Two Pattern Properties of Binary Sequences Invariant under the Continued Fraction Operator K (the Berlekamp-Massey Algorithm)

Mónica del P. Canales Chacón
MATEMATICVM, @matematicvm, Valdivia, Chile
monicadelpilar@gmail.com

Sergio Jara Ceballos
Universidad Austral de Chile, Facultad de Ingeniería, Valdivia, Chile
serjara.ing.mat@gmail.com

Michael Vielhaber
HS Bremerhaven, FB 2, Bremerhaven, Germany
vielhaber@gmail.com

Abstract

We show that a binary sequence $s = (s_1, s_2, \dots) \in \{0,1\}^\omega$ which is zero outside some arithmetic progression (residue class) $[r]_n$, *i.e.* $\mathrm{supp}(s) \subset [r]_n$, maintains this property under forward and backward iteration of the continued fraction operator $\mathbf{K}$: We still have $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$ for all $u \in \mathbb{Z}$.

The isometry $\mathbf{K}$ implements the Berlekamp-Massey Algorithm in such a way that $\mathbf{K}(s)$ is the discrepancy sequence of s and at the same time is the sequence of encodings of the partial denominators of the continued fraction expansion of $G(s) = \sum_{k\in\mathbb{N}} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$.

Furthermore, the property $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$ is maintained under $\mathbf{K}^u, u \in \mathbb{Z}$.

Keywords: Berlekamp-Massey Algorithm, Invariance under the BMA, linear complexity, sequences with restricted support.

Notation:
$\mathbb{N} = \{1, 2, 3, \dots\}$, $A = \{0, 1\}$ is the binary alphabet
0/1-inversion: $\overline{0} = 1,\ \overline{1} = 0,\ \overline{10011} = 01100$
$A^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$ and A^ω are the finite, resp. infinite words over A

1 Introduction

The continued fraction operator **K** is a modification of the well-known Berlekamp-Massey Algorithm (BMA). **K** delivers the linear complexity profile and computes the discrepancy sequence in such a way that it *is* immediately an encoding of the partial denominators (PD) of the binary sequence interpreted as formal power series.

We show that this operator **K**, an isometry on A^ω, with $A = \{0, 1\}$, has the property that sequences s whose support (indices $i \in \mathbb{N}$ with $s_i \neq 0$) lies within some residue class $i \equiv r \mod n$, $\mathrm{supp}(s) \subset [r]_n$, are mapped to sequences $\mathbf{K}^u(s)$, which again satisfy $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$, and this is valid for any number $u \in \mathbb{Z}$ of iterations.

We shall also see that the property $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$, *i.e.* all 0s and 1s appear in pairs or runs of even length, is preserved by $\mathbf{K}^u(s), u \in \mathbb{Z}$ as well.

2 Continued Fractions, Partial Denominators, the Berlekamp-Massey-Algorithm, and the Isometry K

The usual way to compute the continued fraction expansion (CFE) of a formal power series $s := \sum_{k\in\mathbb{N}} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$ starts with $s^{(0)} := s, b_0 := 0$ and then iteratively sets

$$\forall i \in \mathbb{N}\colon\ s^{(i)} := \frac{1}{\{s^{(i-1)}\}} = \frac{1}{s^{(i-1)} - b_{i-1}}, b_i := \lfloor s^{(i)} \rfloor, \text{ yielding } s = 0 + \frac{1\,|}{|b_1} + \frac{1\,|}{|b_2} + \cdots,$$

where $s^{(i)} \in \mathbb{F}_2((x^{-1}))$ has positive degree for $i \in \mathbb{N}$, the floor function $\lfloor s^{(i)} \rfloor$ gives the polynomial part $b_i \in \mathbb{F}_2[x]$ as partial denominator (PD), and we have $\{s^{(i)}\} \in \mathbb{F}_2[[x^{-1}]]$. We also denote the CFE by $s = [b_1, b_2, b_3, \dots]$.

The convergents $A_i/B_i \in \mathbb{F}_2(x)$ to s are obtained via Perron's [13] schema, see Table 1. We use the Thue-Morse sequence $s = 01101001\dots$ (see [1]) with $G(s) = \frac{1\ \ |}{|x^2+x+1} + \frac{1\ \ |}{|x^2+1} + \frac{1\,|}{|x^2} + \cdots$ as example ($b_0 = 0$ is omitted).

i	-1	0	1	2	3	4	$\dots$
b_i			x^2+x+1	x^2+1	x^2	x^2+1	$\dots$
A_i	1	0	1	x^2+1	x^4+x^2+1	x^6+x^2	$\dots$
B_i	0	1	x^2+x+1	x^4+x^3+x	$x^6+x^5+x^3+x^2+x+1$	$x^8+x^7+x^6+x^3+1$	$\dots$

Table 1: Schema for PDs $b_i \in \mathbb{F}_2[x]$ and convergents $A_i/B_i \in \mathbb{F}_2(x)$.

The initial values are $A_{-1} = B_0 = 1$, $B_{-1} = A_0 = 0$ as in the real case, and then $A_i := b_i \cdot A_{i-1} + A_{i-2}$, $B_i := b_i \cdot B_{i-1} + B_{i-2}$. Setting $r := A_i/B_i$ (a rational, *i.e.* ultimately periodic sequence), we have $r_k = s_k$ at least for $1 \le k \le \deg(B_i) + \deg(B_{i-1})$.

The continued fraction expansion and thereby the linear complexity profile is readily computed by the well-known Berlekamp-Massey-Algorithm (BMA).

In order to read off the PDs directly from the discrepancy sequence (d_k) – any sequence with $d_k = 0$, whenever the previous approximation also generates the current sequence

bit s_k, and $d_k = 1$ otherwise –, we have to make 3 simple, but crucial adjustments to the Berlekamp-Massey algorithm, as given by Dornstetter [4]:
1. Start with the convergents $A_{-1}/B_{-1} = 1/0$ and $A_0/B_0 = 0/1$.
2. Use the feedback polynomial, not its reciprocal, the connection polynomial.
3. Do not normalize the polynomials (this has an effect only for char $\mathbb{F}_p \geq 3$).

