ON THE ALGEBRAICITY OF THUE-MORSE AND PERIOD-DOUBLING CONTINUED FRACTIONS

YINING HU AND GUO-NIU HAN

Abstract. The link between automaticity and algebraicity is well established concerning power series in finite characteristics, decimal expansion and continued fraction expansion of real numbers. But the question of whether continued fractions (objects in $\mathbb{F}_q[[1/x]]$) defined by automatic sequences taking values in $\mathbb{F}_q[x]$ are algebraic is still wide open and little studied. In this article we approach this problem by investigating the cases of two classical automatic sequences, namely the Thue-Morse and period-doubling sequences. For each sequence, there are infinitely many cases because of the choice of polynomials representing the terms of the sequence. We present our Guess'n'Prove method, which is implemented to give computer generated proofs of particular instances. We believe our method works for the general case and put forward conjectures.

1. Introduction

1.1. **Background.** We are interested in the continued fractions and Stieltjes continued fractions defined by automatic sequences in finite characteristic, and more precisely their algebraicity or transcendence. We give here the background and motivation for studying such problems. The definitions of related notions will be given in subsection 1.2.

The link between automaticity and algebraicity goes back to the well-known Theorem of Christol, Kamae, Mendès France and Rauzy [9, 10] which states that a formal power series in $\mathbb{F}_q[[x]]$ is algebraic over $\mathbb{F}_q(x)$ if and only if the sequence of its coefficients is q-automatic. The situation is completely different for real numbers. In 2007, Adamczewski and Bugeaud [1] proved that for an integer $b \geq 2$, if the b-ary expansion of an irrational real number ξ forms an automatic sequence, then ξ must be transcendental. In 2013, Bugeaud [8] proved that the continued fraction expansion of an algebraic real number of degree at least 3 is not automatic.

As with real numbers, a formal Laurent series can also be represented by a continued fraction whose partial quotients are polynomials. Unlike for real numbers, the continued fraction expansion of an algebraic Laurent series of degree at least 3 may or may not have automatic partial quotients [5, 6, 18, 3, 19, 14, 15, 16]; see also the introduction of [13].

We could also ask the converse question: what can we say about the algebraicity of a continued fraction whose partial quotients form an automatic sequence? To our knowledge, little has been done in this direction. The authors [13] proved that the

Date: February 3, 2022.

2010 *Mathematics Subject Classification.* 11B85, 11J70, 11B50, 11Y65, 05A15, 11T55.

Key words and phrases. algebraicity, automatic sequence, continued fraction, Thue-Morse sequence.

This work was partially supported by NNSF of China (Grant No. 12001216).

Stieltjes continued fractions defined by the Thue-Morse sequence and the period-doubling sequence in $\mathbb{Z}[[x]]$ are congruent, modulo 4, to algebraic series in $\mathbb{Z}[[x]]$. In 2020, Wu [21] obtained similar results concerning the Stieltjes continued fractions defined by the paperfolding sequence and the Golay-Shapiro-Rudin sequence.

In this article we propose to approach this problem with two classical examples of automatic sequences, the Thue-Morse sequence and the period-doubling sequence. In the real case, the transcendence of the real Thue-Morse continued fraction was first proved by Queffelec [20] in 1998 and a short proof was given by Adamczewski and Bugeaud [2] in 2007.

1.2. **Preliminaries.** We introduce the necessary notions for stating the conjectures and our main results.

1.2.1. *Automatic sequnces.* A sequence is said to be *k-automatic* if it can be generated by a k-DFAO (*deterministic finite automaton with output*). For an integer $k \geq 2$, a k-DFAO is defined to be a 6-tuple

$$M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$$

where Q is the set of states with $q_0 \in Q$ being the initial state, $\Sigma = \{0, 1, \ldots, k-1\}$ the input alphabet, $\delta : Q \times \Sigma \to Q$ the transition function, Δ the output alphabet, and $\tau : Q \to \Delta$ the output function. The k-DFAO M generates a sequence $(c_n)_{n\geq 0}$ in the following way: for each non-negative integer n, the base-k expansion of n is read by M from right to left starting from the initial state q_0, and the automaton moves from state to state according to its transition function δ. When the end of the string is reached, the automaton halts in a state q, and the automaton outputs the symbol $c_n = \tau(q)$.

A necessary and sufficient condition [11] for a sequence to be k-automatic is that its *k-kernel*, defined as the set of subsequences

$$\{(u_{k^d n+j})_{n\geq 0} \mid d \in \mathbb{N},\, 0 \leq j \leq k^d - 1\},$$

is finite. If we let $\Lambda_i^{(k)}$ denote the operator that sends a sequence $(u(n))_{n\geq 0}$ to its subsequence $(u(kn+i))_{n\geq 0}$, then the k-kernel can be defined alternatively as the smallest set containing $\mathbf{u}$ that is stable under $\Lambda_i^{(k)}$ for $0 \leq i < k$. We write Λ_i instead of $\Lambda_i^{(k)}$ when the value of k is clear from the context. We will use the fact that for an integer $m \geq 1$, a sequence is k-automatic if and only if it is k^m-automatic [11].

For a k-automatic sequence $\mathbf{u}$, we can construct a k-DFAO that generates it from its k-kernel. The set of states Q will be in bijection with the k-kernel, so we choose to identify them. For $q \in Q$ and $0 \leq j < k$, the value of the transition function $\delta(q, j)$ is defined as $\Lambda_j q$; the output function τ maps q to the 0-th term of the subsequence in the k-kernel corresponding to q. This automaton has the property that leading 0's in the input does not change the output. It is minimal among k-automata with this property that generates $\mathbf{u}$.

We refer the readers to [4] for a comprehensive exposition of automatic sequences.

In this article we will consider the Thue-Morse sequence and the period-doubling sequence. For two distinct elements a and b from an alphabet, the (a, b)-Thue-Morse sequence is the sequence $\mathbf{t}$ defined as the fixed point $\tau^\infty(a)$ of the substitution $\tau : a \mapsto ab,\ b \mapsto ba$, that is, it is the limit of the sequence $(\tau^j(a))_j$

$$\tau(a) = ab$$

$$\tau^2(a) = abba$$
$$\tau^3(a) = abbabaab$$
$$\tau^4(a) = abbabaabbaababba$$
$$\dots$$

When $(a,b) = (0,1) \in \mathbb{F}_2^2$, the minimal polynomial of the generating series $f(x) = \sum_{n=0}^{\infty} t_n x^n$ is

$$(1+x)^3 f^2 + (1+x)^2 f + x = 0.$$

The (a,b)-period-doubling sequence $\mathbf{p}$ is defined as the fixed point $\sigma(a)$ of the substitution $\sigma : a \mapsto ab,\ b \mapsto aa$. Its first terms are

$$abaaababababaabaa\dots$$

When $(a,b) = (0,1) \in \mathbb{F}_2^2$, the minimal polynomial of the generating series $g(x) = \sum_{n=0}^{\infty} p_n x^n$ is

$$(x^3+x)g^2 + (x^2+1)g + x = 0.$$

From the minimal polymonials we see that the generating series $f(x)$ and $g(x)$ are quadratic.

1.2.2. *Continued fractions.* Let K be a field. Given a sequence of polynomials $a_j(z) \in K[z] \backslash K$, we may define the infinite continued fraction

$$\mathrm{CF}(\mathbf{a}(z)) := \cfrac{1}{a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \cfrac{1}{\ddots}}}} \tag{1.1}$$

as the limit of the finite continued fractions

$$\mathrm{CF}_n(\mathbf{a}(z)) = \cfrac{1}{a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{\ddots + \cfrac{1}{a_n(z)}}}} \in K((1/z)). \tag{1.2}$$

Note that here the index of the partial quotients begins with 0. The existence of the limit is guaranteed by the convergence theorem, whose proof is completely analogous to that for the classical continued fractions with positive integer partial quotients.

Define the sequences $(P_n(z))$ and $(Q_n(z))$ by

$$\begin{pmatrix} P_n(z) & Q_n(z) \\ P_{n-1}(z) & Q_{n-1}(z) \end{pmatrix} := \begin{pmatrix} a_n(z) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1}(z) & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0(z) & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.3}$$

for $n \geq 0$, then

$$\mathrm{CF}_n(\mathbf{a}(z)) = P_n(z)/Q_n(z) \in K((1/z)),$$

for $n \geq 0$. Note that here rational fractions are expanded in $1/z$. The fraction $P_n(z)/Q_n(z)$ is called the n-th *convergent* of $\mathrm{CF}(\mathbf{a}(z))$. All convergents are reduced fractions: to be convinced of this, simply take the determinant of both sides of (1.3).

Conversely, let

$$f(z) = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_0 + c_{-1} z^{-1} + \cdots \tag{1.4}$$

be an arbitrary element of $K((1/z))$. Define the integer part of $f(z)$ as

$$[f(z)] = c_n z^n + c_{n-1} z^{n-1} + \cdots + c_0. \tag{1.5}$$

Set $f_0 = f$, $a_0 = [f_0]$, $f_0 = a_0 + 1/f_1$, $a_1 = [f_1]$, $f_1 = a_1 + 1/f_2$, $a_2 = [f_1]$, ... Then $a_0 \in K[z]$ and $a_j \in K[z]\backslash K$ for $j \geq 1$, and $f(z)$ admits the following continued fraction expansion

$$f(z) = a_0(z) + \cfrac{1}{a_1(z) + \cfrac{1}{a_2(z) + \cfrac{1}{a_3(z) + \cfrac{1}{\ddots}}}}. \tag{1.6}$$

1.2.3. *Stieltjes continued fractions.* Let $(u_j)_{j\geq 0}$ be a sequence taking values in $K^\times$, then the Stieltjes continued fraction

$$\mathrm{Stiel}(x; \mathbf{u}) := \cfrac{u_0}{1 + \cfrac{u_1 x}{1 + \cfrac{u_2 x}{1 + \cfrac{u_3 x}{\ddots}}}} \tag{1.7}$$

is defined to be the limit of the finite Stieltjes continued fractions

$$\mathrm{Stiel}_n(x; \mathbf{u}) := \cfrac{u_0}{1 + \cfrac{u_1 x}{1 + \cfrac{u_2 x}{\ddots \cfrac{}{1 + \cfrac{}{1 + u_n x}}}}} \in K[[x]]. \tag{1.8}$$

It can be easily shown that the sequence $\mathrm{Stiel}_n(x; \mathbf{u})$ is convergent.

