Newton's Forward Difference Equation for Functions from Words to Words

Jean-Eric Pin

Newton's Forward Difference Equation for Functions from Words to Words

Jean-Éric Pin[1]

LIAFA, Université Paris-Diderot and CNRS, Case 7014, F-75205 Paris Cedex 13.

Abstract. Newton's forward difference equation 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. An extension of this formula to functions from A^* to $\mathbb{Z}$ was given in 2008 by P. Silva and the author. In this paper, the formula is further extended to functions from A^* into the free group over B.

Let A be a set. In this paper, we denote by A^* the free monoid over A and by $FG(A)$ the free group over A. The empty word, which is the unit of both A^* and $FG(A)$, is denoted by 1.

Original motivation.

The characterization of the regularity-preserving functions is the original motivation of this paper, but since there is a long way to go from this problem to Newton's forward difference equation, it is worth relating the story step by step.

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. Several families of regularity-preserving functions have been identified in the literature [3,8,10,11,12,18,19], but finding a complete description of these functions seems to be currently out of reach. Following a dubious, but routine mathematical practice consisting to offer generalizations rather than solutions to open problems, I proposed a few years ago the following variation: given a class $\mathcal{C}$ of regular languages, characterize the $\mathcal{C}$-preserving functions. Of course, a function f is *$\mathcal{C}$-preserving* if $L \in \mathcal{C}$ implies $f^{-1}(L) \in \mathcal{C}$.

For instance, a description of the sequential functions preserving star-free languages (respectively group-languages) is given in [17]. A similar problem was also recently considered for formal power series [4]. The question is of special interest for varieties of languages. Recall that a *variety of languages* $\mathcal{V}$ associates with each finite alphabet A a set $\mathcal{V}(A^*)$ of regular languages closed under finite Boolean operations and quotients, with the further property that, for each morphism $\varphi : A^* \to B^*$, the condition $L \in \mathcal{V}(B^*)$ implies $\varphi^{-1}(L) \in \mathcal{V}(A^*)$.

Algebra and topology step in.

It is interesting to see how algebra and topology can help characterizing $\mathcal{V}$-preserving functions. Let us start with algebra.

Eilenberg [5] proved that varieties of languages are in bijection with varieties of finite monoids. A *variety of finite monoids* is a class of finite monoids closed under taking submonoids, homomorphic images and finite products. For instance, the variety of all finite monoids corresponds to the variety of regular languages, and the variety of aperiodic finite monoids corresponds to the variety of star-free languages.

Topology is even more relevant to our problem. To each variety of finite monoids $\mathbf{V}$, one can attach a pseudometric $d_{\mathbf{V}}$, (called the *pro-*$\mathbf{V}$ *pseudometric*, see [1,14,16] for more details). Now, if $\mathcal{V}$ is the variety of languages corresponding to $\mathbf{V}$, the following property holds: a function is $\mathcal{V}$-preserving if and only if it is uniformly continuous with respect to $d_{\mathbf{V}}$. This result motivated P. Silva and the author to investigate more closely uniform continuity with respect to various varieties of monoids [14]. Simultaneously, we started to investigate a specific example, the variety $\mathbf{G}_p$ of finite p-groups, where p is a given prime [13,15]. Then the corresponding pseudometric is a metric denoted by d_p.

This case is interesting because there are relevant known results both in algebra and in topology. First, Eilenberg and Schützenberger [5, p. 238] gave a very nice description of the languages recognized by a p-group. Secondly, the free monoid over a one-letter alphabet is isomorphic to $\mathbb{N}$, and the metric d_p is the *p-adic metric*, a well known mathematical object. The completion of the metric space $(\mathbb{N}, d_p)$ is the space of *p-adic numbers*. Thirdly, the uniformly continuous functions from $(\mathbb{N}, d_p)$ to itself are characterized by Mahler's theorem, a celebrated result of number theory. This is the place where *Newton's forward difference equation* is needed.

Newton's forward difference equation.

This result states that for each function $f : \mathbb{N} \to \mathbb{Z}$ and for all $n \in \mathbb{N}$, the following equality holds:

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

where Δ is the *difference operator*, defined by $(\Delta f)(n) = f(n+1) - f(n)$.

Mahler's theorem states that a function $f : \mathbb{N} \to \mathbb{N}$ is uniformly continuous for d_p if and only if $\lim_{k\to\infty} |\Delta^k f(0)|_p = 0$, where $|n|_p$ denotes the *p-adic norm* of n. This gives a complete characterization of the d_p-uniformly continuous functions from a^* to a^*.

