer

## **► To cite this version:**

Jean-Eric Pin, Christophe Reutenauer. A Mahler's Theorem for Word Functions. 46th ICALP (ICALP 2019), Jul 2019, Patras, Greece.  $\langle 10.4230/LIPIcs.ICALP.2019.125 \rangle$ .  $\langle \text{hal-02422662} \rangle$

**HAL Id: hal-02422662**

**<https://hal.science/hal-02422662v1>**

Submitted on 22 Dec 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

# A Mahler's Theorem for Word Functions

Jean-Éric Pin<sup>1</sup>

IRIF, Université Paris Denis Diderot, CNRS - Case 7014 - F-75205 Paris Cedex 13, France  
Jean-Eric.Pin@irif.fr

Christophe Reutenauer

Mathématiques, Université du Québec à Montréal, CP 8888, succ. Centre Ville, Canada H3C 3P8  
reutenauer.christophe@uqam.ca

---

## Abstract

Let  $p$  be a prime number and let  $\mathcal{G}_p$  be the variety of all languages recognised by a finite  $p$ -group. We give a construction process of all  $\mathcal{G}_p$ -preserving functions from a free monoid to a free group. Our result follows from a new noncommutative generalization of Mahler's theorem on interpolation series, a celebrated result of  $p$ -adic analysis.

**2012 ACM Subject Classification** Theory of computation → Formal languages and automata theory; Theory of computation → Algebraic language theory

**Keywords and phrases** group languages, interpolation series, pro- $p$  metric, regularity preserving

**Digital Object Identifier** 10.4230/LIPIcs.ICALP.2019.125

**Category** Track B: Automata, Logic, Semantics, and Theory of Programming

**Funding** Jean-Éric Pin: DeLTA project (ANR-16-CE40-0007)

Christophe Reutenauer: Nserc Canada

## 1 Introduction

Throughout this paper,  $p$  denotes a prime number. A finite  $p$ -group is a group whose order is a power of  $p$ . Let  $\mathcal{G}_p$  denote the variety of all languages recognised by a finite  $p$ -group. This variety, first studied over forty years ago [2, p. 238] is generated by the  $p$ -binomial languages, as explained in Section 4.

A function  $f$  from  $A^*$  to  $B^*$  is *regularity-preserving* if, for each regular language  $L$  of  $B^*$ , the language  $f^{-1}(L)$  is also regular. In a series of papers [8, 9, 10], Silva and the first author considered a more general situation: given a variety  $\mathcal{V}$  of regular languages, a function  $f$  from  $A^*$  to  $B^*$  is  $\mathcal{V}$ -preserving if  $L \in \mathcal{V}$  implies  $f^{-1}(L) \in \mathcal{V}$ . These functions admit a simple topological characterization. Indeed, one can attach to each variety  $\mathcal{V}$  a metric<sup>2</sup>  $d_{\mathcal{V}}$ , called the *pro- $\mathcal{V}$  metric*, for which the following property holds: a function is  $\mathcal{V}$ -preserving if and only if it is uniformly continuous with respect to  $d_{\mathcal{V}}$  [10, Theorem 4.1]. However, this characterization does not solve the following more difficult question:

**Synthesis problem for  $\mathcal{V}$ .** *Provide a construction process of all  $\mathcal{V}$ -preserving functions.*

For instance, although several families of regularity-preserving functions have been identified, the synthesis problem for these functions is still a major open problem.

The aim of this paper is to solve the synthesis problem for the variety  $\mathcal{G}_p$ . We actually solve this problem for all functions from  $A^*$  to the free group  $F(B)$ , a slightly more general setting, since the free monoid  $B^*$  embeds in  $F(B)$ . In a free group, the class  $\mathcal{G}_p$  is defined in the same way: a subset of  $F(B)$  is in  $\mathcal{G}_p$  if it is recognized by a finite  $p$ -group.

---

<sup>1</sup> Corresponding author.

<sup>2</sup> Actually, it is only a pseudometric in the general case, but a metric in the case considered in this paper.



**One-letter case.** If  $A$  and  $B$  are one-letter alphabets, then  $A^*$  is isomorphic to  $\mathbb{N}$ ,  $F(B)$  is isomorphic to  $\mathbb{Z}$  and  $d_p$  is the  $p$ -adic metric. The  $p$ -adic distance between two distinct integers  $r$  and  $s$  is the real  $p^{-n}$ , where  $n$  is the exponent of  $p$  in the prime factorization of  $|r - s|$ . It turns out that *Mahler's theorem on interpolation series*, a celebrated result in  $p$ -adic analysis [4, 5] stated below, leads to a construction process of the  $\mathcal{G}_p$ -preserving functions from  $\mathbb{N}$  to  $\mathbb{Z}$ .

Mahler's theorem is based on another result of independent interest. *Newton's forward difference formula* states that for each function  $f: \mathbb{N} \rightarrow \mathbb{Z}$ , there is a unique sequence of integers  $\delta_k f$  such that, for all  $n \in \mathbb{N}$ ,  $f(n) = \sum_{k=0}^{\infty} \binom{n}{k} \delta_k f$ . The value of these coefficients  $\delta_k f$  is given by the formula  $\delta_k f = (\Delta^k f)(0)$ , where  $\Delta^k$  is the  $k$ -th iteration of the *difference operator*  $\Delta$ , defined by  $(\Delta f)(n) = f(n+1) - f(n)$ . A remarkable consequence of Newton's forward difference formula is that the map  $f \rightarrow (\delta_k f)_{k \geq 0}$  defines a *bijection* between functions from  $\mathbb{N}$  to  $\mathbb{Z}$  and integer sequences. We call this bijection *Newton's bijection*.

Mahler's theorem states that the integer sequences that give rise to  $\mathcal{G}_p$ -preserving functions are precisely those converging to 0 in the  $p$ -adic metric. More precisely:

► **Theorem 1.1** (Mahler). *The following conditions are equivalent:*

- (1)  $f: \mathbb{N} \rightarrow \mathbb{Z}$  is a  $\mathcal{G}_p$ -preserving function,
- (2)  $f$  is uniformly continuous for the  $p$ -adic metric,
- (3) the functions  $\Delta^n f$  tend uniformly to the constant function  $\mathbf{0}$  when  $n$  tends to  $\infty$ ,
- (4) the  $p$ -adic norm of  $\delta_n f$  tends to 0 when  $n$  tends to  $\infty$ ,
- (5)  $f$  is the uniform limit of the polynomial functions  $f_r(n) = \sum_{k=0}^r \binom{n}{k} \delta_k f$ .

This leads to a simple construction process of all  $\mathcal{G}_p$ -preserving functions from  $\mathbb{N}$  to  $\mathbb{Z}$ : take a sequence  $(\delta_k)_{k \geq 0}$  of integers converging to 0 and set  $f(n) = \sum_{k=0}^{\infty} \binom{n}{k} \delta_k$ .

**Functions from  $A^*$  to  $F(B)$ .** When  $B$  is a one-letter alphabet, a construction process of all  $\mathcal{G}_p$ -preserving functions was obtained by Silva and the first author in [10, 11]. We rely on this result to treat the general case where  $B$  is any finite alphabet.