Define the sequence $(P_n(x))$ and $(Q_n(x))$ by

$$\begin{pmatrix} P_n(x) & Q_n(x) \\ P_{n-1}(x) & Q_{n-1}(x) \end{pmatrix} := \begin{pmatrix} 1 & u_n x \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & u_{n-1} x \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & u_0 x \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1/x & 0 \end{pmatrix} \tag{1.9}$$

for $n \geq 0$. Then

$$\mathrm{Stiel}_n(x; \mathbf{u}) = \frac{P_n(x)}{Q_n(x)},$$

for $n \geq 0$. The non-reduced fraction $P_n(x)/Q_n(x)$ is called the n-th *convergent* of $\mathrm{Stiel}(x; \mathbf{u})$.

It should be noted that while every formal power series in $K[[x]]$ can be expanded as a continued fraction, only a subset can be expanded as a Stieltjes continued fractions.

1.3. **Conjectures and main results.** We put forward the following conjectures concerning the Thue-Morse and period-doubling continued fractions and Stieltjes continued fractions.

Conjecture 1.1. *Let a, b be two distinct elements from $\mathbb{F}_2[z]\backslash\mathbb{F}_2$. Let $\mathbf{u}(z)$ be the (a,b)-Thue-Morse sequence. The continued fraction $\mathrm{CF}(\mathbf{u}(z))$ is algebraic of degree 4 over $\mathbb{F}_2(z)$.*

Theorem 1.2. *Conjecture 1.1 holds for every distinct elements a, b in $\mathbb{F}_2[z]\backslash\mathbb{F}_2$ with $\deg a + \deg b \leq 7$.*

A more precise statement is given in Theorem 2.1 for the pair $(a, b) = (z, z^2 + z + 1)$.

Conjecture 1.3. *Let $k \geq 2$ be an integer. Let a, b be two distinct elements from $\mathbb{F}_{2^k}^{\times}$. Let $\mathbf{u}$ be the (a,b)-Thue-Morse sequence. The Stieltjes continued fraction $\mathrm{Stiel}(x;\mathbf{u})$ is algebraic over $\mathbb{F}_{2^k}(x)$. Its minimal polynomial is*

$$p_0(x) + p_1(x)y + p_2(x)y^2 + p_4(x)y^4,$$

where

$$\begin{aligned} p_0(x) &= ((a^2b^4 + b^6)/a^4)x^2 + b^5/(a^5 + a^4b), \\ p_1(x) &= ((ab^4 + b^5)/a^5)x + b^4/a^5, \\ p_2(x) &= (b^4/a^5)x + b^4/(a^6 + a^5b), \\ p_4(x) &= (b^4/(a^6 + a^5b))x^2. \end{aligned}$$

Theorem 1.4. *Conjecture 1.3 holds for $k = 2, 3, 4$.*

Based on our calculation, we believe that the period-doubling continued fractions are also algebraic. However, the period-doubling Stieltjes continued fractions seem to be transcendental.

Conjecture 1.5. *Let a, b be two distinct elements from $\mathbb{F}_2[z]\backslash\mathbb{F}_2$. Let $\mathbf{u}(z)$ be the (a,b)-period-doubling sequence. The continued fraction $\mathrm{CF}(\mathbf{u}(z))$ is algebraic of degree 4 over $\mathbb{F}_2(z)$.*

Theorem 1.6. *Let $(a, b) = (z^3, z^2 + z + 1) \in (\mathbb{F}_2[z]\backslash\mathbb{F}_2)^2$. Let $\mathbf{p}$ be the (a,b)-period-doubling sequence. The power series $\mathrm{CF}(\mathbf{p}(z))$ is algebraic over $\mathbb{F}_2(z)$; its minimal polynomial is*

$$y^4 + (z^5 + z^4 + z^3)y^2 + (z^8 + z^6 + z^5 + z^3)y + z^5 + z^3 + z^2 = 0.$$

Conjecture 1.7. *Let $J \in \mathbf{F}_4\backslash\{0, 1\}$. Let $\mathbf{u}$ be the $(1, J)$-period-doubling sequence. The Stieltjes continued fraction $\mathrm{Stiel}(x;\mathbf{u})$ is transcendental over $\mathbb{F}_2(x)$.*

1.4. **Method.** For the verification of conjectures 1.1 and 1.3a, we use the Guess 'n' Prove method. We refer the reader to [12] and to [17] where the Guess 'n' Prove method is used in the context of automatic sequences and continued fractions, respectively, even though the techniques involved are different.

Initially we were able to prove by hand some special cases of 1.1, each in a different way. Then we develop a method that works for all these cases. We implemented this method in SageMath, and checked by computer that conjecture 1.1 holds for all pairs (a, b) of elements from $\mathbb{F}_2[z]\backslash\mathbb{F}_2$ such that $\deg a + \deg b \leq 7$, and that conjecture 1.3a holds for all $a \in \mathbb{F}_{2^k}\backslash\{0, 1\}$ for $k = 2, 3, 4$. This method

cannot be used to prove directly conjecture 1.3b, because in this version of the conjecture, the coefficients of the power series lie in $\mathbb{F}_2(a)$, which is not a finite field, and therefore the algorithm described in Section 5 would not terminate.

For conjecture 1.1, our program takes the pair (a, b) as input, and, for the (a, b)-Thue-Morse sequence $\mathbf{u}$, uses the Derksen algorithm for Padé-Hermite approximants (we implemented the version of the Derksen algorithm described in [7]) to guess the minimal polynomial of $\mathrm{CF}(\mathbf{u}(z))$. If the guess does not stabilize as we increase the precision, then the program exits with an error message. To prove that the guess is correct, it only needs to prove the algebraicity of 16 auxiliary series. For this, it first guesses the algebraic equations of these 16 series. Then it guesses and proves several lemmas concerning the properties of 16 series defined by the guessed algebraic equations and relations between these algebraic series and the auxiliary series (namely that they are the same). The particular forms of the lemmas depend on the choice of (a, b). In Section 2 we illustrate our method with an example of computer generated proof. The proofs for the other pairs that we have tested can be found on the personal web page of the authors [1].

For conjecture 1.3a (an equivalent formulation of conjecture 1.3, specified in Section 3), the situation is similar, except that we choose to regard a as a formal variable whenever we can. In this way we prepare a common part for all a, and to prove that conjecture 1.3a holds for a certain a, we only need to fill in the rest of the proof for this specific a.

In the proofs, we exploit the structure of the automata that generates the algebraic series in question. The automata are used in the following way: the infinitely many conditions (because of the infinitely many values of $\mathbf{u}$) on the series in lemma 2.4 and lemma 4.2 are translated to finitely many conditions on the automata, which we could check directly. To obtain a k-automaton of an algebraic series from an annihilating polynomial of it, we implement an algorithm based on the proof of theorem 1 of [10]. In Section 5 we describe this algorithm for self-containedness.

Our method for checking conjecture 1.1 can be adapted for the verification of conjecture 1.5. We give an example in Section 4. We believe that our method works for every case of conjecture 1.5 as well, even though the proofs are slightly more complicated because the shape of the blocks in lemma 4.2 and lemma 4.3 are less regular than that in lemma 2.4 and lemma 2.5.

Concerning the efficiency of the verification, once we observe patterns like those found in lemma 2.4 and lemma 2.5, we are almost certain that our method works for this case, and this step is very fast. But we still need to give a rigorous proof, and the proofs for the equivalent of lemma 2.4 and lemma 2.3 become too slow as the degree goes up.

We also investigated some other automatic sequences, but the continued fractions that they define seem to be transcendental, or maybe more terms than our computers can handle are needed for the Dersken algorithm to have a correct guess.

[1] `http://irma.math.unistra.fr/~guoniu/frconj/`

2. Thue-Morse Continued Fraction

Our program tests conjecture 1.1 for a given pair of distinct elements (a, b) from $\mathbb{F}_2[z]\setminus\mathbb{F}_2$. We have checked that the conjecture holds in the case where $\deg a + \deg b \leq 7$.

The following is an example of proof that conjecture 1.1 holds for $(a, b) = (z, z^2+z+1)$. Both the statement of the theorem and its proof are generated automatically by our program. The exact statement of theorem 2.1, lemma 2.4 and 2.5 depends on the choice of (a, b). In the proof, for a series $f(x) = \sum_{j=0}^{\infty} f_j x^j$, the notation $f[m : n]$ means $\sum_{j=m}^{n-1} f_j x^j$ and $f[: n]$ means $\sum_{j=0}^{n-1} f_j x^j$.

2.1. Statement of the theorem for $(a, b) = (z, z^2 + z + 1)$.

Theorem 2.1. *Let $(a, b) = (z, z^2 + z + 1) \in (\mathbb{F}_2[z]\setminus\mathbb{F}_2)^2$. Let $\mathbf{t}$ be the (a, b)-Thue-Morse sequence, and $\bar{\mathbf{t}}$, the (b, a)-Thue-Morse sequence. The two power series $\mathrm{CF}(\mathbf{t}(z))$ and $\mathrm{CF}(\bar{\mathbf{t}}(z))$ are algebraic over $\mathbb{F}_2(z)$, with minimal polynomials of the form*

$$p_4(z)y^4 + p_3(z)y^3 + p_2(z)y^2 + p_1(z)y + p_0(z) = 0.$$

For $\mathrm{CF}(\mathbf{t}(z))$

$$\begin{aligned}
p_0(z) &= z^9 + z^7 + z^6 + z^5 + z^4 + z + 1,\\
p_1(z) &= z^{11} + z^{10} + z^8 + z^6 + z^5 + z^3 + z^2 + z,\\
p_2(z) &= z^{12} + z^{10} + z^2,\\
p_3(z) &= z^{11} + z^{10} + z^8 + z^6 + z^5 + z^3 + z^2 + z,\\
p_4(z) &= z^{10} + z^9 + z^7 + z^6 + z^5 + z^2 + z,
\end{aligned}$$

and for $\mathrm{CF}(\bar{\mathbf{t}}(z))$

$$\begin{aligned}
p_0(z) &= z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z,\\
p_1(z) &= z^{11} + z^{10} + z^8 + z^6 + z^5 + z^3 + z^2 + z,\\
p_2(z) &= z^{12} + z^{10} + z^2,\\
p_3(z) &= z^{11} + z^{10} + z^8 + z^6 + z^5 + z^3 + z^2 + z,\\
p_4(z) &= z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^2 + z + 1.
\end{aligned}$$

