Régularité de l’ évolution des continuants à cours de l’ algorithme d’ Euclide.

Applications à l’ analyse du pgcd "diviser pour régner” et du comportement des progressions arithmétiques modulaires.

Brigitte Vallée, Creyg, CRNS et Université de Caen

Loïck Thore, Véronique Maume-Dechaumes, Alién Plagne,

Travail commun avec Eda Cesaratto, Benoit Daireaux,

et du cours de l’ algorithme d’ Euclide.

Applications de l’ évolution des continuants.
The Euclid Algorithm.

On the input \((u, v)\), it computes the \(\gcd\) of \(u\) and \(v\), together with the Continued Fraction Expansion of \(u/v\).

\[
\begin{align*}
v_0 &= v \\
v_1 &= u \\
v_0 &\geq v_1 > 0 \\
\vdots &\quad \vdots &\quad \vdots \quad \vdots \\
v_p - 1 &= m_p v_p - m_{p-1} v_{p-1} + v_p - 1 \\
v_p &= 0
\end{align*}
\]

\(v_p\) is the \(\gcd\) of \(u\) and \(v\), \((m_1, m_2, m_3, \ldots, m_p)\) are the digits. \((v_0, v_1, v_2, \ldots, v_p)\) are the remainders.

The depth of the pair \((u, v)\) is \(d\).

\[
\begin{align*}
0 &= 1 + d_n \\
1 - d_n &> d_n \geq 0 \\
\vdots &\quad \vdots &\quad \vdots \quad \vdots \\
1_n &> \varepsilon_n \geq 0
\end{align*}
\]

The Continued Fraction Expansion of \(u/v\), \((\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_p)\) is the \(\gcd\) of \(u\) and \(v\), together with the \(\gcd\) of \(u\) and \(v\).
Continued Fraction Expansions.

Onestep $v = m \cdot u + r$ transforms $(u, v)$ into $(r, u)$.

With $H = \{h; h: x \mapsto 1 + \frac{1}{m + x}, m \geq 1\}$,

$x = 1 + \frac{1}{m + 1} + \frac{1}{m + 2} + \cdots + \frac{1}{m + p}$

is written as $x = \frac{h_1 \circ h_2 \circ \cdots \circ h_p(0)}{h_p(0)}$ with $h \in H$.

This gives rise to the CFE of $u/v$:

$$\frac{u}{v} = \left( \frac{1}{m} \right) + \cdots + \frac{1}{m + 2} + \frac{1}{m + 1} = \frac{a}{n}$$

It is written as $h(0)$.

With $\frac{n}{\lambda} = h, \frac{a}{n} = x, \{I \geq w, \frac{x + w}{1} \leftrightarrow x : y, \{y\} = H$.

One step $\lambda + n \cdot w = \lambda$.

Continued Fraction Expansions.
The main subject of interest for this talk.

When split at depth \( k \leq p \), the CFE of two rationals, denominators \( q_k \) and \( v_k \) are called the continuants, the \( k \)-th beginning continuant \( q_k \) and the \( k \)-th ending continuant \( v_k \).

\[
\frac{3\alpha}{1+\gamma \omega} = (0)^{d\gamma} \circ \cdots \circ 2^{\gamma \omega} \circ 1^{\gamma \omega} =
\]

\[
\frac{3\beta}{\gamma \delta} = (0)^{\gamma \omega} \circ \cdots \circ 2^{\gamma \omega} \circ 1^{\gamma \omega} =
\]

\[
\frac{\gamma \mu}{\omega I} + \cdots + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I} + \frac{\gamma \mu}{\omega I}
\]

Continuants
With some of its extensions, this is our main tool.

