Mesures de complexité pour les suites automatiques et leurs sous-suites

Pierre Popoli, supervisé par
Damien Jamet (LORIA) et Thomas Stoll (IECL)

Journées SDA2 2020: Systèmes Dynamiques,
Automates & Algorithmes 3-4 Dec 2020

Sommaire

Soient $k \geq 2$ et Σ un alphabet fini, Σ^* l'ensemble des mots finis ou infinis sur Σ. Un morphisme $f : \Sigma \to \Sigma^*$ est dit

- *k-uniforme* si toutes les images ont la même taille.
- *prolongeable* en b si $f(b)$ commence par b, i.e. $f(b) = bu$. On a alors

$$f^n(b) = buf(u)\dots f^{n-1}(u),$$
$$f^\omega(b) = \lim_{n\to+\infty} f^n(b).$$

Suites morphiques et automatiques

Une suite x est dite *morphique* si $x = \pi(f^\omega(b))$, où f est b-prolongeable et π est un morphisme. Elle est dite *k-automatique* si de plus f est k-uniforme.

Soient $k \geq 2$ et Σ un alphabet fini, Σ^* l'ensemble des mots finis ou infinis sur Σ. Un morphisme $f : \Sigma \to \Sigma^*$ est dit

- *k-uniforme* si toutes les images ont la même taille.
- *prolongeable* en b si $f(b)$ commence par b, i.e. $f(b) = bu$. On a alors

$$f^n(b) = buf(u)\dots f^{n-1}(u),$$
$$f^\omega(b) = \lim_{n\to+\infty} f^n(b).$$

Suites morphiques et automatiques

Une suite x est dite *morphique* si $x = \pi(f^\omega(b))$, où f est b-prolongeable et π est un morphisme. Elle est dite *k-automatique* si de plus f est k-uniforme.

Automate fini déterministe avec sorties (DFAO)

C'est la donnée de $\mathcal{A} = (\Sigma, \mathcal{Q}, q_0, \delta, \pi)$ avec

- $\Sigma = \{0, \ldots, k-1\}$,
- $\mathcal{Q}$ est l'ensemble des états et q_0 l'état initial,
- $\delta : \mathcal{Q} \times \Sigma \to \mathcal{Q}$, fonction de transition, étendue en $\delta^* : \mathcal{Q} \times \Sigma^* \to \mathcal{Q}$,
- $\pi : \mathcal{Q} \to A$.

Une suite $(a_n)_n$ est k-automatique s'il existe $\mathcal{A}$ un DFAO tel que $a_n = \pi\left(\delta(q_0, (n)_k)\right)$.

Automate fini déterministe avec sorties (DFAO)

C'est la donnée de $\mathcal{A} = (\Sigma, \mathcal{Q}, q_0, \delta, \pi)$ avec

- $\Sigma = \{0, \ldots, k-1\}$,
- $\mathcal{Q}$ est l'ensemble des états et q_0 l'état initial,
- $\delta : \mathcal{Q} \times \Sigma \to \mathcal{Q}$, fonction de transition, étendue en $\delta^* : \mathcal{Q} \times \Sigma^* \to \mathcal{Q}$,
- $\pi : \mathcal{Q} \to A$.

Une suite $(a_n)_n$ est k-automatique s'il existe $\mathcal{A}$ un DFAO tel que $a_n = \pi\left(\delta(q_0, (n)_k)\right)$.

Suite de Thue–Morse $\mathcal{T} = (t(n))_n$

$$f : \begin{cases} 0 \mapsto 01 \\ 1 \mapsto 10 \end{cases} \quad \Longrightarrow \quad \begin{aligned} & f(0) = 01 \\ & f(1) = 0110 \\ & \cdots \\ & \mathbf{t} = f^{\omega}(0) = 0110100110010\ldots \end{aligned}$$

Figure: DFAO pour la suite de Thue–Morse.

$$(n)_2 = \varepsilon_r \ldots \varepsilon_0 \quad \Longrightarrow \quad \begin{cases} (2n)_2 & = \varepsilon_r \ldots \varepsilon_0 0 \\ (2n+1)_2 & = \varepsilon_r \ldots \varepsilon_0 1. \end{cases}$$

Alors $t(n) \equiv s_2(n) \pmod 2$, la somme des chiffres de n en base 2.

Suite de Thue–Morse $\mathcal{T} = (t(n))_n$

$$f : \begin{cases} 0 \mapsto 01 \\ 1 \mapsto 10 \end{cases} \quad \Longrightarrow \quad \begin{aligned} & f(0) = 01 \\ & f(1) = 0110 \\ & \cdots \\ & \mathbf{t} = f^{\omega}(0) = 0110100110010\ldots \end{aligned}$$

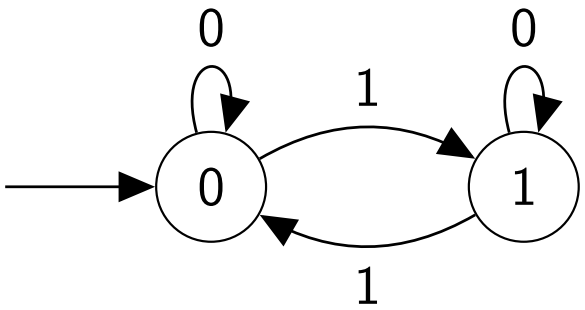


Figure: DFAO pour la suite de Thue–Morse.

$$(n)_2 = \varepsilon_r \ldots \varepsilon_0 \quad \Longrightarrow \quad \begin{cases} (2n)_2 & = \varepsilon_r \ldots \varepsilon_0 0 \\ (2n+1)_2 & = \varepsilon_r \ldots \varepsilon_0 1. \end{cases}$$

Alors $t(n) \equiv s_2(n) \pmod 2$, la somme des chiffres de n en base 2.