2.2. Proof.

Define

$$M_n(x) = x^{\deg(t_{2^n-1})}\begin{pmatrix} t_{2^n-1}(1/x) & 1\\ 1 & 0\end{pmatrix} x^{\deg(t_{2^n-2})}\begin{pmatrix} t_{2^n-2}(1/x) & 1\\ 1 & 0\end{pmatrix}\cdots x^{\deg(t_0)}\begin{pmatrix} t_0(1/x) & 1\\ 1 & 0\end{pmatrix}$$

and

$$W_n(x) = x^{\deg(\bar{t}_{2^n-1})}\begin{pmatrix} \bar{t}_{2^n-1}(1/x) & 1\\ 1 & 0\end{pmatrix} x^{\deg(\bar{t}_{2^n-2})}\begin{pmatrix} \bar{t}_{2^n-2}(1/x) & 1\\ 1 & 0\end{pmatrix}\cdots x^{\deg(\bar{t}_0)}\begin{pmatrix} \bar{t}_0(1/x) & 1\\ 1 & 0\end{pmatrix}$$

where $\bar{\mathbf{t}}$ is the (b,a)-Thue-Morse sequence. By the property of the Thue-Morse sequence, we have for all $n \geq 0$

$$M_{n+1}(x) = W_n(x) \cdot M_n(x),$$
$$W_{n+1}(x) = M_n(x) \cdot W_n(x).$$

Define $x := 1/z$. For an non-zero polynomial $P(z)$, we define $\tilde{P}(x)$ to be $P(1/x)$. Then

$$\mathrm{CF}_n(\mathbf{t}(z)) = \frac{P_n(z)}{Q_n(z)} = \frac{\tilde{P}_n(x)}{\tilde{Q}_n(x)} \in \mathbb{F}_2((x)) = \mathbb{F}_2((1/z)).$$

Comparing the definition of $M_n(x)$ with definition (1.3), we see that

$$M_n(x)_{0,1} = x^{d_n}\tilde{P}_{2^n-1}(x),$$
$$M_n(x)_{0,0} = x^{d_n}\tilde{Q}_{2^n-1}(x),$$

for some positive integer d_n, and

$$\mathrm{CF}_{2^{2n}-1}(\mathbf{t}(z)) = \frac{\tilde{P}_{2^{2n}-1}(x)}{\tilde{Q}_{2^{2n}-1}(x)} = \frac{M_{2n}(x)_{0,1}}{M_{2n}(x)_{0,0}}. \tag{2.1}$$

Our strategy is to first prove that both $M_{2n}(x)_{0,1}$ and $M_{2n}(x)_{0,0}$ converge to algebraic series in $\mathbb{F}_2[[x]]$, and then use their minimal polynomials to obtain that of $\mathrm{CF}_n(\mathbf{t}(z))$.

Actually, we will prove that for all i,j in $\{0,1\}$, the four sequences $(M_{2n}(x)_{i,j})_n$, $(M_{2n+1}(x)_{i,j})_n$, $(W_{2n}(x)_{i,j})_n$, and $(W_{2n+1}(x)_{i,j})_n$ converge to algebraic series in $\mathbb{F}_2[[x]]$. For this purpose, we define four 2×2 matrices M^e, M^o, W^e, W^o as follows: For each $T \in \{M^e, M^o, W^e, W^o\}$ and i,j in $\{0,1\}$, $T_{i,j}$ is defined to be the unique root in $\mathbb{F}_2[[x]]$ of the polynomial $\phi(T,i,j)$ with prescribed first terms of its expansion.

All 16 polynomials are of the form

$$p_0(x) + p_3(x)y^3 + p_6(x)y^6 + p_9(x)y^9 + p_{12}(x)y^{12},$$

and the 8 first terms of $T_{i,j}$ suffice to determine a unique root.

We give the explicit form $\phi(M^e,0,0)$ below; the others can be found on the web page of the authors.

$$\begin{aligned}
p_0(x) &= x^{66}+x^{64}+x^{62}+x^{60}+x^{58}+x^{56}+x^{52}+x^{50}+x^{36}+x^{32}+x^{30}\\
&\quad +x^{20}+x^{16}+x^{14}+x^{12},\\
p_3(x) &= x^{62}+x^{60}+x^{58}+x^{56}+x^{52}+x^{50}+x^{48}+x^{44}+x^{42}+x^{38}+x^{36}\\
&\quad +x^{32}+x^{28}+x^{22}+x^{20}+x^{18}+x^{14}+x^{12},\\
p_6(x) &= x^{56}+x^{44}+x^{40}+x^{38}+x^{36}+x^{32}+x^{30}+x^{26}+x^{20}+x^{18}+x^{16}\\
&\quad +x^{14}+x^{2}+1,\\
p_9(x) &= x^{64}+x^{62}+x^{58}+x^{56}+x^{54}+x^{52}+x^{48}+x^{42}+x^{32}+x^{30}+x^{26}\\
&\quad +x^{20}+x^{18}+x^{14}+x^{12}+x^{10}+x^{8}+x^{2},\\
p_{12}(x) &= x^{64}+x^{56}+x^{40}+x^{32}+x^{16}+x^{8}+1,
\end{aligned}$$

and the first terms of $M^e_{0,0}$ are $1+x^8+x^{10}+x^{14}+x^{20}+\cdots$. In order to uniquely determine the root, we only need to know that $M^e_{0,0} = 1+O(x^8)$.

We will prove that these four matrices, whose components are algebraic by definition, are the limits of $(M_{2n}(x))_n$, $(M_{2n+1}(x))_n$, $(W_{2n}(x))_n$, and $(W_{2n+1}(x))_n$.

Let us explain how the polynomials $\phi(T,i,j)$ are found, and how many first terms are to be specified in order to guarantee the existence and unicity of the root. For i,j in $\{0,1\}$, the the coefficients of the polynomial $\phi(M^e,i,j)$ (resp. $\phi(M^o,i,j)$, $\phi(W^e,i,j)$, and $\phi(W^o,i,j)$) are the Padé-Hermite approximants of type

$$(75,75,75,75,75)$$

of the vector

$$(1,f^3,f^6,f^9,f^{12}),$$

where $f = M_{12,i,j}$ (resp. $M_{11,i,j}$, $W_{12,i,j}$, and $W_{11,i,j}$). See Chapter 7 of [7] for a description of the Derksen algorithm that is used here to find the Padé-Hermite approximants. These 16 polynomials together with the first 8 terms of the corresponding polynomial f satisfy the conditions of the following lemma, so that the root exists and is unique.

Lemma 2.2. *Let $P(x,y)$ be a polynomial in $\mathbb{F}_2[x,y]$. If for some polynomial $\sum_{j=0}^{n-1} a_j x^j$ in $\mathbb{F}_2[x]$, $P(x,\sum_{j=0}^{n-1} a_j x^j) = O(x^n)$ and $Q(x,y) := P(x,\sum_{j=0}^{n-1} a_j x^j + x^n y)$ can be written as $x^m \sum_{j=0}^{N} q_j(x) y^j$ where m and N are integers and $q_j(x)$ are polynomials for $j \geq 0$, $q_1(0) = 1$, and $q_j(0) = 0$ for $j > 1$, then there exists a unique series $f(x) \in \mathbb{F}_2[[x]]$ whose first terms are $\sum_{j=0}^{n-1} a_j x^j$ and $P(x,f(x)) = 0$.*

Proof. The conclusion of the lemma can be rephrased as: there is a unique series $g(x)$ in $\mathbb{F}_2[[x]]$ such that $P(x,\sum_{j=0}^{n-1} a_j x^j + x^n g(x)) = 0$. But this is equivalent to saying that $g(x)$ is the unique root of $Q(x,y)$, and therefore of the polynomial

$$\sum_{j=0}^{N} q_j(x) y^j.$$

Let us plug in the expression of $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots$ in the above polynomial. We get

$$q_0(x) + q_1(x)(g_0 + g_1 x + g_2 x^2 + \cdots) + \cdots + q_N(x)(g_0 + g_1 x + g_2 x^2 + \cdots)^N = 0.$$

For all integer n, let c_n denote the coefficient of x^n in the left hand side of the above identity, then c_n is a polynomial of $g_0, g_1, \ldots, g_n$. The condition $q_j(0) = 0$ for $j > 1$ implies that there is only one term in c_n that contains g_n, namely $q_1(0) g_n$, and this term is not zero because $q_1(0) = 1$. This shows that g_n can be expressed in terms of $g_0, g_1, \ldots, g_{n-1}$ and $q_0(x), q_1(x), \ldots, q_N(x)$. Thus we have established the existence and unicity of $g(x)$, and therefore that of $f(x)$. □

We state two lemmas concerning the four matrices M^e, M^o, W^e, W^o. The first one is about relations between them; the second, about the structure of each matrix.

Lemma 2.3. *We have*

$$M^e = W^o \cdot M^o, \tag{2.2}$$

$$M^o = W^e \cdot M^e, \tag{2.3}$$

$$W^e = M^o \cdot W^o, \tag{2.4}$$

$$W^o = M^e \cdot W^e. \tag{2.5}$$

Proof. We give the proof of the identity

$$M^e_{0,0} = W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0},$$

the proofs of the others being similar.

First, we compute the minimal polynomials of $W^o_{0,0}M^o_{0,0}$ and $W^o_{0,1}M^o_{1,0}$. We know that

$$P(x,y) = \mathrm{Res}_z\left(\phi(W^o,0,0)(x,z),\ z^{12}\cdot\phi(M^o,0,0)(x,y/z)\right)$$

is an annihilating polynomial of $W^o_{0,0}M^o_{0,0}$; here Res_z means the resultant with respect to the variable z (see Chapter 6 of [7]). We use Padé-Hermite approximation to find a candidate for the minimal polynomial of $W^o_{0,0}M^o_{0,0}$, that will be called $\phi_0(x,y)$. To prove that $\phi_0(x,y)$ is indeed the minimal polynomial, it suffices to prove that it is an irreducible factor of $P(x,y)$ of multiplicity m and that $Q(x,y) := P(x,y)/\phi_0(x,y)^m$ is not an annihilating polynomial of $W^o_{0,0}M^o_{0,0}$. We verify the first point directly. For the second point, we truncate $W^o_{0,0}M^o_{0,0}$ to order 270 and substitute it for y in $Q(x,y)$. We get a series of valuation less than 270, which proves that $Q(x,y)$ is not an annihilating polynomial of $W^o_{0,0}M^o_{0,0}$. We find the minimal polynomial $\phi_1(x,y)$ of $W^o_{0,1}M^o_{1,0}$ in a similar way.

Now we prove that $\phi(M^e,0,0)$ is the minimal polynomial of $W^o_{0,0}M^o_{0,0}+W^o_{0,1}M^o_{1,0}$. We know that

$$S(x,y) = \mathrm{Res}_z\left(\phi_0(x,z),\ \phi_1(x,y+z)\right)$$

is an annihilating polynomial of $W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0}$. We verify that $\phi(M^e,0,0)$ is an irreducible factor of $S(x,y)$ of multiplicity μ, and that the quotient $Q(x,y) := S(x,y)/\phi(M^e,0,0)^\mu$ is not an annihilating polynomial of $W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0}$. To see the last point, we truncate $W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0}$ to order 330 and substitute it for y in $Q(x,y)$. We get a series of valuation less than 330, and therefore $Q(x,y)$ is not an annihilating polynomial of $W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0}$.