$G_s$ can be viewed as a generating operator for continuants. $G_s$ generates the continuants of depth $k$.

\[
(x) y \circ f_s \left| (x) y \right| \underbrace{\sum_{h \in H} \left| h \right|}_{G_s} = (x) [f] y. \]

The transfer operator $G_s$ acts on $C_1([0,1])$. Its $k$-th iterate satisfies

\[
(x) y \circ f_s \left| (x) y \right| \underbrace{\sum_{h \in H} \left| h \right|}_{G_s} = (x) [f] y. \]

Therefore, for coprime $(n',n)$, if

\[
\left. \frac{z(p + x c)}{y \det} \right|_{y} = (x) y \quad \text{then} \quad \frac{p + x c}{q + x a} = (x) y \leftarrow x : y.
\]

Main fact: If $y$ generates of continuants, via transfer operators
### The transfer operators of use: The family $G$

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition of component operator of variables applied to some function $F$ at points $x$ or $(h, x)$ or $(h, x, y)$ or $(h, x, y, z)$</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$(z^{(h)}(x)y) \cdot s</td>
<td>(x), y</td>
</tr>
<tr>
<td>2</td>
<td>$(h^{(h)}(x)y) \cdot s</td>
<td>(x), y</td>
</tr>
<tr>
<td>3</td>
<td>$((z^{(h)}(x)y) \cdot s</td>
<td>(z), y</td>
</tr>
<tr>
<td>4</td>
<td>$(h^{(h)}(x)y) \cdot s</td>
<td>(h), y</td>
</tr>
<tr>
<td>5</td>
<td>$(x)y \circ F \cdot s</td>
<td>(x), y</td>
</tr>
<tr>
<td>6</td>
<td>$(z^{(h)}(x)y) \cdot s</td>
<td>(x), y</td>
</tr>
</tbody>
</table>

Note: The table above lists the transfer operators with their corresponding definitions and numbers. Each row provides a specific transfer operator along with its application to a function at various points. The operators are categorized by their number, which is indicated in the last column.
The operators of the continued fraction expansion.

For real \( s \), \( G \) possesses a unique dominant eigenvalue \( \lambda(s) \).

The operators of \( G \) act on the convenient spaces \( C \).

For \( s = 1 \), \( \lambda(s) = 1 \).

\[
\Lambda(s) := \log \lambda(s)
\]

is called the pressure, and \( -\Lambda'(1) \) is the entropy of the dynamical system underlying the continued fraction expansion.
Study of continuants crucial for real related to the (best) approximations of \( x \) by rationals.

A well-known "continuous" result:

\[
\log q_k \text{ is } \sim \frac{1}{2} \Lambda'(1) \cdot k,
\]

Result I. Philipp, "The logarithm of the \( k \)-th continuant \( q_k(x) \) of a real \( x \in \mathbb{R} \):"

The continuant \( q_k \):

A well-known "continuous" result: Related to the (best) approximations of \( x \) by rationals.
Does there exist a "discrete version" of this result (for $x$ rational)?
For studying a parameter \( C(n) \) on each \( \mathcal{U} \), one introduces the

Dynamical analýsis method.

1. Transfer these informations on the asymptotic behaviour of \([C]^{u} \mathcal{E}\).
2. Study singularities of \( \mathcal{S}_{C} \).
3. Look for alternative form for \( \mathcal{S}_{C} \) with the various transfer operator.

Three main steps:

\[
\sum_{(u,v) \in \mathcal{V}} C(u,v) = \sum_{k} c_{k} k^{2} s^{C(u,v)} = \sum_{k} a_{k} k^{2} s^{C(u,v)}
\]

where \( a_{k} \) is the coefficient of the series \( \mathcal{S}_{C} \) for \( C = 1 \).