An extension of Mahler's theorem to functions from A^* to $\mathbb{N}$ was given in [13,15], giving in turn a complete characterization of the d_p-uniformly continuous functions from A^* to a^*. This result relies on an extension of Newton's forward difference equation which works as follows. For each function $f : A^* \to \mathbb{Z}$ and for all $u \in A^*$, the following equality holds:

$$f(u) = \sum_{v \in A^*} \binom{u}{v} (\Delta^v f)(1) \tag{2}$$

where $\binom{u}{v}$ denotes the binomial coefficient of two words u and v (see [5, p. 253] and [9, Chapter 6]). If $v = a_1 \cdots a_n$, the binomial coefficient of u and v is defined as follows

$$\binom{u}{v} = \big|\{(u_0, \ldots, u_n) \mid u = u_0 a_1 u_1 \ldots a_n u_n\}\big|.$$

The difference operator Δ^w is now defined by induction on the length of the word w by setting $\Delta^1 f = f$ and, for each letter a,

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

In order to further extend Mahler's theorem to functions from A^* to B^* (for arbitrary finite alphabets A and B), one first need to find a Newton's forward difference equation for functions from A^* to $FG(B)$ and this is precisely the objective of this paper. As the reader will see, it is relatively easy to guess the right formula, but the main difficulty is to find the appropriate framework to prove it formally.

The paper is organized as follows. An intuitive approach to the forward difference equation is given in Section 1. The main tools to formalize this intuitive approach are the near rings, introduced in Section 2 and the noncommutative Magnus transformation presented in Section 3. The formal statement and the proof of the forward difference equation are given in Section 4.

1 The difference operator

Let $f : A^* \to FG(B)$ be a function. For each letter a, the difference operator $\Delta^a f$ is the map from A^* to $FG(B)$ defined by

$$(\Delta^a f)(u) = f(u)^{-1} f(ua) \tag{3}$$

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

$$\Delta^{aw} f = \Delta^a(\Delta^w f). \tag{4}$$

One could also make use of Δ^{wa} instead of Δ^{aw} in the induction step, but the result would be the same, in view of the following result:

Proposition 1.1. *The following formulas hold for all $v, w \in A^*$:*

$$\Delta^{vw} f = \Delta^v(\Delta^w f)$$

Proof. By induction on $|v|$. The result is trivial if v is the empty word. If $v = au$ for some letter a, we get $\Delta^{vw} f = \Delta^{auw} f = \Delta^a(\Delta^{uw} f)$. Now by the induction hypothesis, $\Delta^{uw} f = \Delta^u(\Delta^w f)$ and thus $\Delta^{vw} f = \Delta^a(\Delta^u(\Delta^w f)) = \Delta^{au}(\Delta^w f) = \Delta^v(\Delta^w f)$. □

For instance, we get

$$\begin{aligned}
(\Delta^1 f)(u) &= f(u)\\
(\Delta^a f)(u) &= f(u)^{-1} f(ua)\\
(\Delta^{aa} f)(u) &= f(ua)^{-1} f(u) f(ua)^{-1} f(uaa)\\
(\Delta^{baa} f)(u) &= f(uaa)^{-1} f(ua) f(u)^{-1} f(ua) f(uba)^{-1} f(ub) f(uba)^{-1} f(ubaa)\\
(\Delta^{abaa} f)(u) &= f(ubaa)^{-1} f(uba) f(ub)^{-1} f(uba) f(ua)^{-1} f(u) f(ua)^{-1} f(uaa)\\
&\quad f(uaaa)^{-1} f(uaa) f(ua)^{-1} f(uaa) f(uaba)^{-1} f(uab) f(uaba)^{-1}\\
&\quad f(uabaa)
\end{aligned}$$

A forward difference equation should express f in terms of the values of $(\Delta^w f)(1)$, for all words w. To simplify notation, let us set, for all $w \in A^*$:

$$\Delta^w = (\Delta^w f)(1)$$

A little bit of computation leads to the formulas

$$\begin{aligned}
f(1) &= \Delta^1 & & \\
f(a) &= \Delta^1 \Delta^a & f(b) &= \Delta^1 \Delta^b\\
f(ab) &= \Delta^1 \Delta^a \Delta^b \Delta^{ab} & f(ba) &= \Delta^1 \Delta^b \Delta^a \Delta^{ba}\\
f(bab) &= \Delta^1 \Delta^b \Delta^a \Delta^{ba} \Delta^b \Delta^{bb} \Delta^{ab} \Delta^{bab} & f(aba) &= \Delta^1 \Delta^a \Delta^b \Delta^{ab} \Delta^a \Delta^{aa} \Delta^{ba} \Delta^{aba}
\end{aligned}$$

which give indeed a forward difference equation for $f(w)$ for a few values of w. But how to find a closed formula valid for all values of w? To do so, acting as a physicist, we will generate some formulas without worrying too much about correctness. Then we will describe a rigorous formalism to justify our equations.

