Probabilistic studies in Number Theory and Word Combinatorics: instances of dynamical analysis

Pablo Rotondo

IRIF, Paris 7 Diderot,

Universidad de la República, Uruguay

GREYC, associate

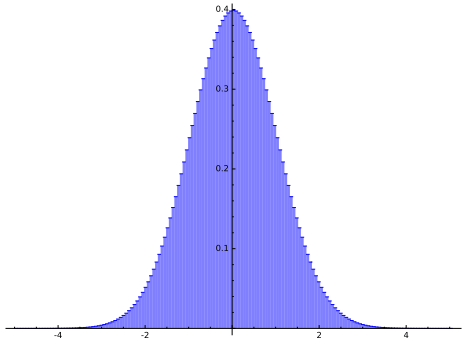
PhD thesis defence, **IRIF**, September 27, 2018.

Deciphering the title

- Probabilistic analysis

Object/experiment/execution?

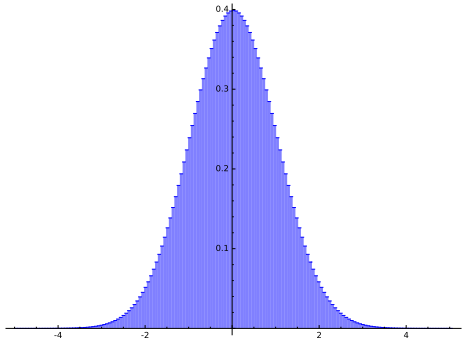
$\Rightarrow$ Models, averages, distribution?



Deciphering the title

- Probabilistic analysis

Object/experiment/execution?
$\Rightarrow$ Models, averages, distribution?



- Number Theory

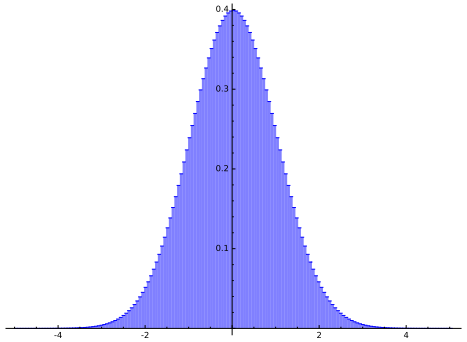
Study of *integers*

$\mathbb{Z}, \quad \{2, 3, 5, 7, 11, \ldots\}, \quad \gcd, \quad \zeta(s)$

Deciphering the title

- Probabilistic analysis

Object/experiment/execution?
$\Rightarrow$ Models, averages, distribution?



- Number Theory

Study of *integers*

$\mathbb{Z}, \quad \{2, 3, 5, 7, 11, \ldots\}, \quad \gcd, \quad \zeta(s)$

- Word Combinatorics

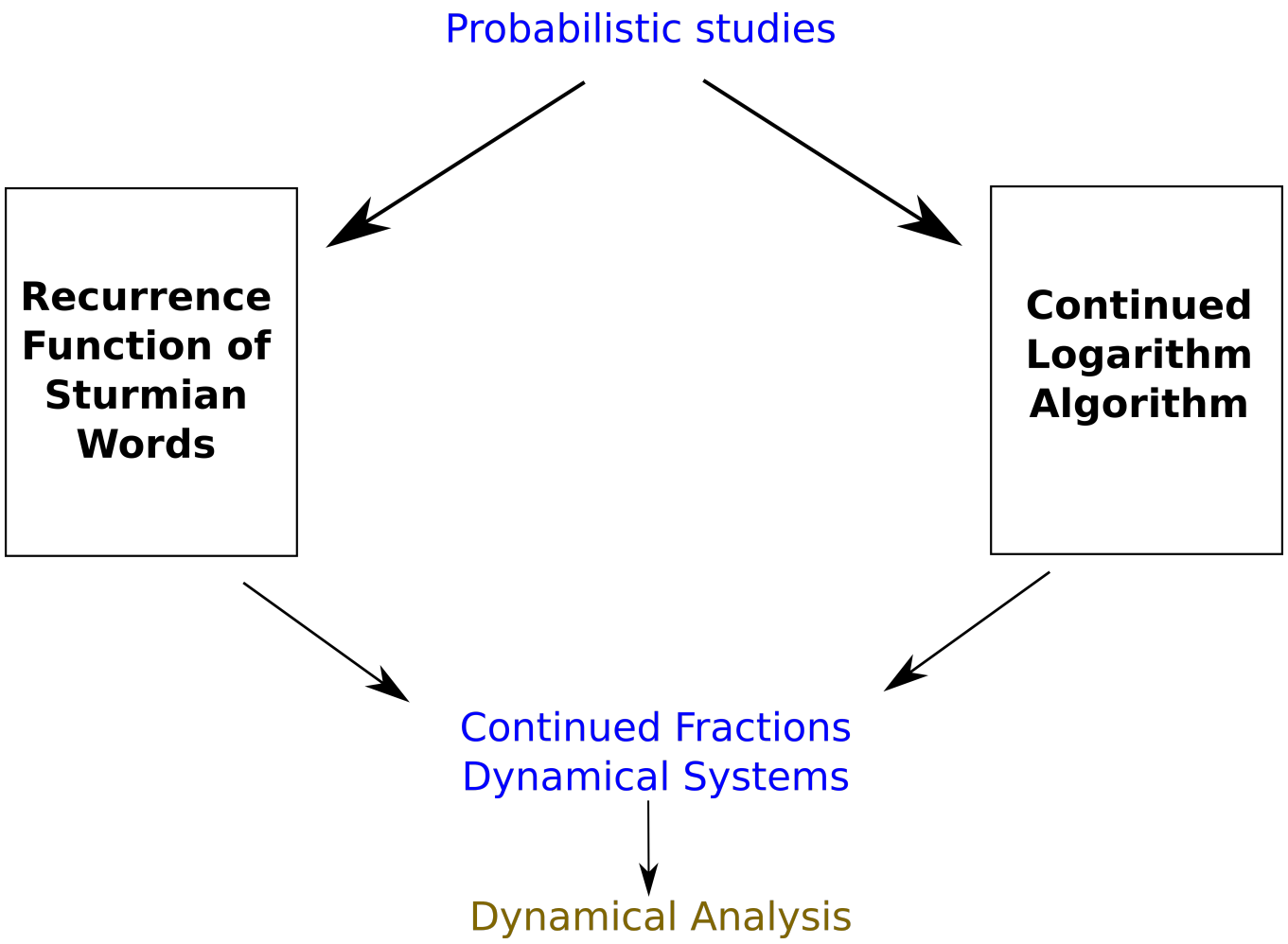
Study of *words*
$\Rightarrow$ subwords (factors), frequencies

Thue-Morse

$\sigma : 0 \mapsto 01,\ 1 \mapsto 10$

$01101001\ldots$

Some key words



Key objects

Sturmian words

- Lowest complexity, not eventually periodic.
- Recurrence function: how often factors reappear?

Continued Logarithm

- Greatest common divisor algorithm.
- Binary shifts and substractions.

Key objects

Sturmian words

- Lowest complexity, not eventually periodic.
- Recurrence function: how often factors reappear?

Continued Logarithm

- Greatest common divisor algorithm.
- Binary shifts and substractions.

Neither had been studied on average.

Key objects

Sturmian words

- Lowest complexity, not eventually periodic.
- Recurrence function: how often factors reappear?

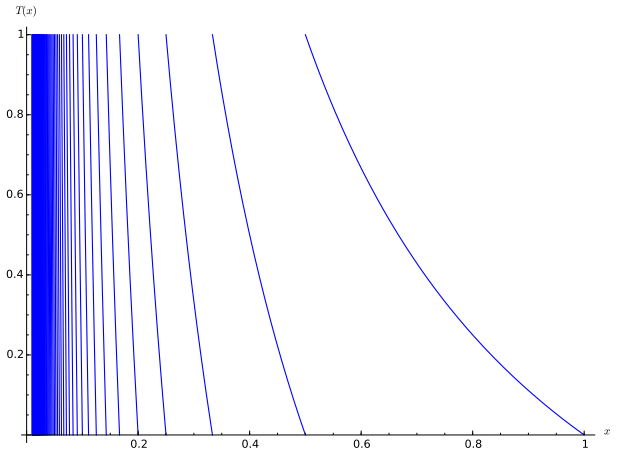
Continued Logarithm

- Greatest common divisor algorithm.
- Binary shifts and substractions.

Neither had been studied on average.

Dynamical analysis

- Objects/algorithms described by dynamical system.
- Tools from dynamical systems.
- Probabilistic analysis.



This talk

1. General Introduction: continued fractions and dynamical systems
   - Continued Fractions
   - Euclidean dynamical system
2. The recurrence function of a random Sturmian word
   - Sturmian words and recurrence
   - Our models and results
   - Comparison between models and slope families
3. The Continued Logarithm
   - Origins and algorithm
   - The CL dynamical system [Chan05]
   - Extended system and results
   - Conclusions and extensions

Section

Continued Fractions

Every irrational number $\alpha \in (0,1)$ has a unique representation

$$\alpha = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots}}$$

where $m_1, m_2, \ldots \geq 1$ are integers called the digits or quotients.

Continued Fractions

Every irrational number $\alpha \in (0,1)$ has a unique representation

$$\alpha = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots}}$$

where $m_1, m_2, \ldots \geq 1$ are integers called the digits or quotients.

Truncating the expansion at depth k we get a convergent

$$\frac{p_k(\alpha)}{q_k(\alpha)} = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots \frac{1}{m_k}}}.$$

The denominators $q_k(\alpha)$ are called the continuants of α.

Euclidean Algorithm and Continued Fractions

Property

Given integers x and y with $0 \leq x \leq y$

$$\gcd(x, y) = \gcd(y \bmod x, x)\,.$$

In conjunction with $\gcd(0, y) = y$, we get the Euclidean Algorithm.

Euclidean Algorithm and Continued Fractions

Property

Given integers x and y with $0 \leq x \leq y$

$$\gcd(x, y) = \gcd(y \bmod x, x)\,.$$

In conjunction with $\gcd(0, y) = y$, we get the Euclidean Algorithm.

This algorithm is equivalent to the continued fraction expansion:

- given the integer division $y = mx + r$,

$$\frac{x}{y} = \frac{1}{m + \frac{r}{x}}\,,$$

  and the process continues with $\frac{r}{x}$.

Euclidean Algorithm and Continued Fractions

Property

Given integers x and y with $0 \leq x \leq y$

$$\gcd(x, y) = \gcd(y \bmod x, x)\,.$$

In conjunction with $\gcd(0, y) = y$, we get the Euclidean Algorithm.

This algorithm is equivalent to the continued fraction expansion:

- given the integer division $y = mx + r$,

$$\frac{x}{y} = \frac{1}{m + \frac{r}{x}}\,,$$

  and the process continues with $\frac{r}{x}$.

Euclidean dynamical system

To get the digits of the continued fraction expansion observe

$$\alpha = \cfrac{1}{m_1 + \cfrac{1}{m_2 + \ddots}}$$

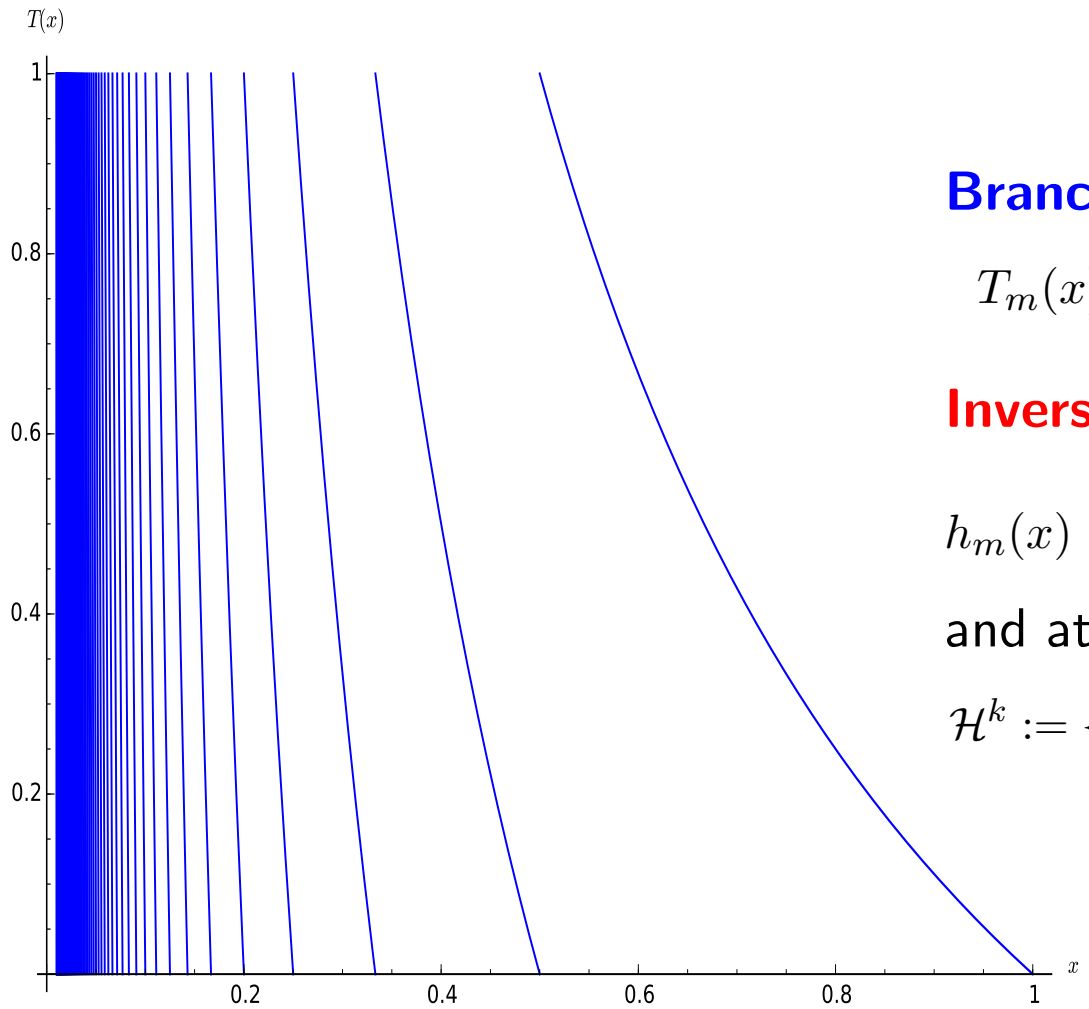
$$\Longrightarrow m_1 = \left\lfloor \frac{1}{\alpha} \right\rfloor , \qquad \cfrac{1}{m_2 + \cfrac{1}{m_3 + \ddots}} = \left\{ \frac{1}{\alpha} \right\} .$$

The map

$$T \colon (0,1) \to (0,1) , \qquad x \mapsto \left\{ \frac{1}{x} \right\} ,$$

is known as the Gauss map.