Then,

\[
\mathcal{S}_{C} \xrightarrow[s^{C} \mathcal{E}_{C}^{-1} \mathcal{C}]{} [C]^{u} \mathcal{E}_{C}^{-1} \mathcal{C}
\]

\[
\mathcal{D}(n)_{C} \xrightarrow[s^{C} \mathcal{E}_{C}^{-1} \mathcal{C}]{} (a \cdot n)_{C} \xrightarrow[s^{C} \mathcal{E}_{C}^{-1} \mathcal{C}]{} (a \cdot n)
\]
An exact generalization of Result I.

\[ u \cdot \frac{|(1)_{\omega V}|}{|\omega V|} (\theta - 1) \theta \sim [\omega \theta]^{u} \Lambda \sim [\omega \Lambda]^{u} \]

\[ u \cdot \theta \sim [\omega \theta]^{u} \quad ; \quad u \cdot (\theta - 1) \sim [\omega \Lambda]^{u} \]

Asymptotic expansions hold for the mean value and the variance

\[ \frac{(u^n)^{1/1}}{n} \]

speed of convergence of order \( n^{-1} \).

Asymptotic expansions hold for the mean value and the variance

\[ (u/n) = (\theta - 1) \theta \sim [\omega \theta]^{u} \Lambda \sim [\omega \Lambda]^{u} \]

\[ \log n = [\omega \theta] \quad ; \quad \log \lambda = [\omega \Lambda] \]

For any rational \( \theta \) of \( [0,1] \).

Result II. Cesariatto-Lhote-Lhote-\( \Lambda \).

For any rational \( \theta \) of \( [0,1] \).

Asymptotic normal-log-normal laws at a rational fraction of the depth.

\[ \theta \]

\[ \Lambda \theta \]

Evolution of the continuants.
Parameters for Result II.

Using Quasi-Power Theorem for moment generating functions

\[
\mathcal{E} \circ \mathcal{C} \in \mathcal{E}^{\mathcal{E}} \quad \text{and} \quad \mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}}
\]

and

\[
\mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}} \quad \text{and} \quad \mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}}
\]

\[
\cdot(0,0)[\mathcal{I}]^{(m-s)}_{[d\mathcal{E}] \circ [d\mathcal{C}]} \mathcal{E} \circ \mathcal{C} \in \mathcal{E}^{\mathcal{E}} \quad \text{and} \quad \mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}}
\]

\[
\cdot(0)[\mathcal{I}]^{[d\mathcal{E}] \circ [d\mathcal{C}]} \in \mathcal{E}^{\mathcal{E}} \quad \text{and} \quad \mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}}
\]

\[
\cdot(0)[\mathcal{I}]^{[d\mathcal{E}] \circ [d\mathcal{C}]} \in \mathcal{E}^{\mathcal{E}} \quad \text{and} \quad \mathcal{E} \circ \mathcal{C} \in \mathcal{C}^{\mathcal{E}}
\]

For \((u,v) \in \Omega_{st} \quad \mathcal{H} \in \mathcal{E} \quad \text{decompose} \quad \mathcal{H} \in \mathcal{E}
\]

and the parameters of interest are

\[
[(\mathcal{O} \circ m \circ \mathcal{E}) \exp u]^{\mathcal{E}} \quad \text{and} \quad [(\mathcal{O} \circ m \circ \mathcal{E}) \exp u]^{\mathcal{E}}
\]

Using Quasi-Power Theorem for moment generating functions

Parameters for Result II.
The transfer operator for Result II.

These are "pseudo-quasi-inverses" $Q_{s,w} := \sum_{p \geq 0} G^p - \lfloor \delta^p \rceil s - w \circ G_{\lfloor \delta^p \rceil} s$.

But, for $w$ near 0, we can hope to have the same properties as the "true" quasi-inverse $(I - G^s)^{-1}$.

Not "true" quasi-inverses, as $(I - G^s)^{-1}$.

These are "pseudo-quasi-inverses"
Problem III-Interrupted Algorithms.

Consider the following "slices" of the Euclid Algorithm where parameters $\gamma, \delta$ may depend on binary length $n$.

1. $\gamma, \delta > 3$

- $[u (u) \gamma]$ and stops when $u$ has lost $[D (u) \gamma]$ iterations at the $k$-th iteration.

- $[D \cdot ((u) \gamma + (u) \gamma)]$ and stops at the $D$-th iteration.

- $[D (u) \gamma]$ and stops at the $D$-th iteration.

