Continued Logarithm Algorithm: A probabilistic study

Pablo Rotondo

LIGM, Paris-Est Marne-la-Vallée

Work with

Brigitte Vallée and Alfredo Viola

RAIM 2018, November 12, 2018.

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 substractions.
- 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 substractions.
- 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):

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

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

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 $\gcd$? $\Rightarrow$ 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

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

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

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

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

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

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.

Main result [RVV18].

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

More precisely

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

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

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

Consider

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

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.

Main result [RVV18].

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

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

Process depends **only** on p/q rather than (p, q).

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

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

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

- Iteration gives a special continued fraction

$$\frac{p}{q} = \frac{1}{2^a \left(1 + \frac{p'}{q'}\right)}.$$

Process depends **only** on p/q rather than (p, q).

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

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

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

- Iteration gives a special continued fraction

$$\frac{p}{q} = \frac{1}{2^a \left(1 + \frac{p'}{q'}\right)}\,.$$

- For Euclid's algorithm, we get the Gauss map

$$S: \mathcal{I} \to \mathcal{I}\,, \quad S(x) = \frac{1}{x} - m\,,$$

where $m = \lfloor 1/x \rfloor$.

- Iteration gives classical continued fractions

$$\frac{p}{q} = \frac{1}{m + \frac{p'}{q'}}\,.$$

Process depends **only** on p/q rather than (p,q).

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

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

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

- Iteration gives a special continued fraction

$$\frac{p}{q} = \frac{1}{2^a\left(1 + \frac{p'}{q'}\right)}.$$

- For Euclid's algorithm, we get the Gauss map

$$S\colon \mathcal{I} \to \mathcal{I}\,, \quad S(x) = \frac{1}{x} - m\,,$$

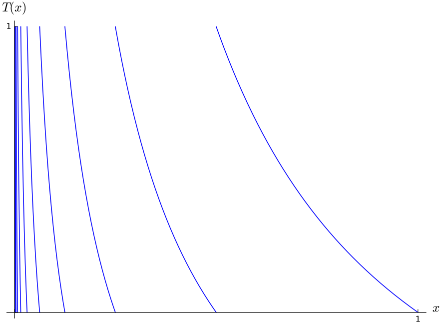
where $m = \lfloor 1/x \rfloor$.

- Iteration gives classical continued fractions

$$\frac{p}{q} = \frac{1}{m + \frac{p'}{q'}}.$$

The continued fraction expansion ends (is finite) when we get 0.

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

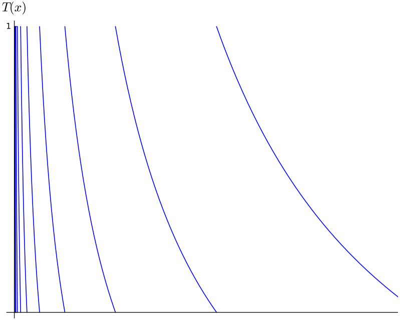
Inverse branches

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

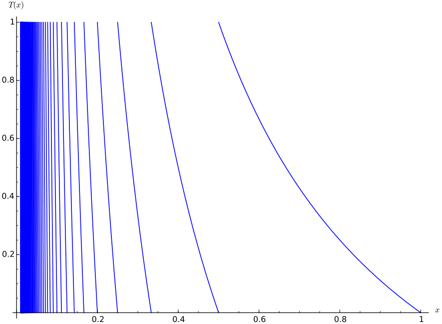
and at depth k

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

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



The map for the CL algorithm



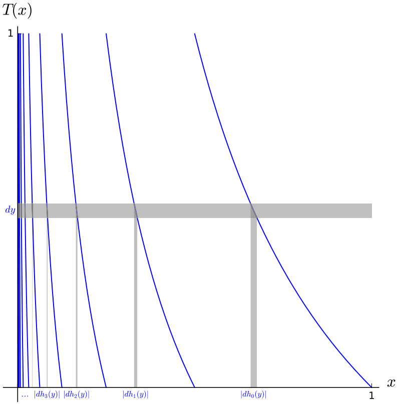
The map for Euclid's algorithm.