Finally, the first 8 terms of $M^e_{0,0}$ and $W^o_{0,0}M^o_{0,0} + W^o_{0,1}M^o_{1,0}$ coincide. As these first terms determine a unique root of $\phi(M^e,0,0)$, we know that the two series are one and the same. □

Define

$$R^e = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad \text{and} \qquad R^o = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Lemma 2.4. *For all integers $k \geq 2$ and $u = 2^{2k-1}$, the following identities hold.*

$$\begin{aligned}
M^e[:6u] &= M^e[:3u] + x^u M^e[:2u] + x^u M^e[:3u] + x^{2u}M^e[:2u] + x^{2u}M^e[:3u]\\
&\quad + x^{3u}M^e[:2u] + (x^{3u}+x^{4u}+x^{5u})R^e,\\
W^e[:6u] &= W^e[:3u] + x^u W^e[:2u] + x^u W^e[:3u] + x^{2u}W^e[:2u] + x^{2u}W^e[:3u]\\
&\quad + x^{3u}W^e[:2u] + (x^{3u}+x^{4u}+x^{5u})R^e.
\end{aligned}$$

For all integers $k \geq 2$ and $u = 2^{2k}$,

$$\begin{aligned}
M^o[:6u] &= M^o[:3u] + x^u M^o[:2u] + x^u M^o[:3u] + x^{2u}M^o[:2u] + x^{2u}M^o[:3u]\\
&\quad + x^{3u}M^o[:2u] + (x^{3u}+x^{4u}+x^{5u})R^o,\\
W^o[:6u] &= W^o[:3u] + x^u W^o[:2u] + x^u W^o[:3u] + x^{2u}W^o[:2u] + x^{2u}W^o[:3u]\\
&\quad + x^{3u}W^o[:2u] + (x^{3u}+x^{4u}+x^{5u})R^o.
\end{aligned}$$

Proof. To prove Lemma 2.4 we first construct an automaton for each sequence concerned, and then transform the conditions on infinitely many k's into finitely many conditions on the states of the automaton. In the following, we will prove that for $T = M^o_{1,0}$, for all integer $k \geq 2$ and $u = 2^{2k}$,

$$T[:6u] = T[:3u] + x^u T[:2u] + x^u T[:3u] + x^{2u} T[:2u] + x^{2u} T[:3u] + x^{3u} T[:2u].$$

The proofs of the other 15 cases are similar. Being in characteristic 2, sums of the same segment of T cancel out, so that we may break down the above identity into 3 parts:

$$\begin{aligned} 0 &= x^{3u} T[:u] + x^u T[2u:3u] + T[3u:4u], \\ 0 &= x^{3u} T[u:2u] + x^{2u} T[2u:3u] + T[4u:5u], \\ 0 &= T[5u:6u], \end{aligned}$$

which can be rewritten as

$$0 = T[[w]_2] + T[[10w]_2] + T[[11w]_2], \tag{2.6}$$

$$0 = T[[1w]_2] + T[[10w]_2] + T[[100w]_2], \tag{2.7}$$

$$0 = T[[101w]_2], \tag{2.8}$$

for all binary words w of length $2k$, where $[w]_2$ denotes the integer whose binary expansion is w.

First we calculate a 2-automaton that generates T from its minimal polynomial and its first terms. This automaton has 124 states; its transition function and output function can be found on the web page of the authors. Let $A(s, w)$ denote the state reached after reading w from right to left starting from the state s, and τ the output function. Let i be the initial state. Define

$$E_{2k} = \{A(i, w) : |w| = 2k\}.$$

Identities (2.6) through (2.8) can be written as

$$0 = \tau(A(s, \epsilon)) + \tau(A(s, 10)) + \tau(A(s, 11)), \tag{2.9}$$

$$0 = \tau(A(s, 1)) + \tau(A(s, 10)) + \tau(A(s, 100)), \tag{2.10}$$

$$0 = \tau(A(s, 101)) \tag{2.11}$$

for all $s \in E_{2k}$. We find that $(A(i, 0^{24}), E_{24}) = (A(i, 0^{16}), E_{16})$, so that we only have to verify that identities (2.9) through (2.11) hold for $2 \leq k \leq 12$, which turns out to be true. □

In the following lemma, we express M_{2k}, M_{2k+1}, W_{2k}, and W_{2k+1} in terms of M^e, M^o, W^e, and W^o.

Lemma 2.5. *For all integer $k \geq 2$, and $u = 2^{2k-1}$,*

$$\begin{aligned} M_{2k} &= M^e[:3u] + x^u M^e[:2u] + x^{3u} R^e, \\ W_{2k} &= W^e[:3u] + x^u W^e[:2u] + x^{3u} R^e. \end{aligned}$$

For all integer $k \geq 2$, and $u = 2^{2k}$,

$$\begin{aligned} M_{2k+1} &= M^o[:3u] + x^u M^o[:2u] + x^{3u} R^o, \\ W_{2k+1} &= W^o[:3u] + x^u W^o[:2u] + x^{3u} R^o. \end{aligned}$$

Proof. Call the four identities in Lemma 2.5 also by the name M_{2k}, W_{2k}, M_{2k+1}, and W_{2k+1}. For $k = 2$, the identities can be verified directly. For $k \geq 2$, we claim that

$$\text{“}M_{2k} \text{ and } W_{2k}\text{” implies “}M_{2k+1} \text{ and } W_{2k+1}\text{”},$$
$$\text{“}M_{2k+1} \text{ and } W_{2k+1}\text{” implies “}M_{2k+2} \text{ and } W_{2k+2}\text{”}.$$

We give the proof of

$$\text{“}M_{2k} \text{ and } W_{2k}\text{” implies } M_{2k+1}, \tag{2.12}$$

the proofs of the other ones being similar. Set $u = 2^{2k}$ and $v = 2^{2k-1}$. By definition and induction hypothesis, the left side of identity M_{2k+1} is equal to

$$W_{2k}M_{2k} = \big(W^e[:3v] + x^v W^e[:2v] + x^{3u}R^e\big) \times \big(M^e[:3v] + x^v M^e[:2v] + x^{3u}R^e\big). \tag{2.13}$$

Call this expression *lhs*. Note that both sides of identity M_{2k+1} have the same term of highest degree $x^{6v}R^o$. Therefore we only need to prove that their difference is $O(x^{6v})$. Using Lemma 2.3 it can be seen that the right side of identity M_{2k+1} is congruent, modulo x^{6v}, to

$$W^e[:6v]M^e[:6v] + x^{2v}W^e[:4v]M^e[:4v].$$

For all $n \leq 6$, replace the occurrences of $W^e[:n \cdot v]$ and $M^e[:n \cdot v]$ in the above expression by the reduction modulo $x^{n \cdot v}$ of the right side of the corresponding identity in Lemma 2.4 and get a new expression, which we call *rhs*. Define

$$\begin{aligned} X &:= x^v, \\ a_n &:= W^e[n \cdot v : (n+1) \cdot v]/X^n, \\ b_n &:= M^e[n \cdot v : (n+1) \cdot v]/X^n, \\ c &:= R^e. \end{aligned}$$

Using the notation introduced above, we can represent the expressions *lhs* (2.13) and *rhs* as polynomials in $\mathbb{F}_2[a_1, ..., a_6, b_1, ..., b_6, c][X]$. Note that it is not a problem that a_j commutes with b_k while W^e does not commute with M^e, because in the expressions concerned, the products of W^e-terms and M^e-terms are always in the same order. We let the computer do the simplification and check that the difference between these two polynomials is indeed $O(X^6)$, which completes the proof. □

Proof of Theorem 2.1. We prove the theorem for $\mathrm{CF}(\mathbf{t}(z))$; for $\mathrm{CF}(\bar{\mathbf{t}}(z))$, the proof is similar. By Lemma 2.5, we have For all j, k in $\{0, 1\}$,

$$\begin{aligned} \lim_{n\to\infty} M_{2n,j,k} &= M^e_{j,k}, \\ \lim_{n\to\infty} M_{2n+1,j,k} &= M^o_{j,k}, \\ \lim_{n\to\infty} W_{2n,j,k} &= W^e_{j,k}, \\ \lim_{n\to\infty} W_{2n+1,j,k} &= W^o_{j,k}. \end{aligned}$$

Let $z = 1/x$. By the convergence theorem and identity (4.1),

$$\mathrm{CF}(\mathbf{t}(z)) = \frac{M^e_{0,1}(x)}{M^e_{0,0}(x)}.$$

By definition, that $\phi(M^e, 0, 1)$ and $\phi(M^e, 0, 0)$ are minimal polynomials of $M^e_{0,1}$ and $M^e_{0,0}$. Therefore

$$P(x, y) = \mathrm{Res}_t \left(\phi(M^e, 0, 1)(x, t), y^{12}\phi(M^e, 0, 1)(x, t/y)\right)$$

is an annihilating polynomial of $f(x) = M^e_{0,1}/M^e_{0,0}$.