Only then, the resulting isometry $\mathbf{K}$ satisfies the observations on the support described in this paper. $\mathbf{K}$ is obtained as composition of three functions (see [15]),

$$\mathbf{K}\colon \text{sequence} \overset{G}{\longmapsto} \text{formal power series} \overset{\mathcal{K}}{\longmapsto} \text{continued fraction expansion} \overset{\pi^\infty}{\longmapsto} \text{discrepancy seq.}$$

We first treat the case of irrational that is aperiodic sequences:

$$\mathbb{F}_2^\omega \ni s \overset{G}{\longmapsto} G(s,x) = \sum_{k=1}^{\infty} s_k x^{-k} \in \mathbb{F}_2[[x^{-1}]]$$

$$G(s,x) = \frac{1}{|b_1(x)} + \frac{1}{|b_2(x)} + \frac{1}{|b_3(x)} + \cdots \overset{\mathcal{K}}{\longmapsto} (b_1, b_2, b_3, \dots) \in (\mathbb{F}_2[x]\backslash\mathbb{F}_2)^\omega$$

$$(b_i)_{i=1}^\infty \overset{\pi^\infty}{\longmapsto} \pi(b_1)\pi(b_2)\pi(b_3)\ldots = \mathbf{K}(s) \in \mathbb{F}_2^\omega,$$

where

$$\pi\colon \mathbb{F}_2[x]\backslash\mathbb{F}_2 \ni p(x) = \sum_{k=0}^{g} a_k x^k \mapsto \pi(p) = 0^{g-1} a_g \ldots a_1 a_0 \in \Pi_2$$

and

$$\Pi_2 := \{(a_1, \dots, a_n) \in \mathbb{F}_2^* \mid \exists g \in \mathbb{N} : n = 2g, a_1 = \cdots = a_{g-1} = 0, a_g \neq 0\}$$

is the set of polynomial encodings. $\Pi_2 \cup 0^\omega$ is a complete prefix code.

In the rational case, the CFE of $G(s)$ has only finitely many PDs and thus
$s \overset{G}{\longmapsto} G(s) = 0 + \frac{1}{|b_1(x)} + \cdots + \frac{1}{|b_n(x)} \overset{\mathcal{K}}{\longmapsto} (b_1, \dots, b_n) \in (\mathbb{F}_2[x]\backslash\mathbb{F}_2)^* \overset{\pi^\infty}{\longmapsto} \pi(b_1)\ldots\pi(b_n)0^\omega$
$= \mathbf{K}(s) \in \mathbb{F}_2^\omega$, including $\mathbf{K}(0^\omega) = 0^\omega$ with the empty tuple from $(\mathbb{F}_2[x]\backslash\mathbb{F}_2)^*$.

$\mathbf{K}$ is an isometry on $\mathbb{F}_2^\omega$, see [15, Thm. 5], and we have the following connection to the linear complexity: Let n_0 be the position (in s and $\mathbf{K}(s)$) at the end of an encoding $\pi(b_{i-1})$, $n_1 = n_0 + g$ the position of the leading coefficient a_g in $\pi(b_i)$, where $g = \deg(b_i)$ and $n_2 = n_1 + g = n_0 + 2g$ is the position of the constant term a_0 of b_i. At position n_1 the linear complexity jumps from $n_0/2$ to $n_2/2$ that is by $g = \deg(b_i)$ and remains otherwise constant within the positions of the encoding $\pi(b_i)$. The linear complexity deviation $L(n) - n/2$ is negative from position $n_0 + 1$ to $n_1 - 1$, it is positive afterwards until $n_2 - 1$ and zero in n_2 as well as in n_0 and in general at the end of every encoding π.

Lemma 1. *The linear complexity is*

$$L(n) = \begin{cases} n_0/2 \\ n_0/2 \\ n_0/2 + g \\ n_2/2 \\ n_2/2 \end{cases} = n/2 + \begin{cases} 0, & n = n_0, \\ -(n - n_0)/2, & n_0 < n < n_1, \\ g/2, & n = n_1, \\ +(n_2 - n)/2, & n_1 < n < n_2, \\ 0, & n = n_2. \end{cases}$$

Proof. See Theorem 6 and Proposition 8 in [15]. □

K is a discrepancy sequence for s since from n_0 to $n_1 - 1$ it is zero, no adjustment of the LFSR length is necessary, at n_1 it is nonzero, and the linear complexity / LFSR length increases by g. From n_1 to n_2, with $L \geq n/2$, no change in the LFSR length will take place.

The implementations of the BMA by Massey [9], by Lidl/Niederreiter [8], and the BMA* by Dornstetter [4] / Vielhaber [15] are pairwise different in the part $a_{g-1} \ldots a_1 a_0$ between n_1 and n_2, but all coincide (of course) in the discrepancy sequence being zero from $n_0 + 1$ to $n_1 - 1$, 0^{g-1}, followed by some nonzero symbol at n_1.

However, *only* the Dornstetter / **K** implementation described here yields immediately useful information on the PDs and *only* for this BMA* implementation, the implications about supports and residue classes in this paper are valid. Fast implementations are given in [2] [11] [12].

Example 2. for **K**

(i) Rational sequence: Let $s = (s_k)_{k=1}^{\infty} = 1(110)^{\omega} \in \mathbb{F}_2^{\omega}$, then

$$G(s) \;=\; \frac{1}{x} + \frac{x+1}{x^3+1} = \frac{x^3+1+x^2+x}{x^4+x} = \frac{1}{\frac{x^4+1+x+1}{(x+1)^3}} = \frac{1 \;\;|}{|x+1} + \frac{1 \;\;|}{|x^2+1}.$$

Thus $\mathcal{K}(G(s)) = (x+1, x^2+1) \in \mathbb{F}_2[x]^*$ and $\mathbf{K}(s) = 1101010^{\omega} \in \mathbb{F}_2^{\omega}$, where $11 = \pi(x+1)$, $0101 = \pi(x^2+1)$.

