Maximum order complexity for some automatic and morphic sequences along polynomial values

Pierre Popoli

Institut Élie Cartan de Lorraine, Vandœuvre-lès-Nancy, France

Combinatorics on Words, June 27, 2022

Summary

Thue–Morse sequence $\mathcal{T}$

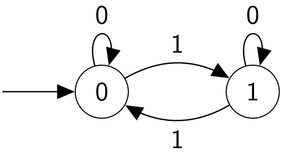
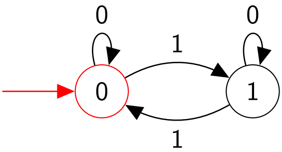


Figure: Automaton of the Thue–Morse sequence $\mathcal{T} = (t(n))_n$

Input: $(13)_2 = 1101$, we read left to right.



Thue–Morse sequence $\mathcal{T}$

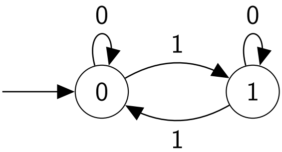
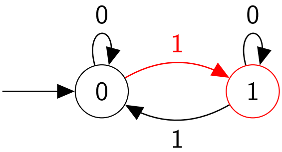


Figure: Automaton of the Thue–Morse sequence $\mathcal{T} = (t(n))_n$

Input: $(13)_2 = 1101$, we read left to right.



Thue–Morse sequence $\mathcal{T}$

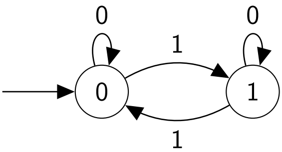
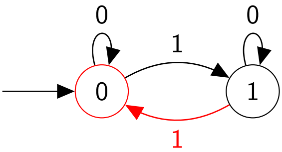


Figure: Automaton of the Thue–Morse sequence $\mathcal{T} = (t(n))_n$

Input: $(13)_2 = 1101$, we read left to right.



Thue–Morse sequence $\mathcal{T}$

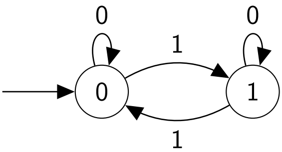
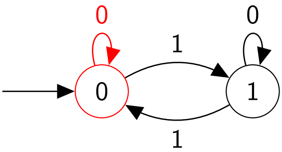


Figure: Automaton of the Thue–Morse sequence $\mathcal{T} = (t(n))_n$

Input: $(13)_2 = 1101$, we read left to right.



Thue–Morse sequence $\mathcal{T}$

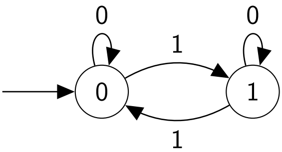
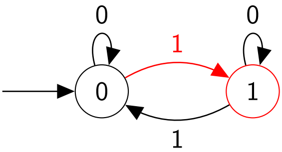


Figure: Automaton of the Thue–Morse sequence $\mathcal{T} = (t(n))_n$

Input: $(13)_2 = 1101$, we read left to right.



Then $t(13) = 1$.

Thue–Morse sequence $\mathcal{T}$

$\mathcal{T}$ can also be generated by the following morphism $f : \begin{cases} 0 \mapsto 01 \\ 1 \mapsto 10. \end{cases}$

This morphism is *uniform*: images have same length.

We apply recursively the corresponding morphism

$$\begin{aligned} &0 \\ &f(0) = 01 \\ &f(01) = f(0)\ f(1) = 01\ 10 \\ &f(0110) = 0110\ 1001 \\ &\vdots \\ &f^{\omega}(0) = 0110100110010110\ldots \end{aligned}$$

Thus $t(n)$ is the n-th value of $f^{\omega}(0)$.

Automatic sequence: generated by an automaton or equivalently as a projection of a fixed point of a uniform morphism.

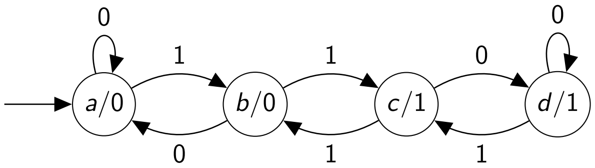


Figure: Automaton of the Golay–Rudin–Shapiro sequence $\mathcal{R} = (r(n))_n$

For $(13)_2 = \texttt{1101}$, we have $r(13) = 1$.