Define

$$Q(x, y) = q_4(x)y^4 + q_3(x)y^3 + q_2(x)y^2 + q_1(x)y + q_0(x),$$

where

$$\begin{aligned}
q_0(x) &= x^{12} + x^{11} + x^8 + x^7 + x^6 + x^5 + x^3,\\
q_1(x) &= x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x,\\
q_2(x) &= x^{10} + x^2 + 1,\\
q_3(x) &= x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + x,\\
q_4(x) &= x^{11} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2.
\end{aligned}$$

The polynomial $Q(x, y)$ is the candidate for the minimal polynomial of $f(x)$ found by Padé-Hermite approximation. To prove that it is indeed the minimal polynomial of $f(x)$, we only need to prove that it is an irreducible factor of $P(x, y)$ of multiplicity m and $R(x, y) := P(x, y)/Q(x, y)^m$ is not an annihilating polynomial of $f(x)$. We verify the first point directly. For the second point, we find that when we truncate $f(x)$ to order 96, and substitute it for y in $R(z, y)$, we get a series with valuation smaller than 96, which proves that $R(z, y)$ is not an annihilating polynomial of $f(x)$. Finally, $z^{12}Q(1/z, y)$ is the minimal polynomial of $\mathrm{CF}(\mathbf{t}(z)) = f(1/z)$. □

3. Thue-Morse Stieltjes Continued Fraction

Let $\mathbf{v}$ be the $(a/b, 1)$-Thue-Morse sequence, then

$$\mathrm{Stiel}(x; \mathbf{u}) = b \cdot \mathrm{Stiel}(bx; \mathbf{v}).$$

Therefore conjecture 1.3 admits the following equivalent form:

Conjecture 1.3a. Let $k \geq 2$ be an integer. Let a be an element from $\mathbb{F}_{2^k}^{\times}$ distinct from 1. Let $\mathbf{u}$ be the $(a, 1)$-Thue-Morse sequence. The Stieltjes continued fraction $\mathrm{Stiel}(x; \mathbf{u})$ is algebraic over $\mathbb{F}_2^k(x)$. Its minimal polynomial is

$$p_0(x) + p_1(x)y + p_2(x)y^2 + p_4(x)y^4,$$

where

$$\begin{aligned}
p_0(x) &= ((a^2 + 1)/a^4)x^2 + 1/(a^5 + a^4),\\
p_1(x) &= ((a + 1)/a^5)x + 1/a^5,\\
p_2(x) &= (1/a^5)x + 1/(a^6 + a^5),\\
p_4(x) &= (1/(a^6 + a^5))x^2.
\end{aligned}$$

Or still

Conjecture 1.3b. We regard a as a formal variable. Let $\mathbf{u}$ be the $(a, 1)$-Thue-Morse sequence. Then the Stieljtes continued fraction $\mathrm{Stiel}(x; \mathbf{u}) \in \mathbb{F}_2(a)[[x]]$ is algebraic over $\mathbb{F}_2(a)(x)$. Its minimal polynomial is

$$p_0(x) + p_1(x)y + p_2(x)y^2 + p_4(x)y^4,$$

where

$$p_0(x) = ((a^2+1)/a^4)x^2 + 1/(a^5+a^4),$$
$$p_1(x) = ((a+1)/a^5)x + 1/a^5,$$
$$p_2(x) = (1/a^5)x + 1/(a^6+a^5),$$
$$p_4(x) = (1/(a^6+a^5))x^2.$$

It is clear that conjecture 1.3b implies conjecture 1.3a, noticing that the only roots of the denominators of the coefficients of $p_j(x)$, $j = 0, 1, 2, 4$, are 0 and 1. On the other hand, if conjecture 1.3b does not hold, then

$$0 \neq p_0(x) + p_1(x)\,\mathrm{Stiel}(x;\mathbf{u}) + p_2(x)\,\mathrm{Stiel}(x;\mathbf{u})^2 + p_4(x)\,\mathrm{Stiel}(x;\mathbf{u})^4 =: \sum_{n=0}^{\infty} c_n(a)x^n,$$

and there exists an $n \in \mathbb{N}$ for which $c_n(a) \in \mathbb{F}_2(a)$ is not zero. Necessarily there exists a $k \geq 2$ and an element $u \in \mathbb{F}_{2^k}\backslash\{0,1\}$ that is not a root of the numerator of $c_n(a)$, and consequently conjecture 1.3a does not hold for $a = u$.

Using our program, we checked that conjecture 1.3a holds for all $a \in \mathbb{F}_{2^k}\backslash\{0,1\}$ for $k = 2, 3, 4$. In this section we present our method.

3.1. **Testing of the conjecture.** For $k \geq 2$, instead of all a in $\mathbb{F}_{2^k}\backslash\{0,1\}$, we only need to test one a in each of the orbits of the Frobenius morphism $\phi : a \mapsto a^2$, because if we let $\mathbf{t}$ denote the $(a,1)$-Thue-Morse sequence and $\phi(\mathbf{t})$ the $(\phi(a),1)$-Thue-Morse sequence, then

$$\mathrm{Stiel}(x;\phi(\mathbf{t})) = \phi(\mathrm{Stiel}(x;\mathbf{t})),$$

and they are either both algebraic or both transcendental.

For example, $\mathbb{F}_8 \cong \mathbb{F}_2[u]/ < u^3+u+1 >$ is partitioned into orbits

$$\{0\}, \{1\},\ \{\bar{u}, \bar{u}^2,\ \bar{u}^4\},\ \text{and}\ \{\bar{u}^3, \bar{u}^6, \bar{u}^5\}.$$

Therefore for $\mathbb{F}_8$, we only have to test the conjecture for $a = \bar{u}$ and $a = \bar{u}^3$. Furthermore, we only have to test those a in $\mathbb{F}_{2^k}\backslash\{0,1\}$ whose orbit contains k elements, because elements whose orbit has size $l < k$ are already tested in $\mathbb{F}_{2^l}$. For example, for $\mathbb{F}_{16} \cong \mathbb{F}_2[u]/ < u^4+u+1 >$, the orbit of $a = \bar{u}^5$ contains only itself and a^2. This means that $a^4 = a$, and therefore it is already treated in $\mathbb{F}_4$.

3.2. **Our method.** The same method for testing conjecture 1.1 can be used here to test conjecture 1.3a for $a \in \mathbb{F}_{2^k}\backslash\{0,1\}$ $(k \geq 2)$, with only slight modifications. As most of the following have a uniform expression for all a, we first regard a as a formal variable.

As in Section 2, we define

$$M_n = \begin{pmatrix} 1 & t_{2^n-1}x \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & t_{2^n-2}x \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & t_0 x \\ 1 & 0 \end{pmatrix}, \tag{3.1}$$

and

$$W_n = \begin{pmatrix} 1 & \bar{t}_{2^n-1}x \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \bar{t}_{2^n-2}x \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & \bar{t}_0 x \\ 1 & 0 \end{pmatrix}, \tag{3.2}$$

where $\mathbf{t}$ is the $(a,1)$-Thue-Morse sequence, and $\bar{\mathbf{t}}$, $(1,a)$-Thue-Morse sequence. We have $M_{n+1} = W_n \cdot M_n$ and $W_{n+1} = M_n \cdot W_n$ for all n.

We define four 2×2 matrices M^e, M^o, W^e and W^o as follows: For all $T \in \{M^e, M^o, W^e, W^o\}$, and all $i, j \in \{0,1\}$, $T_{i,j}$ is defined to be the unique root in

$\mathbb{F}_2(a)[[x]]$ of the polynomial $\phi(T,i,j)$ with prescribed first terms of its expansion. The polynomials $\phi(T,i,j)$ and first terms can be found on the web page of the authors. The reason for defining these matrices and how the polynomials $\phi(T,i,j)$ and initial conditions are found are similar to those given in Section 2.

As expected, the following Lemma holds:

Lemma 3.1.

$$M^e = W^o \cdot M^o, \tag{3.3}$$

$$M^o = W^e \cdot M^e, \tag{3.4}$$

$$W^e = M^o \cdot W^o, \tag{3.5}$$

$$W^o = M^e \cdot W^e. \tag{3.6}$$

Proof. Similar to the proof of Lemma 2.3. □

We have the following observation concerning the structure of the four matrices, where I_2 denote the 2×2 identity matrix.

Observation 3.2. *For $k \geq 2$ and $u = 2^{2k-1}$ the following identities hold:*

$$M^e[u{:}2u] = x^u \cdot (a^u + 1) \cdot M^e[{:}u] + a^{u/2}x^u \cdot I_2, \tag{3.7}$$

$$W^e[u{:}2u] = x^u \cdot (a^u + 1) \cdot W^e[{:}u] + a^{u/2}x^u \cdot I_2; \tag{3.8}$$

for $k \geq 2$ and $u = 2^{2k}$,

$$M^o[u{:}2u] = x^u \cdot (a^u + 1) \cdot M^o[{:}u] + a^{u/2}x^u \cdot I_2, \tag{3.9}$$

$$W^o[u{:}2u] = x^u \cdot (a^u + 1) \cdot W^o[{:}u] + a^{u/2}x^u \cdot I_2. \tag{3.10}$$

Observation 3.3. *For $k \geq 2$ and $u = 2^{2k-1}$,*

$$M_{2k} = M^e[{:}u] + a^{u/2}x^u \cdot I_2,$$
$$W_{2k} = W^e[{:}u] + a^{u/2}x^u \cdot I_2;$$

for $k \geq 2$ and $u = 2^{2k}$,

$$M_{2k+1} = M^o[{:}u] + a^{u/2}x^u \cdot I_2,$$
$$W_{2k+1} = W^o[{:}u] + a^{u/2}x^u \cdot I_2.$$

Lemma 3.4. *Observation 3.2 implies observation 3.3.*

Proof. Let us call the four identities in observation 3.3 also by the name M_{2k}, W_{2k}, M_{2k+1} and W_{2k+1}. Suppose observation 3.3 is true. We want to prove observation 3.2 by induction. For $k = 2$, the identities are verified directly. The inductive step is

$$\text{“}M_{2k} \text{ and } W_{2k}\text{” implies “}M_{2k+1} \text{ and } W_{2k+1}\text{”},$$
$$\text{“}M_{2k+1} \text{ and } W_{2k+1}\text{” implies “}M_{2k+2} \text{ and } W_{2k+2}\text{”}.$$

Let us show for example how to prove

$$\text{“}M_{2k} \text{ and } W_{2k}\text{” implies } M_{2k+1}, \tag{3.11}$$

By definition, the left side of the identity M_{2k+1} is equal to

$$W_{2k} \cdot M_{2k},$$

which, by induction hypothesis, is equal to

$$(W^e[:u] + a^{u/2}x^u I_2) \cdot (M^e[:u] + a^{u/2}x^u I_2),$$

where $u = 2^{2k-1}$. Therefore only need to prove that

$$W^e[:u] \cdot M^e[:u] + a^{u/2}x^u(W^e[:u] + M^e[:u]) - M^o[:2u] \tag{3.12}$$

is equal to zero. As the degree of the above polynomial is at most $2u-1$, we only need to prove that it is $O(x^{2^{2k}})$. By (3.4),

$$\begin{aligned} & M^o[:2u] \\ \equiv\ & W^e[:2u] \cdot M^e[:2u] \mod x^{2u} \\ \equiv\ & W^e[:u] \cdot M^e[:u] + W^e[u:2u] \cdot M^e[:u] + W^e[:u] \cdot M^e[u:2u] \mod x^{2u} \end{aligned}$$

Therefore (3.12) is congruent modulo x^{2u} to

$$a^{u/2}x^u(W^e[:u] + M^e[:u]) + W^e[u:2u] \cdot M^e[:u] + W^e[:u] \cdot M^e[u:2u].$$

Substitute $W^e[u:2u]$ and $M^e[u:2u]$ by the expressions in observation 3.2 and we obtain that the quantity above is $O(x^{2u})$. That is, expression (3.12) is congruent to 0 modulo x^{2u}; since it has no term of order higher than $2u-1$, it is equal to 0. □

Proposition 3.5. *Observation 3.3 implies conjecture 1.3b.*

Proof. First, taking the limit of the identities in observation 3.3, we have for all $j, k \in \{0, 1\}$,

$$\begin{aligned} \lim_{n\to\infty} M_{2n,j,k} &= M^e_{j,k}, \\ \lim_{n\to\infty} M_{2n+1,j,k} &= M^o_{j,k}, \\ \lim_{n\to\infty} W_{2n,j,k} &= W^e_{j,k}, \\ \lim_{n\to\infty} W_{2n+1,j,k} &= W^o_{j,k}. \end{aligned}$$

Therefore

$$\mathrm{Stiel}(x; \mathbf{t}) = \lim_{n\to\infty} \frac{P_n}{Q_n} = \lim_{n\to\infty} \frac{P_{2^{2n}-1}}{Q_{2^{2n}-1}} = \lim_{n\to\infty} \frac{M_{2n,0,1}/x}{M_{2n,0,0}} = \frac{M^e_{0,1}/x}{M^e_{0,0}}.$$

We obtain the minimal polynomial of $\mathrm{Stiel}(x; \mathbf{t})$ from those of $M^e_{0,1}$ and $M^e_{0,0}$, using the method described in the proof of Theorem 2.1. □

Remark 3.1. The above proposition says that observation 3.3 implies conjecture 1.3 when a is regarded as a formal variable. The implication also holds when a specializes as an element in $\mathbb{F}_{2^k} \setminus \{0, 1\}$ $(k \geq 2)$.