Suite de Thue–Morse $\mathcal{T} = (t(n))_n$

$$f : \begin{cases} 0 \mapsto 01 \\ 1 \mapsto 10 \end{cases} \quad \Longrightarrow \quad \begin{aligned} & f(0) = 01 \\ & f(1) = 0110 \\ & \cdots \\ & \mathbf{t} = f^{\omega}(0) = 0110100110010\ldots \end{aligned}$$

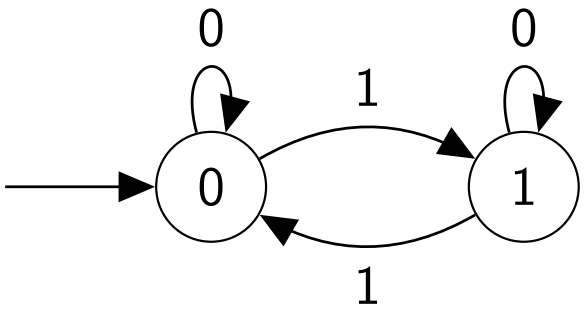


Figure: DFAO pour la suite de Thue–Morse.

$$(n)_2 = \varepsilon_r \ldots \varepsilon_0 \implies \begin{cases} (2n)_2 & = \varepsilon_r \ldots \varepsilon_0 0 \\ (2n+1)_2 & = \varepsilon_r \ldots \varepsilon_0 1. \end{cases}$$

Alors $t(n) \equiv s_2(n) \pmod 2$, la somme des chiffres de n en base 2.

Suite de motifs $\mathcal{P}_k = (p_k(n))_n$

Soit $k \geq 1$, $p_k(n) \equiv s_{2,k}(n) \pmod 2$ avec $s_{2,k}(n)$ qui compte le nombre de fois que le motif $1^{(k)}$ apparaît. Pour $k = 1$ on trouve la suite de Thue–Morse, $k = 2$ celle de Golay–Shapiro. Ce sont toutes des suites automatiques.

Figure: DFAO pour la suite de Golay–Shapiro.

Suite de motifs $\mathcal{P}_k = (p_k(n))_n$

Soit $k \geq 1$, $p_k(n) \equiv s_{2,k}(n) \pmod 2$ avec $s_{2,k}(n)$ qui compte le nombre de fois que le motif $1^{(k)}$ apparaît. Pour $k = 1$ on trouve la suite de Thue–Morse, $k = 2$ celle de Golay–Shapiro. Ce sont toutes des suites automatiques.

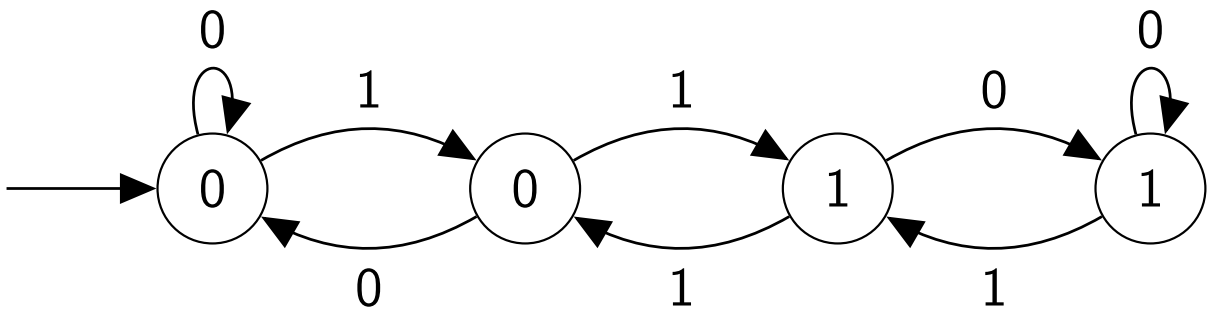


Figure: DFAO pour la suite de Golay–Shapiro.

Soit f un morphisme tel que

- f est b-prolongeable pour un certain $b \in \Sigma$.
- $\lim_{n \to +\infty} |f^n(a)| = +\infty$ pour tout $a \in \Sigma$.

On notera $\mathcal{S}$ le point fixe du morphisme $\mathcal{S} = f^\omega(b)$.

Système dynamique associé à $\mathcal{S}$

On associe à $\mathcal{S}$ le système dynamique $(X(\mathcal{S}), T)$ avec

- T le shift sur $\Sigma^{\mathbb{N}}$.
- $X(\mathcal{S})$ l'adhérence de l'orbite de $\mathcal{S}$ sous l'action de T.