Density transformer

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

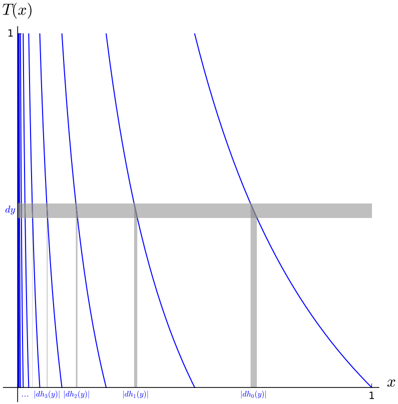
Density transformer

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



Density transformer

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

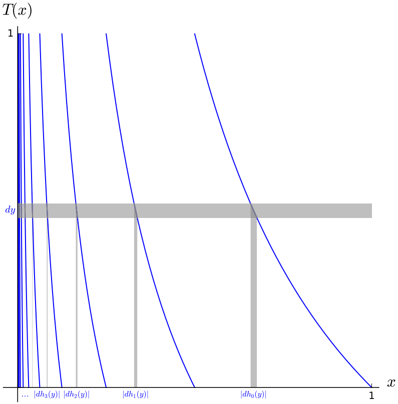


Answer: The density is

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

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

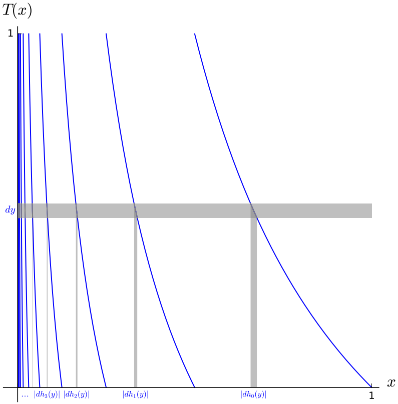
$$\mathbf{H}[g](x) = \sum_{h \in \mathcal{H}} \left|h'(x)\right| g\left(h(x)\right)$$
$$= \frac{1}{(1+x)^2} \sum_{a \geq 0} 2^{-a}\, g\left(\frac{2^{-a}}{1+x}\right).$$

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

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

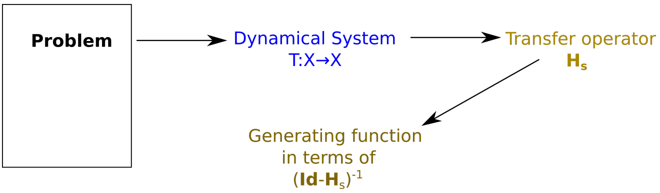
$\implies$ Transfer operator $\mathbf{H}_s$ extends $\mathbf{H}$, introducing a variable s

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

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

Generating functions.

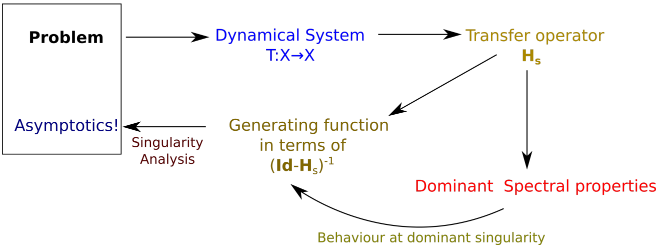
- $\mathbf{H}_s$ describes all executions of depth 1.
- $\mathbf{H}_s^2 = \mathbf{H}_s \circ \mathbf{H}_s$ describes all executions of depth 2.
- $\vdots$
- and $(\mathbf{I} - \mathbf{H}_s)^{-1} = \mathbf{I} + \mathbf{H}_s + \mathbf{H}_s^2 + \ldots$ describes *all* executions.



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.



Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

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

with $\det h_m = -1$.

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

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

p/q reduced.

Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

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

with $\det h_m = -1$.

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

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

p/q reduced.

CL algorithm:

- Homographies

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

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

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

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

p/q reduced.

Reduced denominators and inverse branches

Euclidean algorithm:

- Homographies

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

with $\det h_m = -1$.

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

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

p/q reduced.

CL algorithm:

- Homographies

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

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

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

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

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 $\mathbb{Q}_2$!

Dyadic topology = Divisibility by 2 constraints ,

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

- Introduce dyadic component
  $\Rightarrow$ mixed dynamical system $(x, y) \in \mathcal{I} \times \mathbb{Q}_2$

Recording the dyadic behaviour

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

Dyadic topology $=$ Divisibility by 2 constraints ,

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

- Introduce dyadic component
  $\Rightarrow$ mixed dynamical system $(x, y) \in \mathcal{I} \times \mathbb{Q}_2$
- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?

Recording the dyadic behaviour

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

Dyadic topology = Divisibility by 2 constraints ,

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

- Introduce dyadic component
  $\Rightarrow$ mixed dynamical system $(x, y) \in \mathcal{I} \times \mathbb{Q}_2$
- Incorporate $\mathbb{Q}_2$ into the Transfer Operator?

Idea works!

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

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

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 $\Rightarrow$ 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 $\Rightarrow$ need change of variables formula!

  Haar (translation invariant) measure ν on $\mathbb{Q}_2$ has one!

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

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

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

- 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:

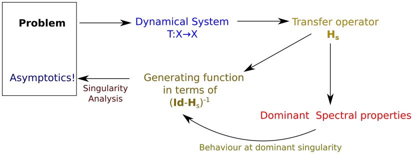
- *sections* F_y fixing $y \in \mathbb{Q}_2$ asked to be $C^1(\mathcal{I})$.
- the dyadic component follows, demanding only integrability of

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

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

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. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

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

Back to $(13, 31)$

i	a_i	p_i	q_i	$\gcd(p_i, q_i)$
0	1	13	31	2^0
1	2	5	26	2^0
2	1	6	20	2^1
3	0	8	12	2^2
4	1	4	8	2^2

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. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

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

Back to $(13, 31)$

i	a_i	p_i	q_i	$\gcd(p_i, q_i)$
0	1	13	31	2^0
1	2	5	26	2^0
2	1	6	20	2^1
3	0	8	12	2^2
4	1	4	8	2^2

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. **Conjecture:** The successive pairs (p_i, q_i) given by the algorithm satisfy

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

   Back to $(13, 31)$

i	a_i	p_i	q_i	$\gcd(p_i, q_i)$
0	1	13	31	2^0
1	2	5	26	2^0
2	1	6	20	2^1
3	0	8	12	2^2
4	1	4	8	2^2

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