(ii) Irrational sequence: The (Prouhet-) Thue-Morse (-Hedlund) sequence $s = 0110.1001.1001.0110.1001\ldots$ is quadratic-algebraic with ultimately periodic CFE $G(s) = [x^2+x+1, (x^2+1, x^2, x^2+1)^{\omega}]$ (the analogue of Lagrange's result [7] for formal power series). We infer $\mathbf{K}(s) = 0111(0101\ 0100\ 0101)^{\omega}$. Note that $\mathrm{supp}(\mathbf{K}(s)) \subset [0]_2 \,\dot\cup\, \{3\}$, but $\mathrm{supp}(s) \not\subset [r]_n$ for no r, n: A single bit outside the residue class completely destroys the pattern.

3 The Main Result: Arithmetic Progressions as Supersets of the Support of a Binary Sequence are Invariant under K

Definition 3. (i) For $n \in \mathbb{N}, r \in \mathbb{Z}$ (usually we take $0 \leq r < n$), let $[r]_n = \{k \in \mathbb{N} \mid k \equiv r \pmod n\} \subset \mathbb{N}$ be an arithmetic progression (residue class from $\mathbb{Z}/n\mathbb{Z}$ restricted to $\mathbb{N}$). We will use the $[r]_n$ as supersets for index sets of formal power series.

(ii) Let $\mathrm{supp}(s) := \{k \mid s_k \neq 0\} \subset \mathbb{N}$ be the support of $s \in A^{\omega}$ or $s \in \mathbb{F}_2[[x^{-1}]]$.

We first mention a technical lemma from [11],which we shall need in parts II and III of the proof of Theorem 6 and in the proof of Theorem 9:

Lemma 4. Equivalence Lemma [11, Lemma 11]

Let A, B be two consecutive PDs of a CFE. Replacing A, B by the three PDs $A+1, 1, 1+B$ does not change the overall value of the CFE.

Proof. See Lemma 11 in [11], also ...

Using Perron's schema with A, B and with $A+1, 1, 1+B$ both yield the same result:

$$x \mid y \overset{A}{\mid} Ay + x \overset{B}{\mid} ABy + Bx + y \text{ and}$$
$$x \mid y \overset{A+1}{\mid} Ay + y + x \overset{1}{\mid} Ay\underline{+y} + x\underline{+y} \overset{B+1}{\mid} ABy + Bx\underline{+Ay + x + Ay} + y\underline{+x}$$

(underlined parts cancel for $\mathbb{F}_2$, the lemma does not carry over to char ≥ 3). □

We have the following lemma concerning the position of nonzero coefficients in PDs, given a formal power series s with $\mathrm{supp}(s) \subset [r]_n$:

Lemma 5. *Let* $\mathrm{supp}(s) \subset [r]_n$ *for some* $n \in \mathbb{N}, 0 \leq r \leq n$.

(i) The first PD, b_1*, has degree* $g_1 \in [r]_n$ *and the nonzero coefficients* a_k*, if any, are also at indices* $k \in [r]_n$.

(ii) The second PD, b_2*, has degree* g_2 *and nonzero coefficients' indices in* $[-r]_n$.

(iii) All PDs with odd index, $b_3, b_5, \ldots$ *behave as* b_1 *does, with support in* $[r]_n$*. The PDs with even indices have support in* $[-r]_n$.

Proof. *(i)* From $\pi(b_1) = 0^{g_1-1}a_{g_1} \ldots a_0$ and $\mathrm{supp}(s) \subset [r]_n$, we have $g_1 = \deg(b_1) \in [r]_n$. The distance from a_{g_1} of all nonzero coefficients in π is a multiple of n and thus their index is in the same residue class, $k \in [g_1]_n = [r]_n$.

(ii) With $|\pi(b_1)| = 2 \cdot g_1$, the position of a_{g_2} in $\pi(b_2)$ is at $2g_1 + g_2 \equiv 2r + g_2 \in [r]_n$ and hence $g_2 \in [-r]_n$. As in *(i)* the same applies for the further nonzero coefficients: $a_k \neq 0$ implies $k \in [-r]_n$.

(iii) From $|\pi(b_1)\pi(b_2)| = 2(g_1+g_2) \equiv 2(r+(-r)) \equiv 0 \mod n$, we see that the situation for the degree g_3 of b_3 is the same as for b_1 in *(i)*, then b_4 behaves as in *(ii)* and the general case follows by induction. □

We now come to the Main Theorem of the paper:

Theorem 6. Invariance of Arithmetic Progressions under **K**

For any given $n \in \mathbb{N}$, $0 \leq r \leq n-1$*, for all binary sequences* $s \in A^\omega$ *such that the support of* s *is contained in* $[r]_n$ *i.e.*

$$G(s,x) = \sum_{k \in \mathbb{N}} s_k x^{-k} = \sum_{k \in [r]_n} s_k x^{-k}$$

the resulting sequences $\mathbf{K}^u(s)$ *again have support* $\mathrm{supp}(\mathbf{K}^{(u)}(s)) \subset [r]_n$*, for all* $u \in \mathbb{Z}$*. In other words* $\forall u \in \mathbb{Z}, \forall n \in \mathbb{N}, \forall 0 \leq r < n$:

$$\mathrm{supp}(s) \subset [r]_n \iff \mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n \iff (\mathbf{K}^u(s))_k = 0, \forall k \notin [r]_n.$$

Proof. For $n = 1$, $[0]_1 = \mathbb{N}$, nothing has to be shown. Otherwise, we proceed in 5 steps.

I. *"Blow-Up" / "Telescoping-out"* (from s to $\mathbf{K}(s)$ at $[0]_n$)

We start with $r = 0, u = 1$, any $n \geq 2 \in \mathbb{N}$. Let $s \in A^\omega$ have $\mathrm{supp}(s) \subset [0]_n$.

Set $\alpha_k := s_{nk}, k \in \mathbb{N}$, the subsequence with indices from $[0]_n$. By construction,

$$G(s,x) = \sum_{k \in \mathbb{N}} s_k x^{-k} = \sum_{k \in [0]_n} s_k x^{-k} = \sum_{k \in \mathbb{N}} s_{k \cdot n} \left(x^n\right)^{-k} = \sum_{k \in \mathbb{N}} \alpha_k \left(x^n\right)^{-k} = G(\alpha, x^n).$$

Let now $\beta := \mathbf{K}(\alpha)$ be the CFE of $G(\alpha, y)$ (where no restrictions on the support apply). Then $\beta = \pi(b_1)\pi(b_2)\dots$ is the concatenation of the encodings of the PDs of $G(\alpha, y) = \frac{1}{|b_1(y)} + \frac{1}{|b_2(y)} + \cdots$. We now do a "Blow-Up" or "Telescoping-out" and set $y := x^n$, effectively introducing $n-1$ zeroes between any two symbols from β.