We first equip both  $A^*$  and  $F(B)$  with the pro- $p$  metric, a natural extension of the  $p$ -adic metric, fully defined in Section 4.1. We follow [7] to extend the difference operators. Let  $f$  be a function from  $A^*$  to a group  $G$ . For each letter  $a$ , the *difference operator*  $\Delta^a$  associates to  $f$  the function  $\Delta^a f: A^* \rightarrow G$  defined by  $\Delta^a f(u) = f(u)^{-1} f(ua)$ . Next we attach a difference operator  $\Delta^w$  to each word  $w = a_1 \cdots a_n$  of  $A^*$  by setting  $\Delta^w f = \Delta^{a_1}(\Delta^{a_2}(\cdots \Delta^{a_n} f) \cdots)$ . Finally, we set  $\delta_w f = \Delta^w f(1)$ , where  $1$  is the empty word.

A noncommutative version of Newton's forward difference formula and of Newton's bijection was given by the first author in [7]. We give a simpler proof of these results in Section 2.5. In this noncommutative setting, Newton's bijection is now the map  $f \rightarrow (\delta_w f)_{w \in A^*}$ . If we just keep the elements  $\delta_w f$  such that  $|w| \leq n$  and replace every other  $\delta_w f$  by the identity of the free group, the inverse of Newton's bijection gives back a function  $f_n$ , called the  $n$ -th *Newton polynomial function associated to  $f$* .

Our main result now offers a noticeable analogy with Mahler's theorem:

► **Theorem 1.2.** *Let  $f: A^* \rightarrow F(B)$  be a function. The following conditions are equivalent:*

- (1)  $f$  is a  $\mathcal{G}_p$ -preserving function,
- (2)  $f$  is uniformly continuous for the pro- $p$  metric,
- (3) the functions  $\Delta^w f$  tend uniformly to the constant function  $\mathbf{1}$  when  $|w|$  tends to  $\infty$ ,
- (4) the elements  $\delta_w f$ , where  $w \in A^*$ , tend to 1 when  $|w|$  tends to  $\infty$ ,
- (5)  $f$  is the uniform limit of its Newton polynomial functions.

**Sequential products.** A new operation on functions plays a key role in our proof of Theorem 1.2. 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  $f: A^* \rightarrow G$ , defined, for each word  $a_1 \cdots a_n \in A^*$ , by  $f(a_1 \cdots a_n) = g \prod_{1 \leq i \leq n} f_{a_i}(a_1 \cdots a_{i-1})$ .

A function  $f$  from  $A^*$  to a group  $G$  is a *Newton polynomial function* if  $\delta_w f = 1$  for almost all words  $w$ . We prove that the set of Newton polynomial functions from  $A^*$  to  $G$  is the smallest set of functions containing the constant functions and closed under sequential product. Moreover, if  $G$  is a finite  $p$ -group equipped with the discrete metric, then the Newton polynomial functions are exactly the uniformly continuous functions from  $A^*$  to  $G$ .

**Two solutions of the synthesis problem.** Theorem 1.2 now leads to two construction processes to obtain all  $\mathcal{G}_p$ -preserving functions from  $A^*$  to  $F(B)$ . The first one consists in taking any family  $(\delta_w)_{w \in A^*}$  of elements of the free group converging to 1 when  $|w|$  tends to  $\infty$  and to use the inverse of Newton's bijection to get in return a  $\mathcal{G}_p$ -preserving function from  $A^*$  to  $F(B)$ . The second method is to start with the constant functions, use the sequential product to generate all Newton polynomial functions and finally take the uniform closure.

**Related work.** Another characterization of  $\mathcal{G}_p$ -preserving functions using profinite equations was obtained in [1, Lemma 3.3], but it only holds for *regular-preserving* functions. In the case of *sequential* and *rational* functions,  $\mathcal{V}$ -preserving functions were first investigated by Schützenberger and the second author [12]. For instance, they proved that a sequential function is  $\mathcal{G}_p$ -preserving if and only if the syntactic semigroup of its minimal sequential transducer is a finite  $p$ -group. Our results are of a different nature, since they concern all  $\mathcal{G}_p$ -preserving functions.

**Organization.** Difference operators and Newton's forward difference formula are introduced in Section 2. Section 3 is devoted to Newton polynomial functions and Section 4 to topological issues. The proof of our main result is presented in Section 5. Due to space constraints, missing proofs are given in the Appendix.

## 2 Difference operators and Newton's forward difference formula

Newton's forward difference formula gives an expression of a function from  $\mathbb{N}$  to  $\mathbb{Z}$  in terms of the initial value of the function and the powers of the forward difference operator. A noncommutative extension of this formula for functions from  $A^*$  to  $F(B)$  was given in [7]. In this section, we give a new proof of these results. We first need to introduce a noncommutative version of the Magnus transformation.

### 2.1 Noncommutative Magnus transformation

Let  $A^{**}$  denote the free monoid freely generated by  $A^*$ . An element of  $A^{**}$  is a finite sequence  $(w_1, \dots, w_n)$  of elements of  $A^*$ . However, to avoid any confusion between the product in  $A^*$  and the product in  $A^{**}$ , we adopt an additive notation for  $A^{**}$ . This means that we replace the notation  $(w_1, \dots, w_n)$  by  $w_1 + \cdots + w_n$ . The addition of two elements  $(u_1 + \cdots + u_m)$  and  $(v_1 + \cdots + v_n)$  of  $A^{**}$  is also denoted additively, which is coherent, since

$$(u_1 + \cdots + u_m) + (v_1 + \cdots + v_n) = u_1 + \cdots + u_m + v_1 + \cdots + v_n.$$

Accordingly, the neutral element of the monoid  $A^{**}$  is denoted 0. Note however that the addition is in general noncommutative. For each  $w \in A^*$  and  $x = x_1 + \cdots + x_n \in A^{**}$ , let  $x \cdot w = x_1 w + \cdots + x_n w$ . This defines a *monoid right action* of  $A^*$  on  $A^{**}$ , which means that the following formulas hold for all  $w, w_1, w_2 \in A^*$ , and for all  $x, x_1, x_2 \in A^{**}$ ,

$$0 \cdot w = 0 \quad (x_1 + x_2) \cdot w = x_1 \cdot w + x_2 \cdot w \quad x \cdot (w_1 w_2) = (x \cdot w_1) \cdot w_2.$$

The *noncommutative Magnus transformation* is the mapping  $\mu$  from  $A^*$  into  $A^{**}$  defined recursively by setting  $\mu(1) = 1$  and, for any  $w \in A^*$  and  $a \in A$ ,

$$\mu(wa) = \mu(w) + \mu(w) \cdot a. \quad (2.1)$$

For instance,  $\mu(a) = 1 + a$ ,  $\mu(ab) = 1 + a + b + ab$ ,  $\mu(abc) = 1 + a + b + ab + c + ac + bc + abc$  and  $\mu(abcd) = 1 + a + b + ab + c + ac + bc + abc + d + ad + bd + abd + cd + acd + bcd + abcd$ .

