On exponentials of exponential generating series

Roland Bacher

On exponentials of exponential generating series

Roland Bacher

July 3, 2008

Abstract[1]*: Identifying the algebra of exponential generating series with the shuffle algebra of formal power series, one can define an exponential map* $exp_!: X\mathbb{K}[[X]] \longrightarrow 1 + X\mathbb{K}[[X]]$ *for the associated Lie group formed by exponential generating series with constant coefficient* 1 *over an arbitrary field* $\mathbb{K}$*. The main result of this paper states that the map* $exp_!$ *(and its inverse map* $log_!$*) induces a bijection between rational, respectively algebraic, series in* $X\mathbb{K}[[X]]$ *and* $1 + X\mathbb{K}[[X]]$ *if the field* $\mathbb{K}$ *is a subfield of the algebraically closed field* $\overline{\mathbb{F}}_p$ *of characteristic* p*.*

1 Introduction

The equality

$$\left(\sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!}\right)\left(\sum_{n=0}^{\infty} \beta_n \frac{X^n}{n!}\right) = \sum_{n=0}^{\infty}\sum_{m=0}^{n} \binom{n+m}{n} \alpha_n\beta_m \frac{X^{n+m}}{(n+m)!}$$

shows that we can define an algebra structure on the vector space

$$\mathcal{E}(\mathbb{K}) = \{\sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!} \mid \alpha_0, \alpha_1, \cdots \in \mathbb{K}\}$$

of exponential generating series with coefficients $\alpha_0, \alpha_1, \ldots$ in an arbitrary field or ring $\mathbb{K}$. For the sake of simplicity we work in the sequel only over fields. The expression $\alpha_n/n!$ should be considered formally since the numerical value of $n!$ is zero over a field of positive characteristic $p \leq n$.

We denote by

$$\mathfrak{m}_{\mathcal{E}} = \{\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!} \mid \alpha_1, \alpha_2, \cdots \in \mathbb{K}\} \subset \mathcal{E}(\mathbb{K})$$

the maximal ideal of the local algebra $\mathcal{E}(\mathbb{K})$. A straightforward computation shows that $a^n/n!$ is well-defined for $a \in \mathfrak{m}_{\mathcal{E}}$ over an arbitrary field.

[1]Keywords: Bell numbers, exponential function, shuffle product, formal power series, rational series, algebraic series, homogeneous form, automaton sequence, Math. class: 11B73, 11B85, 11E08, 11E76, 22E65

Endowing $\mathbb{K}$ with the discrete topology and $\mathcal{E}(\mathbb{K})$ with the topology given by coefficientwise convergency, the functions

$$exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!} \text{ and } log(1+a) = -\sum_{n=1}^{\infty} \frac{(-a)^n}{n}$$

are always defined for $a \in \mathfrak{m}_{\mathcal{E}}$.

Switching back to ordinary generating series

$$A = \sum_{n=1}^{\infty} \alpha_n X^n,\ B = \sum_{n=1}^{\infty} \beta_n X^n \in \mathfrak{m}$$

contained in the maximal ideal $\mathfrak{m} = X\mathbb{K}[[X]]$, of (ordinary) formal power series, we write

$$exp_!(A) = 1 + B$$

if

$$exp\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = 1 + \sum_{n=1}^{\infty} \beta_n \frac{X^n}{n!}\ .$$

It is easy to see that $exp_!$ defines a one-to-one map from $\mathfrak{m}$ onto $1+\mathfrak{m}$ with inverse map

$$1 + B \longmapsto A = log_!(1+B)\ .$$

It satisfies

$$exp_!(A+B) = exp_!(A) \sqcup\!\sqcup exp_!(B)$$

for all $A, B \in \mathfrak{m}$ where the shuffle product

$$\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) \sqcup\!\sqcup \left(\sum_{n=0}^{\infty} \beta_n X^n\right) = \sum_{n,m=0}^{\infty} \binom{n+m}{n} \alpha_n \beta_m X^{n+m}$$

corresponds to the ordinary product of the associated exponential generating series. The map $exp_!$ defines thus an isomorphism from the additive group $(\mathfrak{m}, +)$ onto the *special shuffle-group* $(1+\mathfrak{m},\ \sqcup\!\sqcup\ )$ with group-law given by the shuffle-product. It coincides with the familiar exponential map from the Lie algebra $\mathfrak{m}$ into the special shuffle group, considered as an infinite-dimensional Lie group.

Theorem 1.1. *Let $\mathbb{K}$ be a subfield of the algebraically closed field $\overline{\mathbb{F}}_p$ of positive characteristic p. Given a series $A \in \mathfrak{m} = X\mathbb{K}[[X]]$ the following two assertions are equivalent:*

(i) A is rational.

(ii) $exp_!(A)$ is rational.

Example 1.2. *The Bell numbers $B_0, B_1, B_2, \ldots$, see pages 45,46 in [5] or Example 5.2.4 in [6], are the natural integers defined by*

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}$$

and have combinatorial interpretations.

Reducing the associated ordinary generating series $\sum_{n=0}^{\infty} B_n x^n = exp_!(x/(1-x))$ modulo a prime p defines the series expansion of a rational fraction. A few reductions of the ordinary generating series

$$\sum_{n=0}^{\infty} B_n x^n = 1 + x + 2x^2 + 5x^3 + 15x^4 + 52x^5 + 203x^6 + 877x^7 + 4140x^8 + \ldots$$

of Bell numbers modulo small primes are

$$\frac{1}{1+x+x^2} \pmod 2, \ \frac{1+x+x^2}{1-x^2-x^3} \pmod 3, \ \frac{1+x+2x^2-x^4}{1-x^4-x^5} \pmod 5 .$$

Theorem 1.3. *Let $\mathbb{K}$ be a subfield of the algebraically closed field $\overline{\mathbb{F}}_p$ of positive characteristic p. Given a series $A \in \mathfrak{m} = X\mathbb{K}[[X]]$ the following two assertions are equivalent:*

(i) A is algebraic.

(ii) $exp_!(A)$ is algebraic.

Corollary 1.4. *Over a subfield $\mathbb{K} \subset \overline{\mathbb{F}}_p$, the group isomorphism*

$$exp_! : (\mathfrak{m}, +) \longrightarrow (1 + \mathfrak{m}, \ \sqcup\!\sqcup \ )$$

restricts to an ismorphism between the subgroups of rational elements in $(\mathfrak{m}, +)$ and in $(1 + \mathfrak{m}, \ \sqcup\!\sqcup \ )$.

It restricts also to an isomorphism between the subgroups of algebraic elements in $(\mathfrak{m}, +)$ and in $(1 + \mathfrak{m}, \ \sqcup\!\sqcup \ )$.