2. $\gamma, \delta < 3$

- $\gamma$ may depend on binary length $n$.

- $[u (u) \gamma]$ as soon as $u$ has lost $[u (u) \gamma]$ bits (with $\gamma \geq 0$).

- $\gamma, \delta > 3$

- $\geq 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$

- $\gamma, \delta > 3$

- $\gamma, \delta < 3$
It is close to the number of bits that are lost during the slice.

\[(u)q \cdot \frac{1}{2} \begin{pmatrix} u \cdot (u)q < \left| g(u) - \langle \phi,\langle u \rangle \rangle \right| \end{pmatrix} u \]  

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

Moreover, the binary size \( \langle g,\langle u \rangle \rangle \) of the matrix \( M \) produced by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm provided that

\[\langle \phi,\langle u \rangle \rangle \]

Furthermore, the binary size \( \langle \phi,\langle u \rangle \rangle \) of the matrix \( M \) produced by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm produced \( \langle g,\langle u \rangle \rangle \) \( M \).

... by the algorithm satisfies, for any \(1 < \phi < \langle g,\langle u \rangle \rangle \) the Euclid algorithm provided that
Parameters for Result III.

We have let \( \rho = \epsilon + \epsilon \). Then, \( \frac{\rho \cdot [d \cup \alpha]}{[d \cap \alpha] + [d \cup \alpha]} = (\alpha, n) \in \mathbb{W} \)

We then study the cost with \( m \in \mathbb{W} \). We have

\[
0 > m_A \cdot \left[ \left( \frac{\rho \cdot [d \cup \alpha]}{[d \cap \alpha] + [d \cup \alpha]} \right) \right] u_{\mathbb{W}} = [\exists [\rho \cup d] u_{\mathbb{D}}]
\]

\[
0 < m_A \cdot \left[ \left( \frac{\rho \cdot [d \cup \alpha]}{[d \cap \alpha] + [d \cup \alpha]} \right) \right] u_{\mathbb{W}} = [\forall [\rho \cup d] u_{\mathbb{D}}]
\]

and Markov's inequality entails

\[
\left[ I > \frac{\rho \cdot [d \cup \alpha]}{[d \cap \alpha] + [d \cup \alpha]} \right] \supset [\exists [\rho \cup d] u_{\mathbb{D}}] \quad \text{and} \quad \left[ I < \frac{\rho \cdot [d \cup \alpha]}{[d \cap \alpha] + [d \cup \alpha]} \right] \supset [\forall [\rho \cup d] u_{\mathbb{D}}]
\]

Then, \( u_{\mathbb{W}} - \left( [d \cup \alpha] \right) \gamma \supset (\exists [d \cup \alpha] \gamma) \) stops when \( [\rho \cup d] > 3 \).

Number of iterations: \( N \)
Parameters for Result III.

\begin{align*}
&\text{Size of the matrices produced by the algorithm.} \\
&\text{Study of the events } \ell < \gamma, \delta > \geq (\delta + \epsilon) n, \\
&\text{and } \ell < \gamma, \delta > \leq (\delta - \epsilon) n.
\end{align*}

Coefficient of the matrix produced by the algorithm \( E < \gamma, \delta > \) satisfy
\[
|\langle [d \gamma] n j + ( [d \delta] + [d \gamma] n j - < \gamma, \delta > j \rangle |
\]

Then the probability of the events
\[
\begin{align*}
[u(\epsilon - \varphi) \geq < \varphi, \lambda >] &\quad [u(\epsilon + \varphi) \leq < \varphi, \lambda >]
\end{align*}
\]

\text{can be estimated also with the cost } M \tilde{\mathcal{W}}.

Study of the events of size of the matrices produced by the algorithm.