As a first step, our exponential notation suggests to write Δ^{u+v} for $\Delta^u \Delta^v$, which gives

$$\begin{aligned}
f(1) &= \Delta^1 & & \\
f(a) &= \Delta^{1+a} & f(b) &= \Delta^{1+b}\\
f(ab) &= \Delta^{1+a+b+ab} & f(ba) &= \Delta^{1+b+a+ba}\\
f(bab) &= \Delta^{1+b+a+ba+b+bb+ab+bab} & f(aba) &= \Delta^{1+a+b+ab+a+aa+ba+aba}
\end{aligned}$$

The next step is to observe that, in an appropriate noncommutative setting, one can write

$$\left.\begin{aligned}
(1+a)(1+b) &= 1+a+b+ab\\
(1+b)(1+a) &= 1+b+a+ba\\
(1+b)(1+a)(1+b) &= 1+b+a+ba+b+bb+ab+bab\\
(1+a)(1+b)(1+a) &= 1+a+b+ab+a+aa+ba+aba
\end{aligned}\right\} \qquad (5)$$

which gives for instance the noncommutative difference equations

$$f(aba) = \Delta^{(1+a)(1+b)(1+a)} \quad \text{and} \quad f(bab) = \Delta^{(1+b)(1+a)(1+b)}$$

It is now easy to guess a similar equation for $f(u)$, for any word u...

But it is time to tighten the bolts and justify our adventurous notation. A little bit of algebra is in order to give grounds to the foregoing formulas. Let us start by introducing the relatively little-known notion of a near-ring.

2 Near-rings

A (left) *near-ring* (with unit) is an algebraic structure K equipped with two binary operations, denoted additively and multiplicatively, and two elements 0 and 1, satisfying the following conditions:

(1) K is a group (not necessarily commutative) with identity 0 under addition,

(2) K is a monoid with identity 1 under multiplication,

(3) multiplication distributes on the left over addition: for all $x, y, z \in K$, $z(x + y) = zx + zy$.

An element of z of K is *distributive* if, for all $x, y \in K$, $(x + y)z = xz + yz$.

It follows from the axioms that $x0 = 0$ and $x(-y) = -xy$ for all $x, y \in K$. However, it is not necessarily true that $0x = 0$ and $(-x)y = -xy$. It is even possible that $(-1)x$ is not equal to $-x$.

A well-known example of near-ring is the set of all transformations on a group G, equipped with pointwise addition as addition and composition as product.

Let us now survey a construction first introduced by Fröhlich [6,7]. We follow the presentation of Banaschewski and Nelson [2]. Let M be a monoid. We want to construct a near-ring $FG[M]$ in which the additive group is the free group $FG(M)$ on the set M and the multiplication extends the operation on M. This leads us to denote the operation on M multiplicatively and to use an additive notation for the free group[1].

Let us consider terms of the form

$$\varepsilon_1 u_1 + \cdots + \varepsilon_k u_k$$

with $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, +1\}$ and $u_1, \ldots, u_k \in M$. A term is *reduced* if it does not contain any subterms of the form $u + -u$ or $-u + u$. The *reduction* of a term is obtained by iteratively ruling out the subterms of the form $u + -u$ or $-u + u$ until the term is reduced. One can show that these operations can be done in any order and lead to the same reduced term.

The elements of $FG[M]$ can be represented by reduced terms. The sum of two elements $\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r$ and $\varepsilon_1 v_1 + \cdots + \varepsilon_s v_s$ is obtained by reducing the term

$$\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r + \varepsilon_1 v_1 + \cdots + \varepsilon_s v_s$$

The empty term (corresponding to the case $k = 0$) is the identity for this addition and is simply denoted by 0. The inverse of $\varepsilon_1 u_1 + \cdots + \varepsilon_k u_k$ is $-\varepsilon_k u_k + \cdots + -\varepsilon_1 u_1$.