Complexité en sous-mots

Pour $k \geq 0$, on définit $p_{\mathcal{S}}$ par :

$$p_{\mathcal{S}}(k) = \#\{(b_0, \ldots, b_{k-1}) \in \mathbb{F}_p^k : \exists i, s_i = b_0, \ldots, s_{i+k-1} = b_{k-1}\}.$$

Alors $p_{\mathcal{S}}(k)$ désigne le nombre de sous-mots de taille k.

L'entropie topologique de $(X(\mathcal{S}), T)$ est $\lim_{k \to +\infty} \frac{\log p_{\mathcal{S}}(k)}{k}$.

Une suite d'entropie topologique nulle est dite *déterministe*.

Complexité en sous-mots

Pour $k \geq 0$, on définit $p_{\mathcal{S}}$ par :

$$p_{\mathcal{S}}(k) = \#\{(b_0, \ldots, b_{k-1}) \in \mathbb{F}_p^k : \exists i, s_i = b_0, \ldots, s_{i+k-1} = b_{k-1}\}.$$

Alors $p_{\mathcal{S}}(k)$ désigne le nombre de sous-mots de taille k.

L'entropie topologique de $(X(\mathcal{S}), T)$ est $\lim\limits_{k \to +\infty} \frac{\log p_{\mathcal{S}}(k)}{k}$.

Une suite d'entropie topologique nulle est dite *déterministe*.

Une suite est dite *normale* si pour tout mot $(b_0, \ldots, b_{k-1}) \in \mathbb{F}_p^k$:

$$\lim_{N \to +\infty} \#\{i < N, s_i = b_0, \ldots, s_{i+k-1} = b_{k-1}\} = \frac{1}{p^k}.$$

Dans ce cas l'entropie topologique est maximale, i.e. égale à $\log(p)$.

Suite de Champernowne

$\omega = 0\ 1\ 10\ 11\ 100\ \cdots$, $s(n) = \omega[n]$ est une suite normale de $\mathbb{F}_2$.

Sommaire

Contexte: p premier, $\mathcal{S} = (s_n)_n$ suite sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $N \geq 1$.

Complexité linéaire au rang N

$L(\mathcal{S}, N)$ est le plus petit entier L tel que

$$s_{i+L} = c_0 s_i + \cdots + c_{L-1} s_{i+L-1},$$

avec $c_j \in \mathbb{F}_p$ et $0 \leq i \leq N - L - 1$. On peut engendrer les N premiers termes à partir des L premiers par une récurrence linéaire.

Complexité d'ordre maximal au rang N

$M(\mathcal{S}, N)$ est le plus petit entier M tel que

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

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

On a bien sûr $M(\mathcal{S}, N) \leq L(\mathcal{S}, N)$.

Contexte: p premier, $\mathcal{S} = (s_n)_n$ suite sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $N \geq 1$.

Complexité linéaire au rang N

$L(\mathcal{S}, N)$ est le plus petit entier L tel que

$$s_{i+L} = c_0 s_i + \cdots + c_{L-1} s_{i+L-1},$$

avec $c_j \in \mathbb{F}_p$ et $0 \leq i \leq N - L - 1$. On peut engendrer les N premiers termes à partir des L premiers par une récurrence linéaire.

Complexité d'ordre maximal au rang N

$M(\mathcal{S}, N)$ est le plus petit entier M tel que

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

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

On a bien sûr $M(\mathcal{S}, N) \leq L(\mathcal{S}, N)$.

$G(x)$ la série génératrice de $\mathcal{S}$: $G(x) = \sum_{n \geq 0} s_n x^n$.

Complexité d'expansion au rang N

$E(\mathcal{S}, N)$ est le plus petit degré total de $h(x, y) \in \mathbb{F}_p[X, Y]$ tel que

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

Théorème de Christol (1979)

$\mathcal{S}$ est p-automatique $\Leftrightarrow$ Sa série génératrice est algébrique sur $\mathbb{F}_p$.
$\Leftrightarrow E(S, N) < +\infty$ pour tout $N \geq 1$.

On a les comparaisons suivantes:

$$E(\mathcal{S}, N) \leq L(\mathcal{S}, N) + 1,$$
$$M(\mathcal{S}, N) \leq L(\mathcal{S}, N).$$

$G(x)$ la série génératrice de $\mathcal{S}$: $G(x) = \sum_{n \geq 0} s_n x^n$.

Complexité d'expansion au rang N

$E(\mathcal{S}, N)$ est le plus petit degré total de $h(x, y) \in \mathbb{F}_p[X, Y]$ tel que

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

Théorème de Christol (1979)

$\mathcal{S}$ est p-automatique $\Leftrightarrow$ Sa série génératrice est algébrique sur $\mathbb{F}_p$.
$\Leftrightarrow E(S, N) < +\infty$ pour tout $N \geq 1$.

On a les comparaisons suivantes:

$$E(\mathcal{S}, N) \leq L(\mathcal{S}, N) + 1,$$
$$M(\mathcal{S}, N) \leq L(\mathcal{S}, N).$$

$G(x)$ la série génératrice de $\mathcal{S}$: $G(x) = \sum_{n \geq 0} s_n x^n$.