## 2.2 Difference operators

Let  $G$  be a group and let  $f: A^* \rightarrow G$  be a function. Following [7], we define the difference operators as follows. For each letter  $a \in A$ ,  $\Delta^a f$  is the function  $A^* \rightarrow G$  defined by  $\Delta^a f(w) = f(w)^{-1} f(wa)$  for any word  $w$  in  $A^*$ . We obtain in this way a function  $a \mapsto \Delta^a$  from  $A$  into the set  $\mathcal{M}$  of all mappings from  $G^{A^*}$  into itself. We view  $\mathcal{M}$  as a monoid under the composition of mappings. Since  $A^*$  is the free monoid on  $A$ , this function from  $A$  to  $\mathcal{M}$  extends uniquely to a monoid morphism from  $A^*$  into  $\mathcal{M}$ . Denoting  $w \mapsto \Delta^w$  this extension, we get  $\Delta^1 f = f$  and, for all words  $u, v$  in  $A^*$ ,

$$\Delta^{uv} f = \Delta^u \Delta^v f. \quad (2.2)$$

For instance, one gets, for any  $a, b, c \in A$  and  $u \in A^*$ ,

$$\begin{aligned} (\Delta^1 f)(u) &= f(u) & (\Delta^a f)(u) &= f(u)^{-1} f(ua) & (\Delta^{ab} f)(u) &= f(ub)^{-1} f(u) f(ua)^{-1} f(uab) \\ (\Delta^{abc} f)(u) &= f(ubc)^{-1} f(ub) f(u)^{-1} f(uc) f(uac)^{-1} f(ua) f(uab)^{-1} f(uabc) \end{aligned}$$

Here are two examples of differential operators. First, let us take  $A^* = \mathbb{N}$  and  $G = \mathbb{Z}$ . Switching to additive notation, we find that  $\Delta^1 f(n) = -f(n) + f(n+1)$ , the usual difference operator, and more generally  $\Delta^k f(n) = f(n+k) - \binom{n}{1} f(n+k-1) + \binom{n}{2} f(n+k-2) - \cdots + (-1)^k \binom{n}{k} f(n)$ .

The next example requires an auxiliary definition. The *iterated commutator*  $[x_1, x_2, \dots, x_n]$  of  $n$  elements  $x_1, x_2, \dots, x_n$  of a group is defined by induction by setting  $[x_1] = x_1$  and for  $n \geq 2$ ,  $[x_1, x_2, \dots, x_n] = x_1 [x_2, x_3, \dots, x_n] x_1^{-1} [x_2, x_3, \dots, x_n]^{-1}$ . In particular, since  $[x_1, x_2] = x_1 x_2 x_1^{-1} x_2^{-1}$ , one gets  $[x_1, x_2, \dots, x_n] = [x_1, [x_2, x_3, \dots, x_n]]$ .

► **Proposition 2.1.** *Let  $f: A^* \rightarrow F(A)$  be the function defined by  $f(x) = x^{-1}$ . Then for every  $n > 0$  and for all  $a_1, \dots, a_n \in A$ ,  $\Delta^{a_1 a_2 \cdots a_n} f(x) = x[a_1, a_2, \dots, a_n]^{-1} x^{-1}$ .*

Difference operators commute with group morphisms:

► **Proposition 2.2.** *Let  $f: A^* \rightarrow G$  be a function, let  $\varphi: G \rightarrow H$  be a group morphism and let  $w$  be a word. Then  $\Delta^w(\varphi \circ f) = \varphi \circ (\Delta^w f)$ .*

## 2.3 The integration problem

Let  $G$  be a group and let  $f: A^* \rightarrow G$  be a function. Then  $f$  and the functions  $\Delta^a f$ , for  $a \in A$ , are related by a functional equation.

► **Proposition 2.3.** *Let  $a_1 \cdots a_n$  be a word of  $A^*$ . Then the following formula holds:*

$$f(a_1 \cdots a_n) = f(1) \prod_{1 \leq i \leq n} \Delta^{a_i} f(a_1 \cdots a_{i-1}). \quad (2.3)$$

The functional equation (2.3) gives an expression of  $f$  in terms of  $f(1)$  and of the family  $(\Delta^a f)_{a \in A}$ . We now address the opposite question, which is somewhat similar to the problem of integrating a function from its derivative.

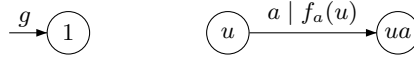
**Integration problem.** *Given an element  $g$  of  $G$  and a family  $(f_a)_{a \in A}$  of functions from  $A^*$  to  $G$ , is there a function  $f$  such that  $f(1) = g$  and  $f_a = \Delta^a f$  for all  $a \in A$ ?*

To solve the integration problem, it is convenient to introduce a new definition. Given an element  $g$  of  $G$  and a family  $(f_a)_{a \in A}$  of functions from  $A^*$  to  $G$ , the *sequential product*  $\text{Seq}(g, (f_a)_{a \in A})$  is the function  $f: A^* \rightarrow G$ , defined, for each word  $a_1 \cdots a_n \in A^*$ , by

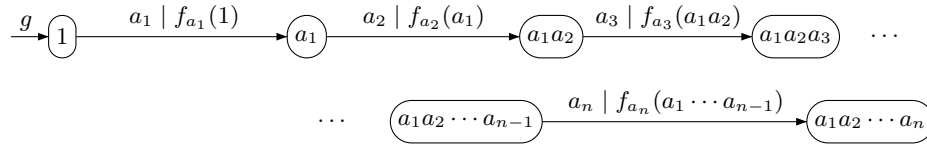
$$f(a_1 \cdots a_n) = g \prod_{1 \leq i \leq n} f_{a_i}(a_1 \cdots a_{i-1}). \quad (2.4)$$

By abuse of language, a function  $f: A^* \rightarrow G$  is called a *sequential product of a family  $(f_a)_{a \in A}$  of functions from  $A^*$  to  $G$*  if, for some  $g \in G$ ,  $f = \text{Seq}(g, (f_a)_{a \in A})$ .

This terminology stems from the fact that  $f$  can be realized by a sequential transducer with infinitely many states. Indeed, consider the sequential transducer  $\mathcal{A} = (A^*, A, G, 1, \cdot, *, g)$ , where  $A^*$  is the set of states,  $A$  the input alphabet,  $G$  the output group,  $1$  the initial state,  $g$  the initial prefix. The transition and the output functions are respectively defined by  $u \cdot a = ua$  and  $u * a = f_a(u)$ .



A typical computation in  $\mathcal{A}$  looks like this



and hence  $\mathcal{A}$  computes the sequential product  $f$  defined by (2.4).

We are now ready to solve the integration problem.

► **Proposition 2.4.** *Let  $g \in G$  and let  $(f_a)_{a \in A}$  be a family of functions from  $A^*$  to  $G$ . Then the sequential product  $\text{Seq}(g, (f_a)_{a \in A})$  is the unique function  $f$  such that  $f(1) = g$  and  $\Delta^a f = f_a$  for all  $a \in A$ .*

**Proof.** Let  $f = \text{Seq}(g, (f_a)_{a \in A})$ . Then  $f(1) = g$  by definition. Let  $u = a_1 \cdots a_n$  be a word and  $a$  be a letter. Since  $\Delta^a f(u) = f(u)^{-1} f(ua)$ , one gets by (2.4)

$$\Delta^a f(u) = \left( g \prod_{1 \leq i \leq n} f_{a_i}(a_1 \cdots a_{i-1}) \right)^{-1} g \left( \prod_{1 \leq i \leq n} f_{a_i}(a_1 \cdots a_{i-1}) \right) f_a(a_1 \cdots a_n) = f_a(a_1 \cdots a_n)$$

whence  $\Delta^a f = f_a$ .