From $\pi(p(y)) = \pi(\sum_{j=0}^{g} p_j y^j) = 0^{g-1}1p_{g-1}p_{g-2}\dots p_1 p_0$, we then get

$$\pi(p(x^n)) = \pi(\sum_{j=0}^{g} p_j x^{n\cdot j}) = 0^{n\cdot g-1}10^{n-1}p_{g-1}0^{n-1}p_{g-2}\dots 0^{n-1}p_1 0^{n-1}p_0,$$

where only the powers of x which are multiples of n are used for the p_j. This gives

$$G(\alpha, x^n) = \frac{1}{|b_1(x^n)} + \frac{1}{|b_2(x^n)} + \frac{1}{|b_3(x^n)} + \cdots = G(s, x).$$

Now, $0^{n\cdot g-1}10^{n-1}p_{g-1}0^{n-1}p_{g-2}\dots 0^{n-1}p_1 0^{n-1}p_0$ has the property that the indices of its coefficients p_j lie in the set $[0]_n$. Since this is valid for all $\pi(b_i(x^n))$, and each of these $\pi(\cdot)$ have a length which is a multiple of n, namely $n \cdot 2 \cdot \deg(b_i(y))$, the whole result $\mathbf{K}(s)$ is covered by $[0]_n$.

II. *"Last Shift"* (from $s, \mathbf{K}(s) \subset [0]_n$ to $s, \mathbf{K}(s) \subset [n-1]_n$)

Let $\mathrm{supp}(s) \subset [n-1]_n, n \geq 2$. Let $\hat{s} := (0, s_1, s_2, \dots)$, hence $\mathrm{supp}(\hat{s}) \subset [0]_n$ and with part I also $\mathrm{supp}(\mathbf{K}(\hat{s})) \subset [0]_n$. Furthermore, we have $G(\hat{s}) = x^{-1} \cdot G(s)$.

The CFE of $G(\hat{s}) = [b_1, b_2, b_3, \dots]$ consists only of PDs with $\deg(b_i)$ a multiple of n, in particular $\deg(b_i) > 1$. Applying the Equivalence Lemma, we generate a new, but equivalent CFE $G(\hat{s}) = [b'_1, b'_2, b'_3, \dots]$, where b'_{2i-1} has constant term zero by, if necessary, inverting this term, introducing a pseudo-PD '1' as b'_{2i}, inverting the constant term of the next PD b'_{2i+1}, and so on.

We then multiply the whole CFE by x, which amounts to alternately divide and multiply the PDs by x:

$$G(s) = x \cdot G(\hat{s}) = [b'_1/x, b'_2 \cdot x, b'_3/x, \dots],$$

where the division at odd indices is well-defined, since $\deg(b'_{2i-1}) > 1$ and the constant term is zero. Also, the pseudo-PDs '1' occur only at even indices and are replaced by x.

Now, in $\mathbf{K}(s) = \pi^{\infty}(b'_1/x, b'_2 \cdot x, b'_3/x, \dots)$, the odd-indexed b'_{2i-1}/x have support and degree in $[-1]_n$, the even-indexed $b'_{2i} \cdot x$ have support and degree in $[1]_n$, including the special case x from '1' with degree 1. Each pair (b'_{2i-1}, b'_{2i}) has an overall degree sum from $[-1]_n + [1]_n = [0]_n$, allowing the induction as in Lemma 5, and giving $\mathrm{supp}(\mathbf{K}(s)) \subset [-1]_n$.

III. *"First Shift"* (from $s, \mathbf{K}(s) \subset [0]_n$ to $s, \mathbf{K}(s) \subset [1]_n$)

This is essentially a repetition of part II, shift direction and parity inverted.

Let $\mathrm{supp}(s) \subset [1]_n, n \geq 2$. Let first $s_1 = 0$. Let $\hat{s} := \sigma(s) := (s_2, s_3, \dots)$, hence $\mathrm{supp}(\hat{s}), \mathrm{supp}(\mathbf{K}(\hat{s})) \subset [0]_n$. Also, $G(\hat{s}) = x \cdot G(s)$.

The CFE of $G(\hat{s}) = [b_1, b_2, b_3, \dots]$ consists only of PDs with $n \mid \deg(b_i)$.

As before, by Lemma 5, we generate an equivalent CFE $G(\hat{s}) = [b'_1, b'_2, b'_3, \dots]$, where now the *even* b'_{2i} have constant term zero, applying Lemma 5, introducing pseudo-PDs '1' as b'_{2i+1} at odd index.

We then divide by x, giving $G(s) = G(\hat{s})/x = [b'_1 \cdot x, b'_2/x, b'_3 \cdot x, \dots]$, where the division at even indices is well-defined, as before and the pseudo-PDs '1', now at odd indices, are again replaced by x.

Now, in $\mathbf{K}(s) = \pi^\infty(b'_1 \cdot x, b'_2/x, b'_3 \cdot x, \dots)$, the odd-indexed $b'_{2i-1} \cdot x$ have support and degree in $[1]_n$, including the special case x from '1' with degree 1. The even-indexed b'_{2i}/x have support and degree in $[-1]_n$. Thus, again each pair (b'_{2i-1}, b'_{2i}) has an overall degree sum from $[1]_n + [-1]_n = [0]_n$, allowing the induction as in Lemma 5.

For $s_1 = 1$, $x \cdot G(s) = 1 + G(\hat{s})$. Observe that $1 + [b_1, b_2, \dots] = 0 + [1, b_1 + 1, b_2, \dots]$ by Lemma 5 with $(1, b_1) \equiv (0, 1, b_1 + 1)$, see [11, Cor. 12], which fits neatly into the overall process, the pseudo-PD being at an odd index. All in all, $\mathrm{supp}(\mathbf{K}(s)) \subset [1]_n$.