Complexité d'expansion au rang N

$E(\mathcal{S}, N)$ est le plus petit degré total de $h(x, y) \in \mathbb{F}_p[X, Y]$ tel que

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

Théorème de Christol (1979)

$\mathcal{S}$ est p-automatique $\Leftrightarrow$ Sa série génératrice est algébrique sur $\mathbb{F}_p$.
$\Leftrightarrow E(S, N) < +\infty$ pour tout $N \geq 1$.

On a les comparaisons suivantes:

$$E(\mathcal{S}, N) \leq L(\mathcal{S}, N) + 1,$$
$$M(\mathcal{S}, N) \leq L(\mathcal{S}, N).$$

Corrélation d'ordre k au rang N

$\mathcal{S}$ suite sur $\mathbb{F}_2$,

$$C_k(\mathcal{S}, N) = \max_{U,D} \left| \sum_{0 \leq n \leq U} (-1)^{s_{n+d_1} + \cdots + s_{n+d_k}} \right|,$$

où le maximum est pris sur tout $D = (d_1, \ldots, d_k)$ entiers tels que $0 \leq d_1 < d_2 < \ldots < d_k$ et U tel que $U + d_k \leq N$.

Théorème: Isik et Winterhof (2017)

$$M(\mathcal{S}, N) \geq N - 2^{M(\mathcal{S},N)+1} \max_{1 \leq k \leq M(\mathcal{S},N)+1} C_k(\mathcal{S}, N), \quad N \geq 1$$

Corrélation d'ordre k au rang N

$\mathcal{S}$ suite sur $\mathbb{F}_2$,

$$C_k(\mathcal{S}, N) = \max_{U,D} \left| \sum_{0 \le n \le U} (-1)^{s_{n+d_1} + \cdots + s_{n+d_k}} \right|,$$

où le maximum est pris sur tout $D = (d_1, \ldots, d_k)$ entiers tels que $0 \le d_1 < d_2 < \ldots < d_k$ et U tel que $U + d_k \le N$.

Théorème: Isik et Winterhof (2017)

$$M(\mathcal{S}, N) \ge N - 2^{M(\mathcal{S},N)+1} \max_{1 \le k \le M(\mathcal{S},N)+1} C_k(\mathcal{S}, N), \quad N \ge 1$$

Suites pseudo-aléatoires

Une suite est dite pseudo-aléatoire si elle possède des mesures de complexité semblables à celle d'une suite aléatoire.

Ordre attendus pour une suite aléatoire binaire

- Complexité d'ordre maximal : $\log N$.
- Corrélation d'ordre k: $\sqrt{kN \log N}$.
- Complexité en sous-mots: 2^N.
- Complexité d'expansion: $\sqrt{N}$.

Objectif

Créer des suites pseudo-aléatoires à partir de suites déterministes en les raréfiant le long de certaines sous-suites: faciles à générer mais difficiles à décrypter $\rightarrow$ possible application en cryptographie.

Suites pseudo-aléatoires

Une suite est dite pseudo-aléatoire si elle possède des mesures de complexité semblables à celle d'une suite aléatoire.

Ordre attendus pour une suite aléatoire binaire

- Complexité d'ordre maximal : $\log N$.
- Corrélation d'ordre k: $\sqrt{kN \log N}$.
- Complexité en sous-mots: 2^N.
- Complexité d'expansion: $\sqrt{N}$.

Objectif

Créer des suites pseudo-aléatoires à partir de suites déterministes en les raréfiant le long de certaines sous-suites: faciles à générer mais difficiles à décrypter $\rightarrow$ possible application en cryptographie.

Notation de Vinogradov: $f \ll g$ veut dire $|f| \leq C|g|$, pour une certaine constante et à partir d'un certain rang.

Suite de Thue–Morse

Pour $N \geq 4$, on a

$$M(\mathcal{T}, N) \gg N. \qquad \checkmark$$

$$p_{\mathcal{T}}(N) \leq \frac{10}{3} N. \qquad \times$$

$$E(\mathcal{T}, N) \leq 5. \qquad \times$$

$$C_2(\mathcal{T}, N) \geq \frac{1}{12} N. \qquad \times$$

Notation de Vinogradov: $f \ll g$ veut dire $|f| \leq C|g|$, pour une certaine constante et à partir d'un certain rang.

Suite de Thue–Morse

Pour $N \geq 4$, on a

$$M(\mathcal{T}, N) \gg N. \qquad \checkmark$$

$$p_{\mathcal{T}}(N) \leq \frac{10}{3} N. \qquad \text{✗}$$

$$E(\mathcal{T}, N) \leq 5. \qquad \text{✗}$$

$$C_2(\mathcal{T}, N) \geq \frac{1}{12} N. \qquad \text{✗}$$

En revanche pour $\mathcal{T}_2 = (t(n^2))_{n\geq 0}$, la suite le long des carrés n'est plus automatique, alors $E(\mathcal{T}_2, N) \to +\infty$. ✓ / ✗

Théorème: Drmota, Mauduit et Rivat (2019) [2]

$\mathcal{T}_2$ est une suite normale. ✓

Théorème: Sun et Winterhof (2019) [5]

$M(\mathcal{T}_2, N) \gg N^{1/2}$. ✓

Donc la suite de Thue–Morse le long des carrés semble être un meilleur candidat pour être une suite pseudo-aléatoire.