Theorem 1.1 and 1.3 can be made effective:

Given a rational series $A \in \mathbb{K}[[X]]$ represented by a reduced fraction f/g where f, g with $g \neq 0$ are two coprime polynomials of degree $\deg(f)$ and $\deg(g)$, we set $\parallel A \parallel = \max(1 + \deg(f), \deg(g))$.

Theorem 1.5. *We have*

$$\parallel exp_!(A) \parallel \leq p^{q^{\parallel A \parallel}} \ \text{ and } \ \parallel log_!(1 + A) \parallel \leq 1 + \parallel 1 + A \parallel^p$$

for a rational series A in $\mathfrak{m} \subset \overline{\mathbb{F}}_p[[X]]$ having all its coefficients in a finite subfield $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing $q = p^e$ elements.

Given a prime p and a formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ in $\mathbb{K}_p[[X]]$ with coefficients in a subfield $\mathbb{K}$ of $\overline{\mathbb{F}}_p$, we define for $f \in \mathbb{N},\ k \in \mathbb{N},\ k < p^f$ the series

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n \ .$$

We denote by $\kappa(C)$ the dimension $\dim(\sum_{k,f} \mathbb{K} C_{k,f}) \in \mathbb{N} \cup \{\infty\}$ of the vector space spanned by all series of the form $C_{k,f}$.

Algebraic series in $\mathbb{K}[[X]]$ for $\mathbb{K}$ a subfield of $\overline{\mathbb{F}}_p$ are characterised by a Theorem of Christol (see Theorem 12.2.5 in [1]) stating that a series C in $\overline{\mathbb{F}}_p[[X]]$ is algebraic if and only if $\kappa(C)$ is finite. We have $\kappa(A+B) \leq \kappa(A) + \kappa(B)$ and an algebraic series $A \in \overline{\mathbb{F}}_p[[X]]$ has a minimal polynomial of degree at most $p^{\kappa(A)}$ with respect to A.

Theorem 1.6. *We have*

$$\kappa(exp_!(A)) \leq q^{\kappa(A)} p^{q^{\kappa(A)}} \text{ and } \kappa(log_!(1+A)) \leq 1 + 4(\kappa(1+A))^p$$

for an algebraic series A in $\mathfrak{m} \subset \overline{\mathbb{F}}_p[[X]]$ having all its coefficients in a finite subfield $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing $q = p^e$ elements.

A map $\mu : \mathcal{V} \longrightarrow \mathcal{W}$ between two $\mathbb{K}-$vector spaces is a homogeneous form of degree d if $l \circ \mu : \mathcal{V} \longrightarrow \mathbb{K}$ is homogeneous of degree d for every linear form $l : \mathcal{W} \longrightarrow \mathbb{K}$.

A useful ingredient for proving Theorems 1.1, 1.3 and their effective versions is the following characterisation of $log_!$:

Proposition 1.7. *Over a field $\mathbb{K} \subset \overline{\mathbb{F}}_p$, the application $log_! : 1 + \mathfrak{m} \longrightarrow \mathfrak{m}$ extends to a homogeneous form of degree p from $\mathbb{K}[[X]]$ into $\mathfrak{m}$.*

Example 1.8. *In characteristic 2, we have*

$$log_!\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=0}^{\infty} \alpha_{2^n}^2 X^{2^{n+1}} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j}$$

for $\sum_{n=0}^{\infty} \alpha_n X^n$ in $1 + X\overline{\mathbb{F}}_2[[X]]$.

Notice that Theorems 1.1 and 1.3 fail in characteristic zero: We have $log_!(1-X) = -\sum_{n=1}^{\infty} (n-1)! X^n$ which is obviously transcendental.

The rest of the paper has two parts. In a first part we recall a few definitions and well-known results and prove all results mentionned above.

In a second part, we generalise Theorems 1.1 and 1.5 to formal power series in several non-commuting variables.

2 Rational and algebraic elements in $\mathbb{K}[[X]]$

This section recalls a few well-known facts concerning rational and algebraic elements in the algebra $\mathbb{K}[[X]]$ of formal power series.

We denote by $\tau : \mathbb{K}[[X] \longrightarrow \mathbb{K}[[X]]$ the shift operator

$$\tau\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=0}^{\infty} \alpha_{n+1} X^n$$

acting on formal power series. The following well-known result characterises rational series:

Proposition 2.1. *A formal power series $A = \sum_{n=0}^{\infty} \alpha_n X^n$ of $\mathbb{K}[[X]]$ is rational if and only if the series $A, \tau(A), \tau^2(A), \ldots, \tau^k(A) = \sum_{n=0}^{\infty} \alpha_{n+k} X^n, \ldots$ span a finite-dimensional vector-space in $\mathbb{K}[[X]]$.*

More precisely, the vector space spanned by $A, \tau(A), \tau^2(A), \ldots, \tau^i(A), \ldots$ has dimension $\| A \| = \max(1 + \deg(f), \deg(g))$ if f/g with $f, g \in \mathbb{K}[X]$ is a reduced expression of a rational series A.

The function $A \longrightarrow \| A \|$ satisfies the inequality

$$\| A + B \| \leq \| A \| + \| B \|$$

for rational series A, B in $\mathbb{K}[[X]]$. As a particular case we have

$$\| A \| - 1 \leq \| 1 + A \| \leq \| A \| + 1 \ .$$

Given a prime p and a formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ in $\overline{\mathbb{F}}_p[[X]]$ we denote by $\kappa(C) \in \mathbb{N} \cup \{\infty\}$ the dimension of the "$p-$kernel"

$$\mathcal{K}(C) = \sum_{f,k} \overline{\mathbb{F}}_p C_{k,f}$$

spanned by all series

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n$$

for $f \in \mathbb{N},\ k \in \mathbb{N},\ k < p^f$.

Algebraic series of $\mathbb{K}[[X]]$ for $\mathbb{K}$ a subfield of the algebraic closure $\overline{\mathbb{F}}_p$ of finite prime characteristic p are characterised by the following Theorem of Christol (see [4] or Theorem 12.2.5 in [1]):

Theorem 2.2. *A formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ of $\overline{\mathbb{F}}_p[[X]]$ is algebraic if and only if $\kappa(C)$ is finite.*

We state without proof the following well-known consequence.