IV. *"General Shift"* (from $[r]_n$ to $[r \pm 1]_n$)

Let $r \notin \{-1, 0, +1\}$ and $\mathrm{supp}(s) \subset [r]_n$. By the condition on r, all PDs have degree at least 2 and all constant terms are zero, also the first bit $s_1 = 0$. The sequence $\overleftarrow{s} := (s_2, s_3, s_4, \dots)$ has $\mathrm{supp}(\overleftarrow{s}) \subset [r-1]_n$, the sequence $\overrightarrow{s} := (0, s_1, s_2, \dots)$ has $\mathrm{supp}(\overrightarrow{s}) \subset [r+1]_n$, by construction.

Hence, from $G(s) =: [b_1, b_2, b_3, \dots]$, we immediately obtain $G(\overleftarrow{s}) = [b_1/x, b_2 \cdot x, b_3/x, \dots]$ and $G(\overrightarrow{s}) = [b_1 \cdot x, b_2/x, b_3 \cdot x, \dots]$, all terms well-defined and no pseudo-PD '1' involved.

Therefore, the 3 sequences $00\pi^\infty(b_1/x, b_2 \cdot x, b_3/x, \dots) = 0\pi^\infty(b_1, b_2, b_3, \dots) = \pi^\infty(b_1 \cdot x, b_2/x, b_3 \cdot x, \dots)$ are one and the same, in other words $\mathrm{supp}(\overleftarrow{s}) \subset [r-1]_n \Leftrightarrow \mathrm{supp}(\mathbf{K}(s)) \subset [r]_n \Leftrightarrow \mathrm{supp}(\overrightarrow{s}) \subset [r+1]_n$.

In parts I, II, III, we have seen that $\mathrm{supp}(s) \subset [a]_n \Leftrightarrow \mathrm{supp}(\mathbf{K}(s)) \subset [a]_n$ for $a \in \{-1, 0, +1\}$. By the previous equality, we can now extend this to $a = 2$ and $a = -2$, and by induction to all $0 \le a, r \le n - 1$.

V. *Isometry & Induction* (from $\mathbf{K}(s)$ to $\mathbf{K}^u(s)$)

We now show for arbitrary $n \in \mathbb{N}$, $0 \le r < n$ and any $u \in \mathbb{Z}$ that $\mathbf{K}^u$ maintains the invariant, $\mathrm{supp}(\mathbf{K}^u(s)) \subset [r]_n$. We have seen that this is true for $u = 1$. By induction, this is also valid for $u \in \mathbb{N}$ (forward application of $\mathbf{K}$).

$\mathbf{K}$ is an isometry. Therefore, restricting $\mathbf{K}$ to the first k coordinates, we have $\mathbf{K}^{2!^k}(s)_{1\dots k} = (s_1, \dots, s_k)$ and thus $\mathbf{K}^{2^k-1}(s)_{1\dots k} = \mathbf{K}^{-1}(s)_{1\dots k}$, since $\mathbf{K}$ is invertible as isometry. Hence, the (positive) case $u = 2^k - 1$ already has shown $\mathrm{supp}(\mathbf{K}^{-1}) \subset [r]_n$ for the first k coordinates. Letting $k \to \infty$ shows the claim for $u = -1$. Applying induction to the (negative) exponent shows it for all $u \in \mathbb{Z}$. □

As a consequence of Main Theorem 6 and Lemma 5, we obtain the following corollary:

Corollary 7. (*i*) *Let* $\mathrm{supp}(s) \subset [0]_n$ *for some* $n \in \mathbb{N}$. *Then all PDs of all* $\mathbf{K}^u(s)$ *have degrees and indices of nonzero coefficients a multiple of* n.

(*ii*) *Let* $\mathrm{supp}(s) \subset [r]_n$ *for some* $n \in \mathbb{N}$ *and* $1 \le r \le n - 1$. *Then all* $\mathbf{K}^u(s)$ *have alternately degrees* $d \equiv r \pmod n$, *for* $b_1, b_3, b_5, \dots$, *and degrees* $d \equiv n - r \pmod n$, *for* $b_2, b_4, b_6, \dots$. *The same applies for the indices of nonzero coefficients.*

In particular, for $n = 2$, *we obtain:*
(*iii*) *Let* $s \in A^\omega$ *be such that* $s_{2i-1} = 0, i \in \mathbb{N}$, *i.e.* $\mathrm{supp}(s) \subset [0]_2$. *Then all odd coefficients of* $\mathbf{K}^u(s), u \in \mathbb{Z}$ *are zero as well and thus the PDs are all of even degree.*

(*iv*) *Similarly, for* $\mathrm{supp}(s) \subset [1]_2$*, only coefficients with odd indices may be non-zero and thus all* $\mathbf{K}^u(s), u \in \mathbb{Z}$ *have only PDs with odd degree.*

Proof. The corollary follows immediately from Lemma 5 and Main Theorem 6. □

Conjecture 8. Theorem 6 is valid for sequences over any finite field $\mathbb{F}_q$.

Proof. Idea: Parts I, IV, and V of the proof carry over without change to any $\mathbb{F}_q$. For parts II and III, we must replace Lemma 4 by the more involved cases treated in [12]. □

4 A Further Sequence Pattern Property Maintained by K

Theorem 9. *Let* $s = (s_1, s_2, \dots) \in A^\omega$ *be a binary sequence with* $s_{2n-1} = s_{2n}, \forall n \in \mathbb{N}$.
Then for any $u \in \mathbb{Z}$, $t = (t_1, t_2, \dots) := \mathbf{K}^u(s)$ *also satisfies* $t_{2n-1} = t_{2n}, \forall n \in \mathbb{N}$.

Proof. Firstly, we have $G(s, x) = (x + 1) \cdot G(\hat{s}, x^2)$ with $\hat{s}_n := s_{2n}$, since two consecutive 1s can be extracted into the factor $(x + 1)$, leaving a single 1 at an even index.