En revanche pour $\mathcal{T}_2 = (t(n^2))_{n\geq 0}$, la suite le long des carrés n'est plus automatique, alors $E(\mathcal{T}_2, N) \to +\infty$. ✓ / ✗

Théorème: Drmota, Mauduit et Rivat (2019) [2]

$\mathcal{T}_2$ est une suite normale. ✓

Théorème: Sun et Winterhof (2019) [5]

$M(\mathcal{T}_2, N) \gg N^{1/2}$. ✓

Donc la suite de Thue–Morse le long des carrés semble être un meilleur candidat pour être une suite pseudo-aléatoire.

En revanche pour $\mathcal{T}_2 = (t(n^2))_{n\geq 0}$, la suite le long des carrés n'est plus automatique, alors $E(\mathcal{T}_2, N) \to +\infty$. ✓ / ✗

Théorème: Drmota, Mauduit et Rivat (2019) [2]

$\mathcal{T}_2$ est une suite normale. ✓

Théorème: Sun et Winterhof (2019) [5]

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

Donc la suite de Thue–Morse le long des carrés semble être un meilleur candidat pour être une suite pseudo-aléatoire.

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré $d \geq 2$. Soit $\mathcal{T}_P = (t(P(n)))_n$, on sait que :

- La complexité en sous-mots de $\mathcal{T}_P$ est exponentielle: $p_{\mathcal{T}_P}(N) \geq c^N$ avec $c = 2^{1/2^{d-2}}$, Moshe (2007) [3].
- La suite n'est pas automatique: $E(\mathcal{T}_P, N) \to +\infty$.

Théorème: P. (2020) [4]

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré d unitaire. Soit $\mathcal{T}_P = (t(P(n)))_n$ et $\mathcal{P}_{k,P} = (p_k(P(n)))_n$, alors on a pour $N \geq N_0(k, P)$,

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

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré $d \geq 2$. Soit $\mathcal{T}_P = (t(P(n)))_n$, on sait que :

- La complexité en sous-mots de $\mathcal{T}_P$ est exponentielle: $p_{\mathcal{T}_P}(N) \geq c^N$ avec $c = 2^{1/2^{d-2}}$, Moshe (2007) [3].
- La suite n'est pas automatique: $E(\mathcal{T}_P, N) \to +\infty$.

Théorème: P. (2020) [4]

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré d unitaire. Soit $\mathcal{T}_P = (t(P(n)))_n$ et $\mathcal{P}_{k,P} = (p_k(P(n)))_n$, alors on a pour $N \geq N_0(k, P)$,

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

Lemme

Soit $\mathcal{S} = \{s_0, \ldots, s_{n-1}\}$ suite de $\mathbb{F}_p$. Soit k la longueur de la plus grande sous-suite de $\mathcal{S}$ qui apparait au moins deux fois avec deux successeurs différents. Alors $\mathcal{S}$ a comme complexité d'ordre maximal $k+1$.

Pour $a, b \geq 0$ et $b < 2^r$ on a $s_2(a2^r + b) = s_2(a) + s_2(b)$.

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

On dit que la somme de a à b est *non interférente* dans ce cas. Soit $l \geq 0$, alors on a pour tout $n < 2^l$

$$s_2(n + 2^l) = s_2(n + 2^{l+1}).$$

Lemme

Soit $\mathcal{S} = \{s_0, \ldots, s_{n-1}\}$ suite de $\mathbb{F}_p$. Soit k la longueur de la plus grande sous-suite de $\mathcal{S}$ qui apparait au moins deux fois avec deux successeurs différents. Alors $\mathcal{S}$ a comme complexité d'ordre maximal $k+1$.

Pour $a, b \geq 0$ et $b < 2^r$ on a $s_2(a2^r + b) = s_2(a) + s_2(b)$.

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

On dit que la somme de a à b est *non interférente* dans ce cas. Soit $l \geq 0$, alors on a pour tout $n < 2^l$

$$s_2(n + 2^l) = s_2(n + 2^{l+1}).$$

- Création des deux blocs égaux.
  Soit $P \in \mathbb{N}[X]$, on montre alors que pour pour tout $r > 0$ et $0 \leq n < c_P 2^l$, on a

$$t(P(n + 2^{dl})) = t(P(n + 2^{dl+r})).$$

- Recherche des deux successeurs distincts.
  On cherche $y, r > 0$ tels que

$$t(P(1 + y2^l + 2^{dl})) \equiv t(P(1 + y2^l + 2^{dl+r})) + 1 \pmod 2.$$

  Revient à trouver (y, r) tels que

$$t(y^d + z) \equiv t(y^d + 2^r z) + 1 \pmod 2$$

  avec $z = P'(1)$. Avec $y = 2^s$ et un bon choix de r c'est possible.

