Continued Logarithm Algorithm. A probabilistic study

Pablo Rotondo

IRIF, Paris 7 Diderot,

Universidad de la República, Uruguay

GREYC, associate

Work with

Brigitte Vallée and Alfredo Viola

$$\frac{13}{31} = \cfrac{2^{-1}}{1 + \cfrac{2^{-2}}{1 + \cfrac{2^{-1}}{1 + \cfrac{2^{0}}{1 + \cfrac{2^{-1}}{1}}}}}$$

EJCIM, **Nancy**, March, 2018.

Table of Contents

The origins

In Hakmem *Gosper* writes

"*There is a mutation of continued fractions, which I call continued logarithms, which have several advantages over regular continued fractions, especially for computational hardware.*

(...) *The primary advantage is the conveniently small information parcel.*

(...) *the continued logarithm of Avogadro's number begins with its binary order of magnitude, and only then begins the description equivalent to the leading digits – a sort of recursive version of scientific notation.*"

The continued logarithm algorithm computes the *odd* $\gcd$ and

- involves quotients that are powers of 2.
- seems simple and efficient.

The origins

In Hakmem *Gosper* writes

"*There is a mutation of continued fractions, which I call continued logarithms, which have several advantages over regular continued fractions, especially for computational hardware.*

(...) *The primary advantage is the conveniently small information parcel.*

(...) *the continued logarithm of Avogadro's number begins with its binary order of magnitude, and only then begins the description equivalent to the leading digits – a sort of recursive version of scientific notation.*"

The continued logarithm algorithm computes the *odd* $\gcd$ and

- involves quotients that are powers of 2.
- seems simple and efficient.
- let us see an example!

Continued Logarithm Algorithm?

A binary "division":

$$q = \mathbf{2^{\boldsymbol{a}}} p + r \,,$$

Continued Logarithm Algorithm?

A binary "division":

$$q = \mathbf{2^{a}} p + r \,,$$

how to choose $a = a(p, q)$?

Continued Logarithm Algorithm?

A binary "division":

$$q = \mathbf{2^{a}} p + r\,,$$

how to choose $a = a(p, q)$? $\Rightarrow$ pick the max!

$$a(p, q) = \max\{k \geq 0 : 2^k p \leq q\}$$

Continued Logarithm Algorithm?

A binary "division":

$$q = \mathbf{2^{a}} p + r \,,$$

how to choose $a = a(p,q)$? $\Rightarrow$ pick the max!

$$a(p,q) = \max\{k \geq 0 : 2^k p \leq q\}$$

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

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

Continued Logarithm Algorithm?

A binary "division":

$$q = \mathbf{2^a} p + r \,,$$

how to choose $a = a(p,q)$? $\Rightarrow$ pick the max!

$$a(p,q) = \max\{k \geq 0 : 2^k p \leq q\}$$

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

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

Remark.

- We ended up with $(8, 0)$, what is the $\gcd$? $\Rightarrow$ odd $\gcd = 1$.

Worst-case studied by Shallit (2016): consider $(1, 2^n - 1)$.

Response. We have at most $O(\log q)$ steps, like Euclid.

Worst-case studied by Shallit (2016): consider $(1, 2^n - 1)$.

Response. We have at most $O(\log q)$ steps, like Euclid.

No apparent gains in number of steps

Shallit then proposed the average case as an open problem.

We considered his question...

the problem turned out to be interesting.

Worst-case studied by Shallit (2016): consider $(1, 2^n - 1)$.

Response. We have at most $O(\log q)$ steps, like Euclid.

No apparent gains in number of steps

Shallit then proposed the average case as an open problem.

We considered his question...

the problem turned out to be interesting.

We provide an answer to his question,

Worst-case studied by Shallit (2016): consider $(1, 2^n - 1)$.

Response. We have at most $O(\log q)$ steps, like Euclid.
No apparent gains in number of steps

Shallit then proposed the average case as an open problem.
We considered his question...
the problem turned out to be interesting.

We provide an answer to his question,
Average number of steps K and shifts S satisfy

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

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

$$k = \frac{2}{H}\,, \quad H = \tfrac{1}{\log(4/3)} \left(\tfrac{\pi^2}{6} + 2\mathrm{Li}_2(-1/2) - (\log 2) \tfrac{\log 27}{\log 16} \right)$$

Worst-case studied by Shallit (2016): consider $(1, 2^n - 1)$.