To prove uniqueness, consider a function  $f$  such that  $f(1) = g$  and  $\Delta^a f = f_a$  for all  $a \in A$ . Then for each word  $a_1 \cdots a_n \in A^*$ , one gets by (2.3),

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

and thus  $f = \text{Seq}(g, (f_a)_{a \in A})$ . ◀

## 2.4 Newton's forward difference formula

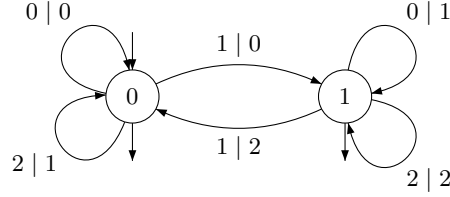
For each  $w \in A^*$  and  $f: A^* \rightarrow G$ , let us set  $\delta_w f = \Delta^w f(1)$  and let  $\delta_f: A^* \rightarrow G$  be the map defined by  $\delta_f(w) = \delta_w f$ . This map extends to a monoid morphism  $\delta_f^*: A^{**} \rightarrow G$ . Thus  $\delta_f^*(w) = \delta_w f$  and if  $w_1 + \dots + w_n$  is an element of  $A^{**}$ , then  $\delta_f^*(w_1 + \dots + w_n) = \delta_{w_1} f \cdots \delta_{w_n} f$ .

► **Theorem 2.5.** *The equality  $f = \delta_f^* \circ \mu$  holds for each function  $f: A^* \rightarrow G$ .*

The equality  $f = \delta_f^* \circ \mu$  yields a noncommutative version of Newton's forward difference formula. Indeed, it extends the formula given in [11, Theorem 2.2] for functions from  $A^*$  to  $\mathbb{Z}$ , which itself extends Newton's forward difference formula for functions from  $\mathbb{N}$  to  $\mathbb{Z}$ . To make this formula a little more concrete, let us compute a few values of  $f(w)$ . Let  $a, b, c, d$  be letters of  $A$ . Then, using the values of  $\mu$  computed on page 4, one gets

$$\begin{aligned} f(1) &= \delta_1 f & f(a) &= (\delta_1 f)(\delta_a f) & f(ab) &= (\delta_1 f)(\delta_a f)(\delta_b f)(\delta_{ab} f) \\ f(abc) &= (\delta_1 f)(\delta_a f)(\delta_b f)(\delta_{ab} f)(\delta_c f)(\delta_{ac} f)(\delta_{bc} f)(\delta_{abc} f) \\ f(abcd) &= (\delta_1 f)(\delta_a f)(\delta_b f)(\delta_{ab} f)(\delta_c f)(\delta_{ac} f)(\delta_{bc} f)(\delta_{abc} f) \\ &\quad (\delta_d f)(\delta_{ad} f)(\delta_{bd} f)(\delta_{abd} f)(\delta_{cd} f)(\delta_{acd} f)(\delta_{bcd} f)(\delta_{abcd} f). \end{aligned}$$

Here is a more complete example. Let  $f: \{0, 1, 2\}^* \rightarrow \{0, 1, 2\}^*$  be the Euclidean division by 2 in base 3, that is, the function which associates to a word  $u \in \{0, 1, 2\}^*$  representing an integer  $\bar{u}$  in base 3, the unique word  $v$  of the same length as  $u$  representing the quotient of the division of  $\bar{u}$  by 2. Since 1 is a letter of the alphabet, we let  $\epsilon$  denote the empty word. The function  $f$  can be realized by the sequential transducer represented below.



For instance,  $f(1212) = 0221$  since  $\overline{1212} = 50$  and  $\overline{0221} = 25 = 50/2$ . Let us compute the functions  $\Delta^x f$ . First, we have

$$\Delta^0 f(w) = \begin{cases} 0 & \text{if } \bar{w} \text{ is even} \\ 1 & \text{if } \bar{w} \text{ is odd} \end{cases} \quad \Delta^1 f(w) = \begin{cases} 0 & \text{if } \bar{w} \text{ is even} \\ 2 & \text{if } \bar{w} \text{ is odd} \end{cases} \quad \Delta^2 f(w) = \begin{cases} 1 & \text{if } \bar{w} \text{ is even} \\ 2 & \text{if } \bar{w} \text{ is odd} \end{cases}$$

The other values of  $\Delta^x f(w)$  can be obtained through the following result:

► **Proposition 2.6.** *Let  $u, v \in A^*$  and let  $g: \{0, 1, 2\}^* \rightarrow A^*$  be the function defined by*

$$g(w) = \begin{cases} u & \text{if } \bar{w} \text{ is even} \\ v & \text{if } \bar{w} \text{ is odd} \end{cases}$$

*Then  $\Delta^x g(w) = \epsilon$  if  $x \notin 1^*$  and  $\Delta^{1^n} g(w) = (u^{-1}v)^{(-1)^{n-1} + \bar{w}2^{n-1}}$  for  $n \geq 1$ .*

It is now easy to compute the elements  $\delta_w = (\Delta^w f)(\epsilon)$ . One gets  $\delta_0 = 0$ ,  $\delta_1 = 0$ ,  $\delta_2 = 1$ ,  $\delta_{1^n 0} = (0^{-1}1)^{(-1)^{n-1}2^{n-1}}$ ,  $\delta_{1^n 1} = (0^{-1}2)^{(-1)^{n-1}2^{n-1}}$ ,  $\delta_{1^n 2} = (1^{-1}2)^{(-1)^{n-1}2^{n-1}}$  and  $\delta_w = \epsilon$  in all other cases. We get for instance

$$\begin{aligned} f(1212) &= \delta_\epsilon \delta_1 \delta_2 \delta_{12} \delta_1 \delta_{11} \delta_{21} \delta_{121} \delta_2 \delta_{12} \delta_{22} \delta_{122} \delta_{12} \delta_{112} \delta_{212} \delta_{1212} \\ &= \delta_1 \delta_2 \delta_{12} \delta_1 \delta_{11} \delta_2 \delta_{12} \delta_{12} \delta_{112} = 01(1^{-1}2)0(0^{-1}2)1(1^{-1}2)(1^{-1}2)^{-2} = 0221. \end{aligned}$$

## 2.5 Newton's bijection

For each  $n \in \mathbb{N}$ , let  $C_n$  be the set of words of  $A^*$  of length at most  $n$ . Let  $\rho_n$  be the monoid endomorphism on  $A^{**}$  which maps every element of  $C_n$  to itself, and maps any other element of  $A^*$  to 0. In other words, if  $x = \sum_{1 \leq i \leq r} u_i$  is an element of  $A^{**}$ , where each  $u_i \in A^*$ , then

$$\rho_n(x) = \sum_{i \in E_n(x)} u_i, \text{ where } E_n(x) = \{i \in \{1, \dots, r\} \mid |u_i| \leq n\}.$$

For each  $n \geq 0$ ,  $C_n$  is a finite subset of  $A^{**}$  and  $C_n^*$  is a free submonoid of  $A^{**}$ . The function  $\mu_n = \rho_n \circ \mu$  from  $A^*$  to the free monoid  $C_n^*$  is called the *truncated noncommutative Magnus transformation*. For instance,  $\mu_2(abcd) = 1 + a + b + ab + c + ac + bc + d + ad + bd + cd$ , a result obtained by only keeping the words of length  $\leq 2$  in  $\mu(abcd)$ .