- Création des deux blocs égaux.
  Soit $P \in \mathbb{N}[X]$, on montre alors que pour pour tout $r > 0$ et $0 \leq n < c_P 2^l$, on a

$$t(P(n + 2^{dl})) = t(P(n + 2^{dl+r})).$$

- Recherche des deux successeurs distincts.
  On cherche $y, r > 0$ tels que

$$t(P(1 + y2^l + 2^{dl})) \equiv t(P(1 + y2^l + 2^{dl+r})) + 1 \pmod 2.$$

  Revient à trouver (y, r) tels que

$$t(y^d + z) \equiv t(y^d + 2^r z) + 1 \pmod 2$$

  avec $z = P'(1)$. Avec $y = 2^s$ et un bon choix de r c'est possible.

Sommaire

Pour α un nombre réel irrationnel, on écrit sa fraction continue

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} = [a_0, a_1, \ldots]$$

On pose $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$ et $q_{-1} = 0$, on a
$p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ et $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$.

Système de numération d'Ostrowski

Soit N un nombre entier, il admet une représentation unique

$$N = \sum_{i \geq 0} b_i q_i,$$

avec les b_i tels que

- $0 \leq b_0 < a_1$,
- $0 \leq b_i \leq a_{i+1}$,
- pour $i \geq 1$, si $b_i = a_{i+1}$ alors $b_{i-1} = 0$.

Pour α un nombre réel irrationnel, on écrit sa fraction continue

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} = [a_0, a_1, \ldots]$$

On pose $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$ et $q_{-1} = 0$, on a
$p_n = a_n p_{n-1} + p_{n-2}$, $q_n = a_n q_{n-1} + q_{n-2}$ et $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$.

Système de numération d'Ostrowski

Soit N un nombre entier, il admet une représentation unique

$$N = \sum_{i \geq 0} b_i q_i,$$

avec les b_i tels que

- $0 \leq b_0 < a_1$,
- $0 \leq b_i \leq a_{i+1}$,
- pour $i \geq 1$, si $b_i = a_{i+1}$ alors $b_{i-1} = 0$.

Pour $\varphi = \frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots]$, on obtient la représentation de Zeckendorf.

Représentation de Zeckendorf

$\mathcal{F} = (F_n)_n$ suite de Fibonacci, $F_2 = 1$ et $F_3 = 2$. Pour n entier naturel peut s'écrire de manière unique

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

Soit $s_F(n) = \sum_{i \geq 0} \varepsilon_i(n)$, $\mathcal{S}_F = (s_F(n))_{n \geq 0}$ est une suite morphique non-automatique avec $f : \begin{cases} a \mapsto ab \\ b \mapsto c \\ c \mapsto cd \\ d \mapsto a \end{cases}$ et $\pi : \begin{cases} a \mapsto 0 \\ b \mapsto 1 \\ c \mapsto 1 \\ d \mapsto 0. \end{cases}$

$$\mathcal{S}_{\mathcal{F}} = \pi \circ f(a) = 01110100100011000101 1 \ldots$$

Pour $\varphi = \frac{1+\sqrt{5}}{2} = [1, 1, 1, \ldots]$, on obtient la représentation de Zeckendorf.

Représentation de Zeckendorf

$\mathcal{F} = (F_n)_n$ suite de Fibonacci, $F_2 = 1$ et $F_3 = 2$. Pour n entier naturel peut s'écrire de manière unique

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

Soit $s_F(n) = \sum_{i \geq 0} \varepsilon_i(n)$, $\mathcal{S}_F = (s_F(n))_{n \geq 0}$ est une suite morphique non-automatique avec $f : \begin{cases} a \mapsto ab \\ b \mapsto c \\ c \mapsto cd \\ d \mapsto a \end{cases}$ et $\pi : \begin{cases} a \mapsto 0 \\ b \mapsto 1 \\ c \mapsto 1 \\ d \mapsto 0. \end{cases}$

$$\mathcal{S}_{\mathcal{F}} = \pi \circ f(a) = 01110100100011000 1011 \ldots$$

Propagation de retenue

- Transversalité:

$$\begin{array}{rccccccc} & 1 & 0 & 0 & 1 & 0 & = 10 \\ + & & & & & 1 & = 1 \\ \hline & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$

Provient de $F_{n+2} = F_{n+1} + F_n$.

- Propagation à droite:

$$\begin{array}{rccccccc} & & 1 & 0 & 0 & 0 & = 5 \\ + & & 1 & 0 & 0 & 1 & = 6 \\ \hline & 1 & 0 & 0 & 1 & 1 & \\ & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$

Provient de $2F_n = F_{n+1} + F_{n-2}$.

Complexité d'ordre maximal

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré d unitaire. $\mathcal{S}_P = (s_F(P(n)))_n$, alors on a pour $N \geq N_0(P)$

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

Le facteur 2 provient de la propagation de la retenue à droite.

Propagation de retenue

- Transversalité:

$$\begin{array}{rccccccl} & 1 & 0 & 0 & 1 & 0 & = 10 \\ + & & & & & 1 & = 1 \\ \hline & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$

Provient de $F_{n+2} = F_{n+1} + F_n$.