$\mathcal{R} = (r(n))_n = 000100100011101\ldots$
Or with the morphism $f : \begin{cases} a \mapsto ab, b \mapsto ac, \\ c \mapsto db, d \mapsto dc. \end{cases}$ and $\pi : \begin{cases} a, b \mapsto 0, \\ c, d \mapsto 1. \end{cases}$

Thus $\begin{cases} f^\omega(a) = abacabdbabacdcac\ldots \\ \pi(f^\omega(a)) = 000100100011101\ldots. \end{cases}$

Generalization

Let w be a word in base 2, $e_w(n)$ counts the number of occurences of w in the expansion of n in base 2.

Then $\mathcal{S} = (s_n)_n = (e_\omega(n) \pmod 2)_n$ is an automatic sequence.

Particular word: $w_k = 1 \cdots 1 = 1^k$.

- $k = 1 \to$ Thue–Morse.
  $t(n)$ counts the number of 1 in $(n)_2$ mod 2.
  $13 = (1101)_2$, $t(13) = 1$.
- $k = 2 \to$ Golay–Rudin–Shapiro.
  $r(n)$ counts the number of 11 in $(n)_2$ mod 2.
  $13 = (1101)_2$, $r(13) = 1$.

For a general k, these sequences are called *pattern sequences*.

Morphic sequences

Morphic sequences are generated by morphisms that are not necessarily uniform.

Example 1: Fibonacci word

$f : \begin{cases} 0 \mapsto 01 \\ 1 \mapsto 0 \end{cases}$, thus we have $f^\omega(0) = 0100101001001\cdots$

We have $|f^n(0)| = F_n$ the n-th Fibonacci number.
Non–automatic sequence: the frequencies of its letters are not rational.

Example 2: The characteristic sequence of squares is a morphic sequence with

$$f : \begin{cases} a \mapsto abcc, \\ b \mapsto bcc, \\ c \mapsto c. \end{cases} \quad \text{and} \quad \pi : \begin{cases} a, b \mapsto 1, \\ c \mapsto 0. \end{cases}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi(f^\omega(a))$	1	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1

Non–automatic sequence (Ritchie, 1963).

Remark

Notice that it is not trivial in general to determine whether a morphic sequence is automatic or not.

$$f : \begin{cases} 0 \mapsto 12 \\ 1 \mapsto 102 \\ 2 \mapsto 0 \end{cases}, \; f^{\omega}(1) = 102120102012\ldots$$

is automatic (Berstel, 1978), with image reduction modulo 3 of

$$g : \begin{cases} 0 \mapsto 12, 1 \mapsto 13 \\ 2 \mapsto 20, 3 \mapsto 21 \end{cases},$$

$$\begin{aligned} g^{\omega}(1) = & 132120132012\ldots \\ & \downarrow \quad (\text{mod } 3) \\ & 102120102012\ldots \end{aligned}$$

Summary

Subword complexity

Let $w = a_0 a_1 a_2 \dots$ be an infinite word on an alphabet Σ. A finite word $u = b_0 b_1 \dots b_{k-1} \in \Sigma^k$ is a *subword* of w if there exists i such that

$$a_i = b_0,\ a_{i+1} = b_1,\ \dots,\ a_{i+k-1} = b_{k-1}.$$

Subword complexity

Let $\mathcal{S} = (s_n)_n$ be a sequence Σ and $w = s_0 s_1 \dots$.
For $k \geq 0$, we define $p_{\mathcal{S}}$ by

$$p_{\mathcal{S}}(k) = \#\{u \in \Sigma^k :\ \text{u is a subword of w}\}.$$

where $w = s_0 s_1 \dots$.

- $p_{\mathcal{S}}(k) \leq \mathrm{Card}(\Sigma)^k$ for all k.
- $\mathcal{S} = \mathtt{01010101}\dots$, $p_{\mathcal{S}}(k) = 2$ for all k.
- If there exists k such as $p_{\mathcal{S}}(k) \leq k$, $\mathcal{S}$ is periodic.
- If $p_{\mathcal{S}}(k) = k + 1$ for all k, $\mathcal{S}$ is said to be *sturmian*.
  Example: Fibonacci word.