We now define a multiplication on $FG[M]$ in two steps. First, given an element $\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r$ of $FG[M]$ and $m \in M$, we set

$$(\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)m = (\varepsilon_1 u_1 m + \cdots + \varepsilon_r u_r m)$$
$$(\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)(-m) = (-\varepsilon_r u_r m + \cdots + -\varepsilon_1 u_1 m)$$

[1] Therefore, the notation $FG(M)$ and $FG[M]$ refer to the same set, but to different structures: the free group on M in the first case, the free near semiring on M in the latter case.

Now, the product of two elements $\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r$ and $\varepsilon'_1 u'_1 + \cdots + \varepsilon_s u'_s$ of $FG[M]$ is defined by

$$\begin{aligned}(\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)(\varepsilon_1 u'_1 + \cdots + \varepsilon_s u'_s) &= (\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)(\varepsilon'_1 u'_1) \\ &+ (\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)(\varepsilon'_2 u'_2) + \cdots + (\varepsilon_1 u_1 + \cdots + \varepsilon_r u_r)(\varepsilon'_s u'_s)\end{aligned} \tag{6}$$

This operation defines a multiplication on $FG[M]$. Together with the addition, $FG[M]$ is now equipped with a structure of near-ring.

Since $(u)(v) = (uv)$, the monoid M embeds into the multiplicative monoid $FG[M]$ and it is convenient to simplify the notation (u) to u. With this convention, the identity of the multiplication of $FG[M]$ is denoted by 1. Furthermore an element $(u_1, \ldots, u_r)$ can be written as $u_1 + \cdots + u_r$ and thus (6) is a consequence of the following natural formulas, where $u_1, \ldots, u_r, v_1, \ldots, v_s, v \in M$ and $w \in FG[M]$:

$$(u_1 + \cdots + u_r)v = u_1 v + \cdots + u_r v \tag{7}$$

$$w(v_1 + \cdots + v_s) = wv_1 + \cdots + wv_s \tag{8}$$

The near-ring $FG[M]$ has the further convenient property that 0 is distributive in $FG[M]$ since $0x = 0$ by definition. Moreover, the equality $(-x)y = -xy$ holds if $y \in M$ but is not necessarily true otherwise. Even the relation $(-1)y = -y$ may fail if y is not an element of M. For instance, if M is the free monoid $\{a, b\}^*$, then $(-1)(a + b) = -a - b$ but $-(a + b) = -b - a$.

Note that if M is the trivial monoid, then $FG[M]$ is isomorphic to the ring $\mathbb{Z}$ of integers. In the sequel, M will be the free monoid A^*.

3 Noncommutative Magnus transformation

Our goal in this section is to justify and to extend the equations (5). As explained in Section 2, we view $FG[A^*]$ as a near-ring.

3.1 Definition of the Magnus transformation

The monoid morphism μ from A^* into the multiplicative monoid $FG[A^*]$ defined, for each letter $a \in A$, by

$$\mu(a) = 1 + a$$

is called the *Magnus transformation*. It extends uniquely to a group morphism from $FG(A^*)$ to the additive group $FG[A^*]$. For instance, if $A = \{a, b\}$, we get

$$\begin{aligned}\mu(1) &= 1 \qquad \mu(a) = 1 + a \qquad \mu(b) = 1 + b \\ \mu(ab) &= 1 + a + b + ab \qquad \mu(1 + a) = 1 + 1 + a \\ \mu(-1 + a - ab) &= -1 + 1 + a - ab - b - a - 1 = a - ab - b - a - 1 \\ \mu(aba) &= 1 + a + b + ab + a + aa + ba + aba\end{aligned}$$

More generally, for each $u \in A^*$,

$$\mu(au) = \mu(a)\mu(u) = (1 + a)\mu(u) = \mu(u) + a\mu(u)$$

Proposition 3.1. *The following formula holds for all $u \in FG[A^*]$ and $v \in A^*$:*

$$\mu(uv) = \mu(u)\mu(v) \tag{9}$$

Proof. Since μ is a monoid morphism μ from A^* into the multiplicative monoid $FG[A^*]$, (9) holds if $u \in A^*$. Next, if $u = \varepsilon_1 u_1 + \cdots + \varepsilon_k u_k$, with $u_1, \ldots, u_k \in A^*$ and $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$, then $uv = \varepsilon_1 u_1 v + \cdots + \varepsilon_k u_k v$ and hence $\mu(uv) = \varepsilon_1 \mu(u_1)\mu(v) + \cdots + \varepsilon_k \mu(u_k)\mu(v) = \mu(u)\mu(v)$. This proves (9). □

However, μ is not a monoid morphism for the multiplicative structure of $FG[A^*]$, since, for instance, $\mu((1+a)(1+b)) \neq \mu(1+a)\mu(1+b)$.

