# A noncommutative extension of Mahler's theorem on interpolation series <br> Jean-Eric Pin, Pedro Silva 

## To cite this version:

Jean-Eric Pin, Pedro Silva. A noncommutative extension of Mahler's theorem on interpolation series. 2011. hal-00654030

HAL Id: hal-00654030

## https://hal.science/hal-00654030

Preprint submitted on 20 Dec 2011

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.

# A noncommutative extension of Mahler's theorem on interpolation series ${ }^{1}$ 

Jean-Éric Pin, ${ }^{2}$ Pedro V. Silva ${ }^{3}$

Tuesday $20^{\text {th }}$ December, 2011


#### Abstract

In this paper, we prove an extension of Mahler's theorem on interpolation series, a celebrated result of $p$-adic analysis. Mahler's original result states that a function from $\mathbb{N}$ to $\mathbb{Z}$ is uniformly continuous for the $p$-adic metric $d_{p}$ if and only if it can be uniformly approximated by polynomial functions. We prove the same result for functions from a free monoid $A^{*}$ to $\mathbb{Z}$, where $d_{p}$ is replaced by the pro- $p$ metric, the profinite metric on $A^{*}$ defined by $p$-groups.


The aim of this paper is to give a noncommutative version of Mahler's theorem on interpolation series [8], which applies to functions from a free monoid to the set of integers. This result was first announced in [15] and this article is the full version of this conference paper.

The classical Stone-Weierstrass approximation theorem states that a continuous function defined on a closed interval can be uniformly approximated by a polynomial function. In particular, if a real function $f$ is infinitely differentiable in the neighbourhood of 0 , it can be approximated, under some convergence conditions, by its Taylor polynomials

$$
\sum_{n=0}^{k} \frac{f^{(n)}(0)}{n!} x^{n}
$$

The $p$-adic analogue of these results is Mahler's interpolation theorem [8]. It is is usually stated for $p$-adic valued functions on the $p$-adic integers, but this full version can be easily recovered from the simpler version given in

[^0]Theorem 1 below. First, for each function $f: \mathbb{N} \rightarrow \mathbb{Z}$, there exists a unique family $a_{k}$ of integers such that, for all $n \in \mathbb{N}$,

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

or, in short notation, $f=\sum_{k=0}^{\infty} a_{k}\binom{-}{k}$. The coefficients $a_{k}$ are given by the formula

$$
a_{k}=\left(\Delta^{k} f\right)(0)
$$

where $\Delta$ is the difference operator, defined by $(\Delta f)(n)=f(n+1)-f(n)$. In other words, the binomial functions $\binom{-}{k}$ form a basis of the $\mathbb{Z}$-module of all functions from $\mathbb{N}$ to $\mathbb{Z}$. The series $\sum_{k=0}^{\infty} a_{k}\binom{-}{k}$ is called the Mahler's expansion of $f$.

Mahler's theorem states that $f$ is uniformly continuous for the $p$-adic metric if and only if the partial sums of its Mahler's expansion converge uniformly to $f$. More precisely:

Theorem 1 (Mahler) Let $\sum_{k=0}^{\infty} a_{k}(-\bar{k})$ be the Mahler's expansion of a function $f: \mathbb{N} \rightarrow \mathbb{Z}$. The following conditions are equivalent:
(1) $f$ is uniformly continuous for the p-adic metric,
(2) the sequence of partial sums $\sum_{k=0}^{n} a_{k}(\bar{k})$ converges uniformly to $f$,
(3) $\lim _{k \rightarrow \infty}\left|a_{k}\right|_{p}=0$.

The most remarkable part of this 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. This nice feature makes Mahler's theorem the dream of students in mathematics: a function is equal to the sum of its Newton series if and only if it is uniformly continuous.

Our goal is to give a noncommutative extension of this result, based on the following observation: since the additive monoid $\mathbb{N}$ is isomorphic to the free monoid on a one-letter alphabet, the free monoid $A^{*}$ on a finite alphabet $A$ can be viewed as a noncommutative generalization of the natural numbers. Accordingly, our noncommutative extension concerns functions from $A^{*}$ to $\mathbb{Z}$. Nevertheless, generalizing Mahler's theorem to these functions requires a few preliminary questions to be solved:
(1) Extend the difference operators to word functions,
(2) Extend the binomial coefficients to words,
(3) Find a metric on $A^{*}$ which generalizes $d_{p}$,
(4) Find a Mahler expansion for functions from $A^{*}$ to $\mathbb{Z}$.

Fortunately, (1) can be readily solved and (2) and (3) have already be addressed by Eilenberg [5]: there is a well-defined notion of binomial coefficients $\binom{u}{v}$ for two words $u$ and $v$ and the pro- $p$ metric on $A^{*}$ is a natural
extension of the $p$-adic metric. Question (4) is the topic of Section 2, which culminates with Theorem 2.2, just like in the commutative case, every function $f: A^{*} \rightarrow \mathbb{Z}$ has a Mahler's expansion of the form $\sum_{v \in A^{*}}\langle f, v\rangle\binom{-}{v}$ where the coefficients $\langle f, v\rangle$ are integers related to the difference operators. There is also a striking similarity between Mahler's theorem and our main result, which can be stated as follows:

Theorem 2 Let $\sum_{v \in A^{*}}\langle f, v\rangle\binom{-}{v}$ be the Mahler's expansion of a function $f: A^{*} \rightarrow \mathbb{Z}$. The following conditions are equivalent:
(1) $f$ is uniformly continuous for the pro-p metric,
(2) the sequence of partial sums $\sum_{0 \leqslant|v| \leqslant n}\langle f, v\rangle\binom{-}{v}$ converges uniformly to $f$,
(3) $\lim _{|v| \rightarrow \infty}|\langle f, v\rangle|_{p}=0$.

Although this result can be considered as interesting on its own right, the reader may wonder about our original motivation for proving this theorem. It was actually inspired by automata theoretic questions related to the classification of regularity-preserving functions in language theory (see [14, 16] for more details). We discuss further this original motivation in Section 7

In Section 3, we introduce the notion of Mahler polynomials and prove some of their properties. Section 4, devoted to uniform continuity, is a crucial step towards the proof of the main theorem, presented in Section 5. In Section 6, we come back to the commutative case by providing an alternative proof for Amice's Theorem, a generalization of Mahler's Theorem to functions from $\mathbb{N}^{k}$ to $\mathbb{Z}$.

## 1 Background and notations

In this paper, $p$ denotes a fixed prime number.