Response. We have at most $O(\log q)$ steps, like Euclid.
No apparent gains in number of steps

Shallit then proposed the average case as an open problem.
We considered his question...
the problem turned out to be interesting.

We provide an answer to his question,
Average number of steps K and shifts S satisfy

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

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

$$k = \frac{2}{H}\,, \quad H = \tfrac{1}{\log(4/3)} \left(\tfrac{\pi^2}{6} + 2\mathrm{Li}_2(-1/2) - (\log 2) \tfrac{\log 27}{\log 16} \right)$$

$\Longrightarrow$ proof turns out to be a bit unexpected.

Procedure summarized in

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

where $a = a(p, q) = \max\{k \geq 0 : 2^k p \leq q\}$.

Procedure summarized in

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

where $a = a(p, q) = \max\{k \geq 0 : 2^k p \leq q\}$.

Note.

- The map $p/q \mapsto p'/q'$ can be extended to $\mathcal{I} = (0, 1)$

$$T\colon \mathcal{I} \to \mathcal{I}\,, \qquad T(x) = \frac{2^{-a}}{x} - 1\,,$$

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

- Algorithm gives rise to a continued fraction

$$\frac{p}{q} = \frac{2^{-a}}{1 + \frac{p'}{q'}}\,.$$

Procedure summarized in

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

where $a = a(p, q) = \max\{k \geq 0 : 2^k p \leq q\}$.

Note.

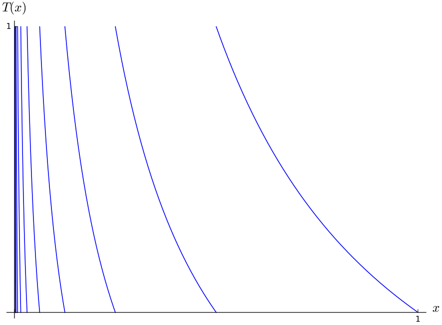
- The map $p/q \mapsto p'/q'$ can be extended to $\mathcal{I} = (0, 1)$

  $$T\colon \mathcal{I} \to \mathcal{I}\,, \qquad T(x) = \frac{2^{-a}}{x} - 1\,,$$

  where $a = \lfloor \log_2(1/x) \rfloor$.
- Algorithm gives rise to a continued fraction

  $$\frac{p}{q} = \frac{2^{-a}}{1 + \frac{p'}{q'}}\,.$$

Dynamical system $(\mathcal{I}, T)$



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

Branches

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

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

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

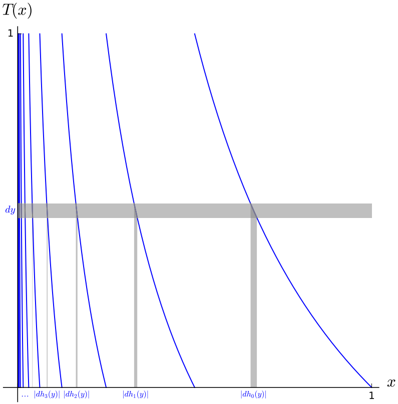
$$\mathcal{H}^k := \{h_{a_1} \circ \cdots \circ h_{a_k} : a_1, \ldots, a_k \in \mathbb{N}\}\,.$$

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 $x \Longrightarrow$ density of $T(x)$?

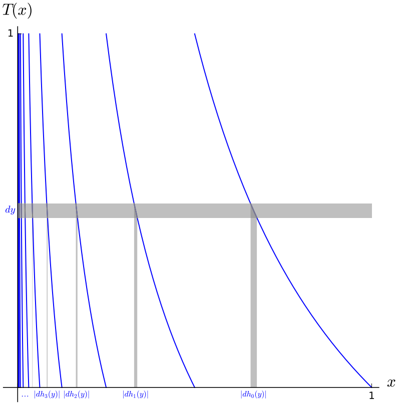


Answer: The density is

$$\mathbf{H}[g](x) = \sum_{h \in \mathcal{H}} \left| h'(x) \right| g\left(h(x)\right)$$
$$= \frac{1}{(1+x)^2} \sum_{a \geq 0} 2^{-a}\, g\left(\frac{2^{-a}}{1+x}\right) .$$

