



**HAL**  
open science

## Arithmetic properties related to the shuffle-product

Roland Bacher

► **To cite this version:**

| Roland Bacher. Arithmetic properties related to the shuffle-product. 2007. hal-00149241v1

**HAL Id: hal-00149241**

**<https://hal.science/hal-00149241v1>**

Preprint submitted on 24 May 2007 (v1), last revised 7 Jun 2007 (v2)

**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.

# Arithmetic properties related to the shuffle-product

Roland Bacher

*Abstract<sup>1</sup>: Properties of the shuffle product in positive characteristic suggest to consider a  $p$ -homogeneous form  $\sigma : \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle \longrightarrow \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$  on the vector space  $\overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$  of formal power series in  $k$  free non-commuting variables. The form  $\sigma$  preserves rational elements in  $\overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ , algebraic series of  $\overline{\mathbb{F}_p}[[X]]$  and induces a bijection on the affine subspace  $1 + \mathfrak{m}$  of formal power series with constant coefficient 1. Conjecturally, this bijection restricts to a bijection of rational elements in  $1 + \mathfrak{m} \subset \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ , respectively algebraic elements in  $1 + X\overline{\mathbb{F}_p}[[X]]$ .*

## 1 Introduction

The aim of this paper is to present some properties and conjectures related to shuffle-products of power series in non-commuting variables. The shuffle product

$$A \amalg B = \sum_{0 \leq i, j} \binom{i+j}{i} \alpha_i \beta_j X^{i+j}$$

of two power series  $A = \sum_{n=0}^{\infty} \alpha_n X^n, B = \sum_{n=0}^{\infty} \beta_n X^n \in \mathbb{K}[[X]]$  in one variable over a commutative field  $\mathbb{K}$  turns the set  $\mathbb{K}^* + X\mathbb{K}[[X]]$  into a commutative group which is not isomorphic to the commutative group on  $\mathbb{K}^* + X\mathbb{K}[[X]]$  associated to the ordinary product of (multiplicatively) invertible formal power series if  $\mathbb{K}$  is of positive characteristic. Shuffle products of rational (respectively algebraic) power series are rational (respectively algebraic). The shuffle product turns the affine subspace  $1 + X\mathbb{K}[[X]]$  into a group which is isomorphic to an infinite-dimensional  $\mathbb{F}_p$ -vector space if  $\mathbb{K}$  is a field of positive characteristic  $p$ . The set of rational (respectively algebraic) elements in  $1 + X\mathbb{K}[[X]]$  (or more generally in  $\mathbb{K}^* + X\mathbb{K}[[X]]$ ) forms thus a group with respect to the shuffle product if  $\mathbb{K}$  is of positive characteristic.

The first interesting case is given by a subfield  $\mathbb{K} \subset \overline{\mathbb{F}_2}$  contained in the algebraic closure of the field  $\mathbb{F}_2$  with two elements. The structure of the  $\mathbb{F}_2$ -vector space induced by the shuffle product on  $1 + X\overline{\mathbb{F}_2}[[X]]$  suggests to

<sup>1</sup>Keywords: Shuffle product, formal power series, rational fraction, algebraic power series, quadratic form, automaton sequence, Math. class: 11B85, 11E08, 11E76

consider the quadratic form

$$\begin{aligned} \sigma \left( \sum_{n=0}^{\infty} \alpha_n X^n \right) &= \sum_{n=0}^{\infty} \alpha_{2n}^2 X^{2n+1} + \sum_{0 \leq i \leq j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j} \\ &= \alpha_0^2 + \sum_{n=0}^{\infty} \alpha_{2n}^2 X^{2n+1} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j} . \end{aligned}$$

The quadratic form  $\sigma : \overline{\mathbb{F}_2}[[X]] \rightarrow \overline{\mathbb{F}_2}[[X]]$  thus defined preserves the vector space of rational or algebraic power series. It induces a bijection of infinite order on the affine subspace  $1 + X\overline{\mathbb{F}_2}[[X]]$ . Orbits are either infinite or of cardinality a power of two. Conjecturally, the inverse bijection  $\sigma^{-1}$  of the set  $1 + X\overline{\mathbb{F}_2}[[X]]$  preserves also rational elements and algebraic elements. We present experimental evidence for this conjecture. An analogous construction yields a homogeneous  $p$ -form (still denoted)  $\sigma : \overline{\mathbb{F}_p}[[X]] \rightarrow \overline{\mathbb{F}_p}[[X]]$  with similar properties for  $p$  an arbitrary prime.

In a second part of the paper, starting with Section 6, we recall the definition of the shuffle product for elements in the vector space  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  of formal power series in free non-commuting variables. The shuffle product preserves again rational formal power series, characterised for instance by a Theorem of Schützenberger. The  $p$ -homogeneous form  $\sigma$  considered above has a natural extension  $\sigma : \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle \rightarrow \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ . This extension of  $\sigma$  still preserves rational elements and induces a bijection on  $1 + \mathfrak{m}$  where  $\mathfrak{m} \subset \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$  denotes the maximal ideal of formal power series without constant coefficient in  $\overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ . Conjecturally, the map  $\sigma$  restricts again to a bijection of the subset of rational elements in  $1 + \mathfrak{m}$ .

## 2 Power series in one variable

We denote by  $\mathbb{K}[[X]]$  the commutative algebra of formal power series over a commutative field  $\mathbb{K}$  with product

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

extending the product of the polynomial subalgebra  $\mathbb{K}[X] \subset \mathbb{K}[[X]]$ . Its unit group  $\mathbb{K}^* + X\mathbb{K}[[X]]$  consists of all (multiplicatively) invertible series and decomposes as a direct product  $\mathbb{K}^* \times (1 + \mathfrak{m})$  with  $\mathfrak{m} = X\mathbb{K}[[X]]$  denoting the maximal ideal of the algebra  $\mathbb{K}[[X]]$ .

A subalgebra containing the field of constants  $\mathbb{K}$  of  $\mathbb{K}[[X]]$  is *rationally closed* if it intersects the unit group  $\mathbb{K}^* + X\mathbb{K}[[X]]$  in a subgroup. The *rational closure* of a subset  $\mathcal{S} \subset \mathbb{K}[[X]]$  is the smallest rationally closed subalgebra of  $\mathbb{K}[[X]]$  which contains  $\mathcal{S} \cup \mathbb{K}$ .

The rational closure of  $X$ , called the *algebra of rational fractions in  $X$*  or the *rational subalgebra* of  $\mathbb{K}[[X]]$ , contains the polynomial subalgebra  $\mathbb{K}[X]$  and is formed by all rational fractions of the form  $\frac{f}{g}$  with  $f, g \in \mathbb{K}[X], g \notin \mathfrak{m}$ . The expression  $\frac{f}{g}$  of such a rational fraction is unique if we require  $g \in 1 + \mathfrak{m}$ .

An element  $y \in \mathbb{K}[[X]]$  is *algebraic* if it satisfies a polynomial identity  $P(X, y) = 0$  for some polynomial  $P \in \mathbb{K}[X, y]$ . Algebraic series of  $\mathbb{K}[[X]]$  form a rationally closed subalgebra containing all rational fractions.

### 3 The shuffle product

The *shuffle product*, defined as

$$A \amalg B = \sum_{n,m=0}^{\infty} \binom{n+m}{n} \alpha_n \beta_m X^{n+m}$$

for  $A = \sum_{n=0}^{\infty} \alpha_n X^n, B = \sum_{n=0}^{\infty} \beta_n X^n \in \mathbb{K}[[x]]$ , yields a bilinear associative and commutative product on the vector space  $\mathbb{K}[[x]]$  of formal power series. We call the corresponding algebra  $(\mathbb{K}[[x]], \amalg)$  the *shuffle-algebra*. The associated unit group, called the *shuffle-group* with elements formed by the set  $\mathbb{K}^* + X\mathbb{K}[[x]]$  underlying the multiplicative unit group decomposes as a direct product  $\mathbb{K}^* \times (1 + X\mathbb{K}[[X]])$ .