Gauss map



Branches

$$T_m(x) := \frac{1}{x} - m\,, \quad x \in \left(\frac{1}{m+1}, \frac{1}{m+0}\right].$$

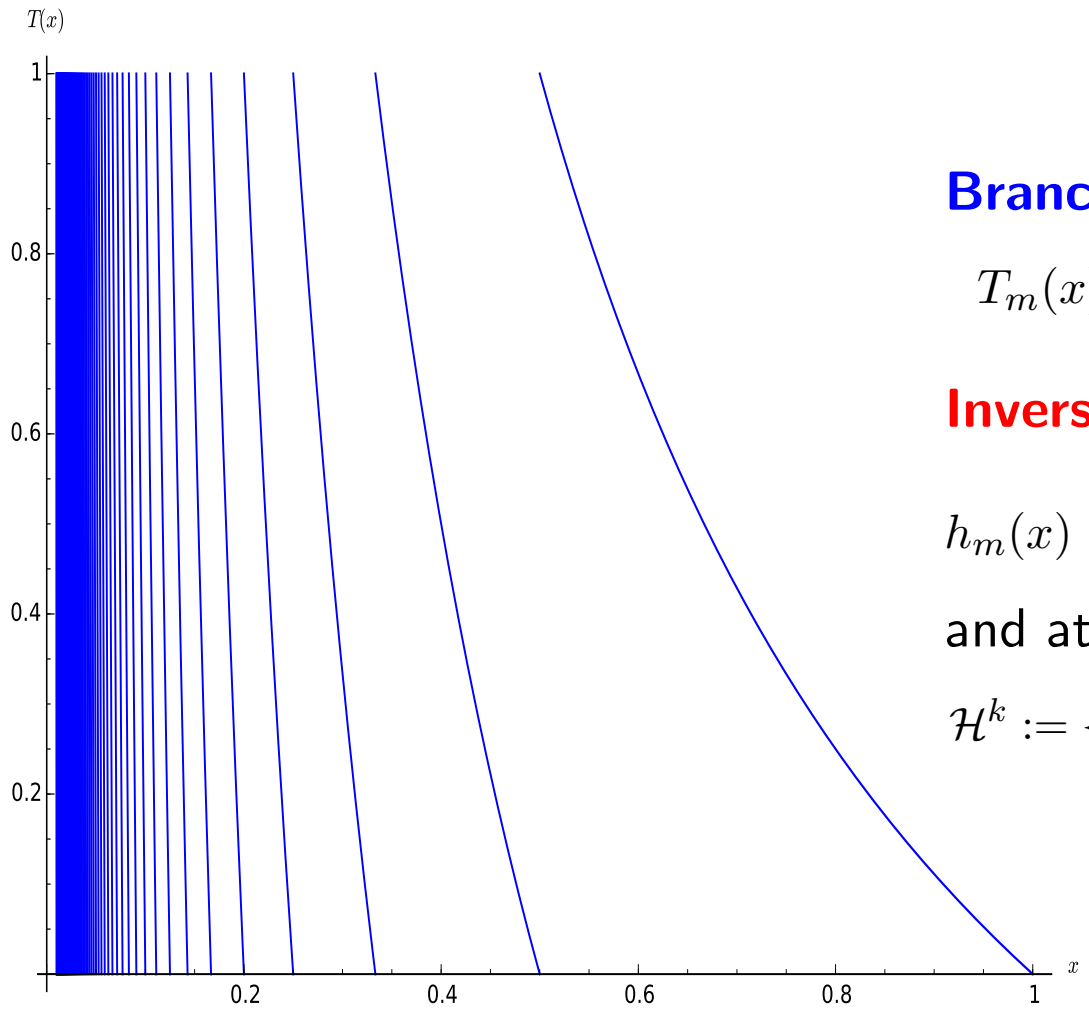
Inverse branches

$$h_m(x) := \frac{1}{m+x}\,, \quad \mathcal{H} := \{h_m : m \in \mathbb{N}\}\,,$$

and at depth k

$$\mathcal{H}^k := \{h_{m_1} \circ \cdots \circ h_{m_k} : m_1, \ldots, m_k \in \mathbb{N}\}\,.$$

Gauss map



Branches

$$T_m(x) := \frac{1}{x} - m\,, \quad x \in \left(\frac{1}{m+1}, \frac{1}{m+0}\right].$$

Inverse branches

$$h_m(x) := \frac{1}{m+x}\,, \quad \mathcal{H} := \{h_m : m \in \mathbb{N}\}\,,$$

and at depth k

$$\mathcal{H}^k := \{h_{m_1} \circ \cdots \circ h_{m_k} : m_1, \ldots, m_k \in \mathbb{N}\}\,.$$

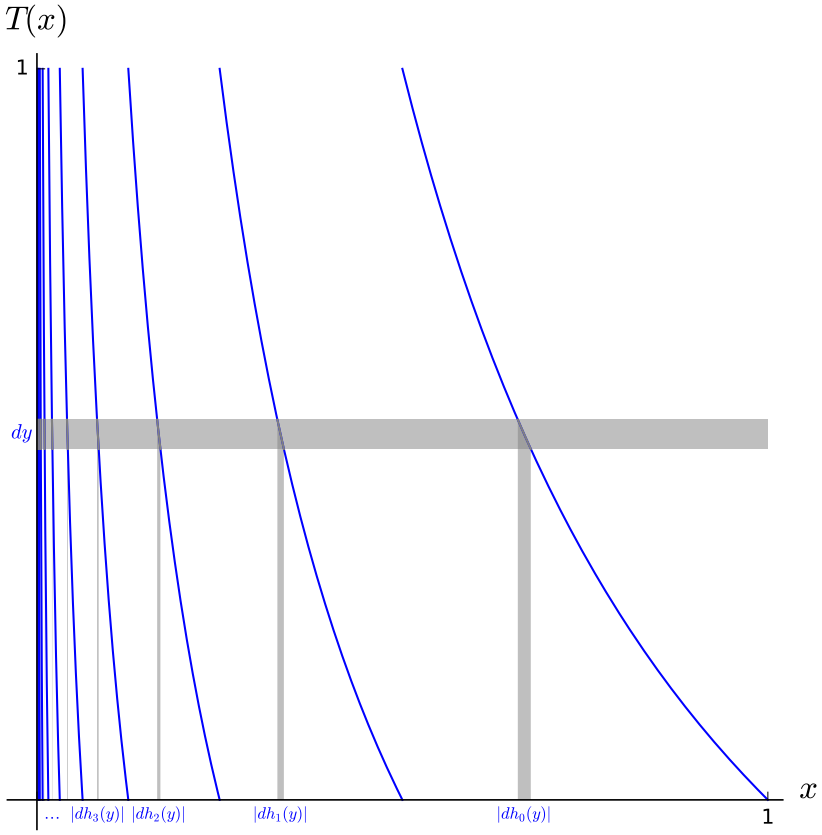
Property. Let $h := h_{m_1} \circ \cdots h_{m_k}$, if $h(0) = \frac{p}{q} \Longrightarrow |h'(0)| = \frac{1}{q^2}$.

Density transformer

Question: If $g \in \mathcal{C}^0(\mathcal{I})$ were the density of $x \Longrightarrow$ density of $T(x)$?

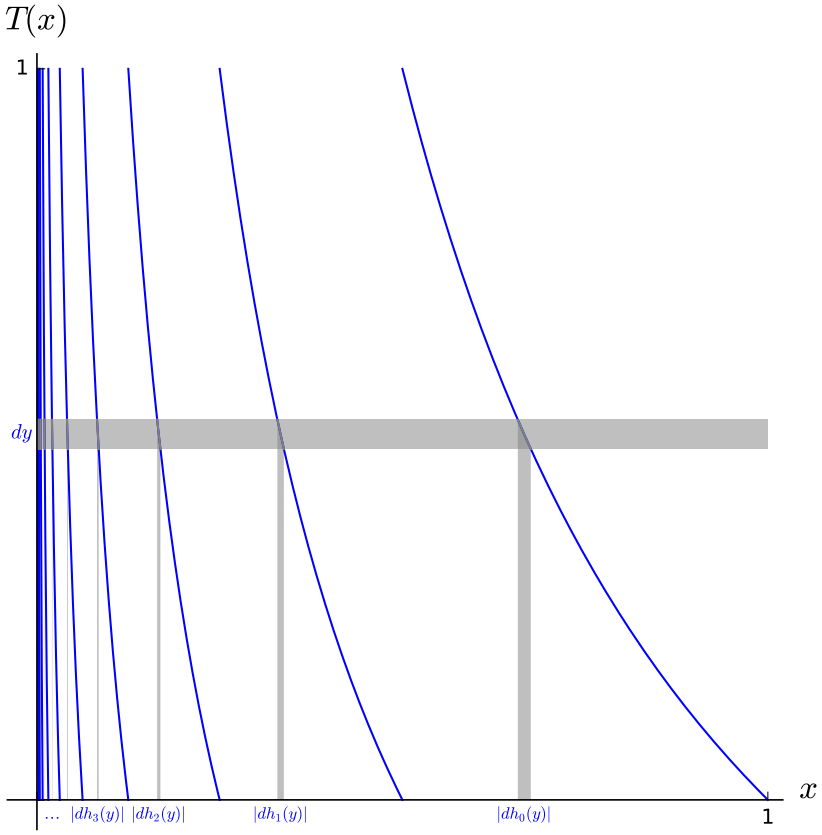
Density transformer

Question: If $g \in \mathcal{C}^0(\mathcal{I})$ were the density of $x \implies$ density of $T(x)$?



Density transformer

Question: If $g \in \mathcal{C}^0(\mathcal{I})$ were the density of $x \Longrightarrow$ density of $T(x)$?



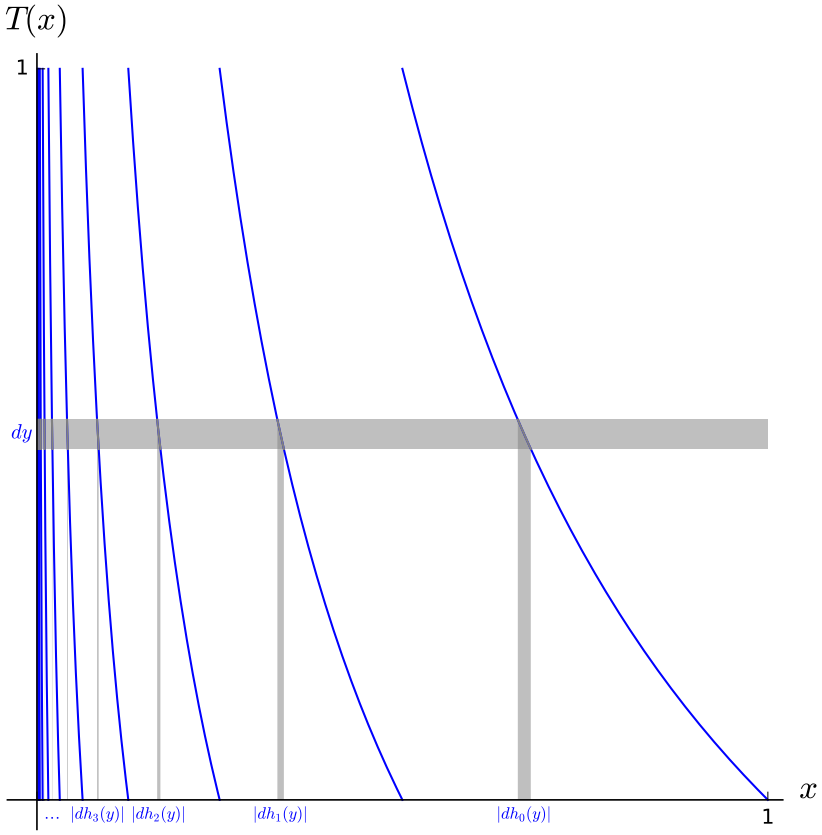
Answer: The density is

$$\mathbf{H}[g](x) = \sum_{h \in \mathcal{H}} \left|h'(x)\right| \, g\left(h(x)\right)$$

$$= \sum_{m \geq 0} \frac{1}{(m+x)^2} \, g\left(\frac{1}{m+x}\right) .$$

Density transformer

Question: If $g \in \mathcal{C}^0(\mathcal{I})$ were the density of $x \Longrightarrow$ density of $T(x)$?