Corollary 2.3. *An algebraic series of $\overline{\mathbb{F}}_p[[X]]$ has all its coefficients in a finite subfield of $\overline{\mathbb{F}}_p$.*

Proposition 2.4. *Let $C = \sum_{n=0}^{\infty} \gamma_n X^n$ be an algebraic series with coefficients in a subfield $\mathbb{K} \subset \overline{\mathbb{F}}_p$.*

(i) We have

$$\mathcal{K}(\tau(C)) \subset \mathcal{K}(C) + \tau(\mathcal{K}(C))$$

which implies

$$\kappa(\tau(C)) \leq 2\kappa(C) \ .$$

(ii) We have

$$\mathcal{K}(C) \subset \mathbb{K} + \mathcal{K}(\tau(C)) + X\mathcal{K}(\tau(C))$$

which implies

$$\kappa(C) \leq 1 + 2\kappa(\tau(C)) \ .$$

Proof Assertion (i) follows from an iterated application of the easy computations

$$(\tau(C))_{k,1} = C_{k+1,1}$$

if $0 \leq k < p-1$ and

$$(\tau(C))_{p-1,1} = \tau(C_{0,1}) \ .$$

The proof of assertion (ii) is similar. □

3 The shuffle algebra

This section recalls mostly well-known results concerning shuffle products of elements in the set $\mathbb{K}[[X]]$ of formal power series over a commutative field $\mathbb{K}$ which is arbitrary unless specified otherwise.

The *shuffle product*

$$A \sqcup\!\sqcup B = C = \sum_{n=0}^{\infty} \gamma_n X^n$$

of $A = \sum_{n=0}^{\infty} \alpha_n X^n$ and $B = \sum_{n=0}^{\infty} \beta_n X^n$ is defined by

$$\gamma_n = \sum_{k=0}^{n} \binom{n}{k} \alpha_k \beta_{n-k}$$

and corresponds to the usual product $ab = c$ of the associated exponential generating series

$$a = \sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!}, \ b = \sum_{n=0}^{\infty} \beta_n \frac{X^n}{n!}, \ c = \sum_{n=0}^{\infty} \gamma_n \frac{X^n}{n!} \ .$$

The *shuffle algebra* is the algebra $(\mathbb{K}[[X]],\ \sqcup\!\sqcup\ )$ obtained by endowing the vector space $\mathbb{K}[[X]]$ of ordinary generating series with the shuffle product. By construction, the shuffle algebra is isomorphic to the algebra $\mathcal{E}(\mathbb{K})$ of exponential generating series. In characteristic zero, the trivial identity

$$\sum_{n=0}^{\infty} \alpha_n X^n = \sum_{n=0}^{\infty} (n!\alpha_n) \frac{X^n}{n!}$$

gives an isomorphism between the usual algebra $\mathbb{K}[[X]]$ of ordinary generating series and the shuffle algebra $(\mathbb{K}[[X]],\ \sqcup\!\sqcup\ )$.

The identity $\left(\sum_{n\geq 0} \lambda^n X^n\right) \sqcup\!\sqcup \left(\sum_{n\geq 0} \mu^n X^n\right) = \sum_{n\geq 0} (\lambda+\mu)^n X^n$, equivalent to $e^{\lambda X} e^{\mu X} = e^{(\lambda+\mu)X}$ implies that the convergency radius of the shuffle product of two complex series with strictly positive convergency radii ρ_1, ρ_2 is at least the harmonic mean $1/\left(\frac{1}{\rho_1} + \frac{1}{\rho_2}\right)$ of ρ_1 and ρ_2.

Proposition 3.1. *The shift operator* $\tau(\sum_{n=0}^{\infty} \alpha_n X^n) = \sum_{n=0}^{\infty} \alpha_{n+1} X^n$ *acts as a derivation on the shuffle algebra.*

Proof The map τ is clearly linear. The computation

$$\tau\left(\sum_{i,j\geq 0} \binom{i+j}{i} \alpha_i \beta_j X^{i+j}\right) = \sum_{i,j\geq 0} \binom{i+j}{i} \alpha_i \beta_j X^{i+j-1} =$$
$$= \sum_{i,j\geq 0} \left(\binom{i+j-1}{i-1} + \binom{i+j-1}{j-1}\right) \alpha_i \beta_j X^{i+j-1}$$

shows that τ satisfies the Leibniz rule $\tau(A \sqcup\!\sqcup B) = \tau(A) \sqcup\!\sqcup B + A \sqcup\!\sqcup \tau(B)$. □

Proposition 3.1 is trivial in characteristic zero: the usual derivation d/dX acts obviously as the shift operator on the algebra $\mathcal{E}(\mathbb{K})$ of exponential generating series over a field of characteristic zero.

Proposition 3.2. *Shuffle products of rational power series are rational.*
More precisely, we have

$$\| A \sqcup\!\sqcup B \| \leq \| A \| \ \| B \|$$

for two rational series A, B *in* $\mathbb{K}[[X]]$.

Proof Proposition 3.1 implies $\tau^n\left(A \sqcup\!\sqcup B\right) = \sum_{k=0}^{n} \binom{n}{k} \tau^k(A) \sqcup\!\sqcup \tau^{n-k}(B)$. The series $\tau^n\left(A \sqcup\!\sqcup B\right)$ belongs thus to the vector space spanned by shuffle products with factors in the vector-spaces $\sum_{n\geq 0} \mathbb{K}\tau^n(A)$ and $\sum_{n\geq 0} \mathbb{K}\tau^n(B)$. This implies the inequality. Proposition 2.1 ends the proof. □

Proposition 3.3. *Shuffle products of algebraic series in* $\overline{\mathbb{F}}_p[[X]]$ *are algebraic.*

More precisely, we have

$$\kappa(A \sqcup\!\sqcup B) \leq \kappa(A)\ \kappa(B)\ .$$

Proof Denoting as in Section 2 by $C_{k,f}$ the series

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n$$

associated to a series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ and by $\kappa(C)$ the dimension of the vector space $\mathcal{K}(C) = \sum_{k,f} \overline{\mathbb{F}}_p C_{k,f}$, Lucas's identity

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{\nu_i}{\kappa_i} \pmod{p}$$

for $n = \sum_{i\geq 0} \nu_i p^i,\ k = \sum_{i\geq 0} \kappa_i p^i$ with $\nu_i, \kappa_i \in \{0, \ldots, p-1\}$ implies

$$\left(A \sqcup\!\sqcup B\right)_{k,1} = \sum_{i=0}^{k} \binom{k}{i} A_{i,1} \sqcup\!\sqcup B_{k-i,1}$$

for $k = 0, \ldots, p-1$. Iteration of this formula shows that $\left(A \sqcup\!\sqcup B\right)_{k,f}$ (for arbitrary $k, f \in \mathbb{N}$ such that $k < p^f$) belongs to the vector space spanned by shuffle products with factors in the vector spaces $\mathcal{K}(A)$ and $\mathcal{K}(B)$ of dimension $\kappa(A)$ and $\kappa(B)$.