Normal sequence

A sequence is said to be *normal* if for every word $b_0 \dots b_{k-1} \in \Sigma^k$:

$$\lim_{N \to +\infty} \frac{1}{N} \#\{i < N, s_i = b_0, \dots, s_{i+k-1} = b_{k-1}\} = \frac{1}{\mathrm{Card}(\Sigma)^k},$$

i.e. every word appears in the sequence and each word of a fixed length appears with the same frequency.

Almost every sequence is normal (Borel, 1909) but relatively few constructions are known.

Example: The Champernowne sequence (1933)

$$\mathcal{S} = 0\ 1\ 10\ 11\ 100\ \dots$$

is a normal sequence on $\{0, 1\}$.

It is conjectured that π is a normal number but still not known.

Feedback shift register (FSR)

Binary FSR with n states

Mapping $\mathfrak{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $n \geq 2$ on the form

$$\mathfrak{F} : (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, x_2, \ldots, x_{n-1}, f(x_0, x_1, \ldots, x_{n-1})),$$

where $f \in \mathbb{F}_2[X_0, \ldots, X_{n-1}]$.

The binary sequence $\mathcal{S} = (s_i)_{i \geq 0}$, with n given terms, and the remaining terms obtained with the relationship recurrence

$$s_{i+n} = f(s_i, \ldots, s_{i+n-1}), \quad i \geq 0.$$

is called the *output* sequence of the FSR.

An output sequence generated by a short FSR is considered **weak** for cryptographic applications since it is too predictable.

Maximum order complexity

Maximum order complexity at rank N

$M(\mathcal{S}, N)$ is the smallest integer M such that

$$s_{i+M} = f(s_i, \ldots, s_{i+M-1}),$$

with $f(X_1, \ldots, X_M) \in \mathbb{F}_p[X_1, \ldots, X_M]$ and $0 \leq i \leq N - M - 1$.

$M(\mathcal{S}, N)$: length of the shortest FSR that generates the first N elements of $\mathcal{S}$.

The maximum order complexity is used as an indicator of the unpredictability of the sequence.

Example 1/2

Let $\mathcal{S} = \texttt{01011}\ldots$. We have $M(\mathcal{S}, 2) = 1$ since the two first letters are not identical.

In order that $M(\mathcal{S}, 3) = 1$, we have to find a polynomial $f(x)$ such that

$$\begin{cases} s_2 = f(s_1), \\ s_1 = f(s_0). \end{cases} \implies \begin{cases} 0 = f(1), \\ 1 = f(0). \end{cases}$$

Thus the polynomial $f(x) = -x + 1$ is convenient.

In order that $M(\mathcal{S}, 4) = 1$, we have to find a polynomial $f(x)$ such that

$$\begin{cases} s_3 = f(s_2), \\ s_2 = f(s_1), \\ s_1 = f(s_0). \end{cases} \implies \begin{cases} 1 = f(0), \\ 0 = f(1), \\ 1 = f(0). \end{cases}$$

Thus the same polynomial as before is convenient.

Example 2/2

$\mathcal{S} = 01011\ldots$.

In order that $M(\mathcal{S},5)=1$, we have to find a polynomial $f(x)$ such that

$$\begin{cases} 1 = f(1), 1 = f(0) \\ 0 = f(1), 1 = f(0) \end{cases} \implies \text{not possible.}$$

We have to increase the number of variables.

In order that $M(\mathcal{S},5)=2$, we have to find a polynomial $f(x,y)$ such that

$$\begin{cases} s_4 = f(s_3, s_2) \\ s_3 = f(s_2, s_1) \\ s_2 = f(s_1, s_0) \end{cases} \implies \begin{cases} 1 = f(1,0) \\ 1 = f(0,1) \\ 0 = f(1,0) \end{cases} \implies \text{again not possible.}$$

In order that $M(\mathcal{S},5)=3$, we have to find a polynomial $f(x,y,z)$ such that

$$\begin{cases} s_4 = f(s_3, s_2, s_1) \\ s_3 = f(s_2, s_1, s_0) \end{cases} \implies \begin{cases} 1 = f(1,0,1) \\ 1 = f(0,1,0) \end{cases}$$

Thus $f(x,y,z) = x + y$ is convenient.

Special factor and maximum order complexity

A finite word u is to be a *special factor* of a word w if there exists at least two different letters α and β such that $u\alpha$ and $u\beta$ are subwords of w.