Answer: The density is

$$\mathbf{H}[g](x) = \sum_{h \in \mathcal{H}} \left|h'(x)\right| \, g\left(h(x)\right)$$

$$= \sum_{m \geq 0} \frac{1}{(m+x)^2} \, g\left(\frac{1}{m+x}\right) .$$

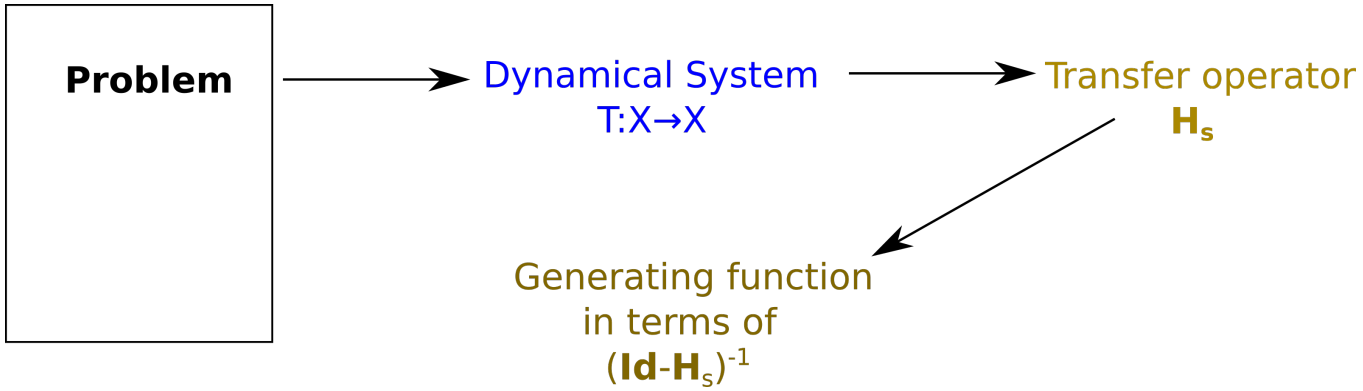
$\Longrightarrow$ Transfer operator $\mathbf{H}_s$ extends $\mathbf{H}$, introducing a variable s

$$\mathbf{H}_s[g](x) = \sum_{h \in \mathcal{H}} \left|h'(x)\right|^s \, g\left(h(x)\right) .$$

Principles of dynamical analysis [Vallée,Flajolet,Baladi,...]:

Generating functions.

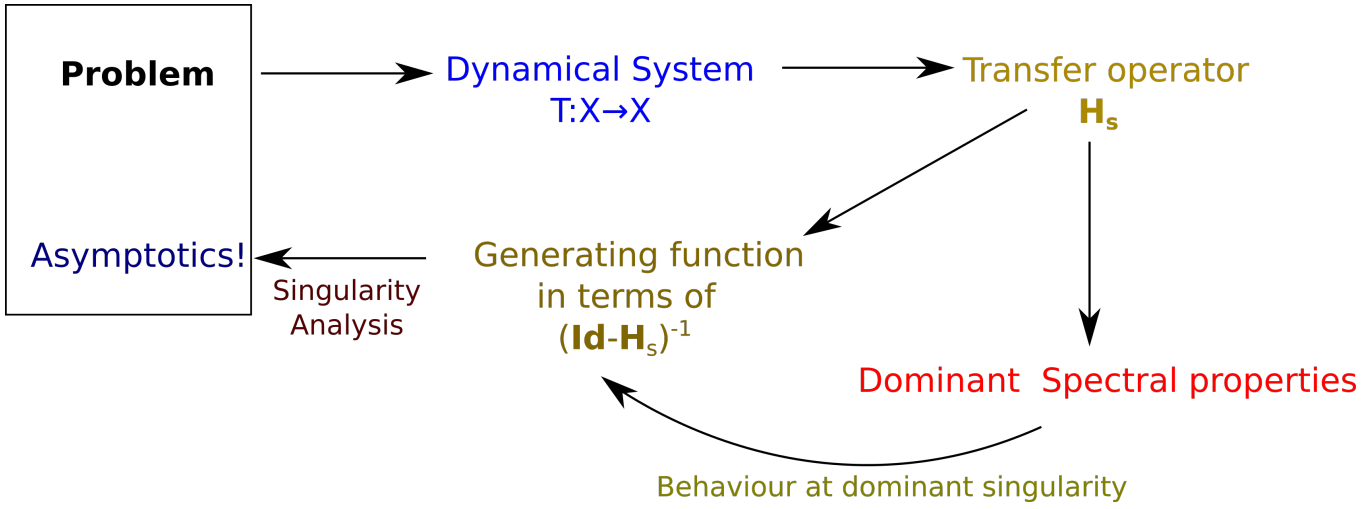
- $\mathbf{H}_s$ describes all executions of depth 1.
- $\mathbf{H}_s^2 = \mathbf{H}_s \circ \mathbf{H}_s$ describes all executions of depth 2.
- $\vdots$
- and $(\mathbf{I} - \mathbf{H}_s)^{-1} = \mathbf{I} + \mathbf{H}_s + \mathbf{H}_s^2 + \ldots$ describes *all* executions.



Principles of dynamical analysis [Vallée,Flajolet,Baladi,...]:

Generating functions.

- $\mathbf{H}_s$ describes all executions of depth 1.
- $\mathbf{H}_s^2 = \mathbf{H}_s \circ \mathbf{H}_s$ describes all executions of depth 2.
- $\vdots$
- and $(\mathbf{I} - \mathbf{H}_s)^{-1} = \mathbf{I} + \mathbf{H}_s + \mathbf{H}_s^2 + \ldots$ describes *all* executions.



Section

Definition of Sturmian words

Definition

Complexity function of an infinite word $\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}}$

$$p_{\boldsymbol{u}} \colon \mathbb{N} \to \mathbb{N}\,, \qquad p_{\boldsymbol{u}}(n) = \#\{\text{factors of length } n \text{ in } \boldsymbol{u}\}\,.$$

Definition of Sturmian words

Definition

Complexity function of an infinite word $\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}}$

$$p_{\boldsymbol{u}} \colon \mathbb{N} \to \mathbb{N}\,, \qquad p_{\boldsymbol{u}}(n) = \#\{\text{factors of length } n \text{ in } \boldsymbol{u}\}\,.$$

Important property

$\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}}$ is not eventually periodic

$\iff p_{\boldsymbol{u}}(n+1) > p_{\boldsymbol{u}}(n)$ for all $n \in \mathbb{N}$

.

Definition of Sturmian words

Definition

Complexity function of an infinite word $\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}}$

$$p_{\boldsymbol{u}} \colon \mathbb{N} \to \mathbb{N}\,, \qquad p_{\boldsymbol{u}}(n) = \#\{\text{factors of length } n \text{ in } \boldsymbol{u}\}\,.$$

Important property

$$\begin{aligned} &\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}} \text{ is not eventually periodic} \\ &\iff p_{\boldsymbol{u}}(n+1) > p_{\boldsymbol{u}}(n) \text{ for all } n \in \mathbb{N} \\ &\implies p_{\boldsymbol{u}}(n) \geq n+1\,. \end{aligned}$$

Sturmian words are the "simplest" that are not eventually periodic.

Definition of Sturmian words

Definition

Complexity function of an infinite word $\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}}$

$$p_{\boldsymbol{u}} \colon \mathbb{N} \to \mathbb{N}\,, \qquad p_{\boldsymbol{u}}(n) = \#\{\text{factors of length } n \text{ in } \boldsymbol{u}\}\,.$$

Important property

$$\begin{aligned} &\boldsymbol{u} \in \mathcal{A}^{\mathbb{N}} \text{ is not eventually periodic} \\ &\iff p_{\boldsymbol{u}}(n+1) > p_{\boldsymbol{u}}(n) \text{ for all } n \in \mathbb{N} \\ &\implies p_{\boldsymbol{u}}(n) \geq n+1\,. \end{aligned}$$

Sturmian words are the "simplest" that are not eventually periodic.

Definition

$\boldsymbol{u} \in \{0,1\}^{\mathbb{N}}$ is Sturmian $\iff p_{\boldsymbol{u}}(n) = n+1$ for each $n \geq 0$.

Sturmian words and digital lines

Sturmian words correspond to discrete codings of lines, from below or above, by horizontal lines and diagonals.

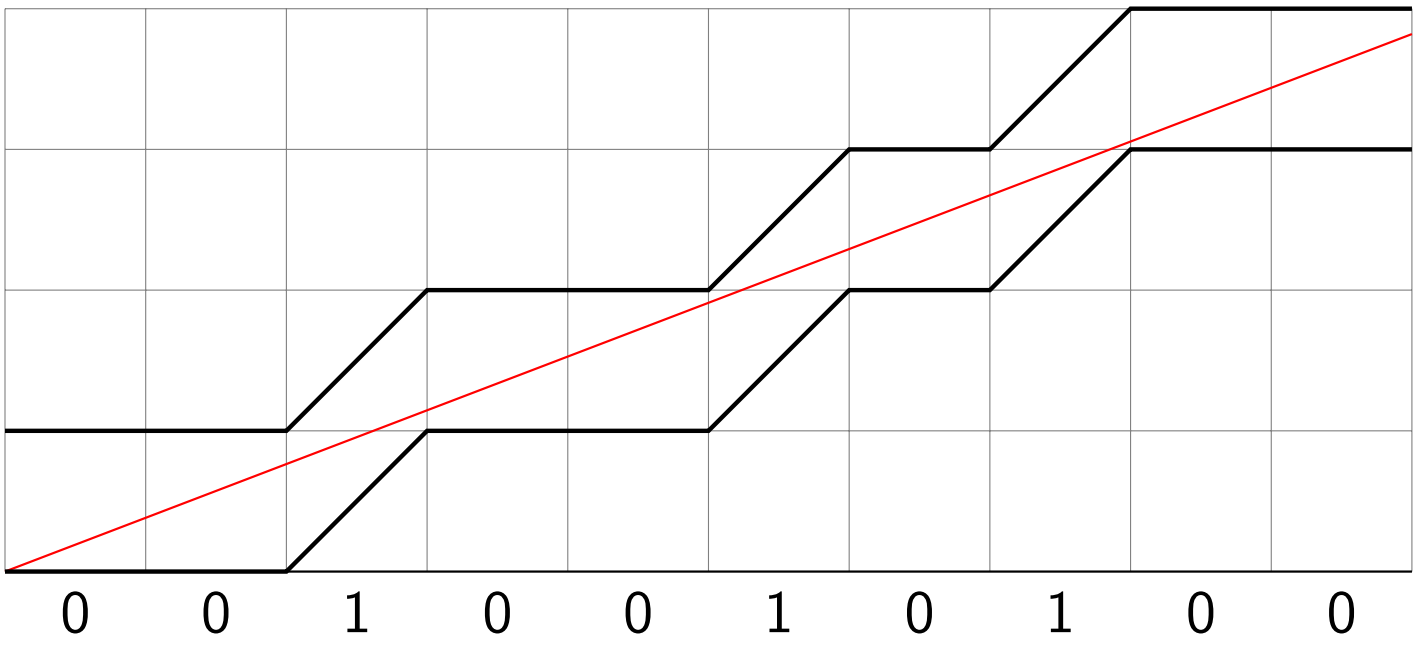


Figure : Coding of the line $y = \alpha x + \beta$.

Sturmian words and digital lines

Sturmian words correspond to discrete codings of lines, from below or above, by horizontal lines and diagonals.