**Remark 3.1.** *Over a field  $\mathbb{K}$  of characteristic zero, the map*

$$\mathbb{K}[[X]] \ni \sum_{n=0}^{\infty} \alpha_n x^n \mapsto \sum_{n=0}^{\infty} n! \alpha_n X^n \in (\mathbb{K}[[X]], \amalg)$$

*defines an isomorphism of algebras between the usual (multiplicative) algebra of formal power series and the shuffle algebra  $(\mathbb{K}[[X]], \amalg)$ . This shows in particular the identity  $(1 - X) \amalg (\sum_{n=0}^{\infty} n! X^n)$ . The shuffle inverse of a rational fraction is thus generally transcendental in characteristic 0.*

**Remark 3.2.** *The inverse for the shuffle product of  $1 - a \in 1 + X\mathbb{K}[[x]]$  is given by*

$$\sum_{n=0}^{\infty} a^{\amalg n} = 1 + a + a \amalg a + a \amalg a \amalg a + \dots$$

*where  $a^{\amalg 0} = 1, a^{\amalg^{n+1}} = a \amalg a^{\amalg n}$  for  $n \geq 1$ .*

*For computations, one can use the recursive formulae  $B_0 = 1, C_0 = a, B_{n+1} = B_n + B_n \amalg C_n, C_{n+1} = C_n \amalg C_n = a^{\amalg^{2n+1}}$  with  $B_n = \sum_{k=0}^{2^n-1} a^{\amalg k}$  converging (quadratically) to the shuffle-inverse of  $1 - a$ .*

**Proposition 3.3.** *The shuffle-group  $1 + X\mathbb{K}[[X]]$  is isomorphic to an infinite-dimensional  $\mathbb{F}_p$ -vector-space if  $\mathbb{K}$  is a field of positive characteristic  $p$ .*

**Corollary 3.4.** *The shuffle-group  $1 + X\mathbb{K}[[X]]$  is not isomorphic to the multiplicative group structure on  $1 + X\mathbb{K}[[X]]$  if  $\mathbb{K}$  is of positive characteristic.*

**Proof of Proposition 3.3** We have

$$A^{\text{III}^p} = \sum_{0 \leq i_1, i_2, \dots, i_p} \binom{i_1 + i_2 + \dots + i_p}{i_1, i_2, \dots, i_p} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_p} X^{i_1 + \dots + i_p} .$$

for  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \mathbb{K}[[X]]$  where  $\binom{i_1 + i_2 + \dots + i_p}{i_1, i_2, \dots, i_p} = \frac{(i_1 + \dots + i_p)!}{i_1! \dots i_p!}$ . Two summands differing by a cyclic permutation of indices  $(i_1, i_2, \dots, i_p) \mapsto (i_2, i_3, \dots, i_p, i_1)$  yield the same contribution to  $A^{\text{III}^p}$ . Over a field  $\mathbb{K}$  of positive characteristic  $p$  we can thus restrict the summation to  $i_1 = i_2 = \dots = i_p$ . Since  $\binom{pi}{i, i, \dots, i} = \frac{(pi)!}{(i!)^p} \equiv 0 \pmod{p}$  except for  $i = 0$ , we have  $A^{\text{III}^p} = \alpha_0^p$  for  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \mathbb{K}[[X]]$ . This implies the result . □

**Proposition 3.5.** *Shuffle products of rational power series are rational.*

**Proof** Suppose first  $\mathbb{K}$  of characteristic zero. The result is obvious for the shuffle product of two polynomials. Extending  $\mathbb{K}$  to its algebraic closure, decomposing into simple fractions and using bilinearity, it is enough to consider shuffle products of the form  $X^h \text{III} \left( \sum_{n=0}^{\infty} n^k \alpha_n X^n \right) = \sum_{n=0}^{\infty} \binom{n+h}{h} n^k \alpha_n X^{n+h}$  which are obviously rational and shuffle products of the form

$$\left( \sum_{n=0}^{\infty} n^h \alpha^n X^n \right) \text{III} \left( \sum_{n=0}^{\infty} n^k \beta^n X^n \right) = \sum_{0 \leq m \leq n} \binom{n}{m} m^h (n-m)^k \alpha^m \beta^{n-m} X^n$$

which are evaluations at  $y = \alpha, z = \beta$  of

$$\left( y \frac{\partial}{\partial y} \right)^h \left( z \frac{\partial}{\partial z} \right)^k \left( \frac{1}{1 - (y+z)X} \right)$$

and are thus rational for  $\mathbb{K}$  of characteristic zero.

In positive characteristic, one can either consider suitable lifts into integer rings of fields of characteristic zero or deduce it as a special case of Corollary 7.3. □

**Remark 3.6.** *The proof of proposition 3.5 implies easily analyticity of shuffle products of analytic power series (defined as formal power series with strictly positive convergence radii) if  $\mathbb{K} \subset \mathbb{C}$  or  $\mathbb{K} \subset \widehat{\mathbb{Q}}_p$ .*

**Proposition 3.7.** *Shuffle products of algebraic series in  $\overline{\mathbb{F}_p}[[X]]$  are algebraic.*

**Sketch of Proof** A Theorem of Christol (see Theorem 12.2.5 in [2]) states that the coefficients of an algebraic series over  $\mathbb{C} \subset \overline{\mathbb{F}_p}$  define a  $q$ -automatic sequence with values in  $\mathbb{F}_q$  for some power  $q = p^e$  of  $p$ . Given a formal power series  $C = \sum_{n=0}^{\infty} \gamma_n X^n \in \overline{\mathbb{F}_p}[[X]]$ , we denote by  $C_{k,f}$  the formal power series  $\sum_{n=0}^{\infty} \gamma_{k+nq^f} X^n$ .

The result follows then from the observation that the series  $(A \text{III} B)_{k,f}$  are linear combination of  $A_{k_1,f} \text{III} B_{k_2,f}$  and span thus a finite-dimensional subspace of  $\overline{\mathbb{F}_p}[[X]]$  for algebraic  $A, B \in \overline{\mathbb{F}_p}[[X]]$ .  $\square$

Propositions 3.3 and 3.5 (respectively 3.3 and 3.7) imply immediately the following result:

**Corollary 3.8.** *Rational (respectively algebraic) elements of the shuffle-group  $1 + X\mathbb{K}[[X]]$  form a subgroup for  $\mathbb{K} \subset \overline{\mathbb{F}_p}$ .*

**Remark 3.9.** *A rational fraction  $A \in 1 + X\mathbb{K}[[X]]$  with  $\mathbb{K} \subset \mathbb{C}$  has a rational inverse for the shuffle-product if and only if  $A = \frac{1}{1-\lambda X}$  with  $\lambda \in \mathbb{K}$ . (Idea of proof: Decompose the two rational elements  $A, B$  such that  $A \text{III} B = 1$  into simple fractions and compute  $A \text{III} B$  using the formulae occuring in the proof of Proposition 3.5.)*

## 4 A quadratic form

The identity  $A \text{III} A = \alpha_0^2$  for  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$  (see the proof of Proposition 3.3) suggests to consider the quadratic map

$$\mathbb{K}[[X]] \ni A = \sum_{n=0}^{\infty} \alpha_n X^n \mapsto \sigma(A) = \alpha_0^2 + \sum_{n=1}^{\infty} \beta_n X^n \in \mathbb{K}[[X]]$$

defined by

$$\left( \sum_{n=0}^{\infty} \tilde{\alpha}_n X^n \right) \text{III} \left( \sum_{n=0}^{\infty} \tilde{\alpha}_n X^n \right) = \tilde{\alpha}_0^2 + 2 \sum_{n=0}^{\infty} \tilde{\beta}_n X^n$$

where  $\tilde{\alpha}_n$  and  $\tilde{\beta}_n$  are lifts into suitable algebraic integers of  $\alpha_n, \beta_n \in \overline{\mathbb{F}_2}$  and where  $\mathbb{K}$  is a subfield of  $\overline{\mathbb{F}_2}$ .