### 1.1 The $p$-adic valuation and the $p$-adic metric

The $p$-adic valuation of a nonzero integer $n$ is the natural number

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

and its $p$-adic norm is the real number

$$
|n|_{p}=p^{-\nu_{p}(n)}
$$

By convention, we set $\nu_{p}(0)=+\infty$ and $|0|_{p}=0$. Note that, for all $x, y \in \mathbb{Z}$,

$$
\begin{align*}
& |x+y|_{p} \leqslant \max \left\{|x|_{p},|y|_{p}\right\} \leqslant|x|_{p}+|y|_{p}  \tag{1.1}\\
& |x y|_{p}=|x|_{p}|y|_{p} \leqslant \min \left\{|x|_{p},|y|_{p}\right\} \tag{1.2}
\end{align*}
$$

The $p$-adic metric $d_{p}$ on $\mathbb{N}$ and $\mathbb{Z}$ is defined by setting, for each pair $(x, y)$ of integers,

$$
\begin{equation*}
d_{p}(x, y)=|x-y|_{p} \tag{1.3}
\end{equation*}
$$

These definitions can be extended to $\mathbb{N}^{k}$ and to $\mathbb{Z}^{k}$ as follows. Given $x=$ $\left(x_{1}, \ldots, x_{k}\right)$ and $y=\left(y_{1}, \ldots, y_{k}\right)$ in $\mathbb{Z}^{k}$ and a positive integer $r$, we write $x \equiv y(\bmod r)$ if, for $1 \leqslant i \leqslant k, x_{i} \equiv y_{i}(\bmod r)$. The $p$-adic valuation of $x$ is

$$
\nu_{p}(x)=\min \left\{n \in \mathbb{N} \mid x \not \equiv 0 \quad\left(\bmod p^{n+1}\right)\right\}
$$

and the $p$-adic norm is $|x|_{p}=p^{-\nu_{p}(x)}$. Finally, the $p$-adic metric on $\mathbb{Z}^{k}$ is defined by the formula 1.3$)$, for each pair $(x, y)$ of elements of $\mathbb{Z}^{k}$.

It is well-known that $d_{p}$ is actually an ultrametric, that is, satisfies the following stronger form of the triangle inequality, for all $u, v, w$ in $\mathbb{Z}^{k}$ :

$$
d_{p}(u, v) \leqslant \max \left\{d_{p}(u, w), d_{p}(w, v)\right\}
$$

### 1.2 Words and languages

Let $A$ be a finite alphabet. Recall that the free monoid $A^{*}$ on $A$ is the set of all words on $A$, endowed with the concatenation operation. The empty word, denoted 1 , is the identity of $A^{*}$. The length of a word $u$ is denoted $|u|$. If $a$ is a letter of $A$, we denote by $|u|_{a}$ the number of occurrences of $a$ in $u$.

A language is a subset of $A^{*}$. An important class of languages is the class of recognizable (also called regular) languages. Recognizable languages admit various characterizations, ranging from automata theory to topology or logic, but we will settle for the following algebraic definition: a language $L$ of $A^{*}$ is recognizable if and only if there exists a monoid morphism $\varphi$ from $A^{*}$ onto some finite monoid $M$ such that $L=\varphi^{-1}(\varphi(L))$. It is then said that $M$ recognizes the language $L$.

### 1.3 Binomial coefficients

Let $u$ and $v$ be two words of $A^{*}$. Let $u=a_{1} \cdots a_{n}$, with $a_{1}, \ldots, a_{n} \in A$. 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 $a a b a$ is a subword of caacabca. Following [5, 7], we define the binomial coefficient of $u$ and $v$ by setting

$$
\binom{v}{u}=\left|\left\{\left(v_{0}, \ldots, v_{n}\right) \mid v=v_{0} a_{1} v_{1} \ldots a_{n} v_{n}\right\}\right|
$$

Observe that if $a$ is a letter, then $\binom{v}{a}$ is equal to $|v|_{a}$. Further, if $u=a^{n}$ and $v=a^{m}$, then

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

and hence these numbers constitute a generalization of the classical binomial coefficients. The next proposition, whose proof can be found in [7, Chapter $6]$, summarizes the basic properties of the generalized binomial coefficients and can serve as an alternative definition.

Lemma 1.1 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) $\binom{u a}{v b}= \begin{cases}\binom{u}{v b} & \text { if } a \neq b \\ \binom{u}{v b}+\binom{u}{v} & \text { if } a=b\end{cases}$

A third way to define the binomial coefficients is to use the Magnus automorphism of the algebra $\mathbb{Z}\langle A\rangle$ of polynomials in noncommutative indeterminates in $A$ defined by $\mu(a)=1+a$ for all $a \in A$. One can show that, for all $u \in A^{*}$,

$$
\begin{equation*}
\mu(u)=\sum_{x \in A^{*}}\binom{u}{x} x \tag{1.4}
\end{equation*}
$$

which leads to the formula

$$
\begin{equation*}
\binom{u_{1} u_{2}}{x}=\sum_{x_{1} x_{2}=x}\binom{u_{1}}{x_{1}}\binom{u_{2}}{x_{2}} \tag{1.5}
\end{equation*}
$$

### 1.4 The pro-p metric

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 $\varphi(u) \neq \varphi(v)$. One can show that any pair of distinct words can be separated by a $p$-group [5]. The pro-p metric $d_{p}$ on $A^{*}$ is defined by setting

$$
\begin{aligned}
r_{p}(u, v) & =\min \left\{n \mid \text { there is a } p \text {-group of order } p^{n+1} \text { separating } u \text { and } v\right\} \\
d_{p}(u, v) & =p^{-r_{p}(u, v)}
\end{aligned}
$$

with the usual convention $\min \emptyset=+\infty$ and $p^{-\infty}=0$. It turns out that $d_{p}$ is an ultrametric. One can also show that the concatenation product on $A^{*}$ is uniformly continuous for this metric. It follows that the completion of the metric space $\left(A^{*}, d_{p}\right)$ is naturally equipped with a structure of monoid. This monoid is in fact a compact group, called the free pro-p group and denoted $\widehat{F}_{p}(A)$. When $A$ is a one-letter alphabet, this group is of course $\mathbb{Z}_{p}$, the additive group of $p$-adic integers.

One can define in a similar way a pro- $p$ metric on $\mathbb{N}^{k}$ or $\mathbb{Z}^{k}$. The attentive reader will notice a potential conflict of notation between the $p$-adic metric and the pro-p metric on $\mathbb{Z}^{k}$, which were both denoted by $d_{p}$. The next lemma gets rid of this ambiguity.

Lemma 1.2 The p-adic metric and the pro-p metric coincide on $\mathbb{N}^{k}$ and on $\mathbb{Z}^{k}$.

Proof. First, the pro- $p$ metric on $\mathbb{N}^{k}$ is the restriction to $\mathbb{N}^{k}$ of the pro- $p$ metric on $\mathbb{Z}^{k}$ since every morphism from $\mathbb{N}^{k}$ onto a group extends uniquely to $\mathbb{Z}^{k}$. Therefore it suffices to prove that for all $u, v \in \mathbb{Z}^{k}$, one has $r_{p}(u, v)=$ $\nu_{p}(u-v)$.

