Markov numbers, Christoffel words, and the uniqueness conjecture

Aldo de Luca   Alessandro De Luca

Università di Napoli Federico II

Giornate di informatica teorica in memoria di Aldo de Luca

Roma, 12 luglio 2019

Outline

1. Characteristic matrices
   - Basics
   - General properties of $\mu(w)$
2. Frobenius' uniqueness conjecture
   - The map $S : w \mapsto \mu(w)_{1,2}$
   - Tight bounds and uniqueness
   - The Fibonacci and Pell cases

Trace Equals 3 Times Upper Right

Definition

A matrix $M \in SL_2(\mathbb{Z})$ is characteristic if

$$\operatorname{tr} M = 3M_{1,2}.$$

Example

$M = \begin{pmatrix} 17 & 10 \\ 22 & 13 \end{pmatrix}$ is characteristic, as

- $\det M = 17 \cdot 13 - 22 \cdot 10 = 1$ and
- $17 + 13 = 3 \cdot 10.$

Simple Constraints

Proposition

Let

$$M = \begin{pmatrix} \alpha & m \\ \beta & \gamma \end{pmatrix}$$

be characteristic. Elements on the same row or column are coprime, and

$$\alpha^2 \equiv \gamma^2 \equiv -1 \pmod{m}.$$

Also, up to switching α and γ, M is determined by any two elements.

Markov Triples = Characteristic Products

Products of char. matrices need not be characteristic, but:

Theorem

Let M', M'' be characteristic and $M = M'M''$. Then M is characteristic $\iff$ the upper right elements m', m'', m (of M', M'', M respectively) verify the Markov equation, i.e.,

$$(m')^2 + (m'')^2 + m^2 = 3m'm''m.$$

The Morphism $\mu : \{a, b\}^* \longrightarrow SL_2(\mathbb{Z})$

Setting

$$\mu(a) = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \mu(b) = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$$

defines an injective morphism $\mu : \{a, b\}^* \longrightarrow SL_2(\mathbb{Z})$.

Note that $\mu(a)$ and $\mu(b)$ are characteristic...

Reversal and μ

Let $\widetilde{w}$ denote the reversal of w.

For instance, if $w = aabab$, then $\widetilde{w} = babaa$.

Lemma

For all $w \in \{a, b\}^*$, $\mu(\widetilde{w}) = \mu(w)^T$.

So, w is a palindrome $\iff$ $\mu(w)$ is symmetric.

Let PAL denote the set of palindromes over $\{a, b\}$.

More Relations on elements

Proposition

Let $w \in \{a,b\}^+$, *and let* $\mu(w) = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. *Then* $p > q, r \geq s$.

Moreover, $q < r \iff w = \widetilde{u} a v b u$ *for suitable* $u, v \in \{a,b\}^*$.

Proposition

Let $u \in \mathrm{PAL}$ *and* $\mu(u) = \begin{pmatrix} p & q \\ q & s \end{pmatrix}$. *Then*

$$q + s \leq p \leq 2q + s$$

with $p = q + s \Leftrightarrow u \in a^*$ *and* $p = 2q + s \Leftrightarrow u \in b^*$.

Characterizing Characteristic $\mu(w)$

Matrices $\mu(w)$ need not be characteristic; for instance,
$\mu(aa) = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ is not.

Theorem

Let $w \in \{a, b\}^*$. Then

$$\mu(w) \textit{ is characteristic} \iff w \in \{a, b\} \cup a\mathrm{PAL}b.$$

A Meaningful Decomposition

Let $\nu : \{a, b\}^* \longrightarrow SL_2(\mathbb{Z})$ be defined by

$$\nu(a) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \nu(b) = \nu(a)^T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is injective and a well-known tool in the study of Christoffel pairs.

It is easy to see that

$$\mu = \nu \circ \zeta$$

where ζ is the injective endomorphism defined by

$$\zeta(a) = ba, \quad \zeta(b) = bbaa.$$

A Consequence

Recall the palindromization map ψ defined by $\psi(\varepsilon) = \varepsilon$ and

$$\psi(vx) = (\psi(v)x)^{(+)} \text{ for } v \in \{a,b\}^*, x \in \{a,b\}$$

where $w^{(+)}$ is the right palindromic closure of w.

Proposition

Let $w = aub$ *with* $u \in$ PAL. *Then*

$$\mu(w)_{1,2} = |a\psi(a\zeta(u)b)b|$$

i.e., it is the length of a Christoffel word whose directive word $a\zeta(u)b$ *has an antipalindromic middle* $\zeta(u)$*.*

A Similar, Nicer Point of View

The following independent result uses almost the same decomposition:

Theorem (Reutenauer & Vuillon 2017)

For all $v \in \{a, b\}^*$,

$$\mu(a\psi(v)b)_{1,2} = |a\psi(\psi_E(av))b|,$$

where $\psi_E = \theta \circ \psi$ *is the antipalindromization map,*
and θ *is the Thue-Morse morphism* ($\theta(a) = ab, \theta(b) = ba$).