For  $A = \sum_{n=0}^{\infty} \alpha_n X^n$ , we get

$$\sigma(A) = \alpha_0^2 + \sum_{n=1}^{\infty} \frac{1}{2} \binom{2n}{n} \alpha_n^2 X^{2n} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j}$$

and  $\binom{2n}{n} \equiv 2 \pmod{4}$  if and only if  $n$  is a power of 2. This yields the formula

$$\sigma(A) = \alpha_0^2 + \sum_{n=0}^{\infty} \alpha_{2^n}^2 X^{2^{n+1}} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j}.$$

**Proposition 4.1.** *The formal power series  $\sigma(A)$  is rational (respectively algebraic) if  $A \in \overline{\mathbb{F}_2}[[X]]$  is rational (respectively algebraic).*

The statement of this proposition in the case of a rational series is a particular case of Proposition 8.1.

Proposition 4.1 can be proven by modifying slightly the arguments used in the proof of Propositions 3.5 and 3.7 and by applying them to a suitable integral lift  $\tilde{A} \in \overline{\mathbb{Q}}[[X]]$  of  $A$ .  $\square$

Finally, one has also the following result whose easy proof is left to the reader:

**Proposition 4.2.** *The quadratic form  $A \mapsto \sigma(A)$  commutes with the Frobenius map  $A \mapsto A^2$ .*

#### 4.1 The main conjecture

**Proposition 4.3.** *The quadratic form  $A \mapsto \sigma(A)$  induces a bijection on the affine subspace  $1 + X\mathbb{K}[[X]]$  for a subfield  $\mathbb{K} \subset \overline{\mathbb{F}_2}$ .*

**Remark 4.4.** *Omitting the restriction to  $1 + X\mathbb{K}[[X]]$ , the quadratic form  $\sigma$  is neither surjective nor injective: One has  $\sigma^{-1}(X) = \emptyset$  and  $\sigma(A) = 0$  if  $A \in X^3\overline{\mathbb{K}}[[X^2]]$ . (The example for non-injectivity is related to the easy observation that  $\sigma(A) = 0$  if and only if  $\sigma(1 + A) = 1 + A$  for  $A \in \overline{\mathbb{F}_2}[[X]]$ .)*

**Proof of Proposition 4.3** This follows from the identity

$$\sigma(A) - \sigma(B) = (\alpha_n - \beta_n)X^n + X^{n+1}\overline{\mathbb{F}_2}[[X]]$$

if  $A = 1 + \sum_{n=1}^{\infty} \alpha_n X^n, B = 1 + \sum_{n=1}^{\infty} \beta_n X^n$  coincide up to  $X^{n-1}$  (ie. if  $\alpha_j = \beta_j$  for  $j = 1, \dots, n-1$ ).  $\square$

Experimental evidence (see Sections 4.5, 4.6 and 4.7 for a few examples) suggests the following conjecture:

**Conjecture 4.5.** *If  $A \in 1 + \overline{\mathbb{F}_2}[[X]]$  is rational (respectively algebraic) then its preimage  $\sigma^{-1}(A)$  is rational (respectively algebraic).*

This conjecture, in the case of rational power series, is a particular case of Conjecture 8.2 (which has, to my knowledge, no algebraic analogue).

**Remark 4.6.** *There is perhaps some hope for proving this conjecture in the rational case using the formulae of the proof of Proposition 3.5: Considering integral lifts into suitable algebraic integers and assuming a bound on the degrees of the numerator and denominator of  $\sigma^{-1}(A)$  (for rational  $A \in 1 + X\overline{\mathbb{F}_2}[[X]]$ ) one gets a system of algebraic equations whose reduction modulo 2 should have a solution.*

## 4.2 Orbits in $1 + X\overline{\mathbb{F}_2}[[X]]$ of $\sigma$

The purpose of this Section is to describe a few properties of the bijection defined by  $\sigma$  on  $1 + X\overline{\mathbb{F}_2}[[X]]$ .

**Proposition 4.7.** (i) *The orbit of  $A \in 1 + X\overline{\mathbb{F}_2}[[X]]$  is infinite if it involves a monomial of the form  $X^{2^k}$ .*

(ii) *The orbit of a polynomial  $A \in 1 + X\overline{\mathbb{F}_2}[X]$  is finite if it involves no monomial of the form  $X^{2^k}$ .*

(iii) *The cardinal of every finite orbit in  $1 + X\overline{\mathbb{F}_2}[[X]]$  of  $\sigma$  is a power of 2.*

**Remark 4.8.** (i) *All elements of the form  $1 + X^3\overline{\mathbb{F}_2}[[X^2]]$  are fixed by  $\sigma$ , cf. Remark 4.4.*

(ii) *The algebraic function  $A = 1 + \sum_{n=0}^{\infty} X^{3 \cdot 4^n}$  (satisfying the equation  $A + A^4 + X^3 = 0$ ) contains no monomial of the form  $X^{2^k}$  and has infinite orbit under  $\sigma$ . I ignore if the affine subspace  $1 + X\overline{\mathbb{F}_2}[[X]]$  contains an infinite orbit formed by rational fractions without monomials of the form  $X^{2^k}$ .*

**Proof of Proposition 4.7** Associate to  $A = 1 + \sum_{n=1}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$  the auxiliary series  $P_A = \sum_{n=0}^{\infty} \alpha_{2^n} t^n \in \mathbb{F}_2[[t]]$ . It is easy to check that  $P_{\sigma^k(A)} = (1+t)^k P_A$  for all  $k \in \mathbb{Z}$ . This implies assertion (i).

Consider a polynomial  $A$  containing only coefficients of degree  $< 2^n$  and no coefficient of degree a power of 2. The formula for  $\sigma(A)$  shows that  $\sigma(A)$  satisfies the same conditions. This implies that the orbit of  $A$  under  $\sigma$  is finite and proves assertion (ii).

If  $A \in 1 + \overline{\mathbb{F}_2}[[X]]$  is such that  $\sigma^{2^k}(A) \equiv A \pmod{X^{N-1}}$ , then  $\sigma^{2^k}(A + X^N) = \sigma^{2^k}(A) + X^N \pmod{X^{N+1}}$ . This implies easily the last assertion.  $\square$

## 4.3 A variation

The series  $P_A = \sum_{n=0}^{\infty} \alpha_{2^n} t^n$  associated to an algebraic power series  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$  as in the proof of proposition 4.7 is always ultimately periodic and thus rational. This implies algebraicity of  $\sum_{n=0}^{\infty} \alpha_{2^n} X^{2^{n+1}}$  for algebraic  $\sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$ . The properties of the quadratic form

$$A = \sum_{n=0}^{\infty} \alpha_n X^n \longmapsto \tilde{\sigma}(A) = \sum_{0 \leq i \leq j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j}$$

with respect to algebraic elements in  $\overline{\mathbb{F}_2}[[X]]$  should thus be somewhat similar to the properties of  $\sigma$ . In particular  $\tilde{\sigma}$  preserves algebraic series and induces a bijection on  $1 + X\overline{\mathbb{F}_2}[[X]]$  which is of infinite order. Orbits are either infinite or finite and the cardinality of a finite orbit is a power of 2. Conjecture 4.5 (if true), together with Proposition 3.7, would imply that  $\tilde{\sigma}^{-1}(A)$  is algebraic for algebraic  $A \in 1 + X\overline{\mathbb{F}_2}[[X]]$ . Remark however that



$\tilde{\sigma}(A)$  is in general not rational for rational  $A \in 1 + X\overline{\mathbb{F}_2}[[X]]$ : An easy computation shows indeed that  $\tilde{\sigma}(\frac{1}{1+X}) = 1 + \sum_{n=0}^{\infty} X^{2^n}$  which satisfies the algebraic equation  $y+y^2+X=0$  but is irrational since coefficients of rational power series over  $\overline{\mathbb{F}_p}$  are ultimately periodic. On the other hand,  $\tilde{\sigma}^{-1}(\frac{1}{1+X})$  is the irrational algebraic series  $y = 1 + X + X^2 + X^4 + X^7 + \dots \in \mathbb{F}_2[[X]]$  satisfying the equation

$$X + (1 + X + X^2)y + (1 + X^2 + X^4)y^3 = 0 .$$

The quadratic map  $\tilde{\sigma}$  behaves however better than  $\sigma$  with respect to polynomials: One can show easily that it induces a bijection of order a power of 2 (depending on  $n$ ) on polynomials of degree  $< 2^n$  in  $1 + X\overline{\mathbb{F}_2}[[X]]$ .