Since $\mathbb{Z}^{k}$ is Abelian, a direct product of groups separates $u$ and $v$ if and only if one of its factors separates $u$ and $v$. Let $C_{r}$ be the cyclic group of order $r$. In view of the structure theorem of Abelian groups, one has

$$
r_{p}(u, v)=\min \left\{n \mid C_{p^{n+1}} \text { separates } u \text { and } v\right\} \leqslant \nu_{p}(u-v)
$$

Further, for every homomorphism $f: \mathbb{Z}^{k} \rightarrow \mathbb{Z}, u \equiv v\left(\bmod p^{n+1}\right)$ implies $f(u) \equiv f(v)\left(\bmod p^{n+1}\right)$. Therefore $u \not \equiv v\left(\bmod p^{n+1}\right)$ is a necessary condition for $C_{p^{n+1}}$ to separate $u$ and $v$. Thus $r_{p}(u, v)=\nu_{p}(u-v)$ as claimed.

There is a nice connection [11] between the pro- $p$ metric and the binomial coefficients, which comes from the characterization of the languages recognized by a $p$-group given by Eilenberg and Schützenberger [5, Theorem 10.1, p. 239]. Let us call a p-group language a language recognized by a $p$-group. Note that such a language is recognizable by definition.

Proposition 1.3 $A$ language of $A^{*}$ is a p-group language if and only if it is a Boolean combination of the languages

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

for $0 \leqslant r<p$ and $x \in A^{*}$.
Let us set now

$$
\begin{aligned}
r_{p}^{\prime}(u, v) & =\min \left\{|x| \mid x \in A^{*} \text { and }\binom{u}{x} \not \equiv\binom{v}{x} \quad(\bmod p)\right\} \\
d_{p}^{\prime}(u, v) & =p^{-r_{p}^{\prime}(u, v)}
\end{aligned}
$$

It is proved in [11, Theorem 4.4] that $d_{p}^{\prime}$ is an ultrametric uniformly equivalent to $d_{p}$. We shall use this fact in the proof of our main theorem.

The following result, which follows from [15, Theorem 2.3] provides a characterization of uniform continuity in terms of $p$-group languages. Let $A$ and $B$ be two finite alphabets.

Theorem 1.4 A function $f: A^{*} \rightarrow B^{*}$ is uniformly continuous for $d_{p}$ if and only if, for every p-group language $L$ of $B^{*}$, the language $f^{-1}(L)$ is a $p$-group language of $A^{*}$.

Since p-group languages are closed under inverse of morphisms [5], one gets the following corollary.

Corollary 1.5 Every monoid morphism from $A^{*}$ to $B^{*}$ is uniformly continuous for $d_{p}$.

As another consequence of Theorem 1.4, we obtain:
Corollary 1.6 For every $v \in A^{*}$, the function from $A^{*}$ into $\mathbb{N}$ which maps every word $x$ onto the binomial coefficient $\binom{x}{v}$ is uniformly continuous for $d_{p}$.

Proof. Let $f_{v}: A^{*} \rightarrow \mathbb{N}$ be the function defined by $f_{v}(x)=\binom{x}{v}$. Since the only $p$-group quotients of $\mathbb{N}$ are the cyclic groups of order $p^{n}$, a language of $\mathbb{N}$ recognized by a $p$-group is a finite union of arithmetic progressions $r+p^{n} \mathbb{N}$ $\left(r \in\left\{0, \ldots, p^{n}-1\right\}\right)$. In view of Theorem 1.4 , and since the class of $p$-group languages is closed under union, we only need to show that $f_{v}^{-1}\left(r+p^{n} \mathbb{N}\right)$ is a $p$-group language. Now, [10, Example 4, p. 450] shows that

$$
f_{v}^{-1}\left(r+p^{n} \mathbb{N}\right)=\left\{x \in A^{*} \left\lvert\,\binom{ x}{v} \equiv r \quad\left(\bmod p^{n}\right)\right.\right\}
$$

is indeed recognized by a $p$-group.

## 2 Mahler's expansions

The first step to extend Mahler's theorem to functions from words to integers is to define a suitable notion of Mahler's expansion for these functions.

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

$$
\left(\Delta^{a} f\right)(u)=f(u a)-f(u)
$$

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

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

For instance,

$$
\Delta^{a a b} f(u)=-f(u)+2 f(u a)+f(u b)-f(u a a)-2 f(u a b)+f(u a a b)
$$

The next proposition gives a direct way to compute the difference operators.
Proposition 2.1 For each word word $w \in A^{*}$, the following relation holds:

$$
\begin{equation*}
\Delta^{w} f(u)=\sum_{0 \leqslant|x| \leqslant|w|}(-1)^{|w|+|x|}\binom{w}{x} f(u x) \tag{2.1}
\end{equation*}
$$

Proof. We prove the result by induction on the length of $w$. If $w$ is the empty word, the result is trivial. Let $w$ be a word and let $a$ be a letter. Then $\left(\Delta^{a w} f\right)(u)=\left(\Delta^{a}\left(\Delta^{w} f\right)\right)(u)=\left(\Delta^{w} f\right)(u a)-\left(\Delta^{w} f\right)(u)$ and by the induction hypothesis applied to $w$,

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

On the other hand, since

$$
\binom{a w}{x}= \begin{cases}\binom{w}{a z}+\binom{w}{z} & \text { if } x=a z \\ \binom{w}{x} & \text { otherwise }\end{cases}
$$

we get

$$
\begin{aligned}
& \sum_{0 \leqslant|x| \leqslant|a w|}(-1)^{|a w|+|x|}\binom{a w}{x} f(u x) \\
&= \sum_{0 \leqslant|a z| \leqslant|w|+1}(-1)^{|w|+|a z|+1}\left(\binom{w}{a z}+\binom{w}{z}\right) f(u a z) \\
&+\sum_{\substack{0 \leqslant|x| \leqslant|w|+1 \\
x \notin a A^{*}}}(-1)^{|w|+|x|+1}\binom{w}{x} f(u x) \\
&= \sum_{0 \leqslant|z| \leqslant|w|}(-1)^{|w|+|z|}\binom{w}{z} f(u a z) \\
&+\sum_{0 \leqslant|x| \leqslant|w|}(-1)^{|w|+|x|+1}\binom{w}{x} f(u x) \\
&= \sum_{0 \leqslant|x| \leqslant|w|}(-1)^{|w|+|x|}\binom{w}{x}(f(u a x)-f(u x))
\end{aligned}
$$

and thus

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

which gives the induction step for the proof of 2.1 .
By Corollary 1.6, for a fixed $v \in A^{*}$, the function $\binom{-}{v}$ from $A^{*}$ to $\mathbb{N}$ which maps a word $u$ to the binomial coefficient $\binom{u}{v}$ is uniformly continuous for $d_{p}$. This family of functions, for $v$ ranging over $A^{*}$, is locally finite in the sense that, for each $u \in A^{*}$, the binomial coefficient $\binom{u}{v}$ is null for all but finitely many words $v$. In particular, if $\left(m_{v}\right)_{v \in A^{*}}$ is a family of integers, there is a well-defined function from $A^{*}$ to $\mathbb{Z}$ defined by the formula

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

We can now state our first result, which doesn't require any assumption on $f$.