Theorem: Jansen (1989)

Let $\mathcal{S} = (s_n)_n$ be a sequence on Σ. Let k be the length of the largest special factor of the word $s_0 s_1 \ldots s_{N-1}$. Then $M(\mathcal{S}, N) = k + 1$.

For example for $w = \texttt{01011}$ we notice that $\texttt{01}$ is the longest special factor of w. Therefore $M(w, 5) = 2 + 1 = 3$.

Expansion complexity

Let $G(x)$ be the generating series of $\mathcal{S}$: $G(x) = \sum_{n \geq 0} s_n x^n$.

Expansion complexity at rank N

$E(\mathcal{S}, N)$ is the least total degree of $h(x, y) \in \mathbb{F}_p[X, Y]$ such that

$$h(x, G(x)) \equiv 0 \mod x^N.$$

Christol's theorem (1979)

$\mathcal{S}$ is p-automatic $\Leftrightarrow$ The generating series of $\mathcal{S}$ is algebraic over $\mathbb{F}_p$.
$\Leftrightarrow$ $E(S, N)$ is bounded.

No relationship between $M(\mathcal{S}, N)$ and $E(\mathcal{S}, N)$.

Summary

Pseudorandom sequence

A sequence $\mathcal{S}$ is said *pseudo-random* if $\mathcal{S}$ has similar complexities as a truly random sequence and can be easily generated.

Expected order for a truly random binary sequence

- Maximum order complexity: $M(\mathcal{S}, N) \simeq \log N$.
- Subword complexity: $p_{\mathcal{S}}(N) \simeq 2^N$.
- Expansion complexity: $E(\mathcal{S}, N) \simeq \sqrt{N}$.

Classical Thue–Morse

Vinogradov's notation: $f \ll g$ means $|f| \leq C|g|$, for some $C \geq 0$ and for N large enough.

Measures for the Thue–Morse sequence

For $N \geq 4$, we have

$$\begin{aligned} M(\mathcal{T}, N) \gg N &: \text{ Sun-Winterhof (2019)}, \\ p_{\mathcal{T}}(N) \ll N &: \text{ Brlek, de Luca-Varricchio (1989)} \\ & \quad \text{ automatic, Allouche-Shallit (2003)}, \\ E(\mathcal{T}, N) \leq 5. & \end{aligned}$$

These measures are very similar for *pattern sequences*.

What happens along squares ?

Let us denote $\mathcal{T}_2 = (t(n^2))_{n \geq 0}$.

$$0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1 \ldots$$

Theorem: Drmota, Mauduit and Rivat (2019)

$\mathcal{T}_2$ is a normal sequence.

$\mathcal{T}_2$ is no longer automatic $\implies E(\mathcal{T}_2, N) \to +\infty$.

Theorem: Sun and Winterhof (2019)

$$M(\mathcal{T}_2, N) \gg N^{1/2}.$$

Thus the Thue–Morse sequence along squares is a better candidate for a pseudorandom sequence.
Again, same phenomenon appears for *pattern sequences*.

The 32×32 first terms of Thue–Morse

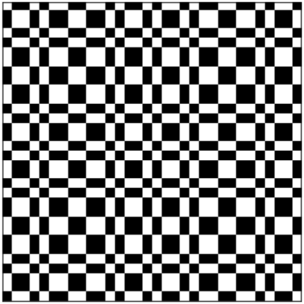


Figure: Classical

Figure: Along squares

Generalization to other polynomial subsequences

Let $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ of degree $d \geq 2$. Let us denote $\mathcal{T}_P = (t(P(n)))_n$. Then

- The subword complexity $\mathcal{T}_P$ is exponential: $p_{\mathcal{T}_P}(N) \geq c^N$ with $c = 2^{1/2^{d-2}}$, Moshe (2007).
- $\mathcal{T}_P$ is not automatic $E(\mathcal{T}_P, N) \to +\infty$.

Theorem: P. (2020)

Let $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ of degree d monic. Let $\mathcal{T}_P = (t(P(n)))_n$ and $\mathcal{P}_{k,P} = (p_k(P(n)))_n$, then we have for $N \geq N_0(k, P)$,

$$M(\mathcal{T}_p, N) \gg N^{1/d},$$
$$M(\mathcal{P}_{k,P}, N) \gg N^{1/d}.$$

Build a special factor of length $N^{1/d}$, up to a constant, in the first N terms.