**Remark 4.9.** *The definition of the quadratic forms  $\sigma$  and  $\tilde{\sigma}$  suggests to consider the quadratic form  $\psi(\sum_{n=0}^{\infty} \alpha_n X^n) = \sum_{i < j} \alpha_i \alpha_j X^{i+j}$  of  $\overline{\mathbb{F}_2}[[X]]$ . Using the fact that rational elements of  $\overline{\mathbb{F}_2}[[X]]$  have ultimately periodic coefficients, it is not hard to show that  $\psi$  preserves rationality. It is also easy to show that  $\psi$  induces a bijection on  $1 + X\overline{\mathbb{F}_2}[[X]]$ . However  $\psi^{-1}(1 + X)$  is apparently neither rational nor algebraic in  $\mathbb{F}_2[[X]]$ .*

#### 4.4 Algorithmic aspects

The *integral Thue-Morse* function  $tm(\sum_{j=0}^{\infty} \epsilon_j 2^j) = \sum_j \epsilon_j$  is defined as the digit sum of a natural binary integer  $n = \sum_{j=0}^{\infty} \epsilon_j 2^j \in \mathbb{N}$ . Setting  $tm(0) = 0$ , it can then be computed recursively by  $tm(2n) = tm(n)$  and  $tm(2n+1) = 1 + tm(n)$ . Kummer's equality  $\binom{i+j}{i} \equiv 2^{tm(i)+tm(j)-tm(i+j)} \pmod{2}$  (which follows also from a Theorem of Lucas, see page 422 of [2]), allows a fast computation of binomial coefficients modulo 2. We have thus

$$\begin{aligned} \sigma(A) &= \alpha_0^2 + \sum_{n=0}^{\infty} \alpha_{2^n}^2 X^{2^{n+1}} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j} \\ &= \alpha_0^2 + \sum_{n=0}^{\infty} \alpha_{2^n}^2 X^{2^{n+1}} + \sum_{0 \leq i < j, tm(i+j)=tm(i)+tm(j)} \alpha_i \alpha_j X^{i+j} \end{aligned}$$

for  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \mathbb{F}_2[[x]]$ . The last formula is suitable for computations.

The preimage  $\sigma^{-1}(A)$  of  $A \in 1 + X\overline{\mathbb{F}_2}[[X]]$  can be computed iteratively as the unique fixpoint in  $\overline{\mathbb{F}_2}[[X]]$  of the map

$$Z \longmapsto Z + A - \sigma(Z) .$$

Starting with an arbitrary initial value  $Z_0$  (eg. with  $Z_0 = A$ ), the sequence  $Z_0, Z_1, \dots, Z_{n+1} = Z_n + A - \sigma(Z_n), \dots \in \overline{\mathbb{F}_2}[[X]]$  converges quadratically (roughly doubling the number of correct coefficients at each iteration) with limit the attractive fixpoint  $\sigma^{-1}(A)$ .

#### 4.4.1 Checking identities in the rational case

Define the degree of a non-zero rational fraction  $A = \frac{f}{g} \in \overline{\mathbb{F}_2}[[X]]$  with  $f \in \overline{\mathbb{F}_2}[X], g \in 1 + \overline{\mathbb{F}_2}[X]$  coprime, by  $\deg(A) = \max(\deg(f), \deg(g))$ . Proposition 8.1 and Remark 7.1 imply the equality

$$\deg(\sigma(A)) \leq 1 + \binom{\deg(A) + 2}{2}.$$

This inequality can be used to prove identities of the form  $\sigma(A) = B$  involving two rational fractions  $A, B \in \overline{\mathbb{F}_2}[X]$  by checking equality of the first  $2 + \binom{\deg(A)+2}{2} + \deg(B)$  coefficients of the series  $\sigma(A)$  and  $B$ .

#### 4.4.2 Checking identities in the algebraic case

Given a power series  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$ , we consider the power series  $A_{k,f} = \sum_{n=0}^{\infty} \alpha_{k+n \cdot 2^f} X^n$  for  $k, f \in \mathbb{N}$  such that  $0 \leq k < 2^f$ . The vector space  $\mathcal{K}(A)$  (called the 2-kernel of  $A$ , see [2]) spanned by all series  $A_{k,f}$  is finite-dimensional if and only if  $A$  is algebraic and one has the inequality

$$\dim(\mathcal{K}(\sigma(A))) \leq 1 + \binom{1 + \dim(\mathcal{K}(A))}{2}.$$

This inequality, together with techniques of [3], reduces the proof of equalities  $\sigma(A) = B$  involving algebraic series  $A, B \in \overline{\mathbb{F}_2}[[X]]$  to the equality among finite series developpements of sufficiently high order  $N$  (depending on combinatorial properties) of  $A$  and  $B$ . The typical value for  $N$  is of order  $2^{2 + \binom{1 + \dim(\mathcal{K}(A))}{2}}$  and is thus unfortunately of no practical value in most cases.

### 4.5 Examples involving rational fractions in $1 + \mathbb{F}_2[[X]]$

#### 4.5.1 A few preimages of polynomials

$$\begin{aligned} \sigma^{-1}(1+X) &= \frac{1}{1+X}, \sigma^{-1}((1+X)^3) = 1+X+X^3, \sigma^{-1}((1+X)^5) = (1+X)^2(1+X+X^2)(1+X^2+X^3), \\ \sigma^{-1}((1+X)^7) &= \frac{1+X^3+X^6}{(1+X)^7}, \sigma^{-1}((1+X)^9) = (1+X)^6(1+X+X^9), \\ \sigma^{-1}(1+X+X^2) &= 1+X, \sigma^{-1}(1+X^2+X^3) = \frac{1+X^2+X^3}{(1+X)^4}, \\ \sigma^{-1}(1+X+X^3) &= \frac{1+X+X^2}{(1+X)^4}, \sigma^{-1}(1+X+X^4) = 1+X+X^2+X^3, \\ \sigma^{-1}(1+X^3+X^4) &= \frac{1+X+X^2}{(1+X)^3}, \sigma^{-1}(1+X+X^2+X^3+X^4) = \frac{1+X+X^3}{(1+X)^4}, \\ \sigma^{-1}(1+X+X^2+X^3+X^5) &= (1+X)(1+X^3+X^4), \sigma^{-1}(1+X+X^3+X^4+X^5) = (1+X+X^2+X^5+X^7), \\ \sigma^{-1}(1+X^2+X^3+X^4+X^5) &= (1+X+X^3)(1+X+X^4), \\ \sigma^{-1}(1+X^2+X^5) &= \frac{(1+X+X^2)(1+X+X^3)}{(1+X)^6}, \sigma^{-1}(1+X+X^2+X^4+X^5) = \frac{(1+X+X^4)}{(1+X)^8}, \\ \sigma^{-1}((1+X+X^2)^3) &= \frac{1+X^2+X^3}{(1+X)^7}, \sigma^{-1}((1+X)(1+X+X^2)) = (1+X)(1+X+X^2), \\ \sigma^{-1}((1+X)^2(1+X+X^2)) &= (1+X+X^2), \sigma^{-1}((1+X)^3(1+X+X^2)) = \frac{1+X^3+X^4}{(1+X)^6}, \\ \sigma^{-1}((1+X)^4(1+X+X^2)) &= \frac{1+X+X^4+X^6+X^7}{(1+X)^8}, \end{aligned}$$

These examples suggest the following conjecture:

**Conjecture 4.10.** For  $P \in 1 + X\mathbb{F}_2[X]$  a polynomial of degree  $\leq 2^k$ , we have  $\sigma^{-1}(P) = \frac{Q_P}{(1+X)^{\alpha_P}}$  with  $0 \leq \alpha_P \leq 2^k$  and  $Q_P \in 1 + X\mathbb{F}_2[X]$  a polynomial of degree  $< 2^k$ .