3.2 The inverse of the Magnus transformation

Let π be the monoid morphism from A^* into the multiplicative monoid $FG[A^*]$ defined, for each letter $a \in A$, by

$$\pi(a) = -1 + a$$

Then π has a unique extension to a group morphism from $FG[A^*]$ into itself and enjoys properties similar to those of μ. Just like μ, π is not a monoid morphism for the multiplicative structure of $FG[A^*]$, but a result analoguous to Proposition 3.1 also holds for π.

Proposition 3.2. *The following formula holds for all $u \in FG[A^*]$ and $v \in A^*$:*

$$\pi(uv) = \pi(u)\pi(v) \tag{10}$$

For instance

$$\begin{aligned}
\pi(aba) = {} & -ab + b - 1 + a - aa + a - ba + aba \\
\pi(abaa) = {} & -aba + ba - a + aa - a + 1 - b + ab - aba + ba - a + aa \\
& - aaa + aa - baa + abaa \\
\pi(abab) = {} & -aba + ba - a + aa - a + 1 - b + ab - abb + bb - b + ab \\
& - aab + ab - bab + abab
\end{aligned}$$

Observe that, for each letter $a \in A$,

$$\mu(\pi(a)) = \mu(-1 + a) = \mu(-1) + \mu(a) = -1 + (1 + a) = a \tag{11}$$

$$\pi(\mu(a)) = \pi(1 + a) = \pi(1) + \pi(a) = 1 + (-1 + a) = a \tag{12}$$

It is tempting to conclude from these equalities that π is the inverse of μ, but the right answer is slightly more involved.

The *reversal* of a word $u = a_1 \cdots a_n$ is the word $\overline{u} = a_n \cdots a_1$. The reversal map is a permutation on A^* which extends by linearity to a group automorphism of the free group $FG[A^*]$.

Proposition 3.3. *The following relations hold for all $u, v \in A^*$,*

$$\mu(v\overline{\pi(\overline{u})}) = \mu(v)u \tag{13}$$

$$\overline{\pi(\overline{\mu(u)}v)} = u\overline{\pi(\overline{v})} \tag{14}$$

Proof. We prove (13) (for all $v \in A^*$) by induction on the length of u. The result is trivial if u is the empty word. Suppose that $u = aw$ for some letter a. Observing that $\overline{u} = \overline{w}a$, we get

$$\pi(\overline{u}) = \pi(\overline{w})\pi(a) = \pi(\overline{w})(-1 + a) = -\pi(\overline{w}) + \pi(\overline{w})a$$

whence

$$\overline{\pi(\overline{u})} = -\overline{\pi(\overline{w})} + a\overline{\pi(\overline{w})}$$

and

$$v\overline{\pi(\overline{u})} = -v\overline{\pi(\overline{w})} + va\overline{\pi(\overline{w})}$$

Applying the induction hypothesis to w, we obtain

$$\begin{aligned}\mu(v\overline{\pi(\overline{u})}) &= -\mu(v\overline{\pi(\overline{w})}) + \mu(va\overline{\pi(\overline{w})}) = -\mu(v)w + \mu(va)w \\ &= -\mu(v)w + \mu(v)\mu(a)w = (-\mu(v) + \mu(v)(1 + a))w \\ &= \mu(v)aw = \mu(v)u\end{aligned}$$

which proves (13).

We also prove (14) by induction on the length of u. The result is trivial if u is the empty word. Suppose that $u = wa$ for some letter a. We get

$$\mu(u) = \mu(wa) = \mu(w)\mu(a) = \mu(w) + \mu(w)a$$

whence

$$\overline{\mu(u)v} = \overline{\mu(w)v} + \overline{\mu(w)av}$$

and

$$\overline{\pi(\overline{\mu(u)}v)} = \overline{\pi(\overline{\mu(w)}v)} + \overline{\pi(\overline{\mu(w)}av)}$$

Applying the induction hypothesis to w, we obtain

$$\overline{\pi(\overline{\mu(u)}v)} = w\overline{\pi(\overline{v})} + w\overline{\pi(\overline{av})} = w(\overline{\pi(\overline{v})} + \overline{\pi(\overline{av})})$$