Parameters for Result III.
\[ m(\epsilon + \varrho - I) + s = +s \quad 'm(\epsilon - \varrho) - s =: _s \]

\[ \begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\text{With the cost}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array}
\end{array} \]

is expressed as \((0)[I]^{m,s} = (m,s)^{\mathcal{W}}_H\) as the Dirichlet series relative to cost \((m,s)^{\mathcal{W}}_H\) with the cost \(m\mathcal{W}\) in the series.

\[ \text{With the cost } \text{Transfer operator for Result III} \]
Consider a multiset \( X \) formed with elements of the circle \( \mathbb{Z}/n\mathbb{Z} \) and consider the \( \delta \)'s distances between two consecutive points.

Order them.

Arnold introduces the normalized mean-value of the \( \delta \)'s,

\[
\left( \sum_{i=1}^{T} \frac{\delta_i}{\mathcal{L}} \right)^2 = (\mathcal{L},X,u)_{s}
\]

which provides a measure of the randomness of \( X \).

The minimum of \( s \) is \( s = 1 \) (for all \( \delta \) equal). Maximum of \( s \) is \( s = T \), when the \( \delta \)'s are nearly equal.

Minimum of \( s \) is \( s \sim 1 \) (for all \( \delta \) equal).

Problem IV—Randomness for modular sequences.

\( \mathcal{L} \sim s \)

When all the \( \delta \)'s are small except one, close to \( n \).

For all \( \delta \) equal, \( \mathcal{L} = s \), except one.

Order them, then:

Minimum of \( s \) is \( s = 1 \) (and one).
When $n$ becomes large, a random choice of independent uniformly distributed points on the circle of length $I$ leads to

\[
\begin{align*}
\infty &\leftarrow L \\
\forall &\leftarrow (L)^*s \\
\frac{1 + \frac{L}{L^*}}{L^*} & = (L)^*s
\end{align*}
\]

the "freedom-like" value

When $n$ becomes large, a random choice of independent uniformly distributed points on the circle of length $I$ leads to
Randomness for modular arithmetic progressions.

For a pair \((u,v)\) ∈ \(\Omega\), and a random \(T < v\), consider the set \(X_u\) defined by the first \(T\) terms of the sequence \(x_i \equiv iu (\text{mod } v)\).

Arnold proposes choosing \(T\) as a (beginning) continuant of \(u/v\), but he does not make precise the choice of the index \(k\).

We make precise the behaviour of the Arnold sum...

...when \(k\) is an admissible function of depth \(P\).

Arnold proposes choosing as a (beginning) continuant of \(u/v\), \(L\) defined by the first terms of the sequence \(x_i \equiv i (\text{mod } n)\).

For a pair \((n, a)\) ∈ \(\Omega\), consider the set \(X = X_a > L\) and a random arithmetic progressions.
Non-randomness of modular arithmetic progressions.

Study of

\[ (\frac{u}{1})O + V = [<d>S]^u \]

then \( \exists \epsilon \neq 0, \epsilon \exists \) with \( \epsilon \in \mathbb{R} \) where function \( \mathcal{F} \) is of the form \( \mathcal{F} \) is \( \epsilon \) \( \mathcal{F} \) \( \mathcal{F} \) satisfies

\[ \forall \mathcal{F} = [<d>S]^u \]

\[ \lim_{n \to \infty} \mathcal{F} \]

1. Cesàro, Plagne, V.

(i) Let \( \mathcal{F} \rightarrow <d>S \) be the Arnold random variable relative to an admissible function \( \mathcal{F} \). The mean value of \( \mathcal{F} \) on the set \( <d>S \) satisfies \( \mathcal{F} \) of the form

\[ \lim_{n \to \infty} \mathcal{F} = A \]

where \( A \) is a constant independent of function \( \mathcal{F} \).

(ii) If \( \mathcal{F} \) is of the form \( \mathcal{F} = \lfloor \gamma p \rfloor \) with \( \gamma \in [0, 1] \), then

\[ \mathcal{F} \rightarrow <d>S = A + O(1/n) \]

Result IV.