#### 4.5.2 A few examples of rational fractions

$$\begin{aligned} \sigma^{-1}\left(\frac{1}{(1+X)^3}\right) &= \frac{(1+X)^2(1+X+X^4)}{(1+X+X^2)^4}, \sigma^{-1}\left(\frac{1}{1+X+X^2}\right) = \frac{(1+X)^3}{1+X^3+X^4}, \sigma^{-1}\left(\frac{1+X}{1+X+X^2}\right) = \\ &= \frac{(1+X)^2}{1+X^3+X^4}, \sigma^{-1}\left(\frac{1+X+X^2}{1+X}\right) = \frac{1+X}{1+X+X^2}, \sigma^{-1}\left(\frac{1+X+X^2}{(1+X)^2}\right) = \frac{1+X+X^3}{(1+X)^2}, \sigma^{-1}\left(\frac{1+X+X^2}{(1+X)^3}\right) = \\ &= \frac{1+X^3+X^7}{(1+X+X^2)^4}, \sigma^{-1}\left(\frac{1+X+X^2}{(1+X)^4}\right) = \frac{(1+X+X^3)(1+X^3+X^4)}{(1+X+X^2)^4}, \\ \sigma^{-1}\left(\frac{1+X+X^2}{(1+X)^5}\right) &= \frac{1+X+X^2+X^3+X^4+X^5+X^6+X^{12}+X^{13}}{(1+X+X^2)^7}, \sigma^{-1}\left(\frac{(1+X+X^2)^2}{1+X}\right) = \frac{1+X+X^2+X^3+X^4}{(1+X+X^2)^4}, \\ \sigma^{-1}\left(\frac{(1+X+X^2)^2}{(1+X)^3}\right) &= \frac{(1+X+X^2)(1+X^2+X^5)}{(1+X)^4}. \end{aligned}$$

#### 4.6 A few iterations of $\sigma$ and $\sigma^{-1}$ on rational fractions in $1 + X\mathbb{F}_2[X]$

##### 4.6.1 Example

Iterating  $\sigma^{-1}$  on  $1 + x$  yields the following rational fractions given by their simplest expression, corresponding not necessarily to the complete factorisation into irreducible polynomials of their numerators and denominators (such a factorisation makes sense when working in the multiplicative algebra  $\mathbb{F}_2[[X]]$  and is probably irrelevant for the map  $\sigma$ , related to the shuffle algebra structure  $(\mathbb{F}_2[[X]], \text{III})$ ).

$$\begin{aligned} \sigma^{-1}(1+X) &= \frac{1}{1+X} \\ \sigma^{-2}(1+X) &= \frac{1}{1+X+X^2} \\ \sigma^{-3}(1+X) &= \frac{(1+X)^3}{1+X^3+X^4} \\ \sigma^{-4}(1+X) &= \frac{1+X+X^4+X^5+X^7}{1+X^4+X^6+X^7+X^8} \\ \sigma^{-5}(1+X) &= \frac{1+X+X^2+X^3+X^4+X^5+X^7+X^8+X^{14}}{1+X^{15}+X^{16}} \\ \sigma^{-6}(1+X) &= \frac{(1+X)^2(1+X+X^2+X^{14}+X^{17}+X^{20}+X^{21}+X^{24}+X^{25}+X^{26}+X^{29})}{1+X^{16}+X^{30}+X^{31}+X^{32}} \end{aligned}$$

### 4.6.2 Example

Iterating  $\sigma^{-1}$  or  $\sigma$  on  $\frac{1+X+X^2}{(1+X)^2} = 1 + X + X^3 + X^5 + X^7 + \dots$  yields the following results (not necessarily completely factored into irreducibles):

$$\begin{aligned} \sigma^{-4} \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^3+X^5+X^6+X^8+X^9+X^{10}+X^{13}+X^{14}}{1+X^8+X^{12}+X^{14}+X^{16}} \\ \sigma^{-3} \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^2+X^3+X^5}{(1+X^3+X^4)^2} \\ \sigma^{-2} \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{(1+X)^3}{(1+X+X^2)^2} \\ \sigma^{-1} \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^3}{(1+X)^2} \\ \sigma^1 \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^4}{(1+X)^2} \\ \sigma^2 \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^8}{(1+X)^4} \\ \sigma^3 \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^2+X^4+X^{10}+X^{12}+X^{16}}{(1+X)^8} \\ \sigma^4 \left( \frac{1+X+X^2}{(1+X)^2} \right) &= \frac{1+X+X^3+X^5+X^6+X^{10}+X^{11}+X^{12}+X^{13}+X^{22}+X^{26}+X^{28}+X^{32}}{(1+X)^{16}} \end{aligned}$$

### 4.6.3 Example

Iterating  $\sigma^{-1}$  on  $\frac{1}{1+X+X^3}$  yields the following (not necessarily completely factored) rational fractions:

$$\begin{aligned} \sigma^{-3} \left( \frac{1}{1+X+X^3} \right) &= \frac{(1+X+X^2+X^4+X^6+X^{12}+X^{15})(1+X^2+X^5+X^6+X^{10}+X^{12}+X^{15})}{1+X^{24}+X^{28}+X^{31}+X^{32}} \\ \sigma^{-2} \left( \frac{1}{1+X+X^3} \right) &= \frac{1+X+X^2+X^3+X^5+X^8+X^{10}+X^{11}+X^{15}}{1+X^8+X^{14}+X^{15}+X^{16}} \\ \sigma^{-1} \left( \frac{1}{1+X+X^3} \right) &= \frac{(1+X)^5}{1+X^7+X^8} \\ \sigma^1 \left( \frac{1}{1+X+X^3} \right) &= \frac{1+X+X^2+X^3+X^4}{1+X^2+X^3} \\ \sigma^2 \left( \frac{1}{1+X+X^3} \right) &= \frac{1+X+X^2+X^3+X^4+X^6+X^8}{(1+X^2+X^3)^2} \\ \sigma^3 \left( \frac{1}{1+X+X^3} \right) &= \frac{1+X+X^4+X^5+X^6+X^8+X^9+X^{10}+X^{12}+X^{13}+X^{14}+X^{16}}{(1+X^2+X^3)^4} \\ \sigma^4 \left( \frac{1}{1+X+X^3} \right) &= \frac{P_4}{(1+X^2+X^3)^8} \end{aligned}$$

**Remark 4.11.** Define the degree of a rational fraction  $A \in \mathbb{F}_2[[x]]$  as  $\deg(A) = \max(\deg(f), \deg(g))$  if  $A = \frac{f}{g}$  with  $f, g \in \mathbb{F}_2[x]$  without common factor. For rational  $A \in 1 + X\mathbb{F}_2[[X]]$  we have  $\lim_{n \rightarrow \pm\infty} \frac{1}{|n|} \log(\deg(\sigma^n A)) = 0$  if the orbit of  $A$  under  $\sigma$  is finite. The three examples of Section 4.6 suggest that this limit exists (it equals  $\log(2)$ ) for these examples). It would be interesting to prove the existence of this limit (or to exhibit a counterexample) for an arbitrary rational fraction  $A \in 1 + \mathbb{F}_2[[X]]$ . Since we have clearly  $\lim_{n \rightarrow \infty} \frac{1}{n} \log(\deg(\sigma^n(A))) = \log(2)$  for  $A \in \mathbb{F}_2[X]$  a polynomial with infinite orbit, one can also ask for the existence of values  $\neq 0, \log(2)$  for this limit which defines obviously an invariant of orbits under the bijection  $\sigma$  on rational fractions in  $1 + \mathbb{F}_2[[X]]$ .