Now, since $\overline{av} = \overline{v}a$, one gets $\pi(\overline{av}) = \pi(\overline{v})\pi(a)$ and hence

$$\begin{aligned}\overline{\pi(\overline{v})} + \overline{\pi(\overline{av})} &= \overline{\pi(\overline{v})} + \overline{\pi(\overline{v})\pi(a)} = \overline{\pi(\overline{v})} + \overline{\pi(\overline{v})(-1 + a)} \\ &= \overline{\pi(\overline{v})a} = a\overline{\pi(\overline{v})}\end{aligned}$$

and finally

$$\overline{\pi(\overline{\mu(u)}v)} = wa\overline{\pi(\overline{v})} = u\overline{\pi(\overline{v})}$$

which proves (14). □

Corollary 3.4. *The function $\mu : FG[A^*] \to FG[A^*]$ is a bijection and its inverse is defined by*

$$\mu^{-1}(u) = \overline{\pi(\overline{u})} \tag{15}$$

Proof. Taking $v = 1$ in (13) and (14) shows that for all $u \in A^*$, $\mu(\overline{\pi(\overline{u})}) = u$ and $\overline{\pi(\overline{\mu(u)})} = u$. The result follows since μ, π and the maps $u \to \overline{\mu(\overline{u})}$ and $u \to \overline{\pi(\overline{u})}$ are group morphisms. □

4 Forward difference equation

Let $\mathcal{F}$ be the set of all functions from A^* into $FG(B)$. Then $\mathcal{F}$ is a group under pointwise multiplication defined by setting

$$(fg)(x) = f(x)g(x)$$

whose identity is the constant map onto the identity of $FG(B)$. Furthermore, the inverse of f in this group is given by the formula

$$f^{-1}(x) = (f(x))^{-1}$$

The map $(u, f) \to \Delta^u f$ from $A^* \times \mathcal{F}$ to $\mathcal{F}$ defines a left action of A^* on $\mathcal{F}$, since $\Delta^1 f = f$ and, by Proposition 1.1, $\Delta^{uv} f = \Delta^u(\Delta^v f)$ for all $u, v \in A^*$.

This action can be extended by linearity to a map from $FG[A^*] \times \mathcal{F}$ to $\mathcal{F}$ as follows: for each element $u = \varepsilon_1 u_1 + \cdots + \varepsilon_k u_k$ of $FG[A^*]$, we define the function $\Delta^u f$ by

$$(\Delta^u f) = (\Delta^{u_1} f)^{\varepsilon_1} \cdots (\Delta^{u_k} f)^{\varepsilon_k}$$

In particular, $\Delta^0 f$ is the constant map onto the identity of $FG(B)$ and $\Delta^1 f = f$.

We are interested in the coefficients $(\Delta^u f)(1)$. To simplify notation, we introduce the following short forms, for all $u, v \in FG[A^*]$:

$$\Delta^u = (\Delta^u f)(1) \qquad \Delta^u \cdot v = (\Delta^u f)(v)$$

The next proposition gives some useful relations between these coefficients.

Proposition 4.1. *The following formulas hold for all $u, v \in A^*$ and $a \in A$:*

$$(\Delta^u \cdot v)(\Delta^{au} \cdot v) = \Delta^u \cdot va \tag{16}$$

$$\Delta^{\mu(vu)} = \Delta^{\mu(u)} \cdot v \tag{17}$$

Proof. By definition, $\Delta^u \cdot v = (\Delta^u f)(v)$ and thus we get

$$\Delta^{au} \cdot v = (\Delta^{au} f)(v) = (\Delta^a(\Delta^u f))(v) = \\ = \big((\Delta^u f)(v)\big)^{-1}(\Delta^u f)(va) = (\Delta^u \cdot v)^{-1}\Delta^u \cdot va$$

from which (16) follows immediately.