22
\[
\left[ \frac{\varepsilon(x + I)}{z} + \frac{\varepsilon(x + I)}{I} \right] \frac{9}{h} + \left[ \frac{\varepsilon(x + I)}{I} + \frac{\varepsilon(x + I)}{I} + \frac{x + I}{I} \right] \frac{3}{I} =: (\tilde{h}, x) \tilde{\varphi}
\]

With

\[
\exp\left(\frac{w}{I}, \frac{x + u}{I}\right) \tilde{\varphi} \varepsilon(x + u) \int_{\mathbb{Z}}^{\mathbb{Z}} (z, x + xz) \int_{1}^{\mathbb{Z}} \frac{\vartheta \varepsilon \log I}{I} + [\varepsilon \vartheta \varepsilon \log I ] + I \frac{3}{I} = A
\]

Our constant is "explicit"
Parameters for Result IV.

Let \((u,v)\) be an element of \(\Omega\), and consider the first \(T\) elements of the sequence \(x_i = \frac{i u}{v} \mod v\) for \(T = qk\).

Then, the two-distance theorem proves that the sequence \(\delta_i\) takes only two values: it equals either \(\frac{v k}{2}\) or \(\frac{v k}{2} + 1\). There are exactly \(qk - qk - 1\) distances \(\delta_i\) equal to \(\frac{v k}{2}\) and \(qk - qk - 1\) distances \(\delta_i\) equal to \(\frac{v k}{2} + 1\).

Then, the three parameters to study ... three Dirichlet series \(S_i(s)\).

\[
(1 + \frac{\alpha}{c} \frac{\beta}{c} \frac{1}{1 - \gamma}) + (1 + \frac{\alpha}{c} \frac{\beta}{c} \frac{1}{1 - \gamma}) + \frac{\alpha}{c} \frac{\beta}{c} \frac{0}{1} = (\alpha, \gamma) \leq \gamma > S
\]

Three parameters to study ... three Dirichlet series \(S_i(s)\).

\[
\cdot \left(1 + \frac{\alpha}{c} \frac{\beta}{c} \frac{1}{1 - \gamma} + \frac{\alpha}{c} \frac{\beta}{c} \frac{1}{1 - \gamma} + \frac{\alpha}{c} \frac{\beta}{c} \right) \frac{0}{1} = (\alpha, \gamma)
\]

Let \(L\) be an element of \(\mathbb{Z}\), and consider the first elements of \(L\).
Transfer operators for Result IV.

For series $S_i(s)$ ($i = 2, 3$):

For series $S_1(s)$:

Again, pseudo-quasi-inverses...
Result III. Two parameters $s$ and $\omega$ (with $\omega$ near $0$), $m$ may vary.

\[ \sum_p G_p - \lfloor \delta_p \rfloor \cdot (s, \cdot) \circ G \lfloor \delta_p \rfloor \cdot (s+1, -1) \]

Result II.

\[ \sum_p \left( G_p - \lfloor \delta_p \rfloor \cdot s - w \circ G \lfloor \delta_p \rfloor \cdot s \right) \geq 0 \]

\[ G_p - \lfloor \delta_p \rfloor \cdot (s, \cdot, \cdot) \circ A^i s \circ G \lfloor \delta_p \rfloor - 1 \cdot (s+1, -1/2, -1/2) \]

Result I. Only one parameter $s$ is fixed.

\[ \sum_p \left( (m-s) \circ_{[d\varphi]} (s-s) \circ_{[d\varphi]} 0 < d \right) \]

\[ \sum_p \left( (m-s) \circ_{[d\varphi]} (s-s) \circ_{[d\varphi]} d \right) \]

\[ \sum_p \left( (m-s) \circ_{[d\varphi]} (s-s) \circ_{[d\varphi]} d \right) \]

Summary of all the pseudo-quasi-inverses. $m$.
\[ \mathscr{O} \subseteq \mathcal{G} \]

The operators act on the convenient space \( \mathcal{C}_1 \).

Similar properties hold for any \( \mathcal{G}^s \in \mathcal{G} \).

For real \( s \), \( \mathcal{G}^s \) possesses a dominant spectral value \( \lambda(s) \) separated from the remainder of the spectrum by a spectral gap.