## 4.7 Examples with algebraic series in $1 + X\mathbb{F}_2[[X]]$

An algebraic power series  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_2}[[X]]$  can be conveniently described by a basis of the finite-dimensional vector space  $\mathcal{K}(A)$  introduced in Section 4.4.2. More precisely, given a word  $\epsilon_1 \dots \epsilon_l \in \{0, 1\}^l$  of finite length  $l \in \mathbb{N}$ , we consider the power series

$$A_{\epsilon_1, \dots, \epsilon_l} = \sum_{n=0}^{\infty} \alpha_{n2^l + \sum_{j=1}^l \epsilon_j 2^{j-1}} X^n.$$

Properties of the Frobenius map imply the identity

$$A_{\epsilon_1, \dots, \epsilon_l} = A_{\epsilon_1, \dots, \epsilon_l 0}^2 + X A_{\epsilon_1, \dots, \epsilon_l 1}^2$$

This can be used for fairly compact descriptions of algebraic series in  $\mathbb{F}_2[[X]]$  as illustrated by a few examples below.

The defining polynomial of an algebraic series  $A \in \mathbb{F}_2[[X]]$  can be of degree  $2^{\dim(\mathcal{K}(A))}$  in the variable  $A$ . One can recover a defining polynomial for  $A$  by applying an algorithm for Gröbner bases to polynomials associated to linear dependencies in  $\mathcal{K}(A)$ .

### 4.7.1 Example

The preimage  $z = \sigma^{-1}(1 + \sum_{n=0}^{\infty} X^{2^n})$  satisfies the polynomial equation  $1 + (1 + X)z^3 = 0$ .

### 4.7.2 Example

Consider the algebraic series  $y = 1 + \sum_{n=0}^{\infty} X^{3 \cdot 4^n}$  satisfying  $y + y^4 + X^3 = 0$  already considered in Remark 4.8. The series  $z = \sigma^{-1}(y)$  satisfies the algebraic equation  $1 + (1 + X^3)z^3$ .

### 4.7.3 Example

Consider the algebraic power series  $y = \sum_{n=0}^{\infty} X^{2^n - 1} = 1 + X + X^3 + X^7 + X^{15} + X^{31} + \dots \in \mathbb{F}_2[[X]]$  satisfying the polynomial equation  $1 + y + Xy^2 = 0$ . The formal power series  $z = \sigma^{-1}(y) = 1 + X + X^2 + \dots$  satisfies the algebraic equation

$$1 + X^2 + X^3 + (1 + X)^4 z + X(1 + X)^4 z^2 = 0$$

and is given by

$$z = \frac{1}{1 + X} + X^3 \left( \sum_{n=0}^{\infty} (tm(n) + tm(n + 1)) X^n \right)^4 \in \mathbb{F}_2[[X]]$$

where  $tm\left(\sum_{j=0}^{\infty} \epsilon_j 2^j\right) = \sum_{j=0}^{\infty} \epsilon_j$  is the Thue-Morse sequence (see also [1] for the sequence  $n \mapsto tm(n) + tm(n + 1) \pmod{2}$ ).

**Remark 4.12.** For all  $n \in \mathbb{N}$ , one can show that  $\sigma^n(y) = y + P_n(X)$  with  $P_n(X) \in \mathbb{F}_2[X]$  a polynomial where  $y = \sum_{n=0}^{\infty} X^{2^n-1}$ . (The series  $\sigma^n(y)$  is of course algebraic for all  $n \in \mathbb{N}$ , see Proposition 4.1.)

#### 4.7.4 Example

Consider the algebraic power series  $y = \sum_{n=0}^{\infty} tm(n+1)X^n = 1 + x + x^3 + x^6 + \dots \in \mathbb{F}_2[[X]]$  (satisfying  $(1 + (1+x)^2)y + x(1+x)^3y^2 = 0$ ) related to the Thue-Morse sequence. The preimage  $z = \sigma^{-1}(y)$  yields the algebraic system of equations

$$\begin{aligned} z &= z_0^2 + Xz_1^2 \\ z_0 &= z_0^2 + Xz_{01}^2 \\ z_1 &= z_{10}^2 + Xz_{11}^2 \\ z_{01} &= z_{01}^2 + X(z_0 + z_{10})^2 \\ z_{10} &= z_{10}^2 + X(z_0 + z_1 + z_{01} + z_{11})^2 = z_1 + X(z_0 + z_1 + z_{01})^2 \\ z_{11} &= (z_1 + z_{10} + z_{11})^2 + X(z_{01} + z_{10} + z_{11})^2 = z_1 + (z_1 + z_{11})^2 + X(z_{01} + z_{10})^2 \end{aligned}$$

#### 4.7.5 Example

Consider the algebraic series  $y = \sigma^{-1}(\sum_{n=0}^{\infty} (tm(n) + tm(n+1))X^n) \in \mathbb{F}_2[[X]]$  (satisfying  $1 + (1+X)y + X(1+X)y^2 = 0$ ). The preimage  $z = \sigma^{-1}(y) \in \mathbb{F}_2[[X]]$  satisfies the algebraic system of equations:

$$\begin{aligned} z &= z_0^2 + Xz_1^2, \\ z_0 &= z_{00}^2 + Xz_0^2, \\ z_1 &= Xz_{11}^2, \\ z_{00} &= z_0^2 + X(z_0 + z_{00})^2, \\ z_{11} &= z_{00}^2 + X(z_0 + z_1 + z_{00})^2 \end{aligned}$$

which, together with the constant terms  $z(0) = z_0(0) = z_{00}(0) = z_{11}(0) = 1, z_1(0) = 0$ , determines the series  $z, z_0 = \frac{1}{1+X+X^2}, z_1, z_{00} = \frac{1+X}{1+X+X^2}, z_{11} = z + \frac{X^2(1+X)}{(1+X+X^2)^2}$  uniquely. Eliminating the series  $z_0, z_1, z_{00}, z_{11}$  by Gröbner-basis techniques produces the algebraic equation

$$1 + X^2 + X^6 + X^{10} + X^{11} + X^{12} + X^{15} + (1+X+X^2)^8 z + X^3(1+X+X^2)^8 z^4 = 0$$

for  $z$ .

#### 4.7.6 Example

The series  $y = \sum_{n=0}^{\infty} \binom{3n}{n} X^n \in \mathbb{F}_2[[X]]$  satisfies the algebraic equation  $y = 1 + Xy^3$  (cf. page 423 of [2]). Its preimage  $z = \sigma^{-1}(y)$  gives rise to the

algebraic system

$$\begin{aligned}
z &= z_0^2 + Xz_1^2, \\
z_0 &= z^2 + Xz_{01}^2, \\
z_1 &= z_{10}^2 + Xz_{11}^2, \\
z_{01} &= z_{010}^2 + Xz_{011}^2, \\
z_{10} &= (z_0 + z_{010})^2 + Xz_{011}^2 &= z_{01} + z_0^2, \\
z_{11} &= z_{010}^2 &= (1 + X)^2 z^4 + z_1^2, \\
z_{010} &= (z + z_{10})^2 + X(z + z_{11})^2 &= (1 + X)z^2 + z_1, \\
z_{011} &= (z + z_{10})^2 + X(z_{01} + z_{10})^2
\end{aligned}$$

## 5 Other primes

There exists an analogue of the quadratic map  $\sigma : \overline{\mathbb{F}_2}[[x]] \longrightarrow \overline{\mathbb{F}_2}[[x]]$  for  $p$  an arbitrary prime. It corresponds to the  $p$ -homogenous form (still denoted)  $\sigma : \overline{\mathbb{F}_p}[[X]] \longrightarrow \overline{\mathbb{F}_p}[[X]]$  defined by

$$\sigma(A) \equiv \tilde{\alpha}_0^p + \sum_{n=1}^{\infty} \tilde{\beta}_n X^n \pmod{p}$$

for  $A = \sum_{n=0}^{\infty} \alpha_n X^n \in \overline{\mathbb{F}_p}[[X]]$  with  $\sum_{n=1}^{\infty} \tilde{\beta}_n X^n \in X\overline{\mathbb{Q}}[[X]]$  given by the equality

$$\tilde{A}^{\text{III}^p} = \tilde{\alpha}_0^p + p \left( \sum_{n=1}^{\infty} \tilde{\beta}_n X^n \right)$$

for  $\tilde{A} \in \overline{\mathbb{Q}}[[X]]$  an integral lift of  $A \equiv \tilde{A} \pmod{p}$ .