Theorem 2.2 Let $f: A^{*} \rightarrow \mathbb{Z}$ be an arbitrary function. Then there exists a unique family $\langle f, v\rangle_{v \in A^{*}}$ of integers such that, for all $u \in A^{*}$,

$$
\begin{equation*}
f(u)=\sum_{v \in A^{*}}\langle f, v\rangle\binom{ u}{v} \tag{2.2}
\end{equation*}
$$

This family is given by

$$
\begin{equation*}
\langle f, v\rangle=\left(\Delta^{v} f\right)(1)=\sum_{0 \leqslant|x| \leqslant|v|}(-1)^{|v|+|x|}\binom{v}{x} f(x) \tag{2.3}
\end{equation*}
$$

Proof. First observe that, according to 2.1

$$
\begin{equation*}
\left(\Delta^{v} f\right)(1)=\sum_{0 \leqslant|x| \leqslant|v|}(-1)^{|v|+|x|}\binom{v}{x} f(x) \tag{2.4}
\end{equation*}
$$

Thus

$$
\begin{aligned}
\sum_{v \in A^{*}}\left(\Delta^{v} f\right)(1)\binom{u}{v} & =\sum_{v \in A^{*}} \sum_{|x| \leqslant|v|}(-1)^{|v|+|x|}\binom{v}{x}\binom{u}{v} f(x) \\
& =\sum_{x \in A^{*}}(-1)^{|u|+|x|}\left(\sum_{0 \leqslant|v| \leqslant|u|}(-1)^{|v|+|u|}\binom{u}{v}\binom{v}{x}\right) f(x) \\
& =f(u)
\end{aligned}
$$

in view of the following relation from [7, Corollary 6.3.8]:

$$
\sum_{0 \leqslant|v| \leqslant|u|}(-1)^{|u|+|v|}\binom{u}{v}\binom{v}{w}= \begin{cases}1 & \text { if } u=w  \tag{2.5}\\ 0 & \text { otherwise }\end{cases}
$$

Uniqueness of the coefficients $\langle f, v\rangle$ follows inductively from the formula

$$
\langle f, u\rangle=f(u)-\sum_{0 \leqslant|v|<|u|}\langle f, v\rangle\binom{ u}{v},
$$

a straightforward consequence of 2.2 .
The series defined by 2.2 is called the Mahler's expansion of $f$.
Example 2.1 Let $A$ be the binary alphabet $\{0,1\}$. The empty word will be exceptionally denoted by $\varepsilon$ to avoid confusion. Let $f: A^{*} \rightarrow \mathbb{N}$ be the function mapping a binary word onto its value as a binary number. For instance $f(010111)=f(10111)=23$. Then one sees easily that

$$
\begin{aligned}
\left(\Delta^{v} f\right) & = \begin{cases}f+1 & \text { if } v \in 1\{0,1\}^{*} \\
f & \text { otherwise }\end{cases} \\
\left(\Delta^{v} f\right)(\varepsilon) & = \begin{cases}1 & \text { if } v \in 1\{0,1\}^{*} \\
0 & \text { otherwise }\end{cases}
\end{aligned}
$$

It follows that the Mahler expansion of $f$ is

$$
f=\sum_{v \in 1\{0,1\}^{*}}\binom{-}{v}
$$

For instance, if $u=01001$, one gets
$f(u)=\binom{u}{1}+\binom{u}{10}+\binom{u}{11}+\binom{u}{100}+\binom{u}{101}+\binom{u}{1001}=2+2+1+1+2+1=9$.

The Mahler's expansion of a function $f: A^{*} \rightarrow \mathbb{Z}$ can be used to compute its uniform norm $\|f\|_{p}$, defined by

$$
\|f\|_{p}=\sup _{u \in A^{*}}|f(u)|_{p}
$$

First observe that $\|f\|_{p}=\max _{u \in A^{*}}|f(u)|_{p}$ since $|f(u)|_{p}$ takes values in the set $\left\{p^{-n} \mid n \geqslant 0\right\} \cup\{0\}$.

Theorem 2.3 Let $\sum_{v \in A^{*}}\langle f, v\rangle\binom{-}{v}$ be the Mahler's expansion of a function $f: A^{*} \rightarrow \mathbb{Z}$. Then $\|f\|_{p}=\max _{v \in A^{*}}|\langle f, v\rangle|_{p}$.

Proof. Let us choose a word $u$ of $A^{*}$ such that $\|f\|_{p}=|f(u)|_{p}$. Then $f(u)=\sum_{|v| \leqslant|u|}\langle f, v\rangle\binom{ u}{v}$ and thus we get by 1.1 ) and 1.2

$$
\|f\|_{p}=|f(u)|_{p} \leqslant \max _{|v| \leqslant|u|}|\langle f, v\rangle|_{p} \leqslant \max _{v \in A^{*}}|\langle f, v\rangle|_{p}
$$

Conversely, let $w$ be a word of minimal length such that

$$
|\langle f, w\rangle|_{p}=\max _{v \in A^{*}}|\langle f, v\rangle|_{p}
$$

The formula

$$
\langle f, w\rangle=f(w)-\sum_{0 \leqslant|v|<|w|}\langle f, v\rangle\binom{ u}{v}
$$

yields, with the help of $(1.1)$ and (1.2),

$$
|\langle f, w\rangle|_{p} \leqslant \max \left(|f(w)|_{p}, \max _{0 \leqslant|v|<|w|}|\langle f, v\rangle|_{p}\right)
$$

Now, for $0 \leqslant|v|<|w|$, one has $|\langle f, v\rangle|_{p}<|\langle f, w\rangle|_{p}$ by the minimality of $|w|$ and thus $\max _{0 \leqslant|v|<|w|}|\langle f, v\rangle|_{p}<|\langle f, w\rangle|_{p}$. It follows that

$$
|\langle f, w\rangle|_{p} \leqslant|f(w)|_{p} \leqslant\|f\|_{p}
$$

and hence $\max _{v \in A^{*}}|\langle f, v\rangle|_{p}=\|f\|_{p}$ as claimed.

## 3 Mahler polynomials

A function $f: A^{*} \rightarrow \mathbb{Z}$ 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. In this section, we prove in particular that Mahler polynomials are closed under addition and product. We first introduce a convenient combinatorial operation, the infiltration product. We follow the presentation of [7].