Christol's Theorem (Theorem 2.2) ends the proof. □

4 The special shuffle-group

We call the group of units of the shuffle algebra $(\mathbb{K}[[X]],\ \sqcup\!\sqcup\ )$ the *shuffle-group*. Its elements are given by the set $\mathbb{K}^* + X\mathbb{K}[[X]]$ underlying the multiplicative unit group. The shuffle-group is the direct product of the unit group $\mathbb{K}^*$ of $\mathbb{K}$ with the *special shuffle-group* $(1 + X\mathbb{K}[[X]],\ \sqcup\!\sqcup\ )$.

The inverse in the shuffle group of $1 - A \in (1 + X\mathbb{K}[[X]],\ \sqcup\!\sqcup\ )$ is given by

$$\sum_{n=0}^{\infty} A^{\sqcup\!\sqcup\, n} = 1 + A + A \sqcup\!\sqcup A + A \sqcup\!\sqcup A \sqcup\!\sqcup A + \ldots$$

where $A^{\sqcup\!\sqcup\, 0} = 1$ and $A^{\sqcup\!\sqcup\, n+1} = A \sqcup\!\sqcup A^{\sqcup\!\sqcup\, n}$ for $n \geq 1$.

This shows in particular the identity $(1 - X) \sqcup\!\sqcup \left(\sum_{n=0}^{\infty} n! X^n\right) = 1$. Invertible rational (analytical) power series have thus generally a transcendental (non-analytical) shuffle-inverse over the complex numbers.

Proposition 4.1. *The special shuffle-group* $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ *is isomorphic to an infinite-dimensional* $\mathbb{F}_p-$*vector-space if the field* $\mathbb{K}$ *is of positive characteristic* p*.*

Proposition 4.1 shows that $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ is not isomorphic to the multiplicative group structure on $1 + X\mathbb{K}[[X]]$ if $\mathbb{K}$ is of positive characteristic.

Proof of Proposition 4.1 Follows directly from the fact that $exp_!$ is a group isomorphism between the $\mathbb{F}_p-$vector space $\mathfrak{m}$ and the special shuffle group.

One can also give a direct proof by computing $A^{\sqcup\!\sqcup\,p}$. □

Remark 4.2. *One can show that a rational fraction* $A \in 1+X\mathbb{C}[[X]]$ *has a rational inverse for the shuffle-product if and only if* $A = \frac{1}{1-\lambda X}$ *with* $\lambda \in \mathbb{C}$*. (Compute* $A \sqcup\!\sqcup B = 1$ *using the decomposition into simple fractions of the rational series* A, B*.)*

5 The exponential and the logarithm for exponential generating functions

Proposition 5.1. *For all natural numbers* $j, k \geq 1$*, the set* $\{1, \ldots, jk\}$ *can be partitioned in exactly*

$$\frac{(jk)!}{(j!)^k\ k!}$$

different ways into k *unordered disjoint subsets of* j *elements.*

In particular, the rational number $(jk)!/((j!)^k\ k!)$ *is an integer for all natural numbers* j, k *such that* $j \geq 1$*.*

Proof The multinomial coefficient $(jk)!/(j!)^k$ counts the number of ways of partitioning $\{1, \ldots, jk\}$ into k disjoint ordered subset of j elements. Dividing by $k!$ removes the order on these k subsets.

This proves that the formula defines an integer for all $j, k \geq 1$ and the integrality holds also obviously for $k = 0$ and $j \geq 1$. □

Proposition 5.2. *For any natural integer* $k \in \mathbb{N}$*, there exists polynomials* $P_{k,n} \in \mathbb{N}[\alpha_1, \ldots, \alpha_n]$ *such that*

$$\frac{1}{k!}\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right)^k = \sum_{n=0}^{\infty} P_{k,n}(\alpha_1, \alpha_2, \ldots, \alpha_n)\frac{X^n}{n!}\ .$$

Proof The contribution of a monomial

$$\alpha_1^{j_1}\alpha_2^{j_2}\ldots\alpha_s^{j_s}\frac{X^{\sum_{i=1}^s ij_i}}{(\sum_{i=1}^s ij_i)!}$$

with $j_1 + j_2 + \cdots + j_s = k$ to $(1/k!)\,(\sum_{n=1}^{\infty} \alpha_n X^n/n!)^k$ is given by

$$\frac{1}{k!}\frac{k!}{(j_1)!(j_2)!\cdots(j_s)!}\frac{(\sum_{i=1}^{s} ij_i)!}{\prod_{i=1}^{s}(i!)^{j_i}}$$

$$= \left(\prod_{i=1}^{s}\frac{(ij_i)!}{(i!)^{j_i}(j_i)!}\right)\frac{(\sum_{i=1}^{s} ij_i)!}{\prod_{i=1}^{s}(ij_i)!}$$

and the last expression is a product of a natural integer by Proposition 5.1 and of a multinomial coefficient. It is thus a natural integer. □

Corollary 5.3. *For $a = \sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}$ the formulae*

$$exp\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} P_{k,n}(\alpha_1, \ldots, \alpha_n)\frac{X^n}{n!}$$

and

$$log\left(1 + \sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = \sum_{k=1}^{\infty}\sum_{n=0}^{\infty}(-1)^{n+1}(n-1)!P_{k,n}(\alpha_1, \ldots, \alpha_n)\frac{X^n}{n!}$$

define the exponential function and the logarithm of an exponential generating series in $a \in \mathfrak{m}_{\mathcal{E}}$ respectively $1 + a \in 1 + \mathfrak{m}_{\mathcal{E}}$ over an arbitrary field $\mathbb{K}$. These functions are one-to-one and mutually reciprocal.

6 The logarithm as a $p-$homogeneous form over $\overline{\mathbb{F}}_p[[x]]$

Given a fixed prime number p, Proposition 4.1 shows that there exists polynomials $P_{p,n} \in \mathbb{N}[\alpha_0, \ldots, \alpha_n]$ for $n \geq 1$ such that

$$\left(\sum_{n=0}^{\infty} \alpha_n X^n\right)^{\sqcup\!\sqcup\,{}^{p}} = \alpha_0^p + p\sum_{n=1}^{\infty} P_{p,n}(\alpha_0, \ldots, \alpha_n)X^n \ .$$

The polynomials $P_{p,n}$ are homogeneous of degree p with respect to the variabels $\alpha_0, \ldots, \alpha_n$ and we denote by

$$\mu_p\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=1}^{\infty} P_{p,n}(\alpha_0, \ldots, \alpha_n)X^n$$

the $p-$homogeneous form defined by the ordinary generating series of the polynomials $P_{p,1}, P_{p,2}, \ldots$.