The  $p$ -homogeneous form  $\sigma$  restricts to a bijection of  $1 + X\overline{\mathbb{F}_p}[[X]]$  and shares most properties holding for  $p = 2$ . In particular, we have:

**Proposition 5.1.** *The formal power series  $\sigma(A)$  is rational (respectively algebraic) if  $A \in \overline{\mathbb{F}_p}[[X]]$  is rational (respectively algebraic).*

**Conjecture 5.2.** *If  $A \in 1 + \overline{\mathbb{F}_p}[[X]]$  is rational (respectively algebraic) then its preimage  $\sigma^{-1}(A)$  is rational (respectively algebraic).*

### 5.1 A few examples for $p = 3$

Values of  $\sigma^{-1}(A) \in \mathbb{F}_3[[X]]$  for a few rational  $A \in 1 + X\mathbb{F}_3[[X]]$  are:

$$\begin{aligned}
\sigma^{-1}(1 + X) &= \frac{1}{1-X}, \quad \sigma^{-1}((1 + X)^2) = \frac{1-X-X^2}{(1+X)^3}, \quad \sigma^{-1}\left(\frac{1}{1+X}\right) = \frac{(1+X)^2}{1-X^2+X^3}, \\
\sigma^{-1}\left(\frac{1}{(1+X)^2}\right) &= \frac{1+X+X^2-X^4+X^5+X^7+X^8}{(1-X^2+X^3)^3}, \quad \sigma^{-1}\left(\frac{1+X}{1-X}\right) = \frac{1-X-X^2}{1-X^2+X^3}, \quad \sigma^{-1}\left(\frac{1+X}{1+X^2}\right) = \\
&= \frac{(1-X)^2}{(1+X)(1-X-X^2)}.
\end{aligned}$$

### 5.1.1 Two algebraic examples for $p = 3$

The algebraic series  $\sum_{n=0}^{\infty} X^{3^n-1} = 1 + X^2 + X^8 + X^{26} + \dots$  is fixed by  $\sigma$ .

The preimage  $z = \sigma^{-1}(1 + \sum_{n=0}^{\infty} X^{3^n})$  satisfies the polynomial equation  $(1 + X)^3(1 - X)z^{13} - 1$ . (The power series  $y = 1 + \sum_{n=0}^{\infty} X^{3^n} \in \mathbb{F}_3[[X]]$  satisfies the algebraic equation  $y = X + y^3$ .)

### 5.2 A few rational examples for $p = 5$

We give here values of  $\sigma^{-1}(A) \in \mathbb{F}_5[[X]]$  for a few rational  $A \in 1 + X\mathbb{F}_5[[X]]$ :

$$\begin{aligned} \sigma^{-1}(1 + X) &= \frac{1}{1-X}, \quad \sigma^{-1}((1 + X)^2) = \frac{(1-X)(1+2X)(1+X+X^2)}{(1-2X)^5}, \quad \sigma^{-1}((1 + X)^3) \\ &= \frac{(1-2X)(1+2X^2-X^3)}{(1+2X)^5}, \quad \sigma^{-1}\left(\frac{1}{1+X}\right) = \frac{(1-2X)(1+X-X^2-2X^3)}{1-X^4+X^5}, \quad \sigma^{-1}\left(\frac{1}{(1+X)^2}\right) \\ &= \frac{1-2X+2X^2+2X^4+2X^5-2X^6-2X^7-X^8+X^9+X^{11}-2X^{13}-2X^{14}-2X^{15}-X^{16}+X^{18}+X^{19}-2X^{21}+X^{24}}{(1-X^4+X^5)^5}, \\ \sigma^{-1}\left(\frac{1+X}{1-X}\right) &= \frac{1+2X+X^2+2X^3-2X^4}{1-X^4-2X^5}, \quad \sigma^{-1}\left(\frac{1+X}{1-2X}\right) = \frac{1-2X-2X^3}{1-X^4+2X^5}, \quad \sigma^{-1}\left(\frac{1+X}{1+2X}\right) = \\ &= \frac{1-X-2X^2-X^3-2X^4}{1-X^4+X^5}. \end{aligned}$$

## 6 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 [5], [4] or a similar book on the subject. Our terminology, motivated by [3], differs however sometimes in the next section.

We denote by  $\mathcal{X}^*$  the free monoid on a set  $\mathcal{X} = \{X_1, \dots, X_k\}$ . 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

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

a non-commutative formal power series where

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

stands for the coefficient function.

A formal power series  $A \in \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  is invertible with respect to the obvious non-commutative product if and only if it has non-zero constant coefficient. We denote by  $\mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  the maximal ideal consisting of formal power series without constant coefficient and by  $\mathbb{K}^* + \mathfrak{m}$  the *unit-group* of the algebra  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  which is thus the non-commutative multiplicative group consisting of all (multiplicatively) invertible elements in  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$ . 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 spanned 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  $1 - a \in 1 + \mathfrak{m}$ .

## 6.1 The shuffle algebra

The *shuffle-product*  $\mathbf{X} \text{III} \mathbf{X}'$  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  $\deg(X_1) = \dots = \deg(X_k) = 1$ ) is the sum of all  $\binom{a+b}{a}$  monomials of degree  $a+b$  obtained by “shuffling” in every possible way the linear factors of  $\mathbf{X}$  with the linear factors of  $\mathbf{X}'$ . Such a monomial contribution to  $\mathbf{X} \text{III} \mathbf{X}'$  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  $\mathbf{X} \text{III} \mathbf{X}'$  can also be recursively defined by  $\mathbf{X} \text{III} 1 = 1 \text{III} \mathbf{X} = \mathbf{X}$  and

$$(\mathbf{X} X_s) \text{III} (\mathbf{X}' X_t) = (\mathbf{X} \text{III} (\mathbf{X}' X_t)) X_s + ((\mathbf{X} X_s) \text{III} \mathbf{X}') X_t$$

for linear monomials  $X_s, X_t \in \mathcal{X} = \{X_1, \dots, X_k\}$ .

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

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

Identifying all variables  $X_j$  of a formal power series  $A \in \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  with a common variable  $X$  yields a homomorphism of algebras (respectively shuffle-algebras) from  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  into the commutative algebra (respectively into the shuffle-algebra)  $\mathbb{K}[[X]]$ .

The commutative unit group (set of invertible elements for the shuffle-product) of the shuffle algebra is given by the set  $\mathbb{K}^* + \mathfrak{m}$  and is isomorphic to the direct product  $\mathbb{K}^* \times (1 + \mathfrak{m})$ . The inverse of an element  $1 - a \in 1 + \mathfrak{m}$  is given by  $\sum_{n=0}^{\infty} a^{\text{III}^n} = 1 + a + a \text{III} a + a \text{III} a \text{III} a + \dots$ , cf. Remark 3.2.