Let $\mathbb{Z}\langle\langle A\rangle\rangle$ be the ring of formal power series in noncommutative indeterminates in $A$. Any series $s$ is written as a formal sum $s=\sum_{u \in A^{*}}\langle s, u\rangle u$, a notation not to be confused with our notation for the Mahler's expansion. The infiltration product is the binary operation on $\mathbb{Z}\langle\langle A\rangle\rangle$, denoted by $\uparrow$ and defined inductively as follows:
for all $u \in A^{*}$,

$$
\begin{equation*}
u \uparrow 1=1 \uparrow u=u \tag{3.1}
\end{equation*}
$$

for all $u, v \in A^{*}$, for all $a, b \in A$

$$
u a \uparrow b v= \begin{cases}(u \uparrow v b) a+(u a \uparrow v) b+(u \uparrow v) a & \text { if } a=b  \tag{3.2}\\ (u \uparrow v b) a+(u a \uparrow v) b & \text { otherwise }\end{cases}
$$

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

$$
\begin{equation*}
s \uparrow t=\sum_{u, v \in A^{*}}\langle s, u\rangle\langle t, v\rangle(u \uparrow v) \tag{3.3}
\end{equation*}
$$

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,

$$
\begin{aligned}
& a b \uparrow a b=a b+2 a a b+2 a b b+4 a a b b+2 a b a b \\
& a b \uparrow b a=a b a+b a b+a b a b+2 a b b a+2 b a a b+b a b a
\end{aligned}
$$

Also note that $\langle u \uparrow v, u\rangle=\binom{u}{v}$. We shall need the following relation (see [7, p.131]). For all $v_{1}, v_{2} \in A^{*}$,

$$
\begin{equation*}
\binom{u}{v_{1}}\binom{u}{v_{2}}=\sum_{x \in A^{*}}\left\langle v_{1} \uparrow v_{2}, x\right\rangle\binom{ u}{x} \tag{3.4}
\end{equation*}
$$

Formula 3.4 leads to an explicit computation of the Mahler's expansion of the product of two functions.

Proposition 3.1 Let $f$ and $g$ be two functions from $A^{*}$ to $\mathbb{N}$. Then the coefficients of the Mahler's expansion of $f g$ are given by the formula:

$$
\langle f g, x\rangle=\sum_{v_{1}, v_{2} \in A^{*}}\left\langle f, v_{1}\right\rangle\left\langle g, v_{2}\right\rangle\left\langle v_{1} \uparrow v_{2}, x\right\rangle
$$

Proof. Indeed, if $f(u)=\sum_{v \in A^{*}}\langle f, v\rangle\binom{ u}{v}$ and $g(u)=\sum_{v \in A^{*}}\langle g, v\rangle\binom{ u}{v}$, then

$$
f g(u)=\sum_{v_{1}, v_{2} \in A^{*}}\left\langle f, v_{1}\right\rangle\left\langle g, v_{2}\right\rangle\binom{ u}{v_{1}}\binom{u}{v_{2}}
$$

and the result follows by Formula (3.4).
It is now easy to prove the result announced at the beginning of this section.
Proposition 3.2 Mahler polynomials form a subring of the ring of all functions from $A^{*}$ to $\mathbb{Z}$ for addition and multiplication.

Proof. It is clear that the difference of two Mahler polynomials is a Mahler polynomial. Further Proposition 3.1 shows that Mahler polynomials are closed under product.

## 4 Uniform continuity

In this section, we give a simple characterization of the uniformly continuous functions from $A^{*}$ to $\mathbb{Z}$. Uniform continuity always refers to the metric $d_{p}$, but it can be replaced by $d_{p}^{\prime}$ whenever convenient in view of [11, Theorem 4.4].

Theorem 4.1 Let $\sum_{v \in A^{*}}\langle f, v\rangle\binom{-}{v}$ be the Mahler's expansion of a function $f: A^{*} \rightarrow \mathbb{Z}$. Then $f$ is uniformly continuous if and only if $\lim _{|v| \rightarrow \infty}|\langle f, v\rangle|_{p}=$ 0.

Proof. Suppose that $\lim _{|v| \rightarrow \infty}|\langle f, v\rangle|_{p}=0$ and let $r \in \mathbb{N}$. Then there exists $s \in \mathbb{N}$ such that, if $|v| \geqslant s, \nu_{p}(\langle f, v\rangle) \geqslant r$. Setting

$$
g=\sum_{|v|<s}\langle f, v\rangle\binom{-}{v} \text { and } h=\sum_{|v| \geqslant s}\langle f, v\rangle\binom{-}{v}
$$

we get $f=g+h$. Further $p^{r}$ divides $\langle f, v\rangle$ for $|v| \geqslant s$. Since $g$ is a Mahler polynomial, it is uniformly continuous by Corollary 1.6 and so there exists $t \in \mathbb{N}$ such that $d_{p}\left(u, u^{\prime}\right) \leqslant p^{-t}$ implies $g(u) \equiv g\left(u^{\prime}\right)\left(\bmod p^{r}\right)$ and hence $f(u) \equiv f\left(u^{\prime}\right)\left(\bmod p^{r}\right)$. Thus $f$ is uniformly continuous.

This proves the easy direction of the theorem. The key argument for the opposite direction is the following approximation result.

Theorem 4.2 Let $f: A^{*} \rightarrow \mathbb{N}$ be a uniformly continuous function. Then there exists a Mahler polynomial $P$ such that, for all $u \in A^{*}, f(u) \equiv P(u)$ $(\bmod p)$.

Proof. We first prove the theorem for some characteristic functions related to the binomial coefficients. The precise role of these functions will appear in the course of the main proof.

Let $x \in A^{*}$ and let $s$ be an integer such that $0 \leqslant s<p$. Let $\chi_{s, x}: A^{*} \rightarrow \mathbb{N}$ be the function defined by

$$
\chi_{s, x}(u)= \begin{cases}1 & \text { if }\binom{u}{x} \equiv s \quad(\bmod p) \\ 0 & \text { otherwise }\end{cases}
$$

Lemma 4.3 There is a Mahler polynomial $P_{s, x}$ such that, for all $u \in A^{*}$, $\chi_{s, x}(u) \equiv P_{s, x}(u)(\bmod p)$.

Proof. Let

$$
P_{s, x}(u)=-\frac{\left[\binom{u}{x}\right]\left[\binom{u}{x}-1\right] \cdots\left[\binom{u}{x}-(p-1)\right]}{\binom{u}{x}-s}
$$

Then $P_{s, x}$ is a Mahler polynomial by Proposition 3.2. If $\binom{u}{x} \not \equiv s(\bmod p)$, then $P_{s, x}(u) \equiv 0(\bmod p)$. If $\binom{u}{x} \equiv s(\bmod p)$, then by Ibn Al-Haytham's theorem (also known as Wilson's theorem),

$$
P_{s, x}(u) \equiv-(p-1)!\equiv 1 \quad(\bmod p)
$$

It follows that $P_{s, x}(u) \equiv \chi_{s, x}(u)(\bmod p)$ in all cases.
We now prove Theorem 4.2. Since $f$ is uniformly continuous for the metric $d_{p}^{\prime}$, there exists a positive integer $n$ such that if, for $0 \leqslant|x| \leqslant n$,

$$
\binom{u}{x} \equiv\binom{v}{x} \quad(\bmod p)
$$

then

$$
f(u) \equiv f(v) \quad(\bmod p)
$$

It follows that the value of $f(u)$ modulo $p$ depends only on the residues modulo $p$ of the family $\left\{\binom{u}{x}\right\}_{0 \leqslant|x| \leqslant n}$.