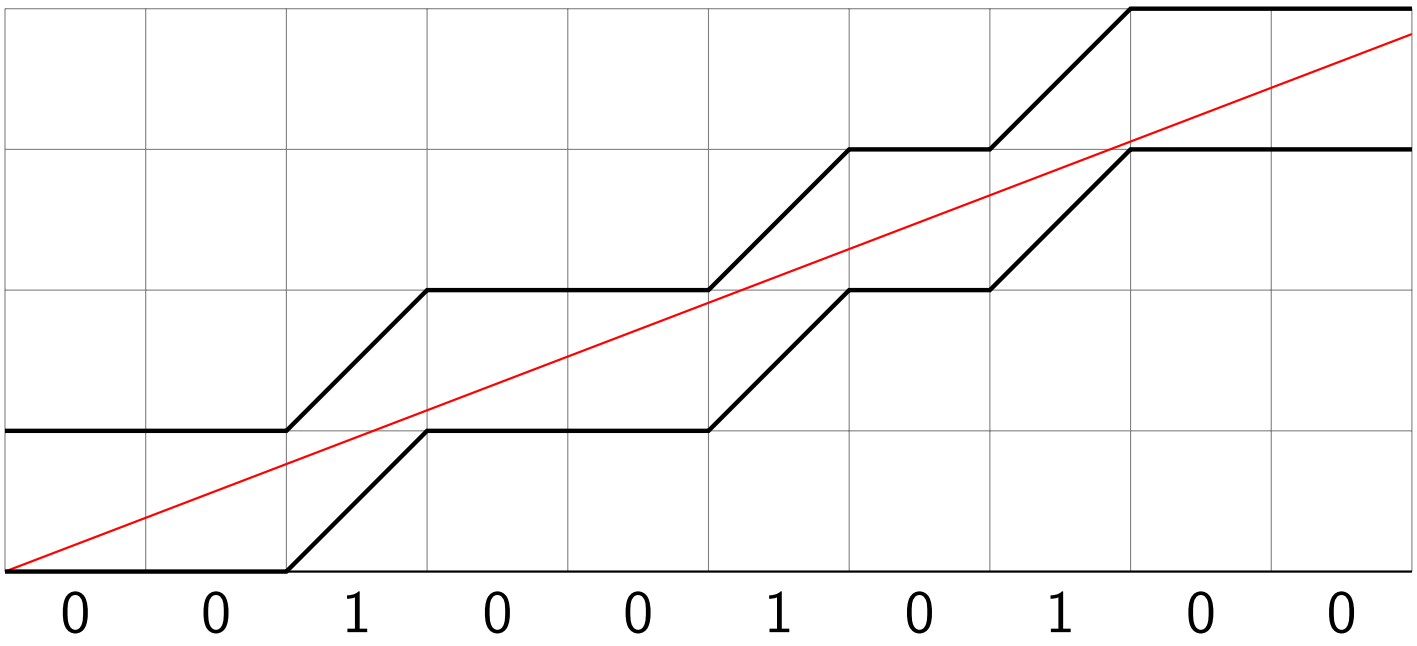


Figure : Coding of the line $y = \alpha x + \beta$.

The *slope* α plays a key role:

the finite factors are determined exclusively by α.

Recurrence of Sturmian words

Definition (Recurrence function)

Consider an infinite word $\boldsymbol{u}$. Its recurrence function is:

$$R_{\boldsymbol{u}}(n) = \inf \{m \in \mathbb{N} : \text{every factor of length } m \\ \textbf{contains} \text{ all the factors of length } n\}.$$

Recurrence of Sturmian words

Definition (Recurrence function)

Consider an infinite word $\boldsymbol{u}$. Its recurrence function is:

$$R_{\boldsymbol{u}}(n) = \inf \{m \in \mathbb{N} : \text{every factor of length } m \text{ } \textbf{contains} \text{ all the factors of length } n\}.$$

- Cost we have to pay to discover the factors if we start from an arbitrary point in $\boldsymbol{u} = u_1 u_2 \ldots$

Recurrence of Sturmian words

Definition (Recurrence function)

Consider an infinite word $\boldsymbol{u}$. Its recurrence function is:

$$R_{\boldsymbol{u}}(n) = \inf \{m \in \mathbb{N} : \text{every factor of length } m \text{ } \textbf{contains} \text{ all the factors of length } n\}.$$

- Cost we have to pay to discover the factors if we start from an arbitrary point in $\boldsymbol{u} = u_1 u_2 \ldots$

Theorem (Morse, Hedlund, 1940)

The recurrence function is piecewise affine and satisfies

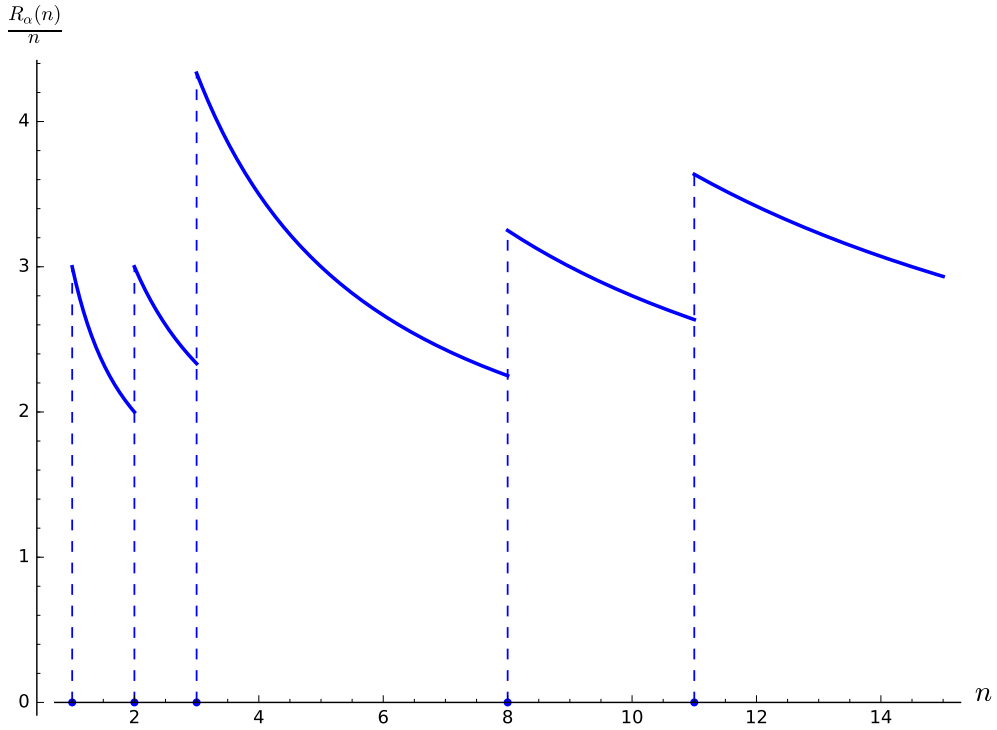
$$R_\alpha(n) = n - 1 + q_{k-1}(\alpha) + q_k(\alpha), \qquad \text{for } q_{k-1}(\alpha) \leq n < q_k(\alpha).$$

Recurrence quotient and its parameters

$$S(\alpha, n) := \frac{R_\alpha(n) + 1}{n} = 1 + \frac{q_{k-1}(\alpha) + q_k(\alpha)}{n}, \quad q_{k-1}(\alpha) \leq n < q_k(\alpha).$$

Recurrence quotient and its parameters

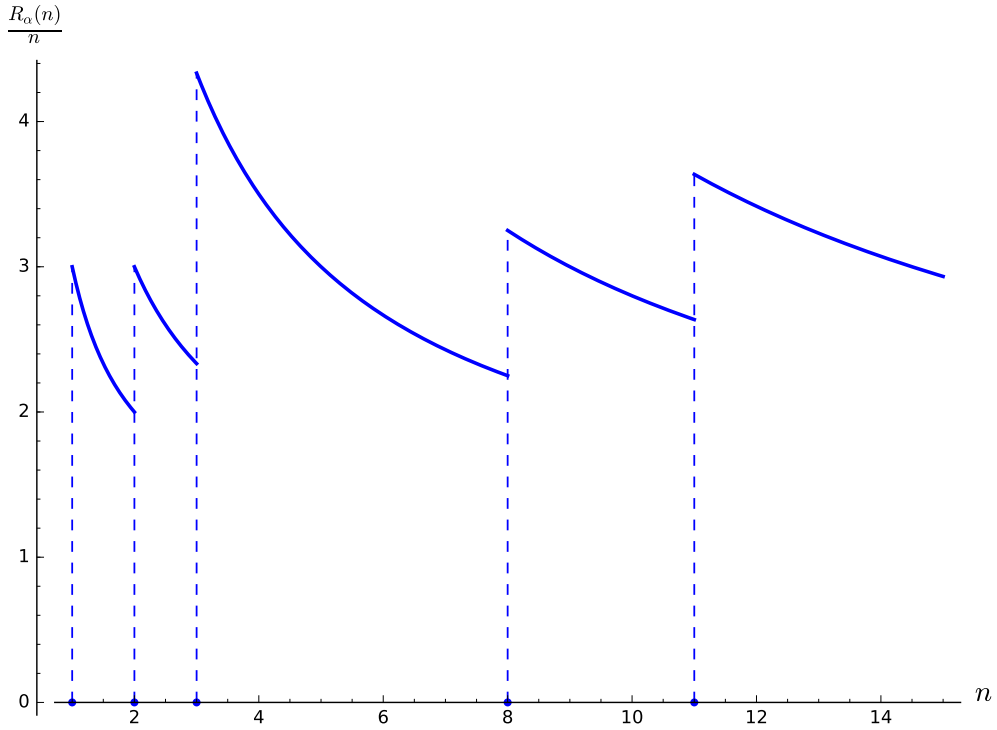
$$S(\alpha, n) := \frac{R_\alpha(n) + 1}{n} = 1 + \frac{q_{k-1}(\alpha) + q_k(\alpha)}{n}, \quad q_{k-1}(\alpha) \leq n < q_k(\alpha).$$



Recurrence quotient $\alpha = e^{-1}$.

Recurrence quotient and its parameters

$$S(\alpha, n) := \frac{R_\alpha(n) + 1}{n} = 1 + \frac{q_{k-1}(\alpha) + q_k(\alpha)}{n}, \quad q_{k-1}(\alpha) \le n < q_k(\alpha).$$



Recurrence quotient $\alpha = e^{-1}$.

Size of $S(\alpha, n)$ dictated by

- the relative position of n within the interval

$$\mu(\alpha, n),$$

- the quotient between the ends of the interval

$$\rho(\alpha, n) = \frac{q_{k-1}(\alpha)}{q_k(\alpha)}.$$

Studies of the recurrence function

Classical results concern the worst case scenarios for *fixed* α:

$\forall \epsilon > 0$, for a.e. α

$$\limsup_{n\to\infty} \frac{S(\alpha, n)}{\log n} = \infty\,, \quad \lim_{n\to\infty} \frac{S(\alpha, n)}{(\log n)^{1+\epsilon}} = 0\,.$$

(Morse&Hedlund '40)

Studies of the recurrence function

Classical results concern the worst case scenarios for *fixed* α:

$\forall \epsilon > 0$, for a.e. α

$$\limsup_{n\to\infty} \frac{S(\alpha,n)}{\log n} = \infty\,, \quad \lim_{n\to\infty} \frac{S(\alpha,n)}{(\log n)^{1+\epsilon}} = 0\,.$$

(Morse&Hedlund '40)

We define two probabilistic models

in both cases α is drawn *uniformly at random*

1) fix the length $n \Rightarrow$ random variables $S_n(\alpha) := S(\alpha,n)$.

in distribution and expectation as $n \to \infty$.

Studies of the recurrence function

Classical results concern the worst case scenarios for *fixed* α:

$\forall \epsilon > 0$, for a.e. α

$$\limsup_{n\to\infty} \frac{S(\alpha,n)}{\log n} = \infty\,, \qquad \lim_{n\to\infty} \frac{S(\alpha,n)}{(\log n)^{1+\epsilon}} = 0\,.$$

(Morse&Hedlund '40)

We define two probabilistic models

in both cases α is drawn *uniformly at random*

1) fix the length $n \Rightarrow$ random variables $S_n(\alpha) := S(\alpha, n)$.
   in distribution and expectation as $n \to \infty$.
2) fix index k of interval $[q_{k-1}(\alpha), q_k(\alpha))$ and
   the relative position $\mu \Rightarrow$ sequence $(n_k(\alpha))_k$.

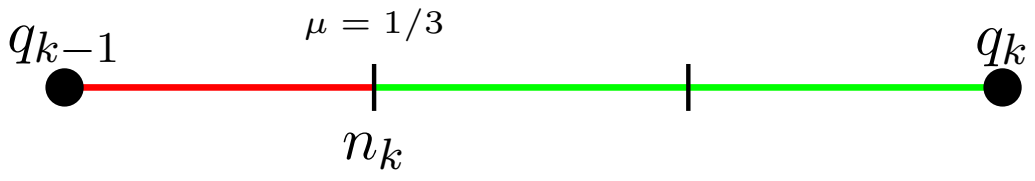


Figure : Sequence of indices $(n_k(\alpha))_k$ for $\mu = 1/3$.

Results

Model: fixed n. [RV17]

- Limit distribution for S_n and more general class.
- Convergence of histograms to limit density.
- Conditional expectations $\mathbb{E}[S_n | \mu_n \geq \epsilon(n)] \sim \left| \log \epsilon(n) \right|$.