Therefore, to prove that conjecture 1.3a holds for a certain $a \in \mathbb{F}_{2^k} \setminus \{0, 1\}$ $(k \geq 2)$, we only need to prove that observation 3.2 holds for a. Because of the following argument, we only have to check (3.7) through (3.10) for finitely many k's instead of for all $k \geq 2$:

For $k \geq 2$ and $u = 2^{2k-1}$, identities (3.7) and (3.8) can be written as

$$T[[1w]_2] = (a^u + 1) \cdot T[[w]_2] \tag{3.13}$$

for every component T of M^e and W^e and all binary words w of length $2k-1$ and $w \neq 0^{2k-1}$; and

$$T[[1w]_2] = (a^u + 1) \cdot T[[w]_2] + a^{u/2} \tag{3.14}$$

for $w = 0^{2k-1}$.

We calculate an automaton for T from the algebraic equation that defines it, following the method in [10] (see Section 5). Let $A(s, w)$ denote the state reached after reading w from right to left starting from the state s, and τ the output function. Define

$$E_{2k-1} = \{A(i, w) \mid |w| = 2k-1, w \neq 0^{2k-1}\}.$$

Identity (3.13) and (3.14) can be written as

$$\tau(A(s, 1)) = (a^u + 1) \cdot \tau(A(s, \epsilon)) \tag{3.15}$$

for all $s \in E_{2k-1}$, and

$$\tau(A(s, 1)) = (a^u + 1) \cdot \tau(A(s, \epsilon)) + a^{u/2} \tag{3.16}$$

for $s = A(i, 0^{2k-1})$.

As E_{2k+1} is completely determined by E_{2k-1}, the sequence $(E_{2k+1})_k$ is ultimately periodic. The sequences $(A(i, 0^{2k-1}))_k$ and $a^{2^{2k-1}}$ are also periodic. Therefore we only need to check (3.15) and (3.16) for finitely many k's.

3.3. **An example.** For $a \in \mathbb{F}_4 \backslash \{0, 1\}$ and $T = Me_{0,0}$, we find that the minimal 2-DFAO of T has as transition function $(n, j) \mapsto \delta(n, j)$ ($\Lambda(n) := [\delta(n, 0), \delta(n, 1)]$):

n	$\Lambda(n)$	n	$\Lambda(n)$	n	$\Lambda(n)$	n	$\Lambda(n)$
0	[1, 2]	5	[2, 8]	10	[7, 8]	15	[13, 17]
1	[3, 4]	6	[9, 4]	11	[8, 13]	16	[18, 4]
2	[5, 6]	7	[10, 4]	12	[14, 4]	17	[19, 12]
3	[1, 7]	8	[11, 6]	13	[15, 16]	18	[16, 6]
4	[4, 4]	9	[6, 12]	14	[12, 16]	19	[17, 8]

and output function $n \mapsto \tau(n)$:

n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$
0	1	3	1	6	$a+1$	9	$a+1$	12	1	15	1	18	a
1	1	4	0	7	0	10	0	13	1	16	a	19	$a+1$
2	a	5	a	8	a	11	a	14	1	17	$a+1$		

The tuple $(A(i, 0^{2k-1}), E_{2k-1})$ has the following values:

$$k = 3 : (1, \{2, 4, 7, 8, 9\}),$$
$$k = 5 : (1, \{2, 4, 7, 8, 9, 13, 14\}),$$
$$k = 7 : (1, \{2, 4, 7, 8, 9, 13, 14, 17, 18\}),$$
$$k = 9 : (1, \{2, 4, 7, 8, 9, 13, 14, 17, 18\}).$$

For all $k \geq 1$, $a^{2^{2k-1}} = a+1$. Therefore we only have to check that identity (3.7) holds for $k = 3, 5, 7$, which turns out to be true.

4. Period-doubling Continued Fractions

The method for checking conjecture 1.1 can be adapted for the verification of conjecture 1.5. In this section, we give an example. First we introduce the notation.

Let (a,b) be in $(\mathbb{F}_2[z]\setminus\mathbb{F}_2)^2$. Let $\mathbf{p}$ be the (a,b)-period-doubling sequence. Define two sequences $A_n(x)$ and $B_n(x)$ by

$$\begin{aligned}
A_0(x) &= x^{\deg(a)}\begin{pmatrix} a(1/x) & 1\\ 1 & 0\end{pmatrix},\\
B_0(x) &= x^{\deg(b)}\begin{pmatrix} b(1/x) & 1\\ 1 & 0\end{pmatrix},\\
A_{n+1}(x) &= B_n(x)A_n(x) \quad \forall n\ge 0,\\
B_{n+1}(x) &= A_n(x)A_n(x) \quad \forall n\ge 0.
\end{aligned}$$

Define $x := 1/z$. For an non-zero polynomial $P(z)$, we define $\tilde{P}(x)$ to be $P(1/x)$. Then

$$\mathrm{CF}_n(\mathbf{p}(z)) = \frac{P_n(z)}{Q_n(z)} = \frac{\tilde{P}_n(x)}{\tilde{Q}_n(x)} \in \mathbb{F}_2((x)) = \mathbb{F}_2((1/z)).$$

Comparing the definition of $A_n(x)$ with definition (1.3), we see that

$$\begin{aligned}
A_n(x)_{0,1} &= x^{d_n}\tilde{P}_{2^n-1}(x),\\
A_n(x)_{0,0} &= x^{d_n}\tilde{Q}_{2^n-1}(x),
\end{aligned}$$

for some positive integer d_n, and

$$\mathrm{CF}_{2^{2^n}-1}(\mathbf{p}(z)) = \frac{\tilde{P}_{2^{2^n}-1}(x)}{\tilde{Q}_{2^{2^n}-1}(x)} = \frac{A_{2n}(x)_{0,1}}{A_{2n}(x)_{0,0}}. \tag{4.1}$$

4.1. **The (z^3, z^2+z+1)-period-doubling sequence.** In this subsection, we prove the theorem 1.6 We define four 2×2 matrices A^e, A^o, B^e and B^o as follows: For all $T\in\{A^e, A^o, B^e, B^o\}$, and all $i,j\in\{0,1\}$, $T_{i,j}$ is defined to be the unique root in $\mathbb{F}_2(a)[[x]]$ of the polynomial $\phi(T,i,j)$ under with prescribed first terms of its exansion. The polynomials $\phi(T,i,j)$ and first terms can be found on the web page of the authors. The reason for defining these matrices and how the polynomials $\phi(T,i,j)$ and initial conditions are found are similar to those given in Section 2.

Lemma 4.1. *The following identities hold:*

$$\begin{aligned}
A^e &= B^o\cdot A^o,\\
A^o &= B^e\cdot A^e,\\
B^e &= A^o\cdot A^o,\\
B^o &= A^e\cdot A^e.
\end{aligned}$$

Proof. Similar to the proof of Lemma 2.3. □

Lemma 4.2. *For $n\ge 2$ even, $u=(2^{n+3}+1)/3$, $v=2^n$,*

$$\begin{aligned}
A^e[:2u] = (1+x^v+x^{2v})\cdot(A^e[:u] + x^vA^e[:u-v]) + x^{4v}A^e[:2u-4v]+\\
(x^u+x^{u+v}+x^{u+2v})\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\\
B^e[:2u] = (1+x^v+x^{2v})\cdot(B^e[:u] + x^vB^e[:u-v]) + x^{4v}B^e[:2u-4v]+\\
\begin{pmatrix}x^{2u-1} & x^{2u-1}+x^{2u-4}\\ 0 & x^{2u-1}\end{pmatrix}.
\end{aligned}$$

For $n \geq 1$ odd, $u = (2^{n+3}+2)/3$, $v = 2^n$,

$$A^o[:2u-1] = (1+x^v+x^{2v}) \cdot (A^o[:u] + x^v A^o[:u-v]) + x^{4v} A^o[:2u-4v-1] + (x^{2u-2}) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$B^o[:2u-1] = (1+x^v+x^{2v}) \cdot (B^o[:u] + x^v B^o[:u-v]) + x^{4v} B^o[:2u-4v-1] + \begin{pmatrix} x^u + x^{u+v} + x^{u+2v} & x^{2u-2} + x^{2u-4} \\ 0 & x^u + x^{u+v} + x^{u+2v} \end{pmatrix}.$$

Proof. We give the proof of the $(0,0)$-th component of the first identity. The proofs of the other 15 identities are similar. Let $T = A^e_{0,0}$. We want to prove that

$$T[:2u] = (1+x^v+x^{2v}) \cdot (T[:u] + x^v T[:u-v]) + x^{4v} T[:2u-4v] + x^u (1+x^v+x^{2v}). \tag{4.2}$$

for all $n \geq 2$ even, $u = (2^{n+3}+1)/3$, and $v = 2^n$. Equation (4.2) can be rewritten as

$$\begin{aligned} T[u:2u] &= x^v T[u-v:u] + x^{2v} T[u-v:u] + x^{3v} T[:u-v] + \\ &\quad x^{4v} T[:2u-4v] + x^u + x^{u+v} + x^{u+2v} \\ &= (x^u + x^v T[u-v:2v]) + (x^v T[2v:u] + x^{3v} T[:u-2v]) + \\ &\quad (x^{u+v} + x^{3v} T[u-2v:v] + x^{2v} T[u-v:2v]) + \\ &\quad (x^{2v} T[2v:u] + x^{3v} T[v:u-v] + x^{4v} T[:u-2v]) + \\ &\quad (x^{u+2v} + x^{4v} T[u-2v:2u-4v]) \end{aligned}$$

noting that $u < 3v < u+v < 4v < u+2v < 2u$. The above identity can be decomposed into five parts:

$$\begin{aligned} T[u:3v] &= x^u + x^v T[u-v:2v] \\ T[3v:u+v] &= x^v T[2v:u] + x^{3v} T[:u-2v] \\ T[u+v:4v] &= x^{u+v} + x^{3v} T[u-2v:v] + x^{2v} T[u-v:2v] \\ T[4v:u+2v] &= x^{2v} T[2v:u] + x^{3v} T[v:u-v] + x^{4v} T[:u-2v] \\ T[u+2v:2u] &= x^{u+2v} + x^{4v} T[u-2v:2u-4v] \end{aligned}$$