Recall that to each function  $f: A^* \rightarrow G$  is associated the map  $\delta_f: A^* \rightarrow G$  defined by  $\delta_f(w) = \delta_w(f)$ . The *Newton map* is the map  $\delta: f \rightarrow \delta_f$ . Let  $f^*: A^{**} \rightarrow G$  denote the unique monoid morphism extending  $f$  and let  $\gamma$  be the map defined by  $\gamma(f) = f^* \circ \mu$ .

► **Theorem 2.7.** *The Newton map  $\delta$  is a permutation on the set of functions from  $A^*$  to  $G$  and its inverse permutation is  $\gamma$ .*

**Proof.** Since  $f = \delta_f^* \circ \mu$  by Theorem 2.5,  $\gamma \circ \delta$  is the identity function. Therefore  $\gamma$  is surjective,  $\delta$  is injective and it suffices to prove that  $\gamma$  is injective. Let  $g, h: A^* \rightarrow G$  be such that  $g^* \circ \mu = h^* \circ \mu$ . Let us show by induction on  $|w|$  that  $g(w) = h(w)$ . If  $|w| = 0$ , then  $w$  is the empty word 1,  $\mu(1) = 1$ ,  $g^*(1) = g(1)$ ,  $h^*(1) = h(1)$  and thus  $g(1) = h(1)$ . Suppose now that  $|w| = n + 1$ . Then  $\mu(w) = \mu_n(w) + w$  and since  $g^*$  and  $h^*$  are monoid morphisms, one gets  $g^* \circ \mu(w) = g^*(\mu_n(w) + w) = g^*(\mu_n(w))g(w)$  and similarly  $h^* \circ \mu(w) = h^*(\mu_n(w))h(w)$ . Since  $\mu_n(w)$  is a sum of words of length  $\leq n$ , the induction hypothesis gives  $g^*(\mu_n(w)) = h^*(\mu_n(w))$ . Now since  $g^* \circ \mu(w) = h^* \circ \mu(w)$ , one gets  $g(w) = h(w)$ , which concludes the induction step. ◀

Theorem 2.7 solves the following interpolation problem.

► **Corollary 2.8.** *For each function  $g: A^* \rightarrow G$ , there exists a unique function  $f: A^* \rightarrow G$  such that, for all  $u \in A^*$ ,  $\delta_u f = g(u)$ .*

## 3 Newton polynomial functions

Let  $G$  be a group. A function  $f: A^* \rightarrow G$  is called a *Newton polynomial function* if  $\delta_w f = 1$  for almost all words  $w \in A^*$ . Note that by Proposition 2.6, the Euclidean division by 2 in base 3 is not a Newton polynomial function.

Let **1** denote the constant function from  $A^*$  to  $G$  that maps every word to 1. The *degree* of a Newton polynomial function is  $-1$  if  $f = \mathbf{1}$ ; otherwise, it is the smallest  $d$  such that  $\delta_w f = 1$  for any word of length  $d + 1$ .

Here is another convenient characterization of Newton polynomial functions.

► **Proposition 3.1.** *A function  $f: A^* \rightarrow G$  is a Newton polynomial function of degree  $d$  if and only if  $d$  is the smallest integer such that  $\Delta^w f = \mathbf{1}$  for all words  $w$  of length  $d + 1$ .*

The following result gives a construction process of the set of Newton polynomial functions.

► **Theorem 3.2.** *The set of Newton polynomial functions from  $A^*$  to  $G$  is the smallest set of functions from  $A^*$  to  $G$  containing the constant functions and closed under sequential product.*

Theorem 3.2 is an immediate consequence of the following proposition.

► **Proposition 3.3.** *Let  $G$  be a group and let  $f: A^* \rightarrow G$  be a function. The following conditions are equivalent:*

- (1)  *$f$  is a Newton polynomial function of degree  $\leq d$ ,*
- (2) *there exists a family  $(f_a)_{a \in A}$  of Newton polynomial functions of degree  $\leq d-1$  such that  $f = \text{Seq}(f(1), (f_a)_{a \in A})$ .*

*In this case, one has  $f_a = \Delta^a f$  for every  $a \in A$ .*

**Proof.** (1) implies (2). Suppose that  $f$  is a Newton polynomial function of degree  $\leq d$ . Then for any letter  $a$ ,  $\Delta^a f$  is a Newton polynomial function of degree at most  $d-1$ . Moreover, Proposition 2.3 shows that  $f(a_1 \cdots a_n) = f(1) \prod_{1 \leq i \leq n} \Delta^{a_i} f(a_1 \cdots a_{i-1})$ , which proves (2).

(2) implies (1). Suppose that (2) holds. Proposition 2.4 shows that, for each letter  $a$ ,  $\Delta^a f = f_a$  and hence  $\Delta^a f$  is a Newton polynomial function of degree  $\leq d-1$ . It follows that  $f$  is a Newton polynomial function of degree  $\leq d$ . ◀

A Newton polynomial function of degree 0 is a constant map different from **1**. A Newton polynomial function of degree 1 is an *affine morphism*, that is, a function  $f$  of the form  $f(w) = f(1)g(w)$  for some monoid morphism  $g: A^* \rightarrow G$ . Equivalently, conjugating by  $f(1)$ , one gets  $f(w) = h(w)f(1)$  for some monoid morphism  $h: A^* \rightarrow G$ .

The function  $f: A^* \rightarrow F(A)$  defined by  $f(a_1 \cdots a_n) = a_1(a_1 a_2)(a_1 a_2 a_3) \cdots (a_1 \cdots a_n)$  is a Newton polynomial function of degree 2. Indeed, it is equal to the sequential product  $\text{Seq}(1, (f_a)_{a \in A})$  where each  $f_a$  is the affine morphism defined by  $f_a(u) = ua$ .

Recall that  $\delta_f^*$  is a map from  $A^{**}$  to  $G$ , but we keep the same notation for its restriction to  $C_n^*$ . Let  $f: A^* \rightarrow G$  be a function. For each  $n \geq 0$ , the  $n$ -th Newton polynomial function associated to  $f$  is the function  $f_n$  from  $A^*$  to  $G$  defined by  $f_n = \delta_f^* \circ \mu_n$ . This terminology is justified by Proposition 3.4 below.

It is not difficult to see that  $f_0$  is the constant function equal to  $f(1)$ . Indeed, since  $\Delta^1 f = f$ , one gets  $f_0(u) = \delta_f^* \circ \mu_0(u) = \delta_f^*(1) = \delta_1 f = \Delta^1 f(1) = f(1)$ .

► **Proposition 3.4.** *For each  $n \geq 0$ ,  $f_n$  is a Newton polynomial function of degree at most  $n$ .*

We need an auxiliary lemma.