- Propagation à droite:

$$\begin{array}{rccccccl} & & 1 & 0 & 0 & 0 & = 5 \\ + & & 1 & 0 & 0 & 1 & = 6 \\ \hline & 1 & 0 & 0 & 1 & 1 & \\ & 1 & 0 & 1 & 0 & 0 & = 11. \end{array}$$

Provient de $2F_n = F_{n+1} + F_{n-2}$.

Complexité d'ordre maximal

Soit $P \in \mathbb{Z}[X]$, $P(\mathbb{N}) \subset \mathbb{N}$ de degré d unitaire. $\mathcal{S}_P = (s_F(P(n)))_n$, alors on a pour $N \geq N_0(P)$

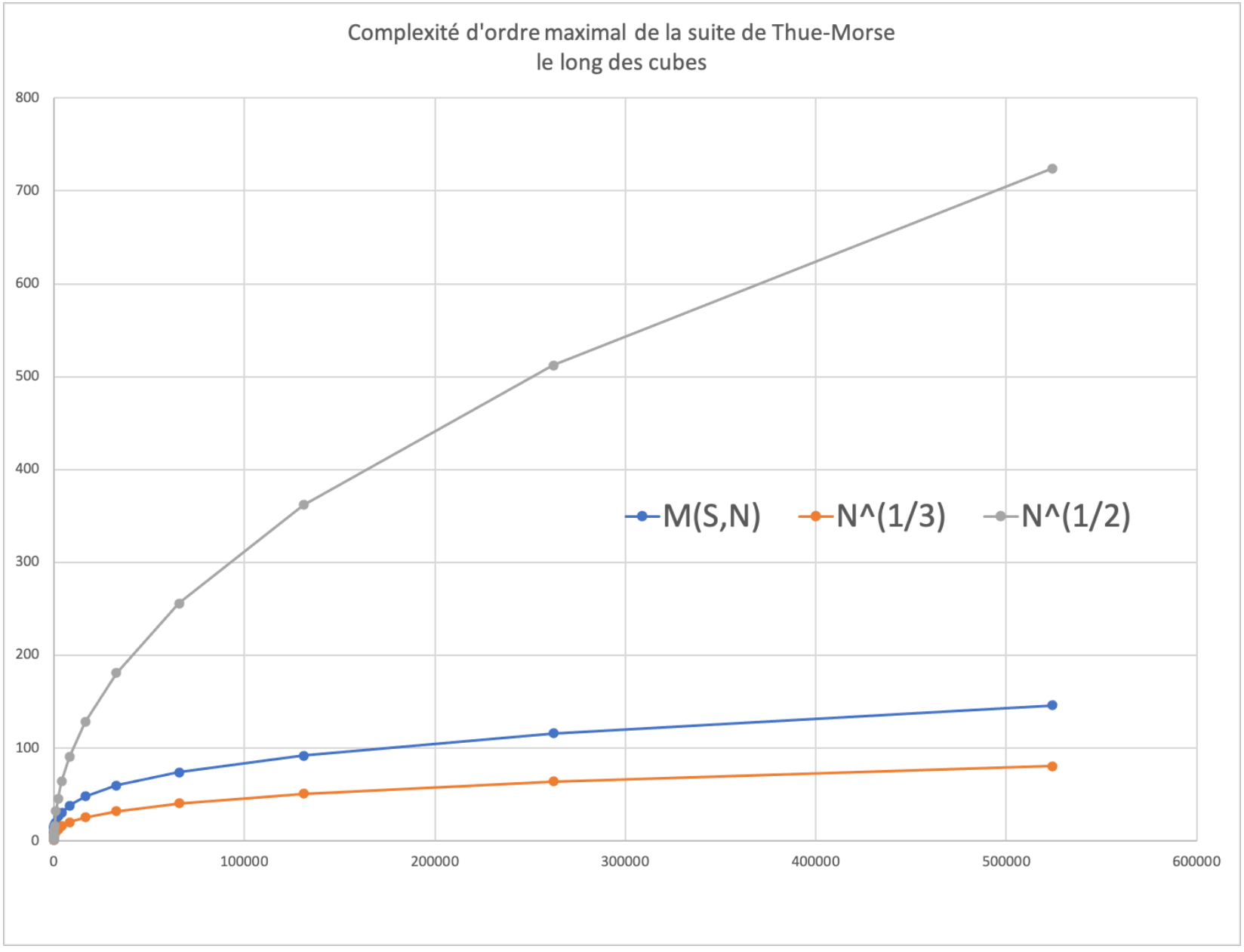
$$M(\mathcal{S}_d, N) \gg N^{1/2d}.$$

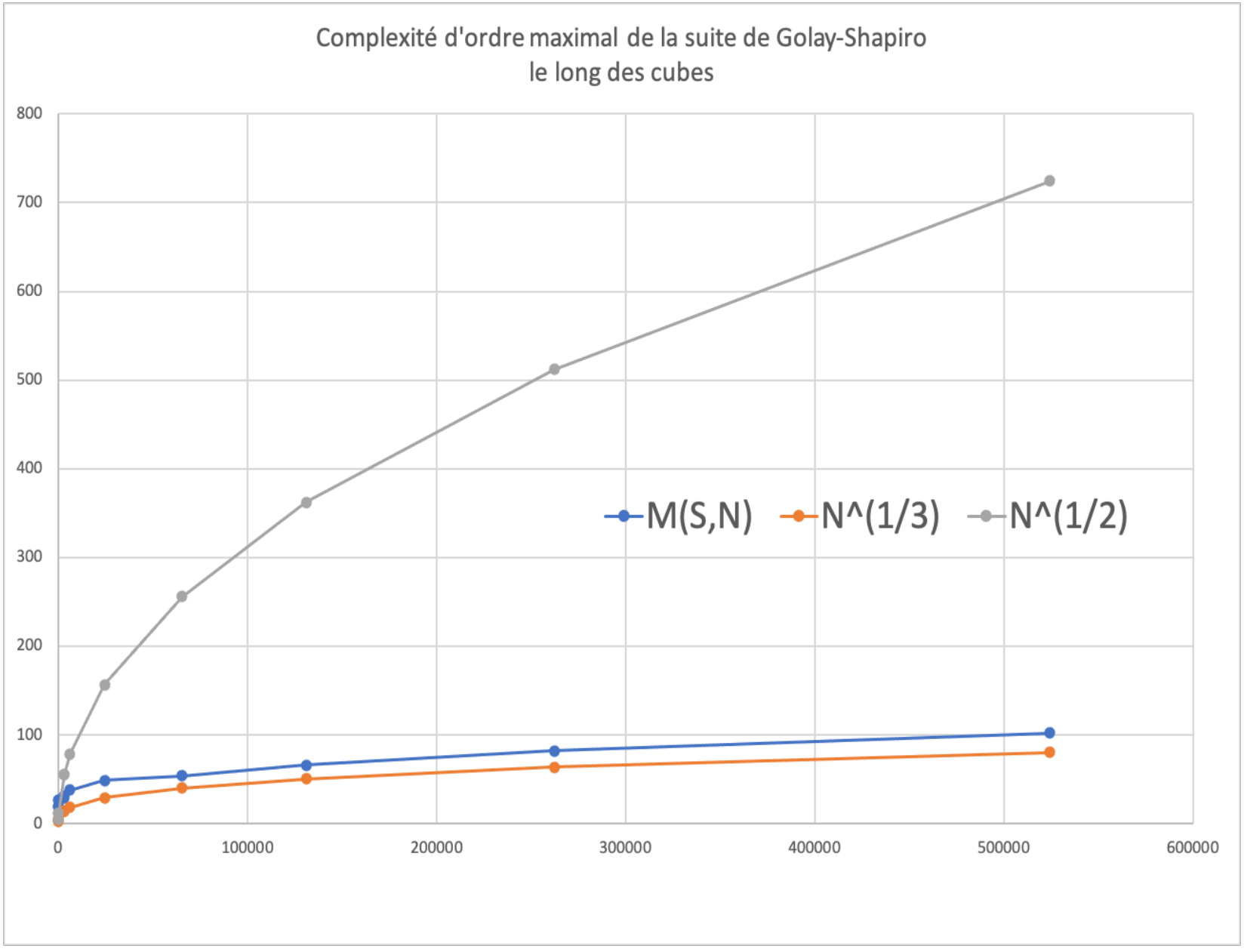
Le facteur 2 provient de la propagation de la retenue à droite.

Sommaire

Problèmes ouverts

- Généraliser le premier théorème à $p_\omega(n) = s_\omega(n) \pmod 2$ qui compte le nombre de fois que le motif binaire ω apparaît dans $(n)_2$.
- Étendre le résultat aux systèmes de numération d'Ostrowski.
- Trouver des bornes supérieures pour $M(\mathcal{T}_P, N)$.


Complexité d'ordre maximal de la suite de Thue-Morse
le long des cubes
800
700
600
500
400
300
200
100
0
0
100000
200000
300000
400000
500000
600000
M(S,N)
N^(1/3)
N^(1/2)


Complexité d'ordre maximal de la suite de Golay-Shapiro
le long des cubes
800
700
600
500
400
300
200
100
0
0
100000
200000
300000
400000
500000
600000
M(S,N)
N^(1/3)
N^(1/2)

[1] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003.

[2] Michael Drmota, Christian Mauduit, and Joël Rivat, *Normality along squares*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 2, 507–548.

[3] Yossi Moshe, *On the subword complexity of Thue-Morse polynomial extractions*, Theoret. Comput. Sci. **389** (2007), no. 1-2, 318–329.

[4] Pierre Popoli, *On The Maximum Order Complexity Of Thue-Morse And Rudin-Shapiro Sequences Along Polynomial Values*, Uniform Distribution Theory **15** (2020), no. 2, 9–22, `arXiv:2011.03457`.

[5] Zhimin Sun and Arne Winterhof, *On the maximum order complexity of subsequences of the Thue-Morse and Rudin-Shapiro sequence along squares*, Int. J. Comput. Math. Comput. Syst. Theory **4** (2019), no. 1, 30–36.

Merci pour votre attention !

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