The following result generalises Proposition 3.3:

**Proposition 6.1.** *Over a field of positive characteristic  $p$ , the subgroup  $1 + \mathfrak{m}$  of the shuffle-group is an  $\mathbb{F}_p$ -vector space of infinite dimension.*

**Proof** Contributions to a  $p$ -fold shuffle product  $A_1 \text{III} A_2 \text{III} \dots \text{III} A_p$  are given by monomials with linear factors coloured by  $p$  colours  $\{1, \dots, p\}$  keeping track of their “origin” with coefficients given by the product of the corresponding “monochromatic” coefficients in  $A_1, \dots, A_p$ . A permutation of the colours  $\{1, \dots, p\}$  (and in particular, a cyclic permutation of all colours) leaves these products invariant if  $A_1 = \dots = A_p$ . Forgetting the colours, coefficients of degree  $> 0$  in  $A^{\text{III}^p}$  are thus zero in characteristic  $p$ .  $\square$

## 7 Rational formal power series

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

The (generalised) *Hadamard matrix*  $H = H(A)$  of

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

is the infinite matrix with rows and columns indexed by the free monoid  $\mathcal{X}^*$  of monomials and entries  $H_{\mathbf{X}\mathbf{X}'} = (A, \mathbf{X}\mathbf{X}')$ . According to [3], we call the rank  $\text{rank}(H) \in \mathbb{N} \cup \{\infty\}$  the *complexity* of  $A$ . The row-span, denoted by  $\overline{A}$ , of  $H$  is the *recursive closure* of  $A$ . It corresponds to the syntactic ideal of [4] and its dimension  $\dim(\overline{A})$  is the complexity of  $A$ .

**Remark 7.1.** *In the case of one variable, the complexity  $\dim(\overline{A})$  of a non-zero rational fraction  $A = \frac{f}{g}$  with  $f \in \mathbb{K}[X]$  and  $g \in 1 + X\mathbb{K}[X]$  is given by  $\dim(\overline{A}) = \max(1 + \deg(f), \deg(g))$ .*

Rational series coincide with series of finite complexity by a Theorem of Schützenberger (cf. [4], Theorem 1 of page 22).

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

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

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

the linear application which associates to  $A = \sum_{\mathbf{X} \in \mathcal{X}^*} (A, \mathbf{X}) \mathbf{X} \in \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  the formal power series  $\rho(\mathbf{T})A = \sum_{\mathbf{X} \in \mathcal{X}^*} (A, \mathbf{X}\mathbf{T}) \mathbf{X}$ . We have  $\rho(\mathbf{T})\rho(\mathbf{T}') = \rho(\mathbf{T}\mathbf{T}')$ . It is easy to check that the set  $\{\rho(\mathbf{T})A\}_{\mathbf{T} \in \mathcal{X}^*}$  spans the recursive closure  $\overline{A}$  of a power series  $A$ .

**Theorem 7.2.** *We have the inclusion*

$$\overline{A \amalg B} \subset \overline{A} \amalg \overline{B}$$

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

**Corollary 7.3.** *We have*

$$\dim(\overline{A \amalg B}) \leq \dim(\overline{A}) \dim(\overline{B})$$

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

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

**Proof of Theorem 7.2** The shuffle product  $A\text{III}B$  is clearly contained in the vector space

$$\overline{A\text{III}B} = \{Y\text{III}Z \mid Y \in \overline{A}, Z \in \overline{B}\}.$$

For  $Y \in \overline{A}, Z \in \overline{B}$  and  $X_s \in \mathcal{X} = \{X_1, \dots, X_k\}$ , the recursive definition of the shuffle product given in Section 6.1 shows

$$\rho(X_s)(Y\text{III}Z) = (\rho(X_s)Y)\text{III}Z + Y\text{III}(\rho(X_s)Z) \in \overline{A\text{III}Z} + \overline{Y\text{III}B} \subset \overline{A\text{III}B}$$

and the vector space  $\overline{A\text{III}B}$  is thus recursively closed.  $\square$

**Remark 7.4.** *Similar arguments show that the set of rational series is also closed under the ordinary product, Hadamard product and composition (where one considers  $A \circ (B_1, \dots, B_k)$  with  $A \in \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  and  $B_1, \dots, B_k \in \mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$ ).*

**Remark 7.5.** *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*

$$\frac{1}{1 - \sum_{j=1}^k \lambda_j X_j} \text{III} \frac{1}{1 - \sum_{j=1}^k \mu_j X_j} = \frac{1}{1 - \sum_{j=1}^k (\lambda_j + \mu_j) X_j}.$$

(As shown by Remark 3.1, this identity corresponds to the equality  $e^{\lambda X} e^{\mu X} = e^{(\lambda+\mu)X}$  in the case of a unique variable  $X = X_1$ .)

By Remark 3.9, there are no other such elements in  $1 + \mathfrak{m}$  in the case of a unique variable  $X = X_1$ . I ignore if the maximal rational shuffle subgroup of  $1 + \mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  (defined as the set of all rational elements in  $1 + \mathfrak{m}$  with rational inverse for the shuffle product) contains other elements if  $k \geq 2$  and if  $\mathbb{K}$  is a suitable field of characteristic 0.

**Remark 7.6.** *Any finite set of rational elements in  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  over a field  $\mathbb{K}$  of positive characteristic is contained in a unique minimal finite-dimensional recursively closed subspace of  $\mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  which intersects the shuffle group  $\mathbb{K}^* + \mathfrak{m}$  in a subgroup.*

## 8 The $p$ -homogeneous form $\sigma : \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle \longrightarrow \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$

Considering an integral lift  $\tilde{A} = \tilde{\alpha} + \tilde{a} \in \overline{\mathbb{Q}}\langle\langle X_1, \dots, X_k \rangle\rangle$  with coefficients in algebraic integers of  $A = \alpha + a \in \alpha + \mathfrak{m} \subset \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ , we define  $\sigma(A)$  by the reduction of  $\tilde{\alpha}^p + \tilde{b}$  modulo  $p$  where

$$\tilde{A}^{\text{III}p} = \tilde{\alpha}^p + p\tilde{b} \in \tilde{\alpha}^p + \mathfrak{m} \subset \overline{\mathbb{Q}}\langle\langle X_1, \dots, X_k \rangle\rangle.$$

This definition corresponds to the definition of  $\sigma$  given in Section 5 in the case of one variable  $X = X_1$ .

**Proposition 8.1.** *One has*

$$\dim(\overline{\sigma(A)}) \leq 1 + \binom{\dim(\overline{A}) + p - 1}{p}$$

for  $A \in \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ .

*In particular,  $\sigma(A)$  is rational for rational  $A \in \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ .*

**Proof** It is always possible to choose an integral lift  $\tilde{A} \in \overline{\mathbb{Q}}\langle\langle X_1, \dots, X_k \rangle\rangle$  of  $A \in \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$  such that  $\dim(\overline{\tilde{A}}) = \dim(\overline{A})$ . The inclusion

$$\overline{(\tilde{A}^{\text{III}^p})} \subset \overline{(\tilde{A})}^{\text{III}^p}$$

implies then easily the result.  $\square$

It is easy to show that  $\sigma$  induces a bijection on the subset  $1 + \mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$  for a field  $\mathbb{K} \subset \overline{\mathbb{F}_p}$ . Computations of a few examples in  $\mathbb{F}_2\langle\langle X_1, X_2 \rangle\rangle$  suggest:

**Conjecture 8.2.** *The formal power series  $\sigma^{-1}(A)$  is rational for rational  $A \in 1 + \mathfrak{m} \subset \overline{\mathbb{F}_p}\langle\langle X_1, \dots, X_k \rangle\rangle$ .*

**Acknowledgements** I thank J-P. Allouche, P. Arnoux, M. Brion, A. Pantchichkine, T. Rivoal, J. Sakarovitch, B. Venkov and J-L. Verger-Gaugry for their interest and helpful remarks.

## References

- [1] J-P. Allouche, A. Arnold, J. Berstel, S. Brlek, W. Jockusch, S. Plouffe, B.E. Sagan, *A relative of the Thue-Morse Sequence*, Discr. Math. **139** (1995), 455-461.
- [2] J.-P. Allouche, J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press (2003).
- [3] R. Bacher, *Recurrence matrices*, in preparation, an unfinished draft is on the arXiv.
- [4] J. Berstel, C. Reutenauer, *Les séries rationnelles et leurs langages*, Masson (1984).
- [5] 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](mailto:Roland.Bacher@ujf-grenoble.fr)