Now, $\mathbf{K}(\hat{s})$ is just some binary sequence, which we call $\hat{t}$. By blow-up with a factor of 2, $G(\hat{s}, x^2)$ has a CFE $[\hat{b}_1, \hat{b}_2, \dots]$ such that $\pi(\hat{b}_1)\pi(\hat{b}_2)\dots = 0\hat{t}_1 0\hat{t}_2 0\hat{t}_3 0\hat{t}_4 \dots$, where the $\hat{b}_i$ are polynomials in x^2, *e.g.* $\pi(x^2) = 0100, \pi(x^2 + 1) = 0101$.

From $G(s, x) = (x + 1) \cdot G(\hat{s}, x^2)$, the desired CFE $\mathbf{K}(s)$ then corresponds to the CFE of $G(s, x) = [\hat{b}_1/(x + 1), \hat{b}_2 \cdot (x + 1), \hat{b}_3/(x + 1), \hat{b}_4 \cdot (x + 1), \dots]$ — if well-defined.

The PDs with odd index therefore have to be multiples of $(x + 1)$, which is equivalent to having an even number of coefficients 1. Again, we apply the Equivalence Lemma.

This time, we include or exclude a constant term $a_0 = 1$ in such a way that $\hat{b}'_{2i-1}$ has an even number of nonzero (*i.e.* 1) coefficients. As before, we introduce a pseudo-PD 1 (=: $\hat{b}'_{2i}$) after $\hat{b}'_{2i-1}$ in this case, toggle the constant coefficient of the next PD, and so on.

We now have PDs with odd index, having an even number of (still isolated) 1s, and PDs with even index, having any number of (isolated) 1s, or being the pseudo-PD 1.

We multiply the PDs with even index by $x+1$, giving a pattern '11' for every (isolated) 1 present previously, and a pseudo-PD 1 is changed to $x + 1$ with $\pi(x + 1) = 11$.

The PDs with odd index have to be divided by $(x + 1)$. Such a PD now has an even number of 1s. Hence we can split the coefficient sequence $0^{l_1}10^{k_1}10^{l_2}10^{k_2}10^{l_3}10^{k_3}1\dots$ into parts $0^{l_i}10^{k_i}1$, corresponding to polynomials $x^{k_i+1} + 1 = (x + 1) \cdot \sum_{j=0}^{k_i} x^j$.

Since all zero runs have odd length (the 1s appear at even positions from $[0]_2$), this polynomial consists of an even number of consecutive coefficients 1, or $(k_i + 1)/2$ patterns '11'. The whole $\pi(\hat{b}'_{2i-1}/(x + 1))$ thus consists of a mix of patterns '00' and '11'. The same is (trivially) true for $\pi(\hat{b}'_{2i} \cdot (x + 1))$, and we obtain $t_{2n-1} = t_{2n}, \forall n \in \mathbb{N}$.

The general case $u \in \mathbb{Z}$ follows as in the proof of Main Theorem 6 by induction and $\mathbf{K}$ being an isometry. □

5 The $\widehat{K}$ Isometry and its Tree Complexity

In this section, we apply Theorems 6 and 9, showing *why* the tree complexity of the isometry induced by linear complexity is so small, compared to those of 2-adic and rational complexity, following the isometric approach as expounded at SETA 2004, [14].

Tree complexity of Isometries

The three complexity measures K (linear), A (2-adic) [5] [6], and R (rational) [16] [17] [18] can be compared via their induced isometries $\mathbf{Y} \in \{\mathbf{K}, \mathbf{A}, \mathbf{R}\}$, determining their tree complexity ([10][14]).

Let an infinite regular binary tree with labels be indexed by $v \in A^*$. Starting with $v = \varepsilon$ at the root, each node v has its left and right child nodes indexed by $v0$ and $v1$, respectively. The label at node v, $\widehat{\mathrm{Y}}(v) := \mathbf{Y}(v0^\omega)_{|v|+1} \in A$ is the result of the mapping $v0\ldots \overset{\mathbf{Y}}{\longmapsto} w\hat{Y}(v)\ldots$. The tree complexity of the labeling (lower bounds from first 36 levels) is given in Table 2.

$\widehat{Y}$	$h=1$	2	3	4	5	6
$\widehat{\mathrm{K}}$	2	8	48	480	2816	21760
$\widehat{\mathrm{A}}$	2	8	128	10506	1931K	91M
$\widehat{\mathrm{R}}$	2	8	118	12244	2195K	45M

Table 2: Tree complexities of induced isometries, $K_B(\widehat{Y}, h)$ for $h = 1, \ldots, 6$.

Apparently, **K** is by far the least complex (in terms of tree complexity) of the three isometries. **A** and **R** are of comparable complexity, also suggested by the fact $\mathbf{A}(v^\omega) = \mathbf{R}(\overleftarrow{v}^\omega), \forall v \in A^+$ (see [18, Thm. 13]).

The Results of Massey/Wang and Carter

We now show that Theorems 6 and 9 together with results by Massey and Wang [19] and by Carter [3] fix a large part of the initial part of the isometry **K**.

Theorem 10. (*Massey and Wang* [19])
A sequence $s \in A^\omega$ has perfect linear complexity profile, i.e. all PDs are of degree 1, if and only if $s_1 = 1$, and $s_{2i+1} = s_i + s_{2i}$ for $i \in \mathbb{N}$. The s_{2i} can be chosen arbitrarily.

Proof. See [19]. □

Theorem 11. (*Carter* [3])
(*i*) *A sequence $s \in A^\omega$ with $s_1 = 0$, and $s_{2i+1} = s_i + s_{2i}$ for $i \in \mathbb{N}$ (where the s_{2i} can be chosen arbitrarily) has only PDs of even degree, or of degree 1. No two consecutive PDs have degree 1.*
(*ii*) *A sequence $s \in A^\omega$ with $s_2 = 1$, and $s_{2i+2} = s_{i+1} + s_{2i+1}$ for $i \in \mathbb{N}$ (where the s_{2i-1} can be chosen arbitrarily) has only PDs of odd degree, or of degree 2.*
(*iii*) *A sequence $s \in A^\omega$ with $s_2 = 0$, and $s_{2i+2} = s_{i+1} + s_{2i+1}$ for $i \in \mathbb{N}$ (where the s_{2i-1} can be chosen arbitrarily) has only PDs of odd degree.*

Proof. See [3], Theorems 4.3.3, 4.3.4 for (*i*), 4.4.3 for (*ii*) and 4.4.2 for (*iii*). □