Proposition 6.1. *The restriction of μ_p to $1 + \mathfrak{m} \subset \overline{\mathbb{F}}_p[[X]]$ coincides with the function $log_!$.*

Proof We have

$$\tau(\mu_p(1+A)) = (1+A) \sqcup\!\sqcup^{p-1} \sqcup\!\sqcup \tau(1+A)$$

for A in $\mathfrak{m}$. This identity defines the restriction of the $p-$homogenous form μ_p to $1+\mathfrak{m}$. The identity $(1+A) \sqcup\!\sqcup^{p-1} \sqcup\!\sqcup (1+A) = 1$ shows that the same equation

$$\tau(log_!(1+A)) = (1+A) \sqcup\!\sqcup^{p-1} \sqcup\!\sqcup \tau(1+A)$$

is also satisfied by the function $log_!$ since τ corresponds to the differential operator d/dX of the associated exponential series and since the shuffle product corresponds to the ordinary product of exponential generating series.

Since both series $\mu_p(1+A)$ and $log_!(1+A)$ are without constant term, the equality $\tau(\mu_p(1+A)) = \tau(log_!(1+A))$ implies the equality $\mu_p(1+A) = log_!(1+A)$. □

7 Proofs

Proposition 7.1. *If A in $X\overline{\mathbb{F}}_p[[X]]$ is rational (respectively algebraic) then the formal power series $log_!(1+A)$ is rational (respectively algebraic).*

More precisely, we have

$$\| \, log_!(1+A) \, \| \leq 1 + \| \, 1+A \, \|^p$$

respectively

$$\kappa(log_!(1+A)) \leq 1 + 4(\kappa(1+A))^p$$

for rational respectively algebraic A in $X\overline{\mathbb{F}}_p[[X]]$.

Proposition 7.2. *If A in $X\overline{\mathbb{F}}_p[[X]]$ is rational (respectively algebraic) then $exp_!(A)$ is rational (respectively algebraic).*

More precisely, denoting by $q = p^e$ the cardinality of a finite field $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing all coefficients of A we have

$$\| \, exp_!(A) \, \| \leq p^{q^{\|A\|}}$$

respectively

$$\kappa(exp_!(A)) \leq q^{\kappa(A)} p^{q^{\kappa(A)}}$$

for rational respectively algebraic A in $\mathfrak{m}$.

Theorems 1.1, 1.3, 1.5 and 1.6 are now simple reformulations of Propositions 7.1 and 7.2.

Proof of Proposition 7.1 We have

$$\tau(log_!(1+A)) = (1+A) \sqcup\!\sqcup^{p-1} \sqcup\!\sqcup \tau(A) \ .$$

This shows

$$\| \tau(log_!(1+A) \| \leq \| 1+A \|^{p-1} \| \tau(A) \| \leq \| 1+A \|^p$$

and implies

$$\| log_!(1+A) \| \leq 1 + \| 1+A \|^p \ .$$

This settles the rational case.

For algebraic A we have similarly

$$\kappa(\tau(log_!(1+A))) \leq (\kappa(1+A))^{p-1} \ \kappa(\tau(A)) \leq (\kappa(1+A))^{p-1} 2\kappa(A) \leq 2(\kappa(1+A))^p$$

showing

$$\kappa(log_!(1+A)) \leq 1 + 2\kappa(\tau(log_!(1+A))) \leq 1 + 4(\kappa(1+A))^p$$

and ending the proof. □

Given a vector-space $\mathcal{V} \subset \mathbb{K}[[X]]$ containing $\mathbb{K}$, we denote by $\Gamma(\mathcal{V})$ the shuffle-subgroup generated by all elements of $\mathcal{V} \cap (1 + X\mathbb{K}[[X]])$.

Lemma 7.3. *Every element of a vector space $\mathcal{V} \subset \mathbb{K}[[X]]$ containing the constants $\mathbb{K}$ can be written as a linear combination of elements in $\Gamma(\mathcal{V})$.*

Proof We have the identity

$$A = (1 - \epsilon(A) + A) + (\epsilon(A) - 1)$$

where $\epsilon(\sum_{n=0}^{\infty} \alpha_n X^n) = \alpha_0$ is the augmentation map and where $(1-\epsilon(A)+A)$ and $(\epsilon(A) - 1)$ are both in $\mathbb{K}\Gamma(\mathcal{V})$ for $A \in \mathcal{V}$. □

Proof of Proposition 7.2 for rational A Corollary 2.3 shows that we can work over a finite subfield $\mathbb{K} = \mathbb{F}_q$ of $\overline{\mathbb{F}}_p$ with $q = p^e$.

Given a rational series A in $\mathfrak{m} = X\mathbb{K}[[X]]$, we denote by Γ_A the shuffle-subgroup generated by all elements of the set

$$\left\{ \bigcup_{n=0}^{\infty} (\tau^n(A) + \mathbb{K}) \right\} \cap \{1 + X\mathbb{K}[[X]]\}.$$

The group Γ_A is an $\mathbb{F}_p-$vector space generated by at most $q^{\|A\|}$ elements. We denote by $\mathbb{K}[\Gamma_A]$ the subalgebra of dimension $\leq p^{q^{\|A\|}}$ in $\mathbb{K}[[X]]$ spanned by all elements of Γ_A. The identity

$$\tau(exp_!(A)) = exp_!(A) \sqcup\!\sqcup \tau(A)$$

and the fact that the linear application τ is a derivation of $\mathbb{K}[[X]]$ show the inclusion

$$\tau^n(exp_!(A)) \in exp_!(A) \sqcup\!\sqcup \mathbb{K}[\Gamma_A]$$

which ends the proof since the right-hand side is a $\mathbb{K}-$vector space of dimension at most $p^{q^{\|A\|}}$.

Proposition 7.4. *We have for every prime number p and for all natural integers j, k such that $j \geq 1$ the identity*

$$\frac{(jk)!}{(j!)^k k!} \equiv \frac{(pjk)!}{((pj)!)^k k!} \pmod{p} .$$

Proof The right-hand-side counts partitions of $\{1, \ldots, pjk\}$ into k subsets of pj elements. Consider the action on such partitions obtained from the group generated by the jk cyclic permutations $(i, i+jk, i+2jk, \ldots, i+(p-1)jk)$ for $i = 1, \ldots, jk$. Its fixpoints are in bijection with partitions of $\{1, \ldots, jk\}$ into k subsets of j elements. □

Corollary 7.5. *$exp_!$ and $log_!$ commute with the "Frobenius substitution"*

$$\varphi(\sum_{n=0}^{\infty} \alpha_n X^n) = \sum_{n=0}^{\infty} \alpha_n X^{pn}$$

for series in $X\overline{\mathbb{F}}_p[[X]]$, respectively in $1 + X\overline{\mathbb{F}}_p[[X]]$.