The operators of \( \mathcal{G}^s \) act on the convenient space \( \mathcal{C}_1 \):
On the left line $\Re s = 1 - \alpha$.

Uniform estimates

Expansion

There exists an only pole

$\alpha > |\Re s - 1|$ in the strip.

For (uniformly) extracting coefficients in Dirichlet series...

Conditions on $Q$ needed for dealing with Perron’s formula.
Two parts in the strip $s$: far from the real axis or near the real axis. Far from the real axis: the true quasi-inverse, due to the form of $Q_{s,w}$.

Closer to the real axis: more difficult than the quasi-inverse, due to the poles that are closer to $\rho_s = 1$ are brought by the dominant term and several remainder terms.

The spectral decomposition for $G_{s,w}$ provides a dominant term $\Delta_{s}^{\pm}$ or $\Delta_{s,w}^{\pm}$ which mainly involves the dominant eigenvalue $\lambda_{s,w}$ of $G_{s,w}$.

Using Dolgopyat's results of Cesaratto, Prove that these bounds also hold for all our operators of interest, and then for $Q_{s,w}$.

$\forall s \in \mathbb{C}$
\[ \Delta_s = A(s) \sum \lambda_p - \lfloor \delta_p \rfloor (s) \lambda_{\lfloor \delta_p \rfloor} \]

The constant \( A \) is just the value \( A(1) \); it involves the various dominant projectors at \( s = 1 \), which are all explicit.

\[ \frac{(s)^{\gamma - 1}}{(s)^{\mathcal{V}}} = (s)^{[d \delta]} \gamma \cdot (s)^{[d \delta]} - d \gamma \sum_{\delta = 1}^{d} (s)^{\mathcal{V}} = s^{\nabla} \]

Study easier for Result IV.
More involved for Results II and III: two distinct values $s^+$ and $s^-$ which depend on $s$, $\vartheta$, $w$.

\[ \Delta_{s,w} = \sum_{p} \lambda_p - \lfloor \delta_p \rfloor (s - \lambda_p \lfloor \delta_p \rfloor (s + 1)). \]

For a rational $\vartheta$ with denominator $D$ large, the nearest pole satisfies $\exp(D/\vartheta) \equiv (m,s) \varphi$, poles occur when

\[ \psi(s,w) = \lambda_1 - \delta(s - \lambda \delta(s + 1)). \]

Poles occur when $\psi(s,w) = \exp(2\pi i L/D)$, located at

\[ s = \sigma L(w). \]

For $D$ large, the nearest $\hat{p}$ satisfies

\[ \Re \sigma_{\hat{p}} = \Theta(1/D^2). \]

Then, the strip $S$ has a width $\Theta(1/D)$ and we need:

\[ \infty \leftarrow \varphi(a_{\vartheta}/n) \Theta. \]

with

\[ (\varphi(a_{\vartheta}/n) \Theta = (m)^0 - (m)^1 \Theta. \]

For $\vartheta$ large, the nearest pole satisfies $\exp(D/\vartheta) \equiv (m,s) \varphi$.

Let $\vartheta = \Theta(D) / T$, $T \exp = (m,s) \varphi$ with

\[ (s)^{\varphi}_{\vartheta} \chi(\vartheta)^{-\vartheta}_{\vartheta} = (m,s) \varphi \]

with

\[ \left( (s^{\vartheta})_{\vartheta} \chi(\vartheta)_{\vartheta}^{\vartheta} \right) \sum_{I = 1}^{I = d} (m,s) \varphi - \frac{I}{1} = m,s \nabla \]

\[ \vartheta \] with denominator $D$.

\[ \left( (d^s)^{\vartheta}_{\vartheta} \chi(\vartheta)^{-d}_{\vartheta} \right) \sum_{d = 1}^{d = D} = m,s \nabla \]

two distinct values $s^+$ and $s^-$ which depend on $s$, $\vartheta$, $w$, and $D$, $T$. More involved for Results II and III.