Sum of digits function

$t(n) \equiv s_2(n) \pmod 2$, $s_2(n)$ is the sum of digits function in base 2.
For $a, b \geq 0$, $b < 2^r$ we have $s_2(a2^r + b) = s_2(a) + s_2(b)$.

$$\begin{array}{cccl} & (a)_2 & 0\cdots 0 & = a2^r \\ + & & (b)_2 & = b \\ \hline & (a)_2 & (b)_2 & = a2^r + b. \end{array}$$

The sum is said to be *non-interfering* since there is no interaction between the digits of a and b.

Then for all $\ell \geq 0$ and $n < 2^\ell$:

$$s_2(n + 2^\ell) = s_2(n + 2^{\ell+1}) \text{ and } \begin{cases} s_2(2^\ell + 2^\ell) = s_2(2^{\ell+1}) = 1 \\ s_2(2^\ell + 2^{\ell+1}) = 0 \pmod 2 \end{cases}$$

$\implies$ special factor of lenght 2^ℓ, for all $\ell \geq 0$.

Sketch of proof

Let $P \in \mathbb{N}[X]$, we have for all $\ell, r > 0$ and $0 \leq n < c_P 2^\ell$, for some $c_P > 0$,

$$t(P(n + 2^{d\ell})) = t(P(n + 2^{d\ell+r})).$$

Exact same proof as before.

Then we seek for all n such as $n > c_P 2^\ell$, "close" of 2^ℓ, such as

$$t(P(n + 2^{d\ell})) \equiv t(P(n + 2^{d\ell+r})) + 1 \pmod 2.$$

Hardest part in general, precise control of the carry propagation is needed.

Summary

Numeration system based on the Fibonnaci sequence:
$F_n = 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$.

Zeckendorf base

$\mathcal{F} = (F_n)_n$ Fibonacci sequence, $F_0 = 0$ et $F_1 = 1$. Each integer n can be represented uniquely by

$$n = \sum_{i \geq 0} \varepsilon_i(n) F_{i+2}, \qquad \text{with } \varepsilon_{i+1}(n)\varepsilon_i(n) = 0.$$

$\varepsilon_{i+1}(n)\varepsilon_i(n) = 0$ hypothesis is to ensure the unicity.

n	Binary	Zeckendorf	n	Binary	Zeckendorf
0	0	0	8	1000	10000
1	1	1	9	1001	10001
2	10	10	10	1010	10010
3	11	100	11	1011	10100
4	100	101	12	1100	10101
5	101	1000	13	1101	100000
6	110	1001	14	1110	100001
7	111	1010	15	1111	100010

Analogus of the Thue–Morse sequence: the sum of digits function

$$s_Z(n) = \sum_{i \geq 0} \varepsilon_i(n).$$

$\mathcal{S}_Z = (s_Z(n) \pmod 2)_{n \geq 0}$ is a morphic sequence (Bruyère) with

$$f : \begin{cases} a \mapsto ab, b \mapsto c \\ c \mapsto cd, d \mapsto a \end{cases} \quad \text{and} \quad \pi : \begin{cases} a \mapsto 0, b \mapsto 1 \\ c \mapsto 1, d \mapsto 0. \end{cases}$$

$\mathcal{S}_Z = \pi \circ f(a) = 01110100100011000 1011\ldots$
$\mathcal{S}_Z$ is not an automatic sequence, Drmota-Müllner-Spiegelhofer (2018).

Carry propagation

- Transversality:
$$\begin{array}{rccccccl} & 1 & 0 & 0 & 1 & 0 & = 10 \\ + & & & & & 1 & = 1 \\ \hline & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$
  due to $F_{n+2} = F_{n+1} + F_n$.
- Right carry propagation:
$$\begin{array}{rcccccl} & & 1 & 0 & 0 & 0 & = 5 \\ + & & 1 & 0 & 0 & 1 & = 6 \\ \hline & 1 & 0 & 0 & 1 & 1 & \\ & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$
  due to $2F_n = F_{n+1} + F_{n-2}$.

Carry propagation works very differently than the base 2.