This implies

$$(exp_!(A))_{0,f} = exp_!(A_{0,f})$$

Lemma 7.6. *We have*

$$(B \sqcup\!\sqcup C)_{0,1} = B_{0,1} \sqcup\!\sqcup C_{0,1}$$

Proof Follows from the identity

$$\binom{pn}{k} \equiv 0 \pmod{p}$$

if $k \not\equiv 0 \pmod{p}$. □

Proof of Proposition 7.2 for algebraic A We work again over a finite subfield $\mathbb{K} = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing all coefficients of A.

Let Γ_A denote the shuffle subgroup generated by all elements in

$$(\mathcal{K}(A) + \mathbb{K}) \cap (1 + X\mathbb{K}[[X]])$$

where $\mathcal{K}(A) = \sum_{k,f} \mathbb{K}A_{k,f}$. We denote by $\mathbb{K}[\Gamma_A] \subset (\mathbb{K}[[X]], \sqcup\!\sqcup)$ the shuffle-subalgebra of dimension at most $p^{q^{\kappa(A)}}$ spanned by all elements of the group $\Gamma(A) \subset (1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$.

Using the convention $A_{0,0} = A$, we have for $B \in \mathbb{K}[\Gamma(A)]$ and for k such that $0 \leq k < p$

$$\left(exp_!(A_{0,f}) \sqcup\!\sqcup B\right)_{k,1} = \left(\tau^k \left(exp_!(A_{0,f}) \sqcup\!\sqcup B\right)\right)_{0,1} =$$

$$= \left(\sum_{j=0}^{k} \binom{k}{j} \tau^j(exp_!(A_{0,f})) \sqcup\!\sqcup \tau^{k-j}(B) \right)_{0,1} =$$

$$= \sum_{j=0}^{k} \binom{k}{j} \left(\tau^j(exp_!(A_{0,f}))\right)_{0,1} \sqcup\!\sqcup B_{k-j,1}$$

where the last equality is due to Lemma 7.6 (and to the equality $(\tau^k(C))_{0,1} = C_{k,1}$ for $0 \leq k < p$).

An iterated application of the identity $\tau(exp_!(A_{0,f})) = exp_!(A_{0,f}) \sqcup\!\sqcup \tau(A_{0,f})$ implies

$$(\tau^j(exp_!(A_{0,f})))_{0,1} \in exp_!(A_{0,f+1}) \sqcup\!\sqcup \mathbb{K}[\Gamma(A)]$$

and shows the inclusion

$$(exp_!(A))_{k,f} \in exp_!(A_{0,f}) \sqcup\!\sqcup \mathbb{K}[\Gamma_A]$$

for all k such that $0 \leq k < p^f$ and for $(k, f) = (0, 0)$. Since the vector space $\sum_f \mathbb{K} exp_!(A_{0,f})$ is of dimension at most $q^{\kappa(A)}$ we have the inequality

$$\kappa(exp_!(A)) \leq q^{\kappa(A)} p^{q^{\kappa(A)}} .$$

This ends the proof. □

8 Power series in free non-commuting variables

This and the next section recall a few basic and well-known facts concerning (rational) power series in free non-commuting variables, see for instance [6], [3] or a similar book on the subject. We use however sometimes a different terminology, motivated by [2].

We denote by $\mathcal{X}^*$ the free monoid on a finite set $\mathcal{X} = \{X_1, \ldots, X_k\}$. We write 1 for the identity element and we use a boldface capital $\mathbf{X}$ for a non-commutative monomial $\mathbf{X} = X_{i_1} X_{i_2} \cdots X_{i_l} \in \mathcal{X}^*$. We denote by

$$A = \sum_{\mathbf{X} \in \mathcal{X}^*} (A, \mathbf{X}) \mathbf{X} \in \mathbb{K}\langle\langle X_1, \cdots, X_k \rangle\rangle$$

a non-commutative formal power series where

$$\mathcal{X}^* \ni \mathbf{X} \longmapsto (A, \mathbf{X}) \in \mathbb{K}$$

stands for the coefficient function.

We denote by $\mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ the maximal ideal consisting of formal power series without constant coefficient and by $\mathbb{K}^* + \mathfrak{m} = \mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle \setminus \mathfrak{m}$ the unit-group of the algebra $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ consisting of all (multiplicatively) invertible elements in $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$. The unit group is isomorphic

to the direct product $\mathbb{K}^* \times (1+\mathfrak{m})$ where $\mathbb{K}^*$ is the central subgroup consisting of non-zero constants and where $1+\mathfrak{m}$ denotes the multiplicative subgroup given by the affine subspace formed by power series with constant coefficient 1. We have $(1-A)^{-1} = 1+\sum_{n=1}^{\infty} A^n$ for the multiplicative inverse $(1-A)^{-1}$ of an element $1-A \in 1+\mathfrak{m}$.

8.1 The shuffle algebra

The *shuffle-product* $\mathbf{X} \sqcup\!\sqcup \mathbf{X}'$ of two non-commutative monomials $\mathbf{X}, \mathbf{X}' \in \mathcal{X}^*$ of degrees $a = deg(\mathbf{X})$ and $b = deg(\mathbf{X}')$ (for the obvious grading given by $deg(X_1) = \cdots = deg(X_k) = 1$) is the sum of all $\binom{a+b}{a}$ monomials of degree $a+b$ obtained by "shuffling" in all possible ways the linear factors (elements of $\mathcal{X}$) involved in $\mathbf{X}$ with the linear factors of $\mathbf{X}'$. A monomial involved in $\mathbf{X} \sqcup\!\sqcup \mathbf{X}'$ can be thought of as a monomial of degree $a+b$ whose linear factors are coloured by two colours with $\mathbf{X}$ corresponding to the product of all linear factors of the first colour and $\mathbf{X}'$ corresponding to the product of the remaining linear factors. The shuffle product $\mathbf{X} \sqcup\!\sqcup \mathbf{X}'$ can also be recursively defined by $\mathbf{X} \sqcup\!\sqcup 1 = 1 \sqcup\!\sqcup \mathbf{X} = \mathbf{X}$ and

$$(\mathbf{X}X_s) \sqcup\!\sqcup (\mathbf{X}'X_t) = (\mathbf{X} \sqcup\!\sqcup (\mathbf{X}'X_t))X_s + ((\mathbf{X}X_s) \sqcup\!\sqcup \mathbf{X}')X_t$$

where $X_s, X_t \in \mathcal{X} = \{X_1, \ldots, X_k\}$ are monomials of degree 1.