► **Lemma 3.5.** *The following formula holds for all  $n > 0$  and  $a \in A$ .*

$$\Delta^a(f_n) = \delta_{\Delta^a f}^* \circ \mu_{n-1} = (\Delta^a f)_{n-1}$$

**Proof of Proposition 3.4.** We prove the result by induction on  $n$ . For  $n = 0$ , we have already seen that  $f_0$  is a constant function, and thus a Newton polynomial function of degree  $\leq 0$ . Applying Proposition 2.3 to  $f_n$ , one gets, for every word  $a_1 \cdots a_k \in A^*$ ,  $f_n(a_1 \cdots a_k) = f_n(1) \prod_{1 \leq i \leq k} \Delta^{a_i} f_n(a_1 \cdots a_{i-1})$ . Now,  $f_n(1) = \delta_f^* \circ \mu_n(1) = \delta_f^*(1) = f(1)$  and  $\Delta^a f_n = (\Delta^a f)_{n-1}$  by Lemma 3.5. It follows that  $f_n(a_1 \cdots a_k) = f(1) \prod_{1 \leq i \leq k} (\Delta^{a_i} f)_{n-1}(a_1 \cdots a_{i-1})$ . By the induction hypothesis applied to  $\Delta^a f$ ,  $(\Delta^a f)_{n-1}$  is a Newton polynomial function of degree at most  $n-1$ . Hence by Proposition 3.3,  $f_n$  is a Newton polynomial function of degree at most  $n$ . ◀

A function  $f: A^* \rightarrow G$  is called a  $G$ -polynomial if  $f(w) = 1$  for almost all words  $w \in A^*$ . The *degree* of a  $G$ -polynomial is  $-1$  if  $f = \mathbf{1}$ ; otherwise, it is the smallest  $d$  such that  $f(w) = 1$  for any word of length  $d+1$ . One can now enrich Theorem 2.7 as follows.

► **Theorem 3.6.** *For each degree  $d$ , the maps  $\delta$  and  $\gamma$  define mutually inverse bijections between the set of Newton polynomial functions of degree  $d$  and the set of  $G$ -polynomials of degree  $d$ .*

**Proof.** It suffices to prove that  $\delta$  and  $\gamma$  define mutually inverse bijections between the set of Newton polynomial functions of degree  $\leq d$  and the set of  $G$ -polynomials of degree  $\leq d$ . Let  $f$  be a Newton polynomial function of degree  $\leq d$ . Then by definition,  $\delta(f)$  is a  $G$ -polynomial of degree  $\leq d$ . Let now  $f$  be a  $G$ -polynomial of degree  $\leq d$ . Theorem 2.7 shows that  $f = \delta \circ \gamma(f) = \delta_{\gamma(f)}$ . It follows that for every word  $w$  of length  $> d$ ,  $1 = f(w) = \delta_{\gamma(f)}(w)$ . Thus  $\gamma(f)$  is a Newton polynomial of degree  $\leq d$ . ◀

## 4 Topology

### 4.1 Pro- $p$ metrics

If  $\bar{B}$  is a copy of  $B$ , the free group  $F(B)$  is the quotient of  $(B \cup \bar{B})^*$  under the congruence generated by the relations  $b\bar{b} = 1 = \bar{b}b$  for all  $b \in B$ .

Recall that a group  $G$  is called *residually  $p$ -finite* if for any  $g \neq 1$  in  $G$ , there is some finite  $p$ -group  $H$  and some morphism  $G \rightarrow H$  whose kernel does not contain  $g$ . It is a well-known fact that free groups are residually  $p$ -finite.

Let  $G$  be a residually  $p$ -finite group and let  $g \in G$ . The *pro- $p$  valuation* of  $g$ , denoted  $v_p(g)$ , is the largest  $n$  such that  $g$  belongs to the kernel of any morphism from  $G$  to a  $p$ -group of order  $p^n$ . The pro- $p$  valuation is always finite, except for  $g = 1$ , in which case it is infinite. The *pro- $p$  norm* of  $g$  is  $|g|_p = p^{-v_p(g)}$ , with the usual convention  $p^{-\infty} = 0$ . Finally  $G$  becomes a metric space for the *pro- $p$  metric*  $d_p: G \times G \rightarrow \mathbb{R}$  defined by  $d_p(x, y) = |x^{-1}y|_p$ .

The condition  $d_p(x, y) \leq p^{-k}$  means that  $x^{-1}y$  is in the kernel of each group morphism from  $G$  into a  $p$ -group of cardinality at most  $p^k$ . We leave to the reader to verify that if  $G = \mathbb{Z}$ , one recovers the usual  $p$ -adic valuation, norm and metric.

Another useful example occurs when  $G$  is a finite  $p$ -group. Recall that the *discrete metric* on  $G$  is the metric  $d$  defined by  $d(x, y) = 1$  if  $x \neq y$  and  $d(x, y) = 0$  if  $x = y$ . In this case, the double inequality  $d_p(x, y) \leq d(x, y) \leq |G| d_p(x, y)$  shows that the pro- $p$  metric is uniformly equivalent to the discrete metric.

There are two equivalent ways to define the pro- $p$  metric on a free monoid  $A^*$ . The first solution is to view  $A^*$  as a subspace of the free group  $F(A)$  and to consider the restriction to  $A^*$  of the pro- $p$  metric on  $F(A)$ .

The second solution is to directly define the pro- $p$  metric as follows. Let us say that a finite  $p$ -group  $G$  *separates* two words  $u$  and  $v$  of  $A^*$  if there exists a monoid morphism  $\varphi: A^* \rightarrow G$  such that  $\varphi(u) \neq \varphi(v)$ . Then  $d_p(u, v) = 0$  if  $u = v$  and  $d_p(u, v) = p^{-n}$ , where  $p^n$  is the minimal size of a  $p$ -group separating  $u$  and  $v$ , if  $u \neq v$ .

► **Proposition 4.1.** *Every monoid morphism from  $A^*$  to a  $p$ -group is uniformly continuous.*

**Proof.** Let  $\pi$  be a monoid morphism from  $A^*$  to a  $p$ -group  $G$  and let  $u, v \in A^*$ . If  $d_p(u, v) \leq |G|^{-1}$ , then  $\pi(u) = \pi(v)$  and thus  $d_p(\pi(u), \pi(v)) = 0$ . Thus  $\pi$  is uniformly continuous. ◀

Let us now review the connections with combinatorics on words and regular languages. A word  $u = a_1a_2 \cdots a_n$  (where  $a_1, \dots, a_n$  are letters) is a *subword* of a word  $v$  if  $v$  can be written as  $v = v_0a_1v_1 \cdots a_nv_n$ . For instance,  $ab$  is a subword of  $cacbc$ .

Following Eilenberg [2] and Lothaire [3, Chapter 6], let  $\binom{v}{u}$  denote the number of distinct ways to write a word  $u$  as a subword of  $v$ . More formally, if  $u = a_1a_2 \cdots a_n$ , then

$$\binom{v}{u} = \text{Card}\{(v_0, v_1, \dots, v_n) \mid v_0a_1v_1 \cdots a_nv_n = v\}$$

## 125:10 A Mahler's Theorem for Word Functions

A language of  $A^*$  is *p-binomial* if for some word  $v$  and some integer  $r$  it is equal to

$$L(v, r) = \{w \in A^* \mid \binom{w}{v} \equiv r \pmod{p}\}.$$

It follows from [2, p. 238] that a language belongs to  $\mathcal{G}_p$  if and only if it is a Boolean combination of *p*-binomial languages. We will also use the following consequence of [11, Proposition 1.3 and Theorem 1.4].