By induction, it suffices to establish (17) for $v = a$. If $\mu(u) = u_1 + \cdots + u_k$, then by Proposition 3.2, $\mu(au) = \mu(a)\mu(u) = u_1 + au_1 + \cdots + u_k + au_k$. Now, (16) shows that for $1 \leqslant i \leqslant k$, $(\Delta^{u_i}\Delta^{au_i}) = \Delta^{u_i} \cdot a$. It follows that

$$\Delta^{\mu(au)} = (\Delta^{u_1}\Delta^{au_1}) \cdots (\Delta^{u_k}\Delta^{au_k}) = (\Delta^{u_1} \cdot a) \cdots (\Delta^{u_k} \cdot a) = \Delta^{\mu(u)} \cdot a$$

which concludes the proof. □

Proposition 4.2. *The following formulas hold for all $u, v \in A^*$:*

$$f(vu) = (\Delta^{\mu(u)} f)(v) \tag{18}$$

$$f(u) = \Delta^{\mu(u)} \tag{19}$$

Proof. Applying (17) with $u = 1$, we get $\Delta^{\mu(v)} = \Delta^{\mu(1)} \cdot v = f(v)$ which gives (19). It follows that $f(vu) = \Delta^{\mu(vu)}$. Now by (17) we also have $\Delta^{\mu(vu)} = (\Delta^{\mu(u)} f)(v)$, which yields (18). □

4.1 Difference expansion

The formula $f(u) = \Delta^{\mu(u)}$ gives a representation of $f(u)$ as a product of elements of the form Δ^v. This expression is called the *difference expansion* of f. For instance we have

$$f(abaa) = \Delta^1\Delta^a\Delta^b\Delta^{ab}\Delta^a\Delta^{aa}\Delta^{ba}\Delta^{aba}\Delta^a\Delta^{aa}\Delta^{ba}\Delta^{aba}\Delta^{aa}\Delta^{aaa}\Delta^{baa}\Delta^{abaa}$$

We now show that this decomposition is unique in a sense that we now make precise.

Let $(c_u)_{u \in A^*}$ be a family of elements of $FG(B)$. The map $u \mapsto c_u$ extends uniquely to a group morphism from $FG[A^*]$ to $FG(B)$. In particular, for each element $\varepsilon_1 u_1 + \cdots + \varepsilon_k u_k$ in $FG[A^*]$, we set

$$c_{\varepsilon_1 u_1 + \cdots + \varepsilon_k u_k} = c_{u_1}^{\varepsilon_1} \cdots c_{u_k}^{\varepsilon_k}$$

We can now state:

Theorem 4.3. *Let f be a function from A^* to $FG(B)$. There is a unique family $(c_u)_{u \in A^*}$ of elements of $FG(B)$ such that, for all $u \in A^*$, $f(u) = c_{\mu(u)}$. This family is given by $c_u = (\Delta^u f)(1)$.*

Proof. The existence follows from (19). Unicity can be proved by induction on the length of u. Necessarily, $c_1 = f(1) = \Delta^1(f)(1)$. Suppose that the coefficients c_u are known to be uniquely determined for $|u| \leqslant n$. Let u be a word of length n and let a be a letter. Then $\mu(u) = u_1 + \cdots + u_{k-1} + u$, where the words $u_1, \ldots, u_{k-1}$ are shorter than u. Furthermore

$$\mu(ua) = u_1 + \cdots + u_{k-1} + u + u_1 a + \cdots + u_{k-1} a + ua$$

where again, ua is the only word of length $n+1$. The condition $f(ua) = c_{\mu(ua)}$ now gives

$$f(ua) = c_{u_1} \cdots c_{u_{k-1}} c_u c_{u_1 a} \cdots c_{u_{k-1} a} c_{ua}$$

It follows than c_{ua} is necessarily equal to

$$f(ua)(c_{u_1} \cdots c_{u_{k-1}} c_u c_{u_1 a} \cdots c_{u_{k-1} a})^{-1}$$

which proves unicity. □

It is a well-known fact that every sequence of real numbers can appear as coefficients of the Maclaurin series of a smooth function. The following corollary can be viewed as a discrete, non-commutative analogue of this result.

Corollary 4.4. *Given, for each $u \in A^*$, an element c_u of $FG(B)$, there exists a unique function $f : A^* \to FG(B)$ such that, for all $u \in A^*$, $\Delta^u f = c_u$. This function is defined by $f(u) = c_{\mu(u)}$ for all $u \in A^*$.*

Corollary 4.4 can also be interpreted as an answer to the following interpolation problem: determine f knowing the coefficients $\Delta^u f$ for all $u \in A^*$.

4.2 The inversion formula

The definition of $\Delta^u f$ was given by induction on the length of u. To conclude this article, we give a close formula that allows one to compute $\Delta^u f$ directly.

Let $f : A^* \to FG(B)$ be a function. Then f can be extended by linearity into a group morphism from $FG[A^*]$ to $FG(B)$.