Density transformer

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



Answer: The density is

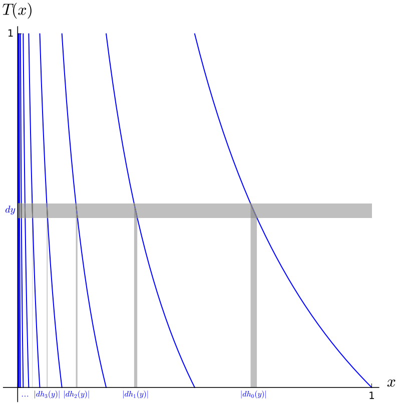
$$\mathbf{H}[g](x) = \sum_{h \in \mathcal{H}} \left| h'(x) \right| \, g\left(h(x)\right)$$
$$= \frac{1}{(1+x)^2} \sum_{a \geq 0} 2^{-a} \, g\left(\frac{2^{-a}}{1+x}\right) .$$

In general $T^k(x)$ has density

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

Density transformer

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



Answer: The density is

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

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

In general $T^k(x)$ has density

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

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

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

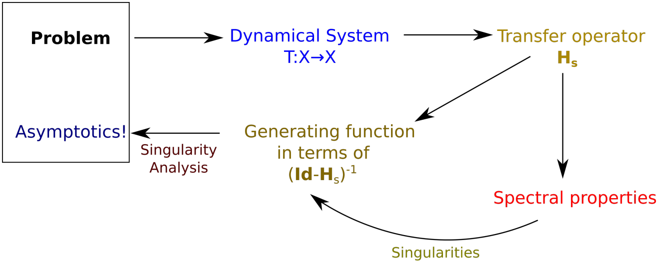
Great!

$\Longrightarrow$ Apply dynamical analysis?

Great!

$\Longrightarrow$ Apply dynamical analysis?

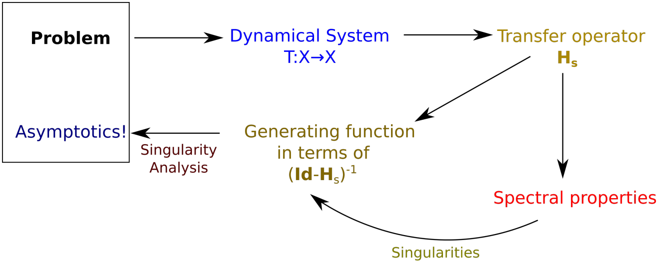
Principles of dynamical analysis:



Great!

$\Longrightarrow$ Apply dynamical analysis?

Principles of dynamical analysis:

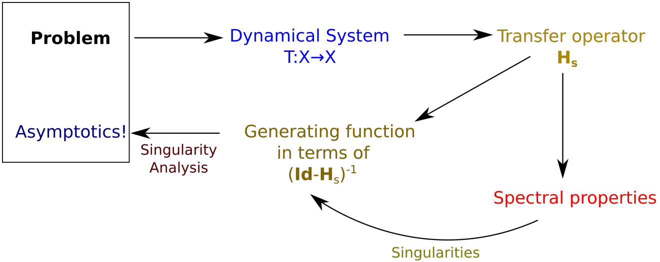


Classical case: $|\det h| = 1 \Longrightarrow |h'(0)| = 1/\text{denominator}^2$.

Great!

$\Longrightarrow$ Apply dynamical analysis?

Principles of dynamical analysis:



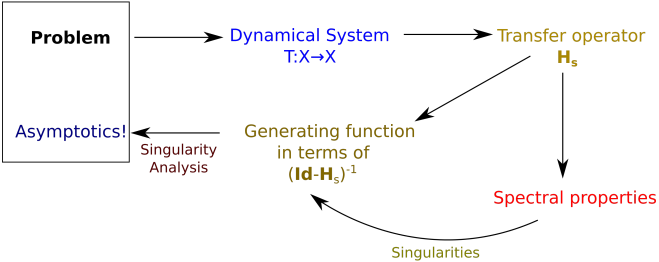
Classical case: $|\det h| = 1 \Longrightarrow |h'(0)| = 1/\text{denominator}^2$.

In our case: Cannot retrieve *reduced* denominator from $|h'(0)|$!

Great!

$\Longrightarrow$ Apply dynamical analysis?

Principles of dynamical analysis:



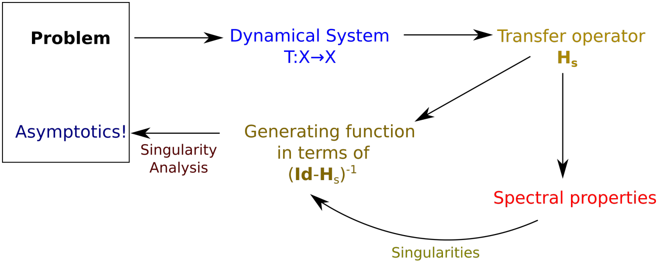
Classical case: $|\det h| = 1 \Longrightarrow |h'(0)| = 1/\text{denominator}^2$.
In our case: Cannot retrieve *reduced* denominator from $|h'(0)|$!