► **Proposition 4.2.** *Let  $f: A^* \rightarrow B^*$  be a function. The following conditions are equivalent:*

- (1)  *$f$  is uniformly continuous for the pro- $p$  metric,*
- (2)  *$f$  is  $\mathcal{G}_p$ -preserving,*
- (3) *for each  $p$ -binomial language  $L$  of  $B^*$ ,  $f^{-1}(L)$  is a Boolean combination of  $p$ -binomial languages in  $A^*$ .*

### 4.2 Uniform continuity and Newton polynomial functions

The aim of this section is to describe the uniformly continuous functions from  $A^*$  to a finite *p*-group. We first give a purely algebraic characterization of these functions (Proposition 4.3). Then we show that these functions are closed under applying differential operators (Proposition 4.4) and under taking sequential products (Proposition 4.5).

► **Proposition 4.3.** *Let  $G$  be a finite  $p$ -group and let  $f: A^* \rightarrow G$  be a function. Then  $f$  is uniformly continuous for the pro- $p$  metric if and only if there exist a finite  $p$ -group  $K$  and a monoid morphism  $\zeta: A^* \rightarrow K$  such that  $f$  factors through  $\zeta$ , that is, there is a map  $\lambda: K \rightarrow G$  such that  $f = \lambda \circ \zeta$ .*

► **Proposition 4.4.** *Let  $G$  be a finite  $p$ -group. If  $f: A^* \rightarrow G$  is uniformly continuous for the pro- $p$  metric, then so is  $\Delta^w f$  for any word  $w \in A^*$ .*

**Proof.** By induction and by Equation (2.2), it is enough to prove the result for  $w = a$  for any letter  $a \in A$ . In this case,  $\Delta^a f: A^* \rightarrow G$  is the composition of the following functions:

$$\begin{array}{lll} A^* \rightarrow A^* \times A^* & A^* \times A^* \rightarrow A^* \times A^* & A^* \times A^* \rightarrow G \times G \\ u \mapsto (u, u) & (u, v) \mapsto (u, va) & (u, v) \mapsto (f(u), f(v)) \\ \\ G \times G \rightarrow G \times G & G \times G \rightarrow G & \\ (g, h) \mapsto (g^{-1}, h) & (g, h) \mapsto gh & \end{array}$$

as shown by the sequence

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

Since the pro- $p$  metric is compatible with the monoid structure (see [6, Section 2] or [11, Section 1.4]), each of these functions is uniformly continuous and so is their composition. ◀

► **Proposition 4.5.** *Let  $G$  be a residually  $p$ -finite group. Any sequential product of uniformly continuous functions from  $A^*$  to  $G$  is uniformly continuous for the pro- $p$  metric.*

Here is an important consequence of these results.

► **Proposition 4.6.** *Let  $G$  be a finite  $p$ -group. Every Newton polynomial function  $f: A^* \rightarrow G$  is uniformly continuous.*

**Proof.** We prove the result by induction on the degree  $d$  of  $f$ . If  $d \leq 0$ , then  $f$  is a constant function and hence  $f$  is uniformly continuous. Otherwise, Proposition 3.3 shows that  $f$  is a sequential product of a family  $(f_a)_{a \in A}$  of Newton polynomial functions of degree  $\leq d - 1$ . By the induction hypothesis, each  $f_a$  is uniformly continuous and hence  $f$  is uniformly continuous by Proposition 4.5.  $\blacktriangleleft$

We now establish the converse of Proposition 4.6.

► **Proposition 4.7.** *Let  $G$  be a finite  $p$ -group. If a function  $f: A^* \rightarrow G$  is uniformly continuous for the pro- $p$  metric, then  $f$  is a Newton polynomial function.*

Several auxiliary definitions are needed to prove this proposition.

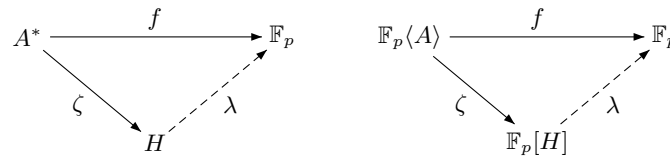
Let  $\mathbb{F}_p$  be the field with  $p$  elements and let  $\mathbb{F}_p[G]$  be the *group algebra* of  $G$  over  $\mathbb{F}_p$ . Each group morphism  $G_1 \rightarrow G_2$  extends uniquely, by linearity, to an  $\mathbb{F}_p$ -algebra morphism from  $\mathbb{F}_p[G_1]$  to  $\mathbb{F}_p[G_2]$ . Similarly, each function from  $G$  to  $\mathbb{F}_p$  extends uniquely, by linearity, to a linear form on  $\mathbb{F}_p[G]$ .

The vector space of linear forms on a  $\mathbb{F}_p$ -algebra  $R$  (that is, the *dual* of  $R$ ) is a left  $R$ -module: the action is defined, for any elements  $x, y$  in  $R$  and any linear form  $f$  on  $R$  by  $(x \cdot f)(y) = f(yx)$ .

**Sketch of the proof of Proposition 4.7.** Let  $p^r$  be the order of  $G$ . We prove the result by induction on  $r$ .

For  $r = 1$ ,  $G = \mathbb{Z}/p\mathbb{Z}$  and we switch to additive notation. Thus we have to show that  $\Delta^w f = \mathbf{0}$  for almost all  $w$ . Since  $\mathbb{Z}/p\mathbb{Z}$  is the additive group of the field  $\mathbb{F}_p$ , we may consider  $f$  as a function  $A^* \rightarrow \mathbb{F}_p$ . Since  $f$  is uniformly continuous, there exist by Proposition 4.3 a finite  $p$ -group  $H$ , a monoid morphism  $\zeta: A^* \rightarrow H$  and a function  $\lambda: H \rightarrow \mathbb{F}_p$  such that  $f = \lambda \circ \zeta$ , see the diagram on the left hand side of the figure below.

We extend by linearity all these functions, as explained previously, and denote these extensions by the same letters. We obtain the diagram on the right hand side of the figure below. Now  $\zeta$  is a morphism of  $\mathbb{F}_p$ -algebra and  $f$ , as well as  $\lambda$ , are  $\mathbb{F}_p$ -linear forms.



With these notations, one can first show that

$$\Delta^w f = \Delta^{a_1 \cdots a_n} f = ((a_1 - 1) \cdots (a_n - 1)) \cdot f|_{A^*}. \quad (4.1)$$

Since  $f = \lambda \circ \zeta$  and  $\zeta((a_1 - 1) \cdots (a_n - 1)) = (\zeta(a_1) - 1) \cdots (\zeta(a_n) - 1)$ , a little bit of work shows that

$$((a_1 - 1) \cdots (a_n - 1)) \cdot f = (((\zeta(a_1) - 1) \cdots (\zeta(a_n) - 1)) \cdot \lambda) \circ \zeta \quad (4.2)$$

Let  $I_H = \left\{ \sum_{g \in H} a_g g \mid \sum_{g \in H} a_g = 0 \right\}$  be the *augmentation ideal* of  $\mathbb{F}_p[H]$ . It follows from [2, Proposition VIII.10.4] that if  $n \geq |H|$ , then  $I_H^n = 0$ . Since every element  $\zeta(a_i) - 1$  belongs to  $I_H$ , one gets  $(\zeta(a_1) - 1) \cdots (\zeta(a_n) - 1) \in I_H^n$  and hence  $((\zeta(a_1) - 1) \cdots (\zeta(a_n) - 1)) = 0$ . Formulas (4.1) and (4.2) now show that  $\Delta^w f = \mathbf{0}$ , which settles the case  $r = 1$ .