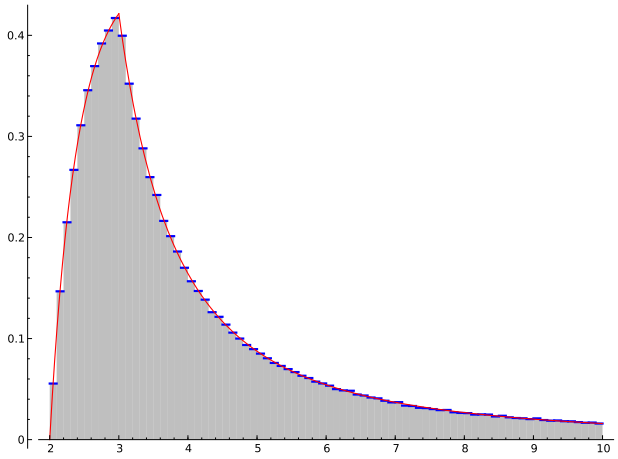


Figure : Limit density of S_n.

Results

Model: fixed n. [RV17]

- Limit distribution for S_n and more general class.
- Convergence of histograms to limit density.
- Conditional expectations $\mathbb{E}[S_n | \mu_n \geq \epsilon(n)] \sim \left| \log \epsilon(n) \right|$.

Model: fixed μ. [BCRVV15]

- Limit distribution of
$$S_\mu^{\langle k \rangle}(\alpha) := S(\alpha, n_k)$$
depending on μ.
- Study of $\mathbb{E}[S_\mu^{\langle k \rangle}(\alpha)]$ as
$$\mu := \mu_k \to 0\,.$$

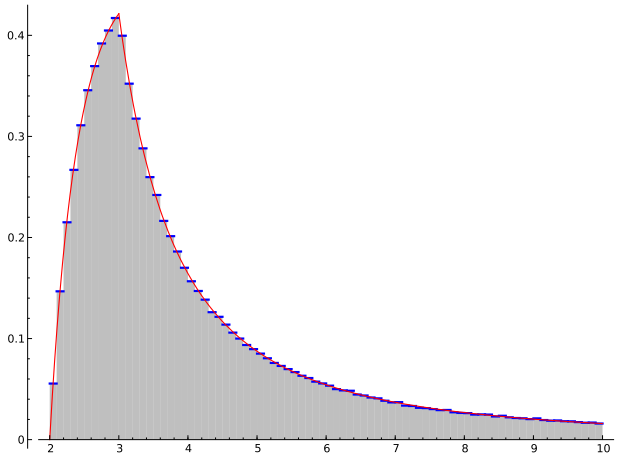


Figure : Limit density of S_n.

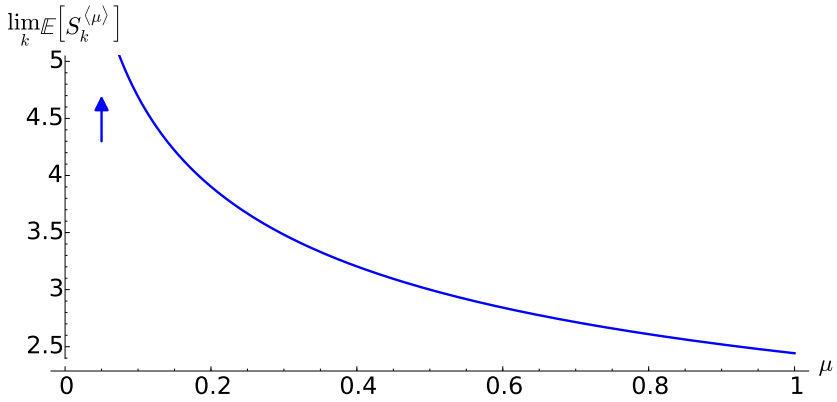


Figure : Limit of $\mathbb{E}[S_\mu^{\langle k \rangle}]$ versus μ.

Coprime Riemann sums: fixed $n \to \infty$

For $q_{k-1}(\alpha) \leq n < q_k(\alpha)$

$$S_n(\alpha) = f(x, y) := 1 + x + y\,, \qquad x = \frac{q_{k-1}(\alpha)}{n}\,, \quad y = \frac{q_k(\alpha)}{n}\,.$$

Coprime Riemann sums: fixed $n \to \infty$

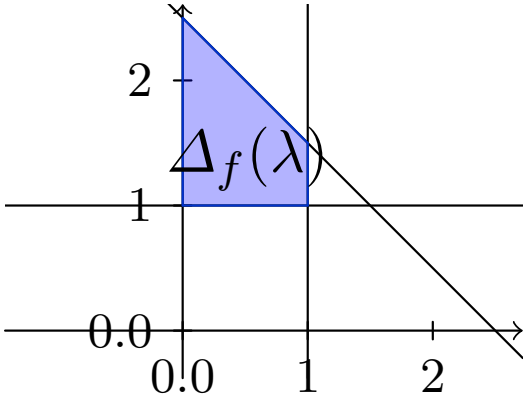
For $q_{k-1}(\alpha) \le n < q_k(\alpha)$

$$S_n(\alpha) = f(x,y) := 1 + x + y\,, \qquad x = \frac{q_{k-1}(\alpha)}{n}\,, \quad y = \frac{q_k(\alpha)}{n}\,.$$

Distribution is a *coprime* Riemann sum

$$\mathbb{P}\left(S_n \le \lambda\right) = \frac{1}{n^2} \sum_{(a,b)\in\mathbb{N}^2:(a,b)=1} \omega\left(\tfrac{a}{n}, \tfrac{b}{n}\right) [\![\left(\tfrac{a}{n}, \tfrac{b}{n}\right) \in \Delta_f(\lambda)]\!]\,,$$

with $\omega(x,y) = \frac{2}{y(x+y)}$, $\Delta_f(\lambda) = \{(x,y) : 0 < x \le 1 < y,\ f(x,y) \le \lambda\}$.



Coprime Riemann sums: fixed $n \to \infty$

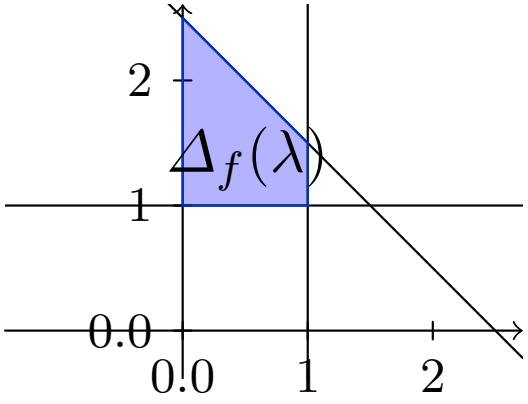
For $q_{k-1}(\alpha) \le n < q_k(\alpha)$

$$S_n(\alpha) = f(x,y) := 1 + x + y\,, \qquad x = \frac{q_{k-1}(\alpha)}{n}\,, \quad y = \frac{q_k(\alpha)}{n}\,.$$

Distribution is a *coprime* Riemann sum

$$\mathbb{P}\left(S_n \le \lambda\right) = \frac{1}{n^2} \sum_{(a,b)\in\mathbb{N}^2:(a,b)=1} \omega\left(\tfrac{a}{n}, \tfrac{b}{n}\right) [\![\left(\tfrac{a}{n}, \tfrac{b}{n}\right) \in \Delta_f(\lambda)]\!]\,,$$

with $\omega(x,y) = \frac{2}{y(x+y)}$, $\Delta_f(\lambda) = \{(x,y) : 0 < x \le 1 < y,\ f(x,y) \le \lambda\}$.



A constant · the integral

$$\lim_{n\to\infty} \mathbb{P}\left(S_n \le \lambda\right) = \frac{6}{\pi^2} \iint_{\Delta_f(\lambda)} \omega(x,y)\,dx\,dy$$

Coprime Riemann sums: fixed $n \to \infty$

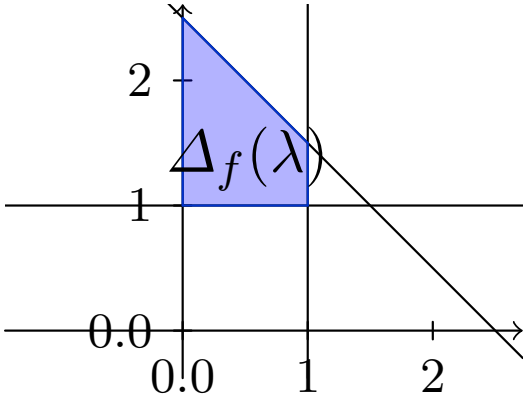
For $q_{k-1}(\alpha) \le n < q_k(\alpha)$

$$S_n(\alpha) = f(x,y) := 1 + x + y\,, \qquad x = \frac{q_{k-1}(\alpha)}{n}\,, \quad y = \frac{q_k(\alpha)}{n}\,.$$

Distribution is a *coprime* Riemann sum

$$\mathbb{P}\left(S_n \le \lambda\right) = \frac{1}{n^2} \sum_{(a,b)\in\mathbb{N}^2:(a,b)=1} \omega\left(\tfrac{a}{n}, \tfrac{b}{n}\right) [\![\left(\tfrac{a}{n}, \tfrac{b}{n}\right) \in \Delta_f(\lambda)]\!]\,,$$

with $\omega(x,y) = \frac{2}{y(x+y)}$, $\Delta_f(\lambda) = \{(x,y) : 0 < x \le 1 < y,\ f(x,y) \le \lambda\}$.



A constant · the integral

$$\lim_{n\to\infty} \mathbb{P}\left(S_n \le \lambda\right) = \frac{6}{\pi^2} \iint_{\Delta_f(\lambda)} \omega(x,y)\,dx\,dy$$

Note. Generalizes to other fs.

Via the Transfer operator

The model $n \to \infty$ is related to the quasi-inverse, how?

Via the Transfer operator

The model $n \to \infty$ is related to the quasi-inverse, how?

- Harmonic sum in $t := 1/n$ with frequencies (q_k)

$$\Pr(S_n \leq \lambda) = \frac{1}{n^2} \sum_k \sum_{m_1,\ldots,m_k \geq 1} g_\lambda \left(\frac{q_{k-1}}{q_k}, \frac{q_k}{n} \right) ,$$

for a certain g_λ.

Via the Transfer operator

The model $n \to \infty$ is related to the quasi-inverse, how?

- Harmonic sum in $t := 1/n$ with frequencies (q_k)

$$\Pr(S_n \leq \lambda) = \frac{1}{n^2} \sum_k \sum_{m_1,\ldots,m_k \geq 1} g_\lambda \left(\frac{q_{k-1}}{q_k}, \frac{q_k}{n} \right) ,$$

  for a certain g_λ.

- Mellin transform turns it into a quasi-inverse

$$(\mathbf{I} - \mathbf{H}_{s/2+1})^{-1} \left[G_s \right] (0) ,$$

  for appropriate G_s that is an integral of g_λ.

Via the Transfer operator

The model $n \to \infty$ is related to the quasi-inverse, how?

- Harmonic sum in $t := 1/n$ with frequencies (q_k)

$$\Pr(S_n \leq \lambda) = \frac{1}{n^2} \sum_k \sum_{m_1,\ldots,m_k \geq 1} g_\lambda \left(\frac{q_{k-1}}{q_k}, \frac{q_k}{n} \right) ,$$

  for a certain g_λ.

- Mellin transform turns it into a quasi-inverse

$$(\mathbf{I} - \mathbf{H}_{s/2+1})^{-1} \left[G_s \right] (0) ,$$

  for appropriate G_s that is an integral of g_λ.

- Requires precise analysis for a vertical strip around $\Re s = 0$
  $\Longrightarrow$ Dolgopyat-Baladi-Vallée estimates.

Via the Transfer operator

The model $n \to \infty$ is related to the quasi-inverse, how?

- Harmonic sum in $t := 1/n$ with frequencies (q_k)

$$\Pr(S_n \leq \lambda) = \frac{1}{n^2} \sum_k \sum_{m_1,\ldots,m_k \geq 1} g_\lambda \left(\frac{q_{k-1}}{q_k}, \frac{q_k}{n} \right) ,$$

  for a certain g_λ.

- Mellin transform turns it into a quasi-inverse

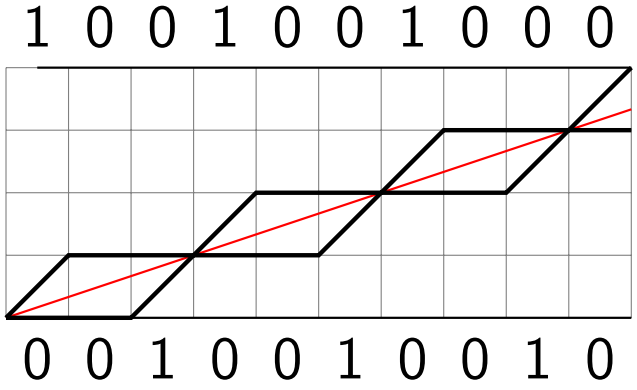
$$(\mathbf{I} - \mathbf{H}_{s/2+1})^{-1} \left[G_s \right] (0) ,$$

  for appropriate G_s that is an integral of g_λ.