Let $R$ be the set of all families $r=\left\{r_{x}\right\}_{0 \leqslant|x| \leqslant n}$ such that $0 \leqslant r_{x}<p$. For $0 \leqslant i<p$, let $R_{i}$ be the set of all families $r$ of $R$ satisfying the following condition:

$$
\begin{equation*}
\text { if, for } 0 \leqslant|x| \leqslant n,\binom{u}{x} \equiv r_{x} \quad(\bmod p), \text { then } f(u) \equiv i \quad(\bmod p) \tag{4.1}
\end{equation*}
$$

The sets $\left(R_{i}\right)_{0 \leqslant i<p}$ are pairwise disjoint and their union is $R$. We claim that, for all $u \in A^{*}$,

$$
\begin{equation*}
f(u) \equiv \sum_{0 \leqslant i<p} i P_{i}(u) \quad(\bmod p) \tag{4.2}
\end{equation*}
$$

where $P_{i}$ is the Mahler polynomial

$$
\begin{equation*}
P_{i}=\sum_{r \in R_{i}} \prod_{0 \leqslant|x| \leqslant n} P_{r_{x}, x} \tag{4.3}
\end{equation*}
$$

First consider, for $r \in R$, the characteristic function

$$
\chi_{r}(u)=\prod_{0 \leqslant|x| \leqslant n} \chi_{r_{x}, x}(u)
$$

By construction, $\chi_{r}$ is defined by

$$
\chi_{r}(u)= \begin{cases}1 & \text { if, for } 0 \leqslant|x| \leqslant n,\binom{u}{x} \equiv r_{x} \quad(\bmod p) \\ 0 & \text { otherwise }\end{cases}
$$

and it follows from 4.1 and from the definition of $R_{i}$ that

$$
\begin{equation*}
f(u) \equiv \sum_{0 \leqslant i<p}\left(i \sum_{r \in R_{i}} \chi_{r}(u)\right) \quad(\bmod p) \tag{4.4}
\end{equation*}
$$

Now Lemma 4.3 gives immediately

$$
\begin{equation*}
\chi_{r}(u) \equiv \prod_{0 \leqslant|x| \leqslant n} P_{r_{x}, x}(u) \quad(\bmod p) \tag{4.5}
\end{equation*}
$$

and thus (4.2) follows now from (4.3), (4.4) and (4.5). The result follows, since

$$
P=\sum_{0 \leqslant i<p} i P_{i}(u)
$$

is a Mahler polynomial.
Theorem 4.2 can be extended as follows.
Corollary 4.4 Let $f: A^{*} \rightarrow \mathbb{N}$ be a uniformly continuous function. Then, for each positive integer $r$, there exists a Mahler polynomial $P_{r}$ such that, for all $u \in A^{*}, f(u) \equiv P_{r}(u)\left(\bmod p^{r}\right)$.

Proof. We prove the result by induction on $r$. For $r=1$, the result follows from Theorem4.2. If the result holds for $r$, there exists a Mahler polynomial $P_{r}$ such that, for all $u \in A^{*}, f(u)-P_{r}(u) \equiv 0\left(\bmod p^{r}\right)$. Let $g=f-P_{r}$. Since $g$ is uniformly continuous, there exists a positive integer $n$ such that if $\binom{u}{x} \equiv\binom{v}{x} \quad(\bmod p)$ for $|x| \leqslant n$, then $g(u) \equiv g(v)\left(\bmod p^{2 r}\right)$. It follows that $\frac{1}{p^{r}} g(u) \equiv \frac{1}{p^{r}} g(v)\left(\bmod p^{r}\right)$, and thus $\frac{1}{p^{r}} g$ is uniformly continuous.

Applying Theorem 4.2 to $\frac{1}{p^{r}} g$, we get a Mahler polynomial $P$ such that, for all $u \in A^{*}$,

$$
\frac{1}{p^{r}} g(u) \equiv P(u) \quad(\bmod p)
$$

Setting $P_{r+1}=P_{r}+p^{r} P$, we obtain finally

$$
f(u) \equiv P_{r+1}(u) \quad\left(\bmod p^{r+1}\right)
$$

which concludes the proof.
We now come back to the proof of Theorem 4.1 For each positive integer $r$, there exists a Mahler polynomial $P_{r}$ such that, for all $u \in A^{*}$, $f(u) \equiv P_{r}(u)\left(\bmod p^{r}\right)$. Using (2.3) to compute explicitly the coefficients $\left\langle f-P_{r}, v\right\rangle$, we obtain

$$
\left\langle f-P_{r}, v\right\rangle \equiv 0 \quad\left(\bmod p^{r}\right)
$$

Since $P_{r}$ is a polynomial, there exists an integer $n_{r}$ such that for all $v \in$ $A^{*}$ such that $|v| \geqslant n_{r},\left\langle P_{r}, v\right\rangle=0$. It follows $|\langle f, v\rangle|_{p} \leqslant p^{-r}$ and thus $\lim _{|v| \rightarrow \infty}|\langle f, v\rangle|_{p}=0$.

## 5 An extension of Mahler's theorem

Mahler's theorem is often presented as an interpolation result (see for instance [9, p. 57]). This can also be extended to functions from words to integers. Given a family of integers $\left(c_{v}\right)_{v \in A^{*}}$, one can ask whether there is a (uniformly) continuous function $f$ from the free pro- $p$ group to $\mathbb{Z}$ such that $f(v)=c_{v}$. The answer to this question is part of our main result:

Theorem 5.1 Let $\sum_{v \in A^{*}}\langle f, v\rangle\binom{-}{v}$ be the Mahler's expansion of a function $f: A^{*} \rightarrow \mathbb{Z}$. Then the following conditions are equivalent:
(1) $f$ is uniformly continuous for $d_{p}$,
(2) the sequence of partial sums $\sum_{0 \leqslant|v| \leqslant n}\langle f, v\rangle\binom{-}{v}$ converges uniformly to $f$,
(3) $\lim _{|v| \rightarrow \infty}|\langle f, v\rangle|_{p}=0$,
(4) $\lim _{|v| \rightarrow \infty}\left\|\Delta^{v} f\right\|_{p}=0$,
(5) $f$ admits a continuous extension from $\widehat{F}_{p}(A)$ to $\mathbb{Z}_{p}$.