0,1 :	fixed value	! :	value fixed, depending on some previous entries
* :	arbitrary value	= :	value repeats the entry immediately before

Source	Pattern in s	Permitted PD degrees in $\mathbf{K}(s)$
MW [19]	`1*!*!*!*!*`	1
C_1 [3]	`0*!*!*!*!*`	1; 2,4,6,..., not 1|1
C_2 [3]	`*1*!*!*!*!`	2; 1,3,5,...
C_3 [3]	`*0*!*!*!*!`	1,3,5,...
$[0]_2$	`0*0*0*0*0*`	2,4,6,...
$[1]_2$	`*0*0*0*0*0`	1,3,5,...
Thm. 9	`*=*=*=*=*=`	1,3,5,...
$[0]_3$	`00*00*00*0`	3,6,9,...
$[1]_3$	`0*00*00*00`	$((2,5,8,\dots)(1,4,7,\dots))^\omega$
$[2]_3$	`*00*00*00*`	$((1,4,7,\dots)(2,5,8,\dots))^\omega$
$[0]_7$	`000000*000`	7,14,21,...
$[1]_7$	`*000000*00`	$((1,8,15,\dots)(6,13,20,\dots))^\omega$
$[5]_7$	`0000*00000`	$((5,12,19,\dots)(2,9,16,\dots))^\omega$

Figure 1: Patterns in s and PD degrees in its Continued Fraction.

Regularity of the isometry induced by K

Summarizing the results of Massey and Wang, Carter, the $[r]_n$ cases of Theorem 6 and Theorem 9, we have the invariant patterns for the support given in Figure 1.

We therefore have the restrictions shown in Figure 2 (**a?** unknown bit, but same **a!** at child nodes) for the tree complexity of $\widehat{K}$, from the following patterns, where the underlined value is mandatory and $va \xrightarrow{\mathbf{K}} wb$ gives $\widehat{K}(v) = a + b$. Theorems 6 and 9 fix 38 out of the first 63 entries of the $\widehat{K}$ tree, and also including the results by Wang and Massey and by Carter as well as LFSR theory, we account for 47 out of these 63 entries in the first 6 levels of the $\hat{K}$ tree:
LFSR theory, LF: $v^\omega \mapsto *^{2|v|}\underline{0}^\omega$, *e.g.* $101010 \mapsto 101\underline{00}$
Thm 6, $[r]_n$: $\forall 0 \le r < n \in \mathbb{N}, \forall v \in A^*$: $(\mathrm{supp}(v) \subset [r]_n) \wedge (|v| + 1 \notin [r]_n) \Rightarrow \mathbf{K}(v) = 0$
Thm 9: $\forall a, b, c, \dots, \exists \alpha, \beta, \gamma, \dots : aabbcc\dots \mapsto \alpha\underline{\alpha}\beta\underline{\beta}\gamma\underline{\gamma}\dots$, *e.g.* $110011 \mapsto 1\underline{1}1\underline{1}1\underline{1}$
Massey-Wang, MW: $(1, a, a+1, b, b+a, c, c+a+1, \underline{d}, d+b, e, e+b+a, \dots)$
$\mapsto \underline{1} * \underline{1} * \underline{1} * \underline{1} * \underline{1} * \dots$, hence $\widehat{K}(\varepsilon) = 1 + 1 = 0, \widehat{K}(1a) = a + 1 + 1 = a$
Carter (i), C_1: $\{(0, a, a+0, b, b+a, c, \dots)\} \to \{00\underline{0}\underline{0}, 1*\underline{0}\underline{0}\underline{0}, \dots\}$
Carter (iii), C_3: $\{(a, 0, b, b+0, c, c+b, \dots)\} \to \{1*1*0\underline{0}, 1*0\underline{0}\underline{0}\underline{0}, 0\underline{0}\underline{0}\underline{0}\underline{0}\underline{0}, \dots\}$

Proposition 12. *Asymptotically, in row $N \in \mathbb{N}$, $\Theta(2^{N/2})$ out of the 2^{N-1} prefixes $v \in A^{N-1}$ have a value $\widehat{K}(v)$ that is determined by one of the cases $[r]_2$, Theorem 9, or MW.*

Proof. For even $|v|$, both $[0]_2$ and MW yield $2^{|v|/2}$ cases where $\mathbf{K}(va)_{|v|+1}$ is restricted to 0, respectively 1. For odd $|v|$, both $[1]_2$ and Theorem 9 yield $2^{(|v|+1)/2}$ cases by restricting $\mathbf{K}(va)_{|v|+1}$ to 0, respectively $\mathbf{K}(va)_{|v|}$. □