Definition of S

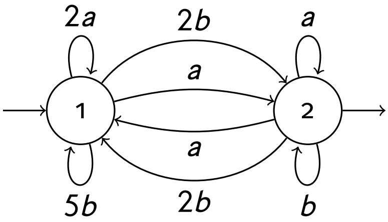
Define a map $S : \{a, b\}^* \longrightarrow \mathbb{N}$ by $S(w) = \mu(w)_{1,2}$.

Since $S(w) = \begin{pmatrix} 1 & 0 \end{pmatrix} \mu(w) \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, when viewed as a formal series,

$$S = \sum_{w \in \{a,b\}^*} S(w) w$$

is rational.

S as a Series



$$S = (2a + 5b + (a + 2b)(a + b)^*(a + 2b))^* \, (a + 2b)(a + b)^*$$

Not Injective in General

Proposition

For all $u \in \{a, b\}^*$,

- $S(aub) = S(a\tilde{u}b)$,
- $S(a\theta(u)b) = S(a\theta(\tilde{u})b)$,

where θ is the Thue-Morse morphism.

Example

- $S(aabb) = 75 = S(abab)$;
- $S(aabbab) = 1130 = S(abaabb)$.

  Thus, even the restriction of S to $\{a, b\} \cup a\text{PAL}b$ is not injective…

What about Christoffel?

Let CH be the set of (lower) Christoffel words over $\{a, b\}$.

Theorem (Borel, Laubie 1993, etc.)

The following holds:

$$\mathrm{CH} = \{a, b\} \cup \left(a\mathrm{PAL}b \cap (\{a, b\} \cup a\mathrm{PAL}b)^2 \right).$$

That is, Christoffel words can be recursively defined:
$w \in \mathrm{CH} \iff w$ *is either a letter or a word of* $a\mathrm{PAL}b$
that is the concatenation of two shorter Christoffel words.

Hence, Markov Triples

We have seen that:

1. $w \in \mathrm{CH} \iff w \in \{a, b\}$ or
   $w \in a\mathrm{PAL}b$ and $w = w'w''$ with $w', w'' \in \{a, b\} \cup a\mathrm{PAL}b$;
2. $w \in \{a, b\} \cup a\mathrm{PAL}b \iff \mu(w)$ is characteristic;
3. Characteristic matrices $M', M'', M'M''$ correspond
   (by their upper right elements) to Markov triples.

Corollary (see Cohn 1972, Reutenauer 2009, etc.)

S maps Christoffel pairs to (nonsingular) Markov triples, i.e., if $w = w'w''$, $w, w', w'' \in \mathrm{CH}$, then

$$S(w')^2 + S(w'')^2 + S(w)^2 = 3S(w')S(w'')S(w).$$

The Conjecture: S Injective on Christoffel

The previous map is actually a bijection, so that the

Conjecture (Frobenius 1913)

Markov triples are uniquely determined by their maximal element.

is equivalent to

Conjecture

The restriction $S|_{\mathrm{CH}}$ is injective.

Evidence Suggesting More Conjectures

Our *limited* experiments *(Markov numbers grow fast!...)* also suggest that:

1. if $w \neq w'$ and $S(w) = S(w')$, then $w, w' \in a\{a, b\}^*b$;
2. if $w \in a\mathrm{PAL}b$ and $S(w)$ is a Markov number, then $w \in \mathrm{CH}$.

Proving Uniqueness via Matrices

A Markov number m is unique if it is the maximal element of a unique Markov triple, or equivalently, if the set

$$S|_{\mathrm{CH}}^{-1}(m) = \{w \in \mathrm{CH} \mid S(w) = m\}$$

is a singleton.

Since μ is injective, and matrices $\mu(w)$ are uniquely determined by any two elements,

$$m \text{ is unique} \iff \exists! \, \gamma : \begin{pmatrix} \alpha & m \\ \beta & \gamma \end{pmatrix} \in \mu(\mathrm{CH}) \text{ for suitable } \alpha, \beta.$$

(Extended) Known Bounds

Hence, as $\gamma^2 \equiv -1 \pmod{m}$, m is closer to uniqueness when this has few solutions for γ.

Theorem

If $w \in a\mathrm{PAL}b$ and $\mu(w) = \begin{pmatrix} \alpha & m \\ \beta & \gamma \end{pmatrix}$, then

$$\left(2 - \sqrt{2}\right) m < \gamma < \frac{\sqrt{5} - 1}{2} m.$$

$$\left\lceil \left(2 - \sqrt{2}\right) m \right\rceil \leq \gamma \leq \left\lfloor \frac{\sqrt{5} - 1}{2} m \right\rfloor .$$

Tight Versions

The previous bounds are tight, since for example

- $