- Requires precise analysis for a vertical strip around $\Re s = 0$
  $\Longrightarrow$ Dolgopyat-Baladi-Vallée estimates.

Important subfamilies

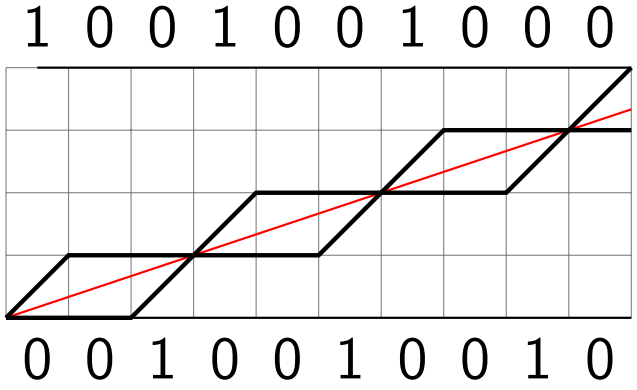
- Slope α rational:
  periodic, Christoffel words.



- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

Important subfamilies

- Slope α rational:
  periodic, Christoffel words.



- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

We expect unified solution with the real case:

- similar results under appropriate models.
- methods involve Dirichlet series.

Section

The origins

Introduced by Gosper as a mutation of continued fractions:

- gives rise to a $\gcd$ algorithm akin to Euclid's.
- quotients are powers of two:
  - small information parcel.
  - employs only shifts and subtractions.
- appears to be simple and efficient.

The origins

Introduced by Gosper as a mutation of continued fractions:

- gives rise to a $\gcd$ algorithm akin to Euclid's.
- quotients are powers of two:
  - small information parcel.
  - employs only shifts and subtractions.
- appears to be simple and efficient.

More recently:

- Shallit studied its worst-case performance in 2016.
- We consider its average performance!

Continued Logarithm Algorithm

A sequence of binary "divisions" beginning from (p, q):

$$q = \mathbf{2^a} p + r\,, \qquad 0 \le r < 2^a p\,.$$

Continued Logarithm Algorithm

A sequence of binary "divisions" beginning from (p, q):

$$q = \mathbf{2^a} p + r\,, \qquad 0 \le r < 2^a p\,.$$

Note. $a = \max\{k \ge 0 : 2^k p \le q\}$

Continued Logarithm Algorithm

A sequence of binary "divisions" beginning from (p, q):

$$q = \mathbf{2^a} p + r\,, \qquad 0 \le r < 2^a p\,.$$

Note. $a = \max\{k \ge 0 : 2^k p \le q\}$

Continue with the new pair

$$(p, q) \mapsto (p', q') = (r, 2^a p)\,,$$

until the remainder r equals 0.

Continued Logarithm Algorithm

A sequence of binary "divisions" beginning from (p, q):

$$q = \mathbf{2^a} p + r\,, \qquad 0 \le r < 2^a p\,.$$

Note. $a = \max\{k \ge 0 : 2^k p \le q\}$

Continue with the new pair

$$(p, q) \mapsto (p', q') = (r, 2^a p)\,,$$

until the remainder r equals 0.

Example. Let us find $\gcd(13, 31)$.

a	p	q	r	$2^a p$
1	13	31	5	26
2	5	26	6	20
1	6	20	8	12
0	8	12	4	8
1	4	8	0	8

Continued Logarithm Algorithm

A sequence of binary "divisions" beginning from (p, q):

$$q = \mathbf{2^a} p + r\,, \qquad 0 \le r < 2^a p\,.$$

Note. $a = \max\{k \ge 0 : 2^k p \le q\}$

Continue with the new pair

$$(p, q) \mapsto (p', q') = (r, 2^a p)\,,$$

until the remainder r equals 0.

Example. Let us find $\gcd(13, 31)$.

a	p	q	r	$2^a p$
1	13	31	5	26
2	5	26	6	20
1	6	20	8	12
0	8	12	4	8
1	4	8	0	8

- Ended with $(0, 8)$, what is the $\gcd$?
  $\Rightarrow$ odd $\gcd \times$ parasitic powers of 2.

Consider

$$\Omega_N = \{(p,q) \in \mathbb{N} \times \mathbb{N} : p \leq q \leq N\}.$$

Worst-case studied by Shallit (2016): $2\log_2 N + O(1)$ steps.

Consider

$$\Omega_N = \{(p,q) \in \mathbb{N} \times \mathbb{N} : p \leq q \leq N\}\,.$$

Worst-case studied by Shallit (2016): $2\log_2 N + O(1)$ steps.

- Family $(p,q) = (1, 2^n - 1)$ gives the bound asymptotically.

Consider

$$\Omega_N = \{(p,q) \in \mathbb{N} \times \mathbb{N} : p \leq q \leq N\}.$$

Worst-case studied by Shallit (2016): $2\log_2 N + O(1)$ steps.

- Family $(p,q) = (1, 2^n - 1)$ gives the bound asymptotically.

We studied the average number of steps over Ω_N, posed by Shallit.

Consider

$$\Omega_N = \{(p,q) \in \mathbb{N} \times \mathbb{N} : p \le q \le N\}\,.$$

Worst-case studied by Shallit (2016): $2\log_2 N + O(1)$ steps.
◦ Family $(p,q) = (1, 2^n - 1)$ gives the bound asymptotically.

We studied the average number of steps over Ω_N, posed by Shallit.

Main result [RV18].

Mean number of **steps** $E_N[K]$ and **shifts** $E_N[S]$ are $\Theta(\log N)$.

More precisely

$$E_N[K] \sim k \log N\,, \qquad E_N[S] \sim \tfrac{\log 3 - \log 2}{2\log 2 - \log 3}\, E_N[K]$$

for an *explicit constant* $k \doteq 1.49283\ldots$ given by

$$k = \frac{2}{H}\,, \quad H = \text{entropy of appropriate DS}$$

Consider

$$\Omega_N = \{(p,q) \in \mathbb{N} \times \mathbb{N} : p \le q \le N\}\,.$$

Worst-case studied by Shallit (2016): $2\log_2 N + O(1)$ steps.

◦ Family $(p,q) = (1, 2^n - 1)$ gives the bound asymptotically.

We studied the average number of steps over Ω_N, posed by Shallit.

Main result [RV18].

Mean number of **steps** $E_N[K]$ and **shifts** $E_N[S]$ are $\Theta(\log N)$.

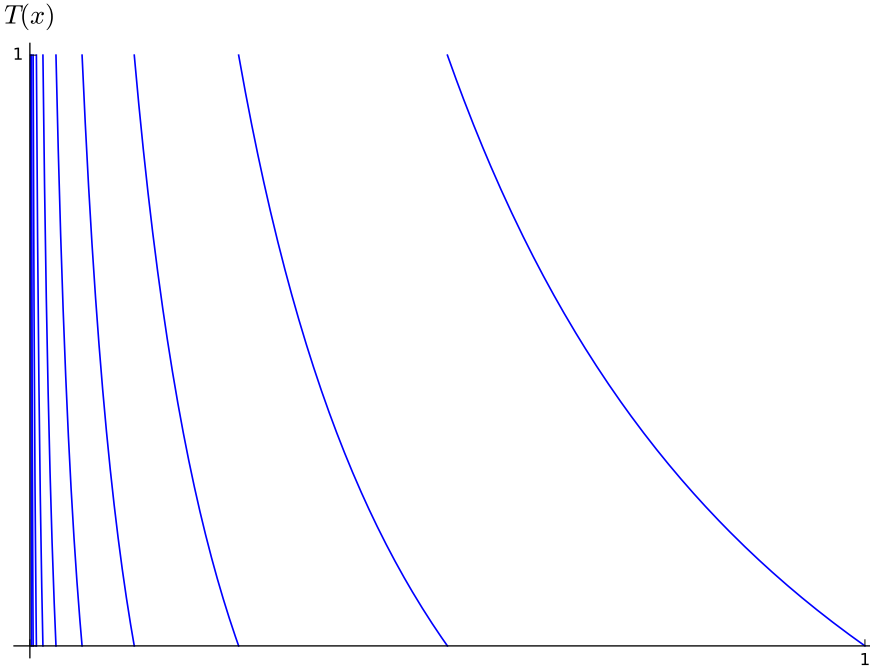
More precisely

$$E_N[K] \sim k \log N\,, \qquad E_N[S] \sim \tfrac{\log 3 - \log 2}{2\log 2 - \log 3}\, E_N[K]$$

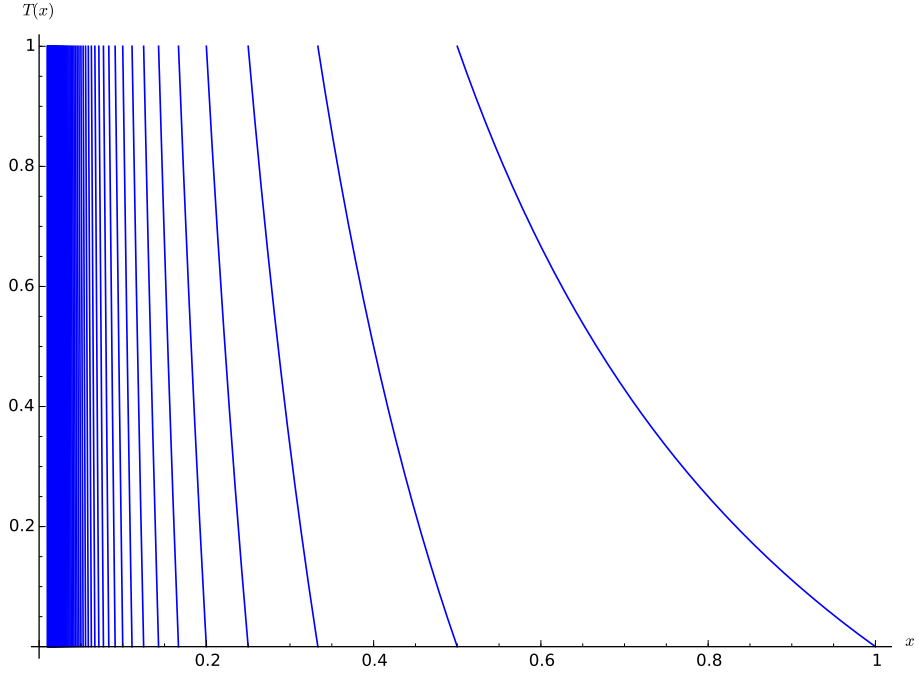
for an *explicit constant* $k \doteq 1.49283\ldots$ given by

$$k = \frac{2}{H}\,, \quad H = \tfrac{1}{\log(4/3)}\left(\tfrac{\pi^2}{6} + 2\sum_j \tfrac{(-1)^j}{2^j j^2} - (\log 2)\tfrac{\log 27}{\log 16}\right)$$

CL dynamical system $(\mathcal{I}, T)$

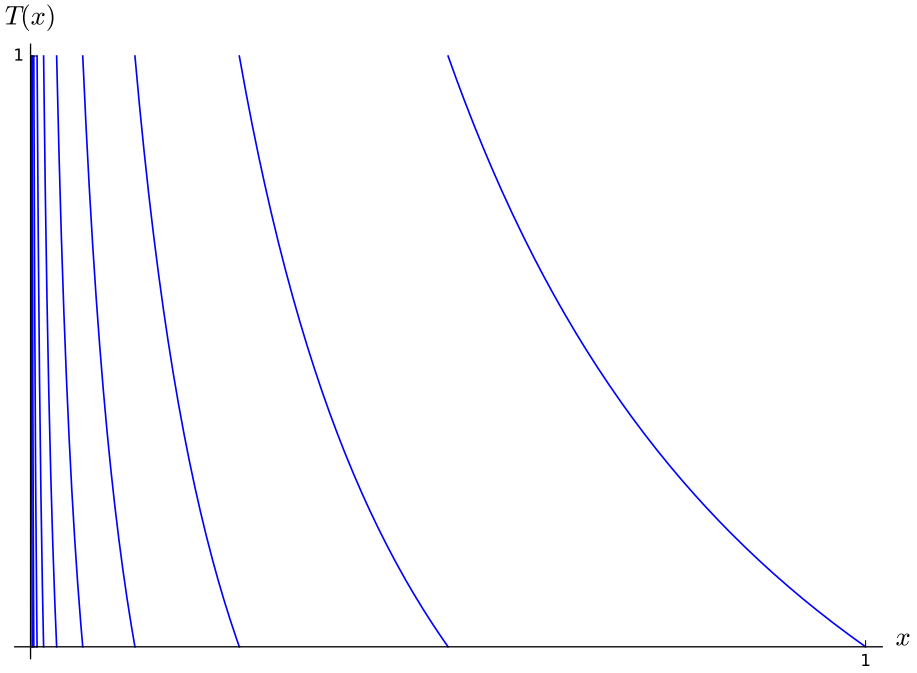


The map for the CL algorithm.