Proof. (1) implies (3) follows from Theorem 4.1.
(3) implies (2). Formulas (1.1) and (1.2) give for all $u \in A^{*}$ and for all $n \in \mathbb{N}$

$$
\left|\sum_{n<|v|}\langle f, v\rangle\binom{ u}{v}\right|_{p} \leqslant \sup _{n<|v| \leqslant|u|}|\langle f, v\rangle|_{p} \leqslant \sup _{n<|v|}|\langle f, v\rangle|_{p}
$$

Let $\varepsilon>0$. By (3), there is an integer $N$ such that if $|v| \geqslant N$, then $|\langle f, v\rangle|_{p}<$ $\varepsilon$. It follows that for all $n \geqslant N$ and for all $u \in A^{*}$,

$$
\left|\sum_{n<|v|}\langle f, v\rangle\binom{ u}{v}\right|_{p} \leqslant \sup _{n<|v|}|\langle f, v\rangle|_{p}<\varepsilon .
$$

which proves (2), in view of (2.1).
(2) implies (1). Theorem 4.1 shows that every Mahler polynomial is uniformly continuous. Now, if a sequence of uniformly continuous functions converges uniformly, then its limit is uniformly continuous as well. Thus (2) implies that $f$ is uniformly continuous.
(3) implies (4). A straightforward induction shows that $\Delta^{u}\left(\Delta^{v} f\right)=$ $\Delta^{u v} f$ holds for all $u, v \in A^{*}$. Hence

$$
\left\langle\Delta^{v} f, u\right\rangle=\Delta^{u}\left(\Delta^{v} f\right)(1)=\Delta^{u v} f(1)=\langle f, u v\rangle
$$

and Theorem 2.3 yields

$$
\begin{equation*}
\left\|\Delta^{v} f\right\|_{p}=\max _{u \in A^{*}}\left|\left\langle\Delta^{v} f, u\right\rangle\right|_{p}=\max _{u \in A^{*}}|\langle f, u v\rangle|_{p} \tag{5.1}
\end{equation*}
$$

Let $\varepsilon>0$. By (3), there exists some $N \in \mathbb{N}$ such that $|\langle f, w\rangle|_{p}<\varepsilon$ whenever $|w| \geqslant N$. Thus, whenever $|v| \geqslant N$, we get $|\langle f, u v\rangle|_{p}<\varepsilon$ and so $\left\|\Delta^{v} f\right\|_{p}<\varepsilon$ by (5.1). Therefore (4) holds.
(4) implies (3) follows immediately from (5.1).
(1) implies (5) since $\widehat{F}_{p}(A)$ (respectively $\mathbb{Z}_{p}$ ) is the completion of $A^{*}$ (respectively $\mathbb{Z}$ ) for $d_{p}$.
(5) implies (1). Since $\widehat{F}_{p}(A)$ is compact, the continuous extension of $f$ to $\widehat{F}_{p}(A)$ is uniformly continuous and its restriction $f$ to $A^{*}$ is uniformly continuous as well.

## 6 The commutative case

A Mahler expansion can also be obtained for functions from $\mathbb{N}^{k}$ into $\mathbb{Z}$. First observe that the family of functions from $\mathbb{N}^{k}$ into $\mathbb{N}$

$$
\left\{\left.\binom{-}{r_{1}}\binom{-}{r_{2}} \cdots\binom{-}{r_{k}} \right\rvert\,\left(r_{1}, \ldots, r_{k}\right) \in \mathbb{N}^{k}\right\}
$$

is locally finite. Thus, given a family $\left(m_{r}\right)_{r \in \mathbb{N}^{k}}$, the formula

$$
f\left(n_{1}, \ldots, n_{k}\right)=\sum_{r \in \mathbb{N}^{k}} m_{r}\binom{n_{1}}{r_{1}} \cdots\binom{n_{k}}{r_{k}}
$$

defines a function $f: \mathbb{N}^{k} \rightarrow \mathbb{Z}$. Conversely, each function from $\mathbb{N}^{k}$ to $\mathbb{Z}$ admits a unique Mahler expansion, a result proved in a more general setting in [2, 1].

Proposition 6.1 Let $f: \mathbb{N}^{k} \rightarrow \mathbb{Z}$ be an arbitrary function. Then there exists a unique family $\langle f, r\rangle_{r \in \mathbb{N}^{k}}$ of integers such that, for all $\left(n_{1}, \ldots, n_{k}\right) \in$ $\mathbb{N}^{k}$,

$$
f\left(n_{1}, \ldots, n_{k}\right)=\sum_{r \in \mathbb{N}^{k}}\langle f, r\rangle\binom{ n_{1}}{r_{1}} \cdots\binom{n_{k}}{r_{k}}
$$

Furthermore, the coefficients are given by

$$
\langle f, r\rangle=\sum_{i_{1}=0}^{r_{1}} \ldots \sum_{i_{k}=0}^{r_{k}}(-1)^{\left(r_{1}+\ldots+r_{k}\right)+\left(i_{1}+\ldots+i_{k}\right)}\binom{r_{1}}{i_{1}} \ldots\binom{r_{k}}{i_{k}} f\left(i_{1}, \ldots, i_{k}\right)
$$

The next lemma relates commutative and noncommutative Mahler expansions. Given a finite alphabet $A$, we denote by $c$ the map from $A^{*}$ to $\mathbb{N}^{|A|}$ which maps every word $u$ onto its commutative image $c(u)=\left(|u|_{a}\right)_{a \in A}$.

Lemma 6.2 Let $\sum_{r \in \mathbb{N}^{k}}\langle f, r\rangle\binom{-}{r_{1}} \cdots\binom{-}{r_{k}}$ be the Mahler expansion of a function $f$ from $\mathbb{N}^{k}$ into $\mathbb{Z}$. Let $A=\left\{a_{1}, \ldots, a_{k}\right\}$ be a $k$-letter alphabet. Then $\langle f, r\rangle=\left\langle f \circ c, a_{1}^{r_{1}} \cdots a_{k}^{r_{k}}\right\rangle$ for every $r \in \mathbb{N}^{k}$.

Proof. One has

$$
\begin{aligned}
f\left(n_{1}, \ldots, n_{k}\right) & =f\left(c\left(a_{1}^{n_{1}} \cdots a_{k}^{n_{k}}\right)\right) \\
& =\sum_{v \in A^{*}}\langle f \circ c, v\rangle\binom{ a_{1}^{n_{1}} \cdots a_{k}^{n_{k}}}{v} \\
& =\sum_{r_{1}=0}^{n_{1}} \ldots \sum_{r_{k}=0}^{n_{k}}\left\langle f \circ c, a_{1}^{r_{1}} \cdots a_{k}^{r_{k}}\right\rangle\binom{ n_{1}}{r_{1}} \cdots\binom{n_{k}}{r_{k}}
\end{aligned}
$$

The uniqueness of the Mahler expansion stated in Proposition 6.1 yields the equality $\langle f, r\rangle=\left\langle f \circ c, a_{1}^{r_{1}} \ldots a_{k}^{r_{k}}\right\rangle$ for every $r \in \mathbb{N}^{k}$.

We can now deduce a new proof for the hard implication of the generalization of Mahler's Theorem to $\mathbb{N}^{k}$ (see [2] or [18, Section 4.2.4]).

Given $r \in \mathbb{N}^{k}$, let us write $|r|$ for $\left|r_{1}\right|+\ldots+\left|r_{k}\right|$.
Corollary 6.3 (Amice [2]) Let $\sum_{r \in \mathbb{N}^{k}}\langle f, r\rangle\binom{-}{r_{1}} \cdots\binom{-}{r_{k}}$ be the Mahler expansion of a function $f$ from $\mathbb{N}^{k}$ into $\mathbb{Z}$. Then $f$ is uniformly continuous for $d_{p}$ if and only if $\lim _{|r| \rightarrow \infty}|\langle f, r\rangle|_{p}=0$.