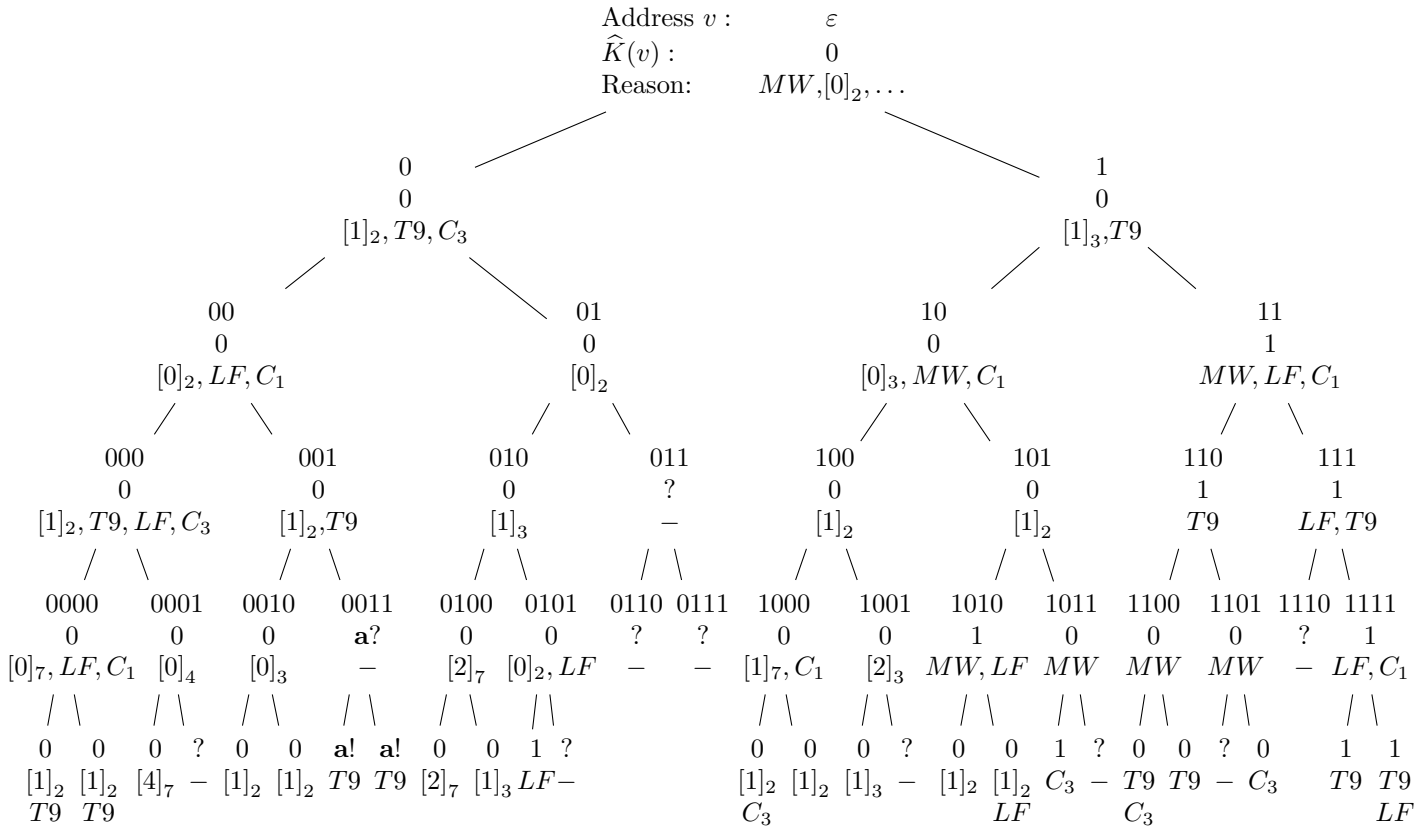

Figure 2: Address $v \in A^*$, $\widehat{K}(v)$, and reason for $\widehat{K}(v)$.

Conjecture 13. Including all $[r]_n$ of Theorem 6 (prime n is sufficient), Carter (i, ii, iii) and LFSR theory does not change the asymptotic result of Proposition 12.

Conclusion

We have shown that for all binary sequences $s \in A^\omega$, the properties $\mathrm{supp}(s) \subset [r]_n$ for any residue class, and $s_{2k-1} = s_{2k}, \forall k \in \mathbb{N}$ are preserved under forward and backward application of the continued fraction operator $\mathbf{K}$ (the modified Berlekamp-Massey Algorithm). We applied the result to the $\widehat{K}$ tree associated with the isometry $\mathbf{K}$.

References

[1] J.-P. Allouche, J. Shallit, *Automatic Sequences*, CUP, 2003.

[2] M. del P. Canales Chacón, M. Vielhaber. Structural and Computational Complexity of Isometries and their Shift Commutators. *Electronic Colloquium on Computational Complexity*, ECCC TR04–057, 2004.

[3] G. D. Carter. Aspects of local linear complexity. *PhD Thesis. Royal Holloway and Bedford New College, London*, 1989.

[4] J. L. Dornstetter. On the equivalence between Berlekamp's and Euclid's algorithm. *IEEE Trans IT*, 33(3):428-431, 1987.

[5] A. Klapper, M. Goresky. Cryptanalysis Based on 2-Adic Rational Approximation. *Crypto '95, LNCS*, 963:262–273, 1995.

[6] A. Klapper, M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J Crypt*, 10:111–147, 1997.

[7] J. L. Lagrange, *Additions au mémoire sur la réduction des equations numériques.* Mémoires de l'Académie royale des sciences et belles-lettres (de Berlin) 24, 1770.

[8] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, CUP, 1994.

[9] J. Massey. Shift-register synthesis and BCH decoding. *IEEE IT*, 15(1):122-127, 1969.

[10] H. Niederreiter, M. Vielhaber. Tree complexity and a doubly exponential gap between structured and random sequences. *J Complexity*, 12(3):187-198, 1996.

[11] H. Niederreiter, M. Vielhaber. Simultaneous shifted continued fraction expansions in quadratic time. *AAECC*, 9(2):125-138, 1998.

[12] H. Niederreiter, M. Vielhaber. An algorithm for shifted continued fraction expansions in parallel linear time. *TCS* 226(1-2):93-104, 1999.

[13] O. Perron. Die Lehre von den Kettenbrüchen, Bd. I. *Teubner, Stuttgart 1954/1977.*

[14] M. Vielhaber. A Unified View on Sequence Complexity Measures as Isometries. **SETA** 2004, *LNCS*, 3486:143-153, 2004.

[15] M. Vielhaber. Continued Fraction Expansion as Isometry - The Law of the Iterated Logarithm for Linear, Jump, and 2-Adic Complexity. *IEEE Trans IT*, 53(11):4383-4391, 2007. (Preprint: `arXiv:cs/0511089`)

[16] M. Vielhaber. V Tree — Continued Fraction Expansion, Stern-Brocot Tree, Minkowski's ?($\mathbf{x}$) Function In Binary: Exponentially Faster. `arXiv:2008.08020`, 2020.

[17] M. Vielhaber, M. del P. Canales, S. Jara. Feedback in Q Shift Registers FQSR: Pseudo-Ultrametric Continued Fractions in R. **SETA** 2020.

[18] M. Vielhaber, M. del P. Canales, S. Jara. Rational complexity of binary sequences, FQSRs, and pseudo-ultrametric continued fractions in $\mathbb{R}$. *Cryptography and Communications*, 14(2):433-457, 2022.

[19] M.-Z. Wang, J. Massey. The characterization of all binary sequences with a perfect linear complexity profile. EUROCRYPT '86, Linköping, 1986.