The map for Euclid's algorithm.

The CL dynamical system [Chan05]



The map $T\colon \mathcal{I} \to \mathcal{I}$

Branches

For $x \in \mathcal{I}_a := [2^{-a-1}, 2^{-a}]$

$$x \mapsto T_a(x) := \frac{2^{-a}}{x} - 1\,.$$

where $a(x) := \lfloor \log_2(1/x) \rfloor\,.$

Inverse branches

$$h_a(x) := \frac{2^{-a}}{1+x}\,, \quad \mathcal{H} := \{h_a : a \in \mathbb{N}\}\,,$$

and at depth k

$$\mathcal{H}^k := \{h_{a_1} \circ \cdots \circ h_{a_k} : a_1, \ldots, a_k \in \mathbb{N}\}\,.$$

Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

$$h_m(x) = \frac{1}{m+x}\,,$$

with $\det h_m = -1$.

- For $h = h_{m_1} \circ \ddots \circ h_{m_k}$

$$h(0) = \frac{p}{q} \Rightarrow |h'(0)| = \frac{1}{q^2}\,,$$

p/q reduced.

Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

$$h_m(x) = \frac{1}{m+x}\,,$$

with $\det h_m = -1$.

- For $h = h_{m_1} \circ \ddots \circ h_{m_k}$

$$h(0) = \frac{p}{q} \Rightarrow |h'(0)| = \frac{1}{q^2}\,,$$

p/q reduced.

CL algorithm:

- Homographies

$$h_a(x) = \frac{1}{2^a(1+x)}\,,$$

with $\det h_a = -2^a$.

- For $h = h_{m_1} \circ \ddots \circ h_{m_k}$

$$h(0) = \frac{p}{q} \Rightarrow |h'(0)| \text{ vs. } \frac{1}{q^2}?$$

p/q reduced.

Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

$$h_m(x) = \frac{1}{m+x}\,,$$

with $\det h_m = -1$.

- For $h = h_{m_1} \circ \ddots \circ h_{m_k}$

$$h(0) = \frac{p}{q} \Rightarrow |h'(0)| = \frac{1}{q^2}\,,$$

p/q reduced.

CL algorithm:

- Homographies

$$h_a(x) = \frac{1}{2^a(1+x)}\,,$$

with $\det h_a = -2^a$.

- For $h = h_{m_1} \circ \ddots \circ h_{m_k}$

$$h(0) = \frac{p}{q} \Rightarrow |h'(0)| \text{ vs. } \frac{1}{q^2}?$$

p/q reduced.

Problem: Denominator retrieved is engorged by powers of two.

Recording the dyadic behaviour

Solution: Dyadic numbers $\mathbb{Q}_2$!

$$\text{Dyadic topology} = \text{Divisibility by 2 constraints},$$

using the dyadic norm $|\cdot|_2$.

Recording the dyadic behaviour

Solution: Dyadic numbers $\mathbb{Q}_2$!

$$\text{Dyadic topology} = \text{Divisibility by 2 constraints}\,,$$

using the dyadic norm $|\cdot|_2$.

Introduce dyadic component

- Mixed dynamical system $(x, y) \in \underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$,

Recording the dyadic behaviour

Solution: Dyadic numbers $\mathbb{Q}_2$!

$$\text{Dyadic topology} = \text{Divisibility by 2 constraints}\,,$$

using the dyadic norm $|\cdot|_2$.

Introduce dyadic component

- Mixed dynamical system $(x, y) \in \underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$,

$$\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}\,, \quad \underline{T}(x, y) = (T_a(x), T_a(y))\,,$$

  for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$ and any $y \in \mathbb{Q}_2$.

Recording the dyadic behaviour

Solution: Dyadic numbers $\mathbb{Q}_2$!

$$\text{Dyadic topology} = \text{Divisibility by 2 constraints}\,,$$

using the dyadic norm $|\cdot|_2$.

Introduce dyadic component

- Mixed dynamical system $(x, y) \in \underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$,

$$\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}\,, \quad \underline{T}(x, y) = (T_a(x), T_a(y))\,,$$

  for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$ and any $y \in \mathbb{Q}_2$.
- Evolution led by the real component, which determines a.

Recording the dyadic behaviour

Solution: Dyadic numbers $\mathbb{Q}_2$!

$$\text{Dyadic topology} = \text{Divisibility by 2 constraints}\,,$$

using the dyadic norm $|\cdot|_2$.

Introduce dyadic component

- Mixed dynamical system $(x, y) \in \underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$,

$$\underline{T}\colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}\,, \quad \underline{T}(x, y) = (T_a(x), T_a(y))\,,$$

  for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$ and any $y \in \mathbb{Q}_2$.
- Evolution led by the real component, which determines a.

Dyadics $\mathbb{Q}_2$ have change of variables rule $\Rightarrow$ Transfer Operator $\underline{\mathbf{H}}_s$!

Functional space $\mathcal{F}$ for the extended operator $\underline{\mathbf{H}}_s$

Real component directs the dynamical system:

- *sections* F_y fixing $y \in \mathbb{Q}_2$ asked to be $C^1(\mathcal{I})$.
- the dyadic component follows, demanding only integrability.

Functional space $\mathcal{F}$ for the extended operator $\underline{\mathbf{H}}_s$

Real component directs the dynamical system:

- *sections* F_y fixing $y \in \mathbb{Q}_2$ asked to be $C^1(\mathcal{I})$.
- the dyadic component follows, demanding only integrability.

Ensuing space $\mathcal{F}$ makes $\underline{\mathbf{H}}_s$

- have a dominant eigenvalue and spectral gap
  relying strongly on the real component.

Functional space $\mathcal{F}$ for the extended operator $\underline{\mathbf{H}}_s$

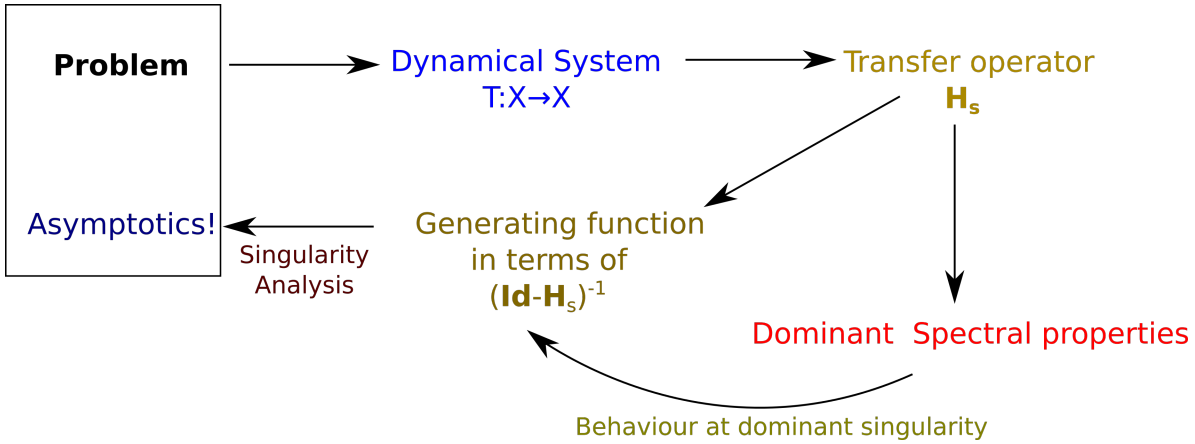
Real component directs the dynamical system:

- *sections* F_y fixing $y \in \mathbb{Q}_2$ asked to be $C^1(\mathcal{I})$.
- the dyadic component follows, demanding only integrability.

Ensuing space $\mathcal{F}$ makes $\underline{\mathbf{H}}_s$

- have a dominant eigenvalue and spectral gap
  relying strongly on the real component.

We can finish the dynamical analysis!



Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Questions:

1. **Comparison to other binary algorithms:** binary GCD, LSB.

Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Questions:

1. **Comparison to other binary algorithms:** binary GCD, LSB.
2. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

$$\lim_{i\to\infty} \tfrac{1}{i} \log_2 \gcd(p_i, q_i) = 1/2\,.$$

Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Questions:

1. **Comparison to other binary algorithms:** binary GCD, LSB.
2. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

$$\lim_{i\to\infty} \tfrac{1}{i} \log_2 \gcd(p_i, q_i) = 1/2\,.$$

   In what sense
   - in expected value for rationals.
   - almost everywhere for real numbers.

Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Questions:

1. **Comparison to other binary algorithms:** binary GCD, LSB.
2. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

$$\lim_{i\to\infty} \tfrac{1}{i} \log_2 \gcd(p_i, q_i) = 1/2\,.$$

In what sense

- in expected value for rationals. Limit exists! value?
- almost everywhere for real numbers.

Conclusion and further questions

- We have studied the average number of shifts and subtractions for the CL algorithm.
- Study makes an interesting use of the **dyadics** in the framework of dynamical analysis.

Questions:

1. **Comparison to other binary algorithms:** binary GCD, LSB.
2. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

$$\lim_{i\to\infty} \tfrac{1}{i} \log_2 \gcd(p_i, q_i) = 1/2\,.$$

In what sense

- in expected value for rationals. Limit exists! value?
- almost everywhere for real numbers. Different problem.

Other research directions and topics

For the first part

- Independence between p_k/q_k and q_{k-1}/q_k.
- Slope subfamilies $\Rightarrow$ work in progress, partial results.
- Multidimensional analogs? Brun?

Other research directions and topics

For the first part

- Independence between p_k/q_k and q_{k-1}/q_k.
- Slope subfamilies $\Rightarrow$ work in progress, partial results.
- Multidimensional analogs? Brun?

For the second part

- More natural $\gcd$ algorithm $(p, q) \mapsto \text{sort}(r, p)$. Competitive?
- Explain

$$\lim_{k\to\infty} \frac{1}{k} \log_2 \gcd(p_k, q_k) = \tfrac{1}{2}\,.$$

Other research directions and topics

For the first part

- Independence between p_k/q_k and q_{k-1}/q_k.
- Slope subfamilies $\Rightarrow$ work in progress, partial results.
- Multidimensional analogs? Brun?

For the second part

- More natural $\gcd$ algorithm $(p, q) \mapsto \text{sort}(r, p)$. Competitive?
- Explain

$$\lim_{k\to\infty} \frac{1}{k} \log_2 \gcd(p_k, q_k) = \tfrac{1}{2}\,.$$

Leftout topics

- Random variable generation

Other research directions and topics

For the first part

- Independence between p_k/q_k and q_{k-1}/q_k.
- Slope subfamilies $\Rightarrow$ work in progress, partial results.
- Multidimensional analogs? Brun?

For the second part

- More natural $\gcd$ algorithm $(p, q) \mapsto \text{sort}(r, p)$. Competitive?
- Explain

$$\lim_{k\to\infty} \frac{1}{k} \log_2 \gcd(p_k, q_k) = \tfrac{1}{2}\,.$$

Leftout topics

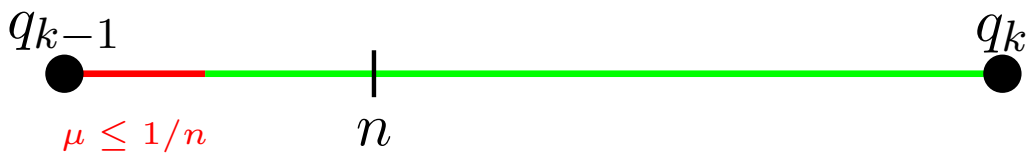
- Random variable generation

Questions?

Conditional expectations

We seek to characterise the $\log n$ behaviour of $S(\alpha, n)$.

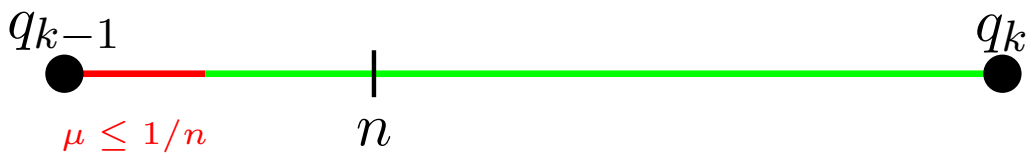
To do this we exclude the cases in which μ is small.



Conditional expectations

We seek to characterise the $\log n$ behaviour of $S(\alpha, n)$.

To do this we exclude the cases in which μ is small.



Theorem

The conditional expectation of S_n with respect to $\mu_n \geq \frac{1}{n}$ satisfies

$$\mathbb{E}\left[S_n \middle| \mu_n \geq \frac{1}{n}\right] = \frac{12}{\pi^2}\log n + O(1)\,.$$

Independence of p_k/q_k and q_{k-1}/q_k

Intuitive [dynamical proof and generalization?]

- Mirror tells us that

$$p_k/q_k = [m_1, \ldots, m_k]\,, \qquad q_{k-1}/q_k = [m_k, m_{k-1}, \ldots, m_1]\,.$$

$\Rightarrow$ Result determined by first digits
and digits have stationary behaviour.

Independence of p_k/q_k and q_{k-1}/q_k

Intuitive [dynamical proof and generalization?]