Extending the shuffle-product in the obvious way to formal power series endows the vector space $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ with an associative and commutative algebra structure called the *shuffle-algebra*. In the case of one variable $X = X_1$ we recover the definition of Section 3.

The group $\mathrm{GL}_k(\mathbb{K})$ acts on the vector-space $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ by linear substitutions. This action induces an automorphism of the multiplicative (non-commutative) algebra-structure or of the (commutative) shuffle algebra-structure underlying the vector space $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$.

Substitution of all variables X_j of formal power series in $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ by X yields a homomorphism of (shuffle-)algebras into the commutative (shuffle-)algebra $\mathbb{K}[[X]]$.

The commutative unit group (set of invertible elements for the shuffle-product) of the shuffle algebra, given by the set $\mathbb{K}^* + \mathfrak{m}$, is isomorphic to the direct product $\mathbb{K}^* \times (1+\mathfrak{m})$ where $1+\mathfrak{m}$ is endowed with the shuffle product. The inverse of an element $1 - A \in (1+\mathfrak{m}, \sqcup\!\sqcup)$ is given by $\sum_{n=0}^{\infty} A^{\sqcup\!\sqcup\, n} = 1 + A + A \sqcup\!\sqcup A + A \sqcup\!\sqcup A \sqcup\!\sqcup A + \ldots$.

The following result generalises Proposition 4.1:

Proposition 8.1. *Over a field of positive characteristic p, the subgroup $1+\mathfrak{m}$ of the shuffle-group is an infinite-dimensional $\mathbb{F}_p-$vector space.*

Proof Contributions to a $p-$fold shuffle product $A_1 \sqcup\!\sqcup A_2 \sqcup\!\sqcup \cdots \sqcup\!\sqcup A_p$ are given by monomials with linear factors coloured by p colours $\{1, \ldots, p\}$

keeping track of their "origin" with coefficients given by the product of the corresponding "monochromatic" coefficients in $A_1, \ldots, A_p$. A permutation of the colours $\{1, \ldots, p\}$ (and in particular, a cyclic permutation of all colours) leaves such a contribution invariant if $A_1 = \cdots = A_p$. Forgetting the colours, coefficients of strictly positive degree in $A \sqcup\!\sqcup^{p}$ are thus zero in characteristic p. □

As in the one variable case, one can prove that

$$\frac{1}{k!} A \sqcup\!\sqcup^{k}$$

is defined over an arbitrary field $\mathbb{K}$ for $A \in \mathfrak{m}$. Indeed, monomials contributing to $A \sqcup\!\sqcup^{k}$ can be considered as colored by k colours and the $k!$ possible colour-permutations yield identical contributions.

For $A \in \mathfrak{m}$, we denote by

$$exp_!(A) = \sum_{n=0}^{\infty} \frac{1}{n!} A \sqcup\!\sqcup^{n}$$

the resulting exponential map from the Lie algebra $\mathfrak{m}$ into the infinite-dimensional commutatif Lie group $(1 + \mathfrak{m}, \sqcup\!\sqcup)$. Its reciprocal function is the as usual defined by

$$log_!(1 + A) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} A \sqcup\!\sqcup^{n} .$$

In the case of a field $\mathbb{K}$ of positive characteristic p the function $log_!$ is again given by the restriction to $1 + \mathfrak{m}$ of a $p-$homogeneous form μ_p.

The form μ_p has all its coefficients in $\mathbb{N}$ and is defined by the equality

$$A \sqcup\!\sqcup^{p} = (A, 1)^p + p\mu_p(A)$$

over an arbitrary field.

9 Rational formal power series

A formal power series A is *rational* if it belongs to the smallest subalgebra in $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ which contains the free associative algebra $\mathbb{K}\langle X_1, \ldots, X_k \rangle$ of non-commutative polynomials and intersects the multiplicative unit group of $\mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$ in a subgroup.

Given a monomial $\mathbf{T} \in \mathcal{X}^*$, we denote by

$$\rho(\mathbf{T}) : \mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle \longrightarrow \mathbb{K}\langle\langle X_1, \ldots, X_k \rangle\rangle$$

the linear application defined by

$$\rho(\mathbf{T})A = \sum_{\mathbf{X}\in\mathcal{X}^*} (A, \mathbf{XT})\mathbf{X}$$

for $A = \sum_{\mathbf{X}\in\mathcal{X}^*}(A, \mathbf{X})\mathbf{X}$ in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$. The identity $\rho(\mathbf{T})(\rho(\mathbf{T}')A) = \rho(\mathbf{TT}')A$ shows that we have a representation

$$\rho : \mathcal{X}^* \longrightarrow \mathrm{End}(\mathbb{K}\langle\langle\mathcal{X}\rangle\rangle)$$

of the free monoid $\mathcal{X}^*$ on $\mathcal{X}$. The *recursive closure* $\overline{A}$ of a power series A is the vector-space spanned by its orbit $\rho(\mathcal{X}^*)A$ under $\rho(\mathcal{X}^*)$. We call the dimension $\dim(\overline{A})$ of $\overline{A}$ the *complexity* of A.

We call a subspace $\mathcal{A} \subset \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ *recursively closed* if it contains the recursive closure of all its elements.

Rational series coincide with series of finite complexity by a Theorem of Schützenberger (cf. [3], Theorem 1 of page 22).

Remark 9.1. *In the case of one variable, the complexity $dim(\overline{A})$ of a reduced non-zero rational fraction $A = \frac{f}{g}$ with $f \in \mathbb{K}[X]$ and $g \in 1 + X\mathbb{K}[X]$ equals $dim(\overline{A}) = max(1 + deg(f), deg(g))$.*

Remark 9.2. *The (generalised) Hankel matrix $H = H(A)$ of*

$$A = \sum_{\mathbf{X}\in\mathcal{X}^*} (A, \mathbf{X})\mathbf{X} \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$$

is the infinite matrix with rows and columns indexed by the free monoid $\mathcal{X}^*$ of monomials and entries $H_{\mathbf{XX}'} = (A, \mathbf{XX}')$. The rank $rank(H)$ is given by the complexity $\dim(\overline{A})$ of A and $\overline{A}$ corresponds to the row-span of H.

Given subspace $\mathcal{A}, \mathcal{B}$ of $\mathbb{K}\langle\langle\mathcal{X}\rangle\rangle$, we denote by $\mathcal{A} \sqcup\!\sqcup \mathcal{B}$ the vector space spanned by all products $A \sqcup\!\sqcup B$ with $A \in \mathcal{A}$ and $B \in \mathcal{B}$.