Determinism of $\mathcal{S}_Z$

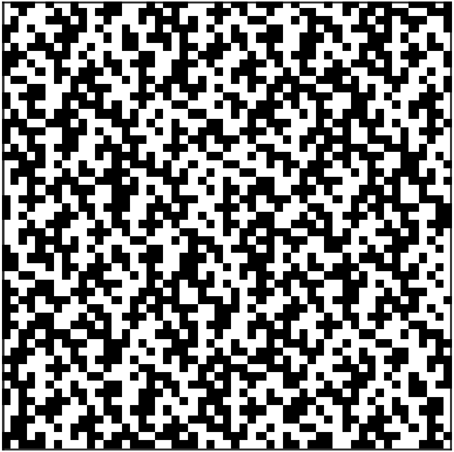


Figure: The 53×53 first terms of $\mathcal{S}_Z$

Determinism of $\mathcal{S}_Z$

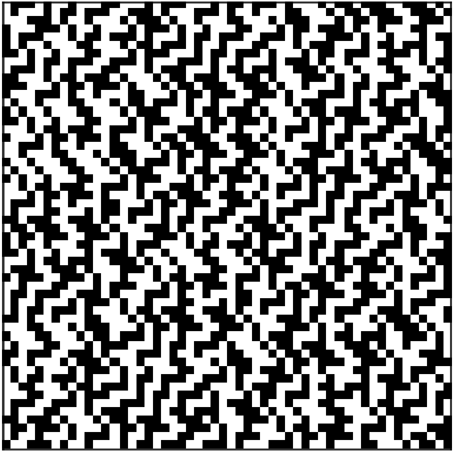


Figure: The 54×54 first terms of $\mathcal{S}_Z$

Determinism of $\mathcal{S}_Z$

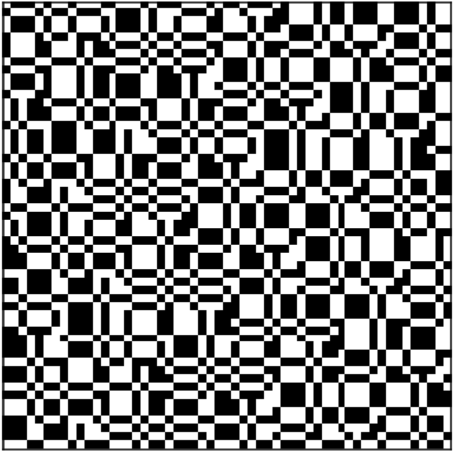


Figure: The 55×55 first terms of $\mathcal{S}_Z$

$55 = F_{10}$.

Maximum order complexity of $\mathcal{S}_Z$

Let $\varphi = \frac{1+\sqrt{5}}{2}$ be the golden ratio.

Theorem: Jamet, P., Stoll (2021)

There exists $N_0 > 0$ such as that for all $N > N_0$

$$M(\mathcal{S}_Z, N) \geq \frac{1}{\varphi + \varphi^3} N + 1.$$

Theorem: Shallit (2022)

$\liminf_{N\to+\infty} \frac{M(S_Z,N)}{N} = \frac{1}{\varphi+\varphi^3}$,
$\limsup_{N\to+\infty} \frac{M(S_Z,N)}{N} = \frac{1}{1+\varphi^2}$.

Thanks to `Walnut`, unfortunately not possible to go on polynomial subsequences.

Randomness of $\mathcal{S}_Z$ along squares

Figure: The 55×55 first terms of $\mathcal{S}_Z$ along squares

Polynomial subsequences

Different result from the Thue–Morse sequence. Factor $2d$ instead of d due to the right carry propagation.

Theorem: Jamet, P., Stoll (2021)

Let $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ monic of degree d.
$\mathcal{S}_{Z,P} = (s_Z(P(n)) \pmod 2)_n$, then

$$M(\mathcal{S}_{Z,P}, N) \gg N^{1/2d}.$$

$(n+2^\ell)^2 = n^2 + 2^{\ell+1}n + 2^{2\ell} \implies$ good expression in base 2.
$(n+F_\ell)^2 = n^2 + 2nF_\ell + F_\ell^2 \implies$ expression in Zeckendorf base ?
Only perfect powers that are Fibonacci numbers are 1, $8 = 2^3$ and $144 = 12^2$.