That the above five identities hold for all $n \geq 2$, $u = (2^{n+3}+1)/3$, and $v = 2^n$ is equivalent to the following identities:

$$T[[10w]_2] = 1 + T[[1w]_2] \qquad \forall w \in L_0 \tag{4.3}$$

$$T[[10w]_2] = T[[1w]_2] \qquad \forall w \in L_1 \tag{4.4}$$

$$T[[11w]_2] = T[[10w]_2] + T[[w]_2] \qquad \forall w \in L_2 \tag{4.5}$$

$$T[[11w]_2] = 1 + T[[w]_2] + T[[1w]_2] \qquad \forall w \in L_0 \tag{4.6}$$

$$T[[11w]_2] = T[[w]_2] + T[[1w]_2] \qquad \forall w \in L_1 \tag{4.7}$$

$$T[[100w]_2] = T[[10w]_2] + T[[1w]_2] + T[[w]_2] \qquad \forall w \in L_2 \tag{4.8}$$

$$T[[100w]_2] = 1 + T[[w]_2] \qquad \forall w \in L_0 \tag{4.9}$$

$$T[[100w]_2] = T[[w]_2] \qquad \forall w \in L_1 \tag{4.10}$$

$$T[[10w]_2] = T[[w]_2] \qquad \forall w \in L_3 \tag{4.11}$$

$$T[[10w]_2] = T[[w]_2] \qquad \forall w \in L_4 \tag{4.12}$$

where

$$\begin{aligned}
L_0 &= L((10)^*11),\\
L_1 &= L((10)^*11\{00,01,10,11\}^+),\\
L_2 &= L((10)^*0\{0,1\}\{00,01,10,11\}^* + (10)^+),\\
L_3 &= L((10)^+0\{00,01,10,11\}^+),\\
L_4 &= L((10)^+\{0,1\}).
\end{aligned}$$

From the minimal polynomial and the first terms of T, we find its minimal automaton. Its transition function δ ($\Lambda(n) := [\delta(n,0), \delta(n,1)]$) and output function τ are as follows:

n	$\Lambda(n)$	n	$\Lambda(n)$	n	$\Lambda(n)$	n	$\Lambda(n)$	n	$\Lambda(n)$
0	[1, 2]	6	[11, 12]	12	[15, 20]	18	[23, 12]	24	[27, 15]
1	[3, 4]	7	[13, 14]	13	[9, 21]	19	[24, 23]	25	[15, 18]
2	[5, 6]	8	[5, 15]	14	[14, 14]	20	[14, 26]	26	[17, 20]
3	[7, 8]	9	[16, 14]	15	[22, 10]	21	[14, 16]	27	[28, 14]
4	[9, 10]	10	[17, 18]	16	[23, 9]	22	[5, 17]	28	[27, 17]
5	[8, 9]	11	[19, 6]	17	[24, 25]	23	[16, 16]		

n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$	n	$\tau(n)$
0	1	5	1	10	0	15	1	20	0	25	1
1	1	6	0	11	0	16	1	21	0	26	0
2	1	7	1	12	1	17	0	22	1	27	0
3	1	8	1	13	1	18	1	23	1	28	0
4	1	9	1	14	0	19	0	24	0		

Let $A(s,w)$ denote the state reached after reading w from right to left starting from the state s. For $j = 0, 1, \ldots, 4$, define

$$E_j = \{A(0,w) \mid w \in L_j\}.$$

We can compute E_j explicitly and find

$$\begin{aligned}
E_0 &= \{6\}\\
E_1 &= \{14,15,16,17,18,20\}\\
E_2 &= \{3,4,5,13,14,15,16,17,19,27\}\\
E_3 &= \{9,14,21,23\}\\
E_4 &= \{8,9\}.
\end{aligned}$$

Equations (4.3) through (4.12) can be written as

$$\tau(A(s,10)) = 1 + \tau(A(s,1)) \qquad \forall s \in E_0 \tag{4.13}$$

$$\tau(A(s,10)) = \tau(A(s,1)) \qquad \forall s \in E_1 \tag{4.14}$$

$$\tau(A(s,11)) = \tau(A(s,10)) + \tau(s) \qquad \forall s \in E_2 \tag{4.15}$$

$$\tau(A(s,11)) = 1 + \tau(s) + \tau(A(s,1)) \qquad \forall s \in E_0 \tag{4.16}$$

$$\tau(A(s,11)) = \tau(s) + \tau(A(s,1)) \qquad \forall s \in E_1 \tag{4.17}$$

$$\tau(A(s,100)) = \tau(A(s,10)) + \tau(A(s,1)) + \tau(s) \qquad \forall s \in E_2 \tag{4.18}$$

$$\tau(A(s,100)) = 1 + \tau(s) \qquad \forall s \in E_0 \tag{4.19}$$

$$\tau(A(s,100)) = \tau(s) \qquad \forall s \in E_1 \tag{4.20}$$

$$\tau(A(s,10)) = \tau(s) \qquad \forall s \in E_3 \tag{4.21}$$

$$\tau(A(s,10)) = \tau(s) \qquad \forall s \in E_4 \tag{4.22}$$

We verify equations (4.13) through (4.22) directly. □

Lemma 4.3. *For $n \geq 2$ even, $u = (2^{n+3}+1)/3$, $v = 2^n$,*

$$A_n = A^e[:u] + x^v \cdot A^e[:u-v] + x^u \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$B_n = B^e[:u] + x^v \cdot B^e[:u-v]$$

For $n \geq 1$ odd, $u = (2^{n+3}+2)/3$, $v = 2^n$,

$$A_n = A^o[:u] + x^v \cdot A^o[:u-v]$$

$$B_n = B^o[:u] + x^v \cdot B^o[:u-v] + x^u \cdot I_2$$

Proof. For $n \geq 2$ even, we prove that

$$A_n \wedge B_n \Rightarrow A_{n+1}.$$

Set $u = (2^{n+3}+1)/3$, $v = 2^n$. Identity A_{n+1} can be written as

$$A_{n+1} = A^o[:2u] + x^{2v} \cdot A^o[2u-2v] \tag{4.23}$$

The left side of Eq. (4.23) is

$$\begin{aligned} & B_n A_n \\ &= (B^e[:u] + x^v \cdot B^e[:u-v]) \left(A^e[:u] + x^v \cdot A^e[:u-v] + x^u \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \\ &= (B^e[:u] + x^v \cdot B^e[:u-v])(A^e[:u] + x^v \cdot A^e[:u-v]) \\ & \quad x^u B^e[:u] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + x^{u+v} B^e[:u-v] \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

By lemma 4.1, the right side of Eq. (4.23) is congruent, modulo x^{2u} to

$$(1+x^{2v})A^o[:2u] \equiv (1+x^{2v})B^e[:2u]A^e[:2u] \pmod{x}^{2u}.$$

We recall that

$$\begin{aligned} A^e[:2u] = (1+x^v+x^{2v}) \cdot (A^e[:u] + x^v A^e[:u-v]) + x^{4v} A^e[:2u-4v] + \\ (x^u + x^{u+v} + x^{u+2v}) \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \\ B^e[:2u] = (1+x^v+x^{2v}) \cdot (B^e[:u] + x^v B^e[:u-v]) + x^{4v} B^e[:2u-4v] + \\ \begin{pmatrix} x^{2u-1} & x^{2u-1}+x^{2u-4} \\ 0 & x^{2u-1} \end{pmatrix}. \end{aligned}$$

Noticing that

$$\begin{pmatrix} x^{2u-1} & x^{2u-1}+x^{2u-4} \\ 0 & x^{2u-1} \end{pmatrix} A^e[:2u] \equiv 0 \mod x^{2u},$$

and

$$(1+x^{2v})(1+x^v+x^{2v})^2 = 1+x^{6v} \equiv 0 \mod x^{2u},$$

we have

$$\begin{aligned}
&(1+x^{2v})\cdot B^e[:2u]A^e[:2u]\\
\equiv&(1+x^{2v})\cdot\big((1+x^v+x^{2v})\cdot(B^e[:u]+x^vB^e[:u-v])+x^{4v}B^e[:2u-4v]\big)\\
&((1+x^v+x^{2v})\cdot(A^e[:u]+x^vA^e[:u-v])+x^{4v}A^e[:2u-4v])\\
&(1+x^{2v})\cdot\big((1+x^v+x^{2v})\cdot(B^e[:u]+x^vB^e[:u-v])+x^{4v}B^e[:2u-4v]\big)\\
&(x^u+x^{u+v}+x^{u+2v})\begin{pmatrix}1&1\\0&1\end{pmatrix}\\
\equiv&(B^e[:u]+x^vB^e[:u-v])\cdot(A^e[:u]+x^vA^e[:u-v])\\
&x^u\cdot(B^e[:u]+x^vB^e[:u-v])\cdot\begin{pmatrix}1&1\\0&1\end{pmatrix}\mod x^{2u}.
\end{aligned}$$

Thus we have proved that both sides of Eq. (4.23) are congruent modulo x^{2u}, so that they must be equal as both have degree at most $2u$. □

Theorem 1.6 can be derived from lemma 4.3 and the definition of A^e, using the same method as in the proof of theorem 2.1.

5. From equation to automaton

In this section we give an description of the algorithm that we implemented to calculate a p-automaton of an algebraic series $T(x)$ in $\mathbb{F}_q[[x]]$ from an annihilating polynomial of it, where $\mathbb{F}_q$ is a finite field of characteristic p. The algorithm is based on the proof of theorem 1 in [10].