Suppose now that  $r > 1$  and let  $f: A^* \rightarrow G$  be a uniformly continuous function for the pro- $p$  metric. By a standard result of group theory [13, Theorem 6.5, p. 116],  $G$  has a normal

subgroup  $C$  of order  $p$ . Now the quotient map  $q: G \rightarrow G/C$  is uniformly continuous and so is  $q \circ f: A^* \rightarrow G/C$ . Since  $|G/C| = p^{r-1}$ , the induction hypothesis can be applied: there exists  $n$  such that for any word  $v$  in  $A^*$  of length  $\geq n$ , one has  $\Delta^v(q \circ f) = 1$ .

Since  $\Delta^v(q \circ f) = q \circ (\Delta^v f)$  by Proposition 2.2, one has, for  $|v| \geq n$ ,  $q \circ (\Delta^v f) = 1$  and hence  $\Delta^v f$  maps  $A^*$  into  $C$ . Note that  $\Delta^v f$  is uniformly continuous by Proposition 4.4. Applying the first part of the proof to  $C$ , we get the following conclusion: for each  $v$  of length  $\geq n$ , there exists  $n_v$  such that for each word  $u$  of length at least  $n_v$ , one has  $\Delta^u \Delta^v f = 1$ . Let  $N$  be the maximum of all  $n_v$  taken over the finitely many  $v$  of length  $n$ . Then for each word  $w$  of length at least  $N + n$ , we may write  $w = uv$ , with  $|v| = n$  and  $|u| \geq N \geq n_v$ . Then  $\Delta^w f = \Delta^u \Delta^v f = 1$  and thus  $f$  is a Newton polynomial function. ◀

Putting Propositions 4.6 and 4.7 together, we get the main result of this section.

► **Theorem 4.8.** *Let  $G$  be a finite  $p$ -group. A function  $f: A^* \rightarrow G$  is uniformly continuous for the pro- $p$  metric if and only if it is a Newton polynomial function.*

## 5 Proof of the main result

We need two results on families of functions uniformly converging for the pro- $p$  metric.

► **Proposition 5.1.** *Let  $f: A^* \rightarrow F(B)$  be a function. If the elements  $\delta_u f$ ,  $u \in A^*$ , tend to 1 when  $|u|$  tends to  $\infty$ , then the sequence  $f_n$  tends uniformly to  $f$ .*

► **Proposition 5.2.** *A family of functions  $(g_u: A^* \rightarrow F(B))_{u \in A^*}$  converges uniformly to the function  $g: A^* \rightarrow F(B)$  when  $|u|$  tends to infinity if and only if, for any finite  $p$ -group  $H$  and any morphism  $\varphi: G \rightarrow H$ , there exists  $N$  such that, for all  $u \in A^*$  such that  $|u| \geq N$ , one has  $\varphi \circ g_u = \varphi \circ g$ .*

**Proof of Theorem 1.2.** The equivalence of (1) and (2) follows from Proposition 4.2. Let us prove that (2) implies (3). Let  $f: A^* \rightarrow F(B)$  be uniformly continuous. Let  $H$  be any finite  $p$ -group and  $\varphi$  be any group morphism  $F(B) \rightarrow H$ . Since  $\varphi$  is uniformly continuous, so is  $\varphi \circ f$ . By Proposition 4.7,  $\varphi \circ f$  is a Newton polynomial function and hence, for almost all  $w \in A^*$ ,  $\Delta^w(\varphi \circ f) = 1$ . Thus, by Proposition 2.2,  $\varphi \circ (\Delta^w f) = 1$ . Thus by Proposition 5.2, (3) holds.

The implication (4)  $\Rightarrow$  (5) follows from Propositions 3.4 and 5.1. Note that (3)  $\Rightarrow$  (4) is clear, and (5)  $\Rightarrow$  (2) follows from general theorems of topology, since, by Proposition 4.6, Newton polynomial functions are uniformly continuous. ◀

## 6 Conclusion and perspectives

By combining topology, algebra, automata and combinatorics on words, we solved the synthesis problem for  $\mathcal{G}_p$  in two different ways. Our results are based on a noncommutative extension of Mahler's theorem, a difficult mathematical result. In addition, we introduced two new concepts that would merit further study: the sequential product and Newton polynomial functions. We used the sequential product to solve the integration problem for a function  $f$  from  $A^*$  to a group  $G$ , knowing its initial value  $f(1)$  and the functions  $\Delta^a f$  for every letter  $a$ . We also proved that Newton's bijection induces a degree-preserving bijection between Newton polynomial functions and functions from  $A^*$  to  $G$  mapping almost every word to 1, a surprising combinatorial result.

Although these results offer exciting new perspectives, there is still a long way to go before one can solve the synthesis problem for regularity preserving functions. Solving the synthesis problem for other varieties of group languages is the next challenge.

---

References

---

- 1 Michaël Cadilhac, Olivier Carton, and Charles Paperman. Continuity and rational functions. In *44th International Colloquium on Automata, Languages, and Programming*, volume 80 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 115, 14. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2017.
- 2 Samuel Eilenberg. *Automata, Languages and Machines*, volume B. Academic Press, New York, 1976.
- 3 M. Lothaire. *Combinatorics on words*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1997.
- 4 Kurt Mahler. An interpolation series for continuous functions of a  $p$ -adic variable. *J. Reine Angew. Math.*, 199:23–34, 1958. Correction **208** (1961), 70–72.
- 5 Kurt Mahler. A correction to the paper “An interpolation series for continuous functions of a  $p$ -adic variable.”. *J. Reine Angew. Math.*, 208:70–72, 1961.
- 6 Jean-Éric Pin. Topologie  $p$ -adique sur les mots. *Journal de théorie des nombres de Bordeaux*, 5:263–281, 1993.
- 7 Jean-Éric Pin. Newton’s forward difference equation for functions from words to words. In Arnold Beckmann, Victor Mitranan, and Mariya Soskova, editors, *Evolving Computability*, volume 9136 of *Lect. Notes Comp. Sci.*, pages 71–82. Springer International Publishing, 2015.
- 8 Jean-Éric Pin and Pedro V. Silva. A topological approach to transductions. *Theoret. Comput. Sci.*, 340:443–456, 2005.
- 9 Jean-Éric Pin and Pedro V. Silva. A Mahler’s theorem for functions from words to integers. In Susanne Albers and Pascal Weil, editors, *25th International Symposium on Theoretical Aspects of Computer Science (STACS 2008)*, pages 585–596, Dagstuhl, Germany, 2008. Internationales Begegnungs- Und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.
- 10 Jean-Éric Pin and Pedro V. Silva. On profinite uniform structures defined by varieties of finite monoids. *Internat. J. Algebra Comput.*, 21:295–314, 2011.
- 11 Jean-Éric Pin and Pedro V. Silva. A noncommutative extension of Mahler’s theorem on interpolation series. *European J. Combin.*, 36:564–578, 2014.
- 12 Christophe Reutenauer and Marcel-Paul Schützenberger. Variétés et fonctions rationnelles. *Theoret. Comput. Sci.*, 145(1-2):229–240, 1995.
- 13 Harvey E. Rose. *A course on finite groups*. Universitext. Springer-Verlag London, Ltd., London, 2009.