Lucas numbers: $\mathcal{L} = (L_n)_n$, and $\begin{cases} L_0 = 2, L_1 = 1 \\ L_{n+2} = L_{n+1} + L_n, n \geq 0. \end{cases}$

$L_n = F_{n+1} + F_{n-1}$ and L_n^d is “simple” in Zeckendorf base.

Summary

DAWG

We can find the special factors of a word by building its DAWG (Direct Acyclic Word Graph).

Let $w = a_1 \dots a_n \in \Sigma^n$.

For a subword y of w, we define the set $E_w(y) = \{i : y = a_{i-|y|+1} \dots a_i\}$, the set of ending positions of y.

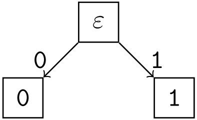
Two subwords y and z are said *suffix-equivalents* if $E_w(y) = E_w(z)$.

The DAWG (Direct Acyclic Word Graph) of a word is the smallest graph that recognizes every subword of a word (Blumer et al.).

The edges are subwords and the vertices are letters. Two subwords are in the same edge if they are suffix-equivalents.
We can find easily the special factor of a word by building its DAWG and looking for the deepest edge with at least two outgoing arrows.

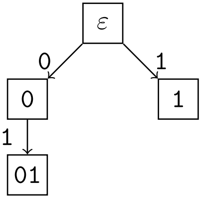
Example

$w = 01011$.
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}$.



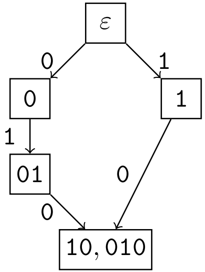
Example

$w = 01011.$
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}.$



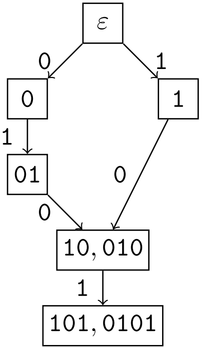
Example

$w = 01011$.
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}$.



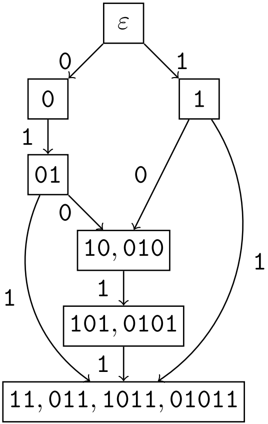
Example

$w = 01011$.
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}$.



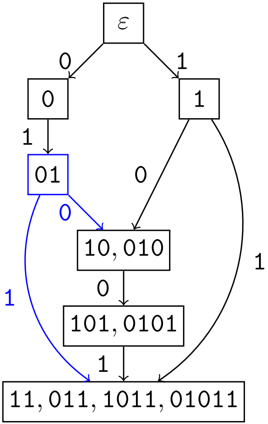
Example

$w = 01011$.
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}$.



Example

$w = 01011$.
$\mathrm{Sub}(w) = \{0, 1, 01, 10, 11, 010, 101, 011, 0101, 1011, 01011\}$.



Thus the longest factor special is the deepest node with at least two outgoing arrows, here this is 01.

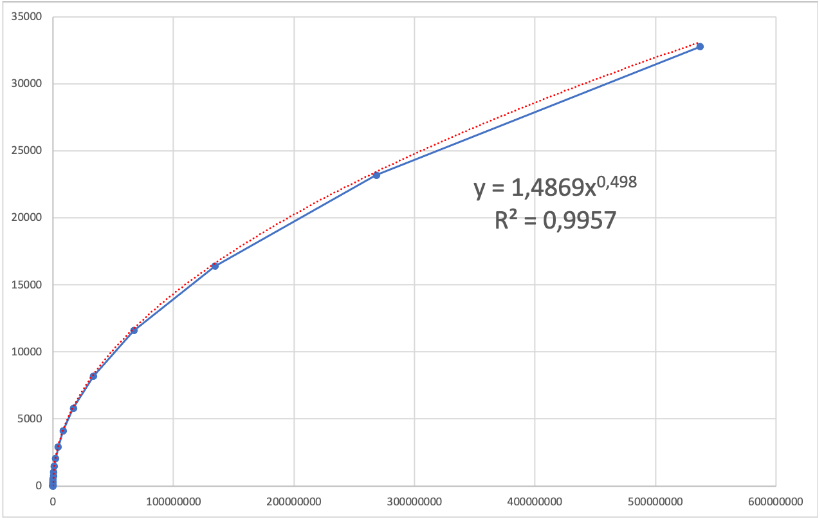


Figure: Maximum order complexity at rank N of the Thue–Morse sequence along squares.