- Mirror tells us that

$$p_k/q_k = [m_1, \ldots, m_k]\,, \qquad q_{k-1}/q_k = [m_k, m_{k-1}, \ldots, m_1]\,.$$

$\Rightarrow$ Result determined by first digits
and digits have stationary behaviour.

Useful

- Limits in fixed n model are independent from distribution of $\alpha \in [0, 1]$ as long as it has a density w.r.t. Lebesgue.

Independence of p_k/q_k and q_{k-1}/q_k

Intuitive [dynamical proof and generalization?]

- Mirror tells us that

$$p_k/q_k = [m_1, \ldots, m_k]\,, \qquad q_{k-1}/q_k = [m_k, m_{k-1}, \ldots, m_1]\,.$$

$\Rightarrow$ Result determined by first digits
and digits have stationary behaviour.

Useful

- Limits in fixed n model are independent from distribution of $\alpha \in [0,1]$ as long as it has a density w.r.t. Lebesgue.
- Could be used (??) for other expansions like *CL*

$$P_k/Q_k = \langle a_1, \ldots, a_k \rangle\,, \quad 2^{a_k} Q_{k-1}/Q_k = \langle 1, a_k, a_{k-1}, \ldots, a_2 \rangle\,,$$

$\Rightarrow$ $2^{a_k} Q_{k-1}/Q_k$ distributed with Gauss-density on $[1/2, 1]$.

Independence of p_k/q_k and q_{k-1}/q_k

Recall (classical)

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k \Rightarrow p_k = \left((-1)^{k+1} q_{k-1}^{-1}\right) \bmod q_k \,.$$

Independence of p_k/q_k and q_{k-1}/q_k

Recall (classical)

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k \Rightarrow p_k = \left((-1)^{k+1} q_{k-1}^{-1}\right) \bmod q_k \,.$$

$\Rightarrow$ q_{k-1} and p_k are almost modular inverses.

Notice

Fractions have two developments, with different parities

$\Longrightarrow$ Enough to solve the case in which $p_k = q_{k-1}^{-1} (\mathrm{mod}.q_k)$.

Independence of p_k/q_k and q_{k-1}/q_k

Recall (classical)

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k \Rightarrow p_k = \left((-1)^{k+1} q_{k-1}^{-1}\right) \bmod q_k \,.$$

$\Rightarrow$ q_{k-1} and p_k are almost modular inverses.

Notice

Fractions have two developments, with different parities
$\Longrightarrow$ Enough to solve the case in which $p_k = q_{k-1}^{-1} (\mathrm{mod}.q_k)$.

Theorem (see e.g. Shparlinski)

Let $q \in \mathbb{Z}_{>0}$ and let $[a_1, b_1], [a_2, b_2] \subset [0, 1]$, then for any $\epsilon > 0$

$$\frac{1}{\varphi(q)} \sum_{\substack{1 \le a \le q\,, \\ \gcd(a,q)=1}} \mathbf{1}_{\left(\frac{a}{q}, \frac{a^{-1} \bmod q}{q}\right) \in [a_1,b_1] \times [a_2,b_2]}$$

$$= (b_1 - a_1)\,(b_2 - a_2) + O(q^{-1/2+\epsilon})\,.$$

Independence of p_k/q_k and q_{k-1}/q_k

Recall (classical)

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k \Rightarrow p_k = \left((-1)^{k+1} q_{k-1}^{-1}\right) \bmod q_k \,.$$

$\Rightarrow$ q_{k-1} and p_k are almost modular inverses.

Notice

Fractions have two developments, with different parities
$\Longrightarrow$ Enough to solve the case in which $p_k = q_{k-1}^{-1} (\mathrm{mod}.q_k)$.

Theorem (see e.g. Shparlinski)

Let $q \in \mathbb{Z}_{>0}$ and let $[a_1, b_1], [a_2, b_2] \subset [0, 1]$, then for any $\epsilon > 0$

$$\frac{1}{\varphi(q)} \sum_{\substack{1 \le a \le q\,, \\ \gcd(a,q)=1}} \mathbf{1}_{\left(\frac{a}{q}, \frac{a^{-1} \bmod q}{q}\right) \in [a_1,b_1] \times [a_2,b_2]}$$
$$= (b_1 - a_1)\,(b_2 - a_2) + O(q^{-1/2+\epsilon})\,.$$

$\Longrightarrow$ $\frac{a}{q}$ and $\frac{a^{-1} \bmod q}{q}$ behave as if they were independent!

Important subfamilies

- Slope α rational:
  periodic, Christoffel words.
- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

Important subfamilies

- Slope α rational:
  periodic, Christoffel words.
- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

Two elements

- key prefix $(m_1, \ldots, m_k)$ with k such that $q_{k-1}(\alpha) \leq n < q_k(\alpha)$.
- completion $(m_{k+1}, \ldots, m_p)$ of the "period".

Important subfamilies

- Slope α rational:
  periodic, Christoffel words.
- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

Two elements

- key prefix $(m_1, \ldots, m_k)$ with k such that $q_{k-1}(\alpha) \leq n < q_k(\alpha)$.
- completion $(m_{k+1}, \ldots, m_p)$ of the "period".

Generating functions are now Dirichlet series.

$\Rightarrow$ Quasi-inverse $(\mathbf{I} - \mathbf{H}_s)^{-1}$
applied to another one similar to the previous slide.

Important subfamilies

- Slope α rational:
  periodic, Christoffel words.
- Slope α quadratic irrational:
  come up naturally as fixed points of substitution.

Two elements

- key prefix $(m_1, \ldots, m_k)$ with k such that $q_{k-1}(\alpha) \leq n < q_k(\alpha)$.
- completion $(m_{k+1}, \ldots, m_p)$ of the "period".

Generating functions are now Dirichlet series.

$\Rightarrow$ Quasi-inverse $(\mathbf{I} - \mathbf{H}_s)^{-1}$
applied to another one similar to the previous slide.

We expect unified solution with the real case

Slope subfamilies

Models.

- For rational $\alpha = h_{\boldsymbol{m}}(0)$: size$(\alpha) = q$
  here $q = |h'_{\boldsymbol{m}}(0)|^{-1/2}$ is the reduced denominator.
- For quadratic irrational $\alpha = h_{\boldsymbol{m}}(\alpha)$: size$(\alpha) := v(\alpha)^{-1}$
  here $v(\alpha)^{-1} = |h'_{\boldsymbol{m}}(\alpha)|^{-1/2}$ is the analog of q.

Slope subfamilies

Models.

- For rational $\alpha = h_{\boldsymbol{m}}(0)$: size$(\alpha) = q$
  here $q = |h'_{\boldsymbol{m}}(0)|^{-1/2}$ is the reduced denominator.
- For quadratic irrational $\alpha = h_{\boldsymbol{m}}(\alpha)$: size$(\alpha) := v(\alpha)^{-1}$
  here $v(\alpha)^{-1} = |h'_{\boldsymbol{m}}(\alpha)|^{-1/2}$ is the analog of q.

Bound the size by D and pick random α with size$(\alpha) \leq D$.
$\Rightarrow$ study $\mathbb{P}_D(S_n(\alpha) \leq \lambda)$ as $D, n \to \infty$ in some way ?

Slope subfamilies: quadratic irrationals

Write $\alpha = h_{\boldsymbol{w}}(\alpha) = [\boldsymbol{w}, \boldsymbol{w}, \ldots]$ for some $\boldsymbol{w} \in \mathbb{Z}^+_{>0}$ and fix n.

To compute $S(\alpha, n)$ we only require

$$v = (w_1, \ldots, w_k)$$

with $q_{k-1}(\alpha) \leq n < q_k(\alpha)$. Write

$$v = w^\ell v' \,, \qquad \epsilon \neq v' \preceq w \,,$$

the index $\ell = \ell(\alpha, n)$ is known as the **number of turns**.

Slope subfamilies: quadratic irrationals

Write $\alpha = h_{\boldsymbol{w}}(\alpha) = [\boldsymbol{w}, \boldsymbol{w}, \ldots]$ for some $\boldsymbol{w} \in \mathbb{Z}^+_{>0}$ and fix n.

To compute $S(\alpha, n)$ we only require

$$v = (w_1, \ldots, w_k)$$

with $q_{k-1}(\alpha) \leq n < q_k(\alpha)$. Write

$$v = w^\ell v' \,, \qquad \epsilon \neq v' \preceq w \,,$$

the index $\ell = \ell(\alpha, n)$ is known as the **number of turns**.

Number of turns is key

- Case $\ell = 0$ is the simplest, and closely related to the rationals.
- Case $\ell > 0$ is more complicated, seems to simplify as $\ell \to \infty$.

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Adapting our methods to this context is work **in progress**:

- behaviour of continuants Q_k *differs* from rational case.

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Adapting our methods to this context is work **in progress**:

- behaviour of continuants Q_k *differs* from rational case.
- we *conjecture* $-\frac{1}{k}\mathbb{E}[\log_2 |Q_k|_2] \sim 1/2$

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Adapting our methods to this context is work **in progress**:

- behaviour of continuants Q_k *differs* from rational case.
- we *conjecture* $-\frac{1}{k}\mathbb{E}[\log_2 |Q_k|_2] \sim 1/2$

  $\rightarrow$ we have proved the **limit exists**

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Adapting our methods to this context is work **in progress**:

- behaviour of continuants Q_k *differs* from rational case.
- we *conjecture* $-\frac{1}{k}\mathbb{E}[\log_2 |Q_k|_2] \sim 1/2$

  $\rightarrow$ we have proved the **limit exists**

  ... explicit invariant density $\Psi(x, y)$?

Continued Logarithm expansion over the reals: intro

Chan studied from an *Ergodic perspective*

- the averages $(a_1(x) + \ldots + a_M(x))/M$.
- the exponential growth of "natural continuants" $Q_k(x)$.

Results concerning almost every $x \in \mathcal{I}$

$\Longrightarrow$ truncate the expansion $a_1(x), a_2(x), \ldots$ at depth k.

Adapting our methods to this context is work **in progress**:

- behaviour of continuants Q_k *differs* from rational case.
- we *conjecture* $-\frac{1}{k}\mathbb{E}[\log_2 |Q_k|_2] \sim 1/2$

  $\rightarrow$ we have proved the **limit exists**

  ... explicit invariant density $\Psi(x, y)$?

$\rightarrow$ related to growth of $\gcd(p, q)$ in the algorithm!

Mirrors

The conjecure

$$\log_2 \gcd (p_i, q_i) \sim i/2 \,.$$

leads us to mirrors.

Mirrors

The conjecure

$$\log_2 \gcd (p_i, q_i) \sim i/2 \,.$$

leads us to mirrors.

- The successive pairs (p_i, q_i) correspond to convergents

$$\langle a_k, \ldots, a_p \rangle \,, \qquad k = 1, \ldots, p \,.$$

Mirrors

The conjecure

$$\log_2 \gcd (p_i, q_i) \sim i/2 \,.$$

leads us to mirrors.

- The successive pairs (p_i, q_i) correspond to convergents

$$\langle a_k, \ldots, a_p \rangle \,, \qquad k = 1, \ldots, p \,.$$

- Moreover

$$Q(a_k, a_{k+1}, \ldots, a_p) = 2^{a_k} Q(1, a_p, a_{p-1} \ldots, a_{k+1}) \,.$$

$\Rightarrow$ related to convergents of the mirror expansion

Mirrors

The conjecure

$$\log_2 \gcd (p_i, q_i) \sim i/2 \,.$$

leads us to mirrors.

- The successive pairs (p_i, q_i) correspond to convergents

$$\langle a_k, \ldots, a_p \rangle \,, \qquad k = 1, \ldots, p \,.$$

- Moreover

$$Q(a_k, a_{k+1}, \ldots, a_p) = 2^{a_k} Q(1, a_p, a_{p-1} \ldots, a_{k+1}) \,.$$

$\Rightarrow$ related to convergents of the mirror expansion

$$\langle a_p, a_{p-1}, \ldots, a_1 \rangle \,.$$

- Average properties of mirror strongly associated with a "mirrored" transfer operator

$$\underline{\mathbf{H}}_{1,1-w,w,1-w} \,.$$

Binary $\gcd$ algorithms

Other well-known binary algorithms include

- The binary GCD
- The LSB (least significant bits) algorithm
  – Informally "the Tortoise and the Hare".

Binary $\gcd$ algorithms

Other well-known binary algorithms include

- The binary GCD
- The LSB (least significant bits) algorithm
  – Informally "the Tortoise and the Hare".

The dyadics play different roles in the dynamical analysis

- For the binary GCD: dyadics are drawn
  probabilistically and independently.
- For the LSB: dyadics play the main role!

Binary $\gcd$ algorithms

Other well-known binary algorithms include

- The binary GCD
- The LSB (least significant bits) algorithm
  – Informally "the Tortoise and the Hare".

The dyadics play different roles in the dynamical analysis

- For the binary GCD: dyadics are drawn
  probabilistically and independently.
- For the LSB: dyadics play the main role!

Unify the analysis to better understand the role of the dyadics?