Problem: Denominator retrieved is engorged by powers of two.

Great!

$\Longrightarrow$ Apply dynamical analysis?

Principles of dynamical analysis:



Classical case: $|\det h| = 1 \Longrightarrow |h'(0)| = 1/\text{denominator}^2$.

In our case: Cannot retrieve *reduced* denominator from $|h'(0)|$!

Problem: Denominator retrieved is engorged by powers of two.

$\Longrightarrow$ Need a dyadic component to mark these!

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

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

Dyadic topology $=$ Divisibility by 2 constraints ,

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

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

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

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

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

- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

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

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

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

- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?
- Careful! Add dyadic component y to "real" dynamical system!

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

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

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

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

- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?
- Careful! Add dyadic component y to "real" dynamical system!
- Variations in y add powers of two to Transfer operator

Recording the dyadic behaviour

Dyadic behaviour is related to divisibility

$\Longrightarrow$ ... but we employ analysis!

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

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

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

- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?
- Careful! Add dyadic component y to "real" dynamical system!
- Variations in y add powers of two to Transfer operator
  $\Rightarrow$ yet the real component that "leads".

Idea works!

Average behaviour of the CL algorithm

Input model:

$$\Omega := \{(p,q) : 0 < p < q,\ \gcd(p,q) = 1\}\,, \quad \Omega_N := \Omega \cap [N] \times [N]\,,$$

take uniform probability on Ω_N

Average behaviour of the CL algorithm

Input model:

$$\Omega := \{(p,q) : 0 < p < q,\ \gcd(p,q) = 1\}\,, \quad \Omega_N := \Omega \cap [N] \times [N]\,,$$

take uniform probability on $\Omega_N \Rightarrow$ expected value E_N.

Average behaviour of the CL algorithm

Input model:

$$\Omega := \{(p, q) : 0 < p < q,\ \gcd(p, q) = 1\}\,, \quad \Omega_N := \Omega \cap [N] \times [N]\,,$$

take uniform probability on $\Omega_N \Rightarrow$ expected value E_N.

Result.

The mean value of **steps** $E_N[K]$ and **shifts** $E_N[S]$ performed during the execution of the CL algorithm are $\Theta(\log N)$.

Average behaviour of the CL algorithm

Input model:

$$\Omega := \{(p,q) : 0 < p < q,\ \gcd(p,q) = 1\}, \quad \Omega_N := \Omega \cap [N] \times [N],$$

take uniform probability on $\Omega_N \Rightarrow$ expected value E_N.

Result.

The mean value of **steps** $E_N[K]$ and **shifts** $E_N[S]$ performed during the execution of the CL algorithm are $\Theta(\log N)$.

We have explicit constants

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

here H is known as the entropy of the system,

$$H = \frac{1}{\log(4/3)} \left(\frac{\pi^2}{6} + 2\mathrm{Li}_2\left(-\tfrac{1}{2}\right) - (\log 2)\frac{\log 27}{\log 16} \right),$$

numerically $H \doteq 1.33973\ldots$

The extended dynamical system

⊛ Introduce $\underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$ and $\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}$ as follows

$$\underline{T}(x, y) = \left(T_a(x), T_a(y)\right),$$

for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$. This gives inverse branches

$$\underline{h}_a(x, y) = \left(h_a(x), h_a(y)\right), \qquad (x, y) \in \underline{\mathcal{I}}.$$

The extended dynamical system

⊛ Introduce $\underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$ and $\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}$ as follows

$$\underline{T}(x, y) = (T_a(x), T_a(y)) \,,$$

for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$. This gives inverse branches

$$\underline{h}_a(x, y) = (h_a(x), h_a(y)) \;, \qquad (x, y) \in \underline{\mathcal{I}} \,.$$

Evolution is lead by the real component, which determines a.

The extended dynamical system

⊛ Introduce $\underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$ and $\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}$ as follows

$$\underline{T}(x, y) = (T_a(x), T_a(y)) \,,$$

for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$. This gives inverse branches

$$\underline{h}_a(x, y) = (h_a(x), h_a(y)) \;, \qquad (x, y) \in \underline{\mathcal{I}} \,.$$

Evolution is lead by the real component, which determines a.