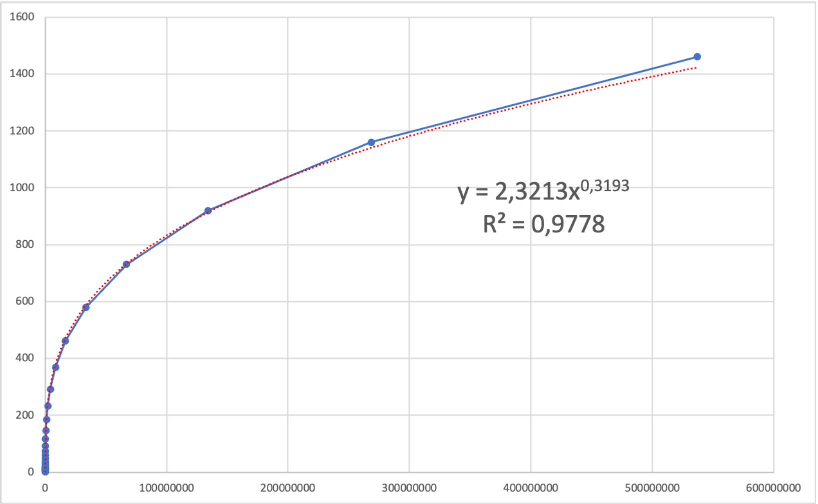


Figure: Maximum order complexity at rank N of the Thue–Morse sequence along cubes.

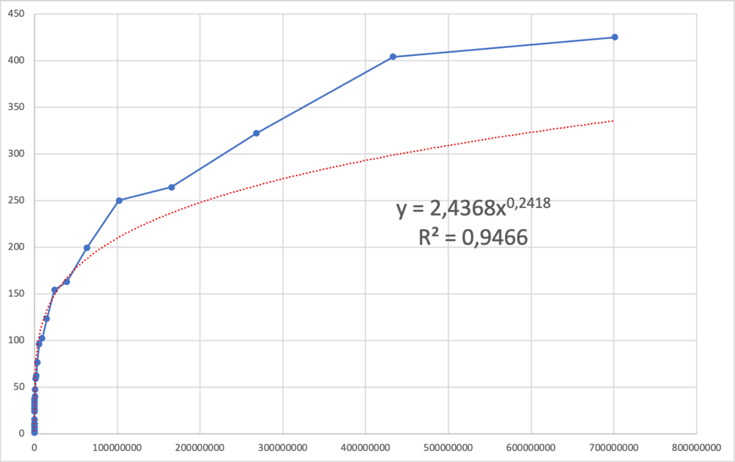


Figure: Maximum order complexity at rank N of Zeckendorf along squares.

Conjectures

- The maximum order complexity of the Thue–Morse sequence along polynomial subsequences of degree d satisfies

$$M(\mathcal{T}_P, N) \asymp N^{1/d}.$$

- The maximum order complexity of the Zeckendorf sequence along polynomial subsequences of degree d satisfies

$$M(\mathcal{S}_{Z,P}, N) \asymp N^{1/2d}.$$

Open problem

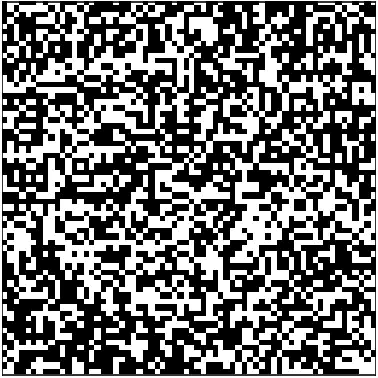


Figure: The 64×64 first terms of Thue–Morse along primes.

Problem: Show a bound of the maximum order complexity for this subsequence. Estimations gives $\log(N)$.

Thank you for your attention !

Contact:
Pierre Popoli
pierre.popoli@univ-lorraine.fr
Institut Élie Cartan de Lorraine
Université de Lorraine