Step one: Normalization
Input: an annihilating polynomial $P(x,y)\in\mathbb{F}_q(x)[y]$ of $T(x)$.
Output: an annihilating polynomial $Q(x,y)\in\mathbb{F}_q(x)[y]$ of $T(x)$ the form

$$y+\frac{a_1(x)}{b_1(x)}y^{p^1}+\frac{a_2(x)}{b_2(x)}y^{p^2}+\cdots+\frac{a_n(x)}{b_n(x)}y^{p^n}.$$

Method: use the relation $P(x,T(x))=0$ to express $T(x)^{p^j}$ as $\mathbb{F}_p(x)$-linear combination of $T(x)^k$, $k=0,1,\ldots,d-1$, where d is the degree of $P(x,y)$ as a polynomial in y. In practice, to find the expression of $T(x)^{p^j}$, we first calculate that of $T(x)^{p^{j-1}}$, then raise it to the p-th power, and finally reduce again using the relation $P(x,T(x))=0$.

We know that the family $T(x)^{p^j}$, $j=0,1,\ldots,d$ is necessarily linearly dependent. However, as it can be costly to compute $T(x)^{p^j}$ when j is large, in reality we stop once the rank of the family $T(x)^{p^j}$, $k=0,1,\ldots,j_0$ is less than j_0+1.

Step two: From normalized equation to kernel
Input: the relation

$$T(x)=\frac{a_1(x)}{b_1(x)}T(x)^{p^1}+\frac{a_2(x)}{b_2(x)}T(x)^{p^2}+\cdots+\frac{a_n(x)}{b_n(x)}T(x)^{p^n}. \tag{5.1}$$

Output: the p-kernel of $T(x)$.
Method: We let ϕ denote the Frobenius morphism and Λ_j the Cartier operator

that maps $\sum a_l x^l$ to $\sum a_{pl+j} x^l$ for $j = 0, 1, \ldots, p-1$. We recall that for a series $f(x) = \sum_{l \geq l_0} c_l x^l \in \mathbb{F}_q((x))$ and polynomials $a(x)$ and $b(x)$,

$$\Lambda_j(a(x)f(x)^p) = \Lambda_j(a(x))\Lambda_0(f(x)^p)$$

for $j = 0, 1, \ldots, p$ and

$$\Lambda_0(f(x)^p) = \Lambda_0 \sum_{l \geq l_0} c_l^p x^{p \cdot l} = \sum_{l \geq l_0} c_l^p x^l = \phi(f)(x).$$

Combining the above two identities and we get

$$\Lambda_j\left(\frac{a(x)}{b(x)} f(x)^p\right) = \Lambda_j\left(a(x)b(x)^{p-1}\frac{f(x)^p}{b(x)^p}\right) = \Lambda_j(a(x)b(x)^{p-1})\frac{\phi(f)(x)}{\phi(b)(x)}. \tag{5.2}$$

When we apply repeatedly Λ_j, $j = 0, 1, \ldots, p-1$ to both sides of (5.1) using the above computation rule and rewrite $\phi^k(T)(x)$ using relation (5.1), we always get an expression of the form (this will be illustrated by example 5.1 below)

$$\frac{c_1(x)}{d_1(x)}\phi^k(T)(x)^{p^1} + \frac{c_2(x)}{d_2(x)}\phi^k(T)(x)^{p^2} + \cdots + \frac{c_n(x)}{d_n(x)}\phi^k(T)(x)^{p^n}, \tag{5.3}$$

where $k = 0, 1, \ldots, \log q / \log p - 1$, and $c_j(x)$ and $d_j(x)$ are polynomial of bounded degree for $j = 1, 2, \ldots, n$. To see the last point, note that for $d_j(x)$ is always a factor of

$$\prod_{l=1}^{n} \phi^k(b_l(x))$$

for some $k \in [0, \log q / \log p)$, and

$$\deg c_j \leq \deg d_j + \max\{\deg a_l - \deg b_l \mid l = 1, 2, \ldots, n\}.$$

The set of expressions of the form (5.3) is therefore finite and the process must terminate. In the end we get a finite set that is the p-kernel of $T(x)$.

In our program, the expression (5.3) is encoded by the tuple

$$\left(\{1 : c_1(x)/d_1(x), 2 : c_2(x)/d_2(x), \ldots, n : c_n(x)/d_n(x)\}, k\right).$$

Remark 5.1. Note that the reason we use powers of p instead of powers of q in (5.1) is that the latter usually needs much larger coefficients.

Example 5.1. Set $a = \bar{u} \in \mathbb{F}_4 = \mathbb{F}_2[u]/ < u^2 + u + 1 >$. Let $T(x)$ be the unique solution in $\mathbb{F}_4[[x]]$ of

$$(x^2 + ax)y^3 + y + a + x = 0.$$

We write the equation in the normalized form, which is really easy for this example:

$$T(x) = \frac{1}{x+a}T(x)^2 + xT(x)^4. \tag{5.4}$$

We use computation rule (5.2) to calculate $\Lambda_0 T(x)$ and $\Lambda_0\Lambda_0 T(x)$ to illustrate this process:

$$\begin{aligned}
\Lambda_0 T(x) &= \Lambda_0(\frac{1}{x+a}T(x)^2) + \Lambda_0(xT(x)^4) \\
&= \Lambda_0\left((x+a)\frac{T(x)^2}{(x+a)^2}\right) + \Lambda_0(x) \cdot \phi(T)(x)^2 \\
&= a\frac{\phi(T)(x)}{x+a+1}.
\end{aligned}$$

To calculate $\Lambda_0\Lambda_0 T(x)$, we need to first put the above expression into form (5.3). Applying ϕ to both sides of (5.4) we get

$$\phi(T)(x) = \frac{1}{x+a+1}\phi(T)(x)^2 + x\phi(T)(x)^4.$$

Therefore

$$\Lambda_0 T(x) = \frac{a}{(x+a+1)^2}\phi(T)(x)^2 + \frac{ax}{(x+a+1)}\phi(T)(x)^4,$$

and

$$\begin{aligned}\Lambda_0\Lambda_0 T(x) &= \Lambda_0\left(\frac{a}{(x+a+1)^2}\phi(T)(x)^2\right) + \Lambda_0\left(\frac{ax(x+a+1)}{(x+a+1)^2}\phi(T)(x)^4,\right)\\ &= \frac{a}{x+a}\phi^2(T)(x) + \frac{a}{x+a}\phi^2(T)(x)^2\\ &= \frac{a}{x+a}T(x) + \frac{ax}{x+a}T(x)^2.\end{aligned}$$

In our program, the series $T(x)$, $\Lambda_0 T(x)$ and $\Lambda_0\Lambda_0 T(x)$ are encoded by

$$(\{0:1\},\ 0),$$
$$(\{0:a/(x+a+1)\},\ 1),$$

and

$$(\{0:a/(x+a),\ 1:ax/(x+a)\},\ 0).$$

Step three: Output function In step two, each element from the p-kernel of $T(x)$ is expressed as an $\mathbb{F}_q(x)$-linear combination of powers of $\phi^k(T)(x)$, for some $k \in [0, \log q/\log p)$. The output function maps the corresponding state to the constant term of the series. To calculate it, we simply plug in $T(x) \mod x^{D+1}$, where D is the maximum of 0 and the minus of the orders of the coefficients of the linear combination.

References

[1] Boris Adamczewski and Yann Bugeaud. On the complexity of algebraic numbers I. expansions in integer bases. *Annals of Mathematics*, pages 547–565, 2007.

[2] Boris Adamczewski and Yann Bugeaud. A short proof of the transcendence of Thue-Morse continued fractions. *Amer. Math. Monthly*, 114(6):536–540, 2007.

[3] Jean-Paul Allouche. Sur le développement en fraction continue de certaines séries formelles. *C. R. Acad. Sci. Paris Sér. I Math.*, 307(12):631–633, 1988.

[4] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences. Theory, Applications, Generalizations*. Cambridge University Press, Cambridge, 2003.

[5] Leonard E. Baum and Melvin M. Sweet. Continued fractions of algebraic power series in characteristic 2. *Ann. of Math. (2)*, 103(3):593–610, 1976.

[6] Leonard E. Baum and Melvin M. Sweet. Badly approximable power series in characteristic 2. *Ann. of Math. (2)*, 105(3):573–580, 1977.

[7] Alin Bostan, Frédéric Chyzak, Marc Giusti, Romain Lebreton, Grégoire Lecerf, Bruno Salvy, and Éric Schost. Algorithmes efficaces en calcul formel. `https://hal.archives-ouvertes.fr/AECF`, 2017.

[8] Yann Bugeaud. Automatic continued fractions are transcendental or quadratic. *Ann. Sci. Éc. Norm. Supér. (4)*, 46(6):1005–1022, 2013.

[9] Gilles Christol. Ensembles presque périodiques k-reconnaissables. *Theoretical Computer Science*, 9(1):141–145, 1979.

[10] Gilles Christol, Teturo Kamae, Michel Mendès France, and Gérard Rauzy. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France*, 108(4):401–419, 1980.

[11] Samuel Eilenberg. *Automata, languages, and machines*. Academic press, 1974.
[12] Hao Fu and Guo-Niu Han. Computer assisted proof for Apwenian sequences. In *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*, pages 231–238. ACM, New York, 2016.
[13] Yining Hu and Guoniu Wei-Han. On the automaticity of sequences defined by the thue-morse and period-doubling stieltjes continued fractions. *International Journal of Number Theory*, pages 1–26, 2020.
[14] Alain Lasjaunias and Jia-Yan Yao. Hyperquadratic continued fractions in odd characteristic with partial quotients of degree one. *J. Number Theory*, 149:259–284, 2015.
[15] Alain Lasjaunias and Jia-Yan Yao. Hyperquadratic continued fractions and automatic sequences. *Finite Fields Appl.*, 40:46–60, 2016.
[16] Alain Lasjaunias and Jia-Yan Yao. On certain recurrent and automatic sequences in finite fields. *J. Algebra*, 478:133–152, 2017.
[17] Sébastien Maulat and Bruno Salvy. Formulas for continued fractions: An automated guess and prove approach. *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, pages 275–282, 2015.
[18] W. H. Mills and David P. Robbins. Continued fractions for certain algebraic power series. *J. Number Theory*, 23(3):388–404, 1986.
[19] Mohamed Mkaouar. Sur le développement en fraction continue de la série de Baum et Sweet. *Bull. Soc. Math. France*, 123(3):361–374, 1995.
[20] M. Queffélec. Transcendance des fractions continues de Thue-Morse. *J. Number Theory*, 73(2):201–211, 1998.
[21] Wen Wu. Stieltjes continued fractions related to the paperfolding sequence and Rudin-Shapiro sequence. *Adv. Appl. Math.*, 118:102040, 2020.

School of Mathematics and Statistics, Huazhong University of Science and Technology, Wuhan, PR China
Email address: huyining@protonmail.com

I.R.M.A., UMR 7501, Université de Strasbourg et CNRS, 7 rue René Descartes, 67084 Strasbourg Cedex, France
Email address: guoniu.han@unistra.fr