Proof. Assume that $f$ is uniformly continuous. Let $A=\left\{a_{1}, \ldots, a_{k}\right\}$. Since $c: A^{*} \rightarrow \mathbb{N}^{k}$ is a morphism, it is uniformly continuous by Corollary 1.5 and so is the function $f \circ c$. By Theorem 4.1, we obtain

$$
\lim _{|v| \rightarrow \infty}|\langle f \circ c, v\rangle|_{p}=0
$$

In particular, $\lim _{|r| \rightarrow \infty}\left|\left\langle f \circ c, a_{1}^{r_{1}} \cdots a_{k}^{r_{k}}\right\rangle\right|_{p}=0$ and so $\lim _{|r| \rightarrow \infty}|\langle f, r\rangle|_{p}=0$ by Lemma 6.2.

The opposite implication is the easy one (see [2]) and can be deduced from the fact that if $n_{1} \equiv n_{2}\left(\bmod p^{s+\nu_{p}(m!)}\right)$ then $\binom{n_{1}}{m} \equiv\binom{n_{2}}{m}\left(\bmod p^{s}\right)$. Details are omitted.

## 7 Back to language theory

Our original motivation was the study of regularity-preserving functions $f$ from $A^{*}$ to $B^{*}$, in the following sense: if $L$ is a regular language of $B^{*}$, then $f^{-1}(L)$ is a regular language of $A^{*}$. More generally, we are interested in functions preserving a given variety of languages $\mathcal{V}$ : if $L$ is a language of $\mathcal{V}$, then $f^{-1}(L)$ is also a language of $\mathcal{V}$. There is an important literature on the regular case [20, 6, 19, 12, 13, 14, 3]. A remarkable contribution to this problem can be found in [17], where a characterization of sequential functions preserving star-free languages (respectively group-languages) is given. A similar problem was also recently considered for formal power series [4].

An open problem is to characterize the functions from $A^{*}$ to $B^{*}$ preserving the $p$-group languages. Theorems 1.4 and 5.1 give a solution when $B$ is a one-letter alphabet.

Theorem 7.1 Let $f$ be a function from $A^{*}$ to $\mathbb{N}$. Then the following conditions are equivalent:
(1) for each p-group language $L$ of $\mathbb{N}, f^{-1}(L)$ is a p-group language of $A^{*}$,
(2) $f$ is uniformly continuous for $d_{p}$,
(3) $\lim _{|v| \rightarrow \infty}\left\|\Delta^{v} f\right\|_{p}=0$.

It would be interesting to find a suitable extension of this result for functions from $A^{*}$ to $B^{*}$, for any alphabet $B$. Another challenge would be to extend other results from $p$-adic analysis to the word case.

## Acknowledgement

The authors would like to thank also Daniel Barsky and Gilles Christol for pointing out several references.

## References

[1] R. Ahlswede and R. Bojanic, Approximation of continuous functions in p-adic analysis, J. Approximation Theory 15,3 (1975), 190-205.
[2] Y. Amice, Interpolation p-adique, Bull. Soc. Math. France 92 (1964), 117-180.
[3] J. Berstel, L. Boasson, O. Carton, B. Petazzoni and J.-É. Pin, Operations preserving recognizable languages, Theoret. Comput. Sci. 354 (2006), 405-420.
[4] M. Droste and G.-Q. Zhang, On transformations of formal power series, Inform. and Comput. 184,2 (2003), 369-383.
[5] S. Eilenberg, Automata, Languages and Machines, vol. B, Academic Press, New York, 1976.
[6] S. R. Kosaraju, Regularity preserving functions, SIGACT News 6 (2) (1974), 16-17. Correction 6 (3) (1974), 22.
[7] M. Lothaire, Combinatorics on words, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1997.
[8] K. Mahler, An interpolation series for continuous functions of a $p$ adic variable., J. Reine Angew. Math. 199 (1958), 23-34. Correction 208 (1961), 70-72.
[9] M. R. Murty, Introduction to p-adic analytic number theory, Studies in Advanced Mathematics, American Mathematical Society, Cambridge, 2002.
[10] J.-É. Pin, Finite group topology and $p$-adic topology for free monoids, in 12th ICALP, Berlin, 1985, pp. 445-455, Lect. Notes Comp. Sci. n ${ }^{\circ}$ 194, Springer-Verlag.
[11] J.-É. Pin, Topologie p-adique sur les mots, Journal de théorie des nombres de Bordeaux 5 (1993), 263-281.
[12] J.-É. Pin and J. Sakarovitch, Operations and transductions that preserve rationality, in 6th GI Conference, Berlin, 1983, pp. 617-628, Lect. Notes Comp. Sci. n 145 , Lect. Notes Comp. Sci.
[13] J.-É. Pin and J. Sakarovitch, Une application de la représentation matricielle des transductions, Theoret. Comput. Sci. 35 (1985), 271293.
[14] J.-É. Pin and P. V. Silva, A topological approach to transductions, Theoret. Comput. Sci. 340 (2005), 443-456.
[15] J.-É. Pin and P. V. Silva, A Mahler's theorem for functions from words to integers, in 25th International Symposium on Theoretical Aspects of Computer Science (STACS 2008), S. Albers and P. Weil (eds.), Dagstuhl, Germany, 2008, pp. 585-596, Internationales BegegnungsUnd Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany.
[16] J.-É. Pin and P. V. Silva, On profinite uniform structures defined by varieties of finite monoids, Internat. J. Algebra Comput. 21 (2011), 295-314.
[17] C. Reutenauer and M.-P. Schützenberger, Variétés et fonctions rationnelles, Theoret. Comput. Sci. 145,1-2 (1995), 229-240.
[18] A. M. Robert, A course in p-adic analysis, Graduate Texts in Mathematics vol. 198, Springer-Verlag, New York, 2000.
[19] J. I. Seiferas and R. McNaughton, Regularity-preserving relations, Theoret. Comp. Sci. 2 (1976), 147-154.
[20] R. E. Stearns and J. Hartmanis, Regularity preserving modifications of regular expressions, Information and Control 6 (1963), 55-69.


[^0]:    ${ }^{1}$ Work supported by the project ANR 2010 BLAN 020202 FREC, the European Regional Development Fund through the programme COMPETE and the Portuguese Government through FCT (Fundação para a Ciência e a Tecnologia) under the project PEstC/MAT/UI0144/2011.
    ${ }^{2}$ LIAFA, Université Paris 7 and CNRS, Case 7014, 75205 Paris Cedex 13, France. Jean-Eric.Pin@liafa.jussieu.fr
    ${ }^{3}$ Centro de Matemática, Faculdade de Ciências, Universidade do Porto, R. Campo Alegre 687, 4169-007 Porto, Portugal. pvsilva@fc.up.pt