⊛ For Transfer operator ⇒ need change of variables formula!

The extended dynamical system

⊛ Introduce $\underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$ and $\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}$ as follows

$$\underline{T}(x, y) = (T_a(x), T_a(y)) \, ,$$

for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$. This gives inverse branches

$$\underline{h}_a(x, y) = (h_a(x), h_a(y)) \ , \qquad (x, y) \in \underline{\mathcal{I}} \, .$$

Evolution is lead by the real component, which determines a.

⊛ For Transfer operator ⇒ need change of variables formula!

Haar (translation invariant) measure ν on $\mathbb{Q}_2$ does satisfy

$$\int_{\mathbb{Q}_2} F(y) d\nu(y) = \int_{\mathbb{Q}_2} F(h(y)) |h'(y)|_2 d\nu(y) \, .$$

The extended dynamical system

⊛ Introduce $\underline{\mathcal{I}} := \mathcal{I} \times \mathbb{Q}_2$ and $\underline{T} \colon \underline{\mathcal{I}} \to \underline{\mathcal{I}}$ as follows

$$\underline{T}(x, y) = (T_a(x), T_a(y)) \,,$$

for $x \in \mathcal{I}_a = [2^{-a-1}, 2^{-a}]$. This gives inverse branches

$$\underline{h}_a(x, y) = (h_a(x), h_a(y)) \,, \qquad (x, y) \in \underline{\mathcal{I}} \,.$$

Evolution is lead by the real component, which determines a.

⊛ For Transfer operator ⇒ need change of variables formula!

Haar (translation invariant) measure ν on $\mathbb{Q}_2$ does satisfy

$$\int_{\mathbb{Q}_2} F(y) d\nu(y) = \int_{\mathbb{Q}_2} F(h(y)) |h'(y)|_2 d\nu(y) \,.$$

$\Longrightarrow$ Consider related measure $\tilde{\nu}$ on $\mathbb{Q}_2$!

⇒ *extended* 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 of

$$y \mapsto \sup_x F_y \,, \qquad \text{and} \qquad y \mapsto \sup_x \partial_x F_y \,.$$

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

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 of

$$y \mapsto \sup_x F_y\,, \qquad \text{and} \qquad y \mapsto \sup_x \partial_x F_y\,.$$

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

- act on $\mathcal{F}$ for $\Re s > 1/2 \Rightarrow$ big enough set of 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 of

$$y \mapsto \sup_x F_y\,, \qquad \text{and} \qquad y \mapsto \sup_x \partial_x F_y\,.$$

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

- act on $\mathcal{F}$ for $\Re s > 1/2 \Rightarrow$ big enough set of s.
- have a dominant eigenvalue and spectral gap

  relying strongly on the real component.

We can finish the dynamical analysis!

Conclusion and further questions

Conclusions:

⊛ We have studied the average number of shifts and substractions for the CL algorithm.

⊛ Study makes an interesting use of the dyadics in the framework of dynamical analysis.

Conclusion and further questions

Conclusions:

⊛ We have studied the average number of shifts and substractions for the CL algorithm.

⊛ Study makes an interesting use of the dyadics in the framework of dynamical analysis.

Questions:

1. **Bit complexity?**

Conclusion and further questions

Conclusions:

⊛ We have studied the average number of shifts and substractions for the CL algorithm.

⊛ Study makes an interesting use of the dyadics in the framework of dynamical analysis.

Questions:

1. **Bit complexity?**
2. **Comparison to other binary algorithms:** binary GCD, LSB.

Conclusion and further questions

Conclusions:

⊛ We have studied the average number of shifts and substractions for the CL algorithm.

⊛ Study makes an interesting use of the dyadics in the framework of dynamical analysis.

Questions:

1. **Bit complexity?**
2. **Comparison to other binary algorithms:** binary GCD, LSB.
3. **Conjecture:** During long developments, $\gcd(p, q)$ is a power of two with exponent $\sim \#steps/2$.

Conclusion and further questions

Conclusions:

⊛ We have studied the average number of shifts and substractions for the CL algorithm.

⊛ Study makes an interesting use of the dyadics in the framework of dynamical analysis.

Questions:

1. **Bit complexity?**
2. **Comparison to other binary algorithms:** binary GCD, LSB.
3. **Conjecture:** During long developments, $\gcd(p, q)$ is a power of two with exponent $\sim \#steps/2$.
4. **Expansion for real numbers:** work in progress!