Proposition 4.5. *The following formula holds for all u in A^* and v in A^*:*

$$\Delta^u f(v) = f(v\overline{\pi(\overline{u})}) \tag{20}$$

Proof. Substituting $\overline{\pi(\overline{u})}$ for u in (18) and using (13) we get

$$f(v\overline{\pi(\overline{u})}) = \Delta^{\mu(\overline{\pi(\overline{u})})} f(v) = \Delta^u f(v)$$

which gives the result. □

Corollary 4.6. *The following formula holds for all $u \in FG[A^*]$*

$$\Delta^u f = f(\overline{\pi(\overline{u})}) = f(\mu^{-1}(u)) \tag{21}$$

Example 4.7. For instance, for $u = abb$, we get $\overline{u} = bba$ and

$$\begin{aligned}
\pi(\overline{u}) = \pi(bba) &= (-1+b)(-1+b)(-1+a) = (-b+1-b+bb)(-1+a) \\
&= -bb+b-1+b-ba+a-ba+bba \\
\overline{\pi(\overline{u})} &= -bb+b-1+b-ab+a-ab+abb \\
\Delta^{abb} &= -f(bb)+f(b)-f(1)+f(b)-f(ab)+f(a)-f(ab)+f(abb)
\end{aligned}$$

Acknowlegements

I would like to thank the anonymous referees for their valuable comments.

References

1. Almeida, J.: Finite semigroups and universal algebra. World Scientific Publishing Co. Inc., River Edge, NJ (1994), translated from the 1992 Portuguese original and revised by the author
2. Banaschewski, B., Nelson, E.: On the non-existence of injective near-ring modules. Canad. Math. Bull. 20(1), 17–23 (1977)
3. Berstel, J., Boasson, L., Carton, O., Petazzoni, B., Pin, J.É.: Operations preserving recognizable languages. Theoret. Comput. Sci. 354, 405–420 (2006)
4. Droste, M., Zhang, G.Q.: On transformations of formal power series. Inform. and Comput. 184(2), 369–383 (2003)
5. Eilenberg, S.: Automata, Languages and Machines, vol. B. Academic Press, New York (1976)
6. Fröhlich, A.: On groups over a d.g. near-ring. I. Sum constructions and free R-groups. Quart. J. Math. Oxford Ser. (2) 11, 193–210 (1960)
7. Fröhlich, A.: On groups over a d.g. near-ring. II. Categories and functors. Quart. J. Math. Oxford Ser. (2) 11, 211–228 (1960)
8. Kosaraju, S.R.: Regularity preserving functions. SIGACT News 6 (2), 16–17 (1974)
9. Lothaire, M.: Combinatorics on words. Cambridge Mathematical Library, Cambridge University Press, Cambridge (1997)
10. Pin, J.É., Sakarovitch, J.: Operations and transductions that preserve rationality. In: 6th GI Conference. pp. 617–628. No. 145 in Lect. Notes Comp. Sci., Lect. Notes Comp. Sci., Berlin (1983)
11. Pin, J.É., Sakarovitch, J.: Une application de la représentation matricielle des transductions. Theoret. Comput. Sci. 35, 271–293 (1985)
12. Pin, J.É., Silva, P.V.: A topological approach to transductions. Theoret. Comput. Sci. 340, 443–456 (2005)
13. Pin, J.É., Silva, P.V.: A Mahler's theorem for functions from words to integers. In: Albers, S., Weil, P. (eds.) 25th International Symposium on Theoretical Aspects of Computer Science (STACS 2008). pp. 585–596. Internationales Begegnungs- Und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, Dagstuhl, Germany (2008)
14. Pin, J.É., Silva, P.V.: On profinite uniform structures defined by varieties of finite monoids. Internat. J. Algebra Comput. 21, 295–314 (2011)
15. Pin, J.É., Silva, P.V.: A noncommutative extension of Mahler's theorem on interpolation series. European J. Combin. 36, 564–578 (2014)
16. Pin, J.É., Weil, P.: Uniformities on free semigroups. International Journal of Algebra and Computation 9, 431–453 (1999)
17. Reutenauer, C., Schützenberger, M.P.: Variétés et fonctions rationnelles. Theoret. Comput. Sci. 145(1-2), 229–240 (1995)
18. Seiferas, J.I., McNaughton, R.: Regularity-preserving relations. Theoret. Comp. Sci. 2, 147–154 (1976)
19. Stearns, R.E., Hartmanis, J.: Regularity preserving modifications of regular expressions. Information and Control 6, 55–69 (1963)