Proposition 9.3. *We have the inclusion*

$$\overline{A \sqcup\!\sqcup B} \subset \overline{A} \sqcup\!\sqcup \overline{B}$$

for the shuffle product $A \sqcup\!\sqcup B$ of $A, B \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$.

Corollary 9.4. *We have*

$$dim(\overline{A \sqcup\!\sqcup B}) \leq dim(\overline{A})\ dim(\overline{B})$$

for the shuffle product $A \sqcup\!\sqcup B$ of $A, B \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$.

In particular, shuffle products of rational elements in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ are rational.

Proof of Proposition 9.3 For $Y \in \overline{A}, Z \in \overline{B}$ and X in $\{X_1, \ldots, X_k\}$, the recursive definition of the shuffle product given in Section 8.1 shows

$$\rho(X)(Y \sqcup\!\sqcup Z) = (\rho(X)Y) \sqcup\!\sqcup Z + Y \sqcup\!\sqcup (\rho(X)Z) \ .$$

We have thus the inclusions

$$\rho(X)(Y \sqcup\!\sqcup Z) \in \overline{A} \sqcup\!\sqcup Z + Y \sqcup\!\sqcup \overline{B} \subset \overline{A} \sqcup\!\sqcup \overline{B}$$

which show that the vector space $\overline{A} \sqcup\!\sqcup \overline{B}$ is recursively closed. Proposition 9.3 follows now from the inclusion $A \sqcup\!\sqcup B \in \overline{A} \sqcup\!\sqcup \overline{B}$. □

Remark 9.5. *Similar arguments show that the set of rational elements in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ is also closed under the ordinary product (and multiplicative inversion of invertible series), Hadamard product and composition (where one considers $A \circ (B_1, \ldots, B_k)$ with $A \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ and $B_1, \ldots, B_k \in \mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$).*

Remark 9.6. *The shuffle inverse of a rational element in $\mathbb{K}^* + \mathfrak{m}$ is in general not rational in characteristic 0. An exception is given by geometric progressions $\frac{1}{1-\sum_{j=1}^k \lambda_j X_j} = \sum_{n=0}^\infty \left(\sum_{j=1}^k \lambda_j X_j\right)^n$ since we have*

$$\frac{1}{1-\sum_{j=1}^k \lambda_j X_j} \sqcup\!\sqcup \frac{1}{1-\sum_{j=1}^k \mu_j X_j} = \frac{1}{1-\sum_{j=1}^k (\lambda_j+\mu_j) X_j}$$

corresponding to $e^{\lambda X} e^{\mu X} = e^{(\lambda+\mu)X}$ in the one-variable case.

There are no other such elements in $1 + \mathfrak{m} \subset \mathbb{K}[[X]]$, see Remark 4.2. I ignore if the maximal rational shuffle subgroup of $1 + \mathfrak{m} \subset \mathbb{C}\langle\langle X_1, \ldots, X_k\rangle\rangle$ (defined as the set of all rational elements in $1 + \mathfrak{m}$ with rational inverse for the shuffle product) contains other elements if $k \geq 2$.

Remark 9.7. *Any finite set of rational elements in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ over a field $\mathbb{K}$ of positive characteristic is included in a unique minimal finite-dimensional recursively closed subspace of $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ which intersects the shuffle group $(\mathbb{K}^* + \mathfrak{m}, \sqcup\!\sqcup)$ in a subgroup.*

10 Main result for generating series in non-commuting variables

Theorem 10.1. *Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{F}}_p$. Given a non-commutative formal power series $A \in \mathfrak{m} \subset \mathbb{K}\langle\langle \mathcal{X}\rangle\rangle$, the following two assertions are equivalent:*

(i) A is rational.

(ii) $exp_!(A)$ is rational.

More precisely, we have for a rational series A in $\mathfrak{m}$ the inequalities

$$\dim\left(\overline{log_!(1+A)}\right) \leq 1 + \left(\dim(\overline{1+A})\right)^p$$

and

$$\dim\left(\overline{exp_{\text{ш}}(A)}\right) \leq p^{q^{\dim(\overline{A})}}$$

where $q = p^e$ is the cardinality of a finite field $\mathbb{F}_q$ containing all coefficients of A.

Proof The identity

$$log_{\text{ш}}(1+A) = \sum_{X \in \mathcal{X}} \left((1+A)^{\text{ш}^{p-1}} \text{ш} \rho(X)A \right) X$$

and Corollary 9.4 show

$$\dim\left(\overline{log_{\text{ш}}(1+A)}\right) \leq 1 + \left(\dim(\overline{1+A})\right)^p \ .$$

For the opposite direction we denote by $\mathbb{K} = \mathbb{F}_q$ a finite subfield of $\overline{\mathbb{F}}_p$ containing all coefficients of A. We have

$$\overline{exp_{\text{ш}}(A)} \subset exp_{\text{ш}}(A) \text{ ш } \mathbb{K}[\Gamma(A)]$$

where $\mathbb{K}[\Gamma(A)]$ is the shuffle subalgebra of dimension $\leq p^{q^{\dim(\overline{A})}}$ generated by all elements of the form

$$(\overline{A} + \mathbb{K}) \cap (1 + \mathfrak{m}) \ .$$

This implies the inequality

$$\dim\left(\overline{exp_{\text{ш}}(A)}\right) \leq p^{q^{\dim(\overline{A})}}$$

which ends the proof. □

Acknowledgements I thank J-P. Allouche, M. Brion, A. Pantchichkine, T. Rivoal and B. Venkov for their interest in a preliminary version and helpful remarks.

References

[1] J.-P. Allouche, J. Shallit, Automatic Sequences. Theory, Applications, Generalizations, Cambridge University Press (2003).

[2] R. Bacher, *Determinants related to Dirichlet characters modulo* 2, 4 *and* 8 *of binomial coeffficients and the algebra of recurrence matrices*, Int. J. of Alg. and Comp., vol. 18 No. 3 (2008), 535–566.

[3] J. Berstel, C. Reutenauer, Rational Series and Their Languages, electronic book available at the author's website's.

[4] G. Christol, *Ensembles presque périodiques k-reconnaissables*. Theoret. Comput. Sci. **9** (1979), 141–145.

[5] L. Comtet, Analyse combinatoire, Tome second, Presses Universitaires de France, (1970).

[6] R.P. Stanley, Enumerative Combinatorics, Volume 2, Cambridge University Press (1999).

Roland BACHER
INSTITUT FOURIER
Laboratoire de Mathématiques
UMR 5582 (UJF-CNRS)
BP 74
38402 St Martin d'Hères Cedex (France)

e-mail: Roland.Bacher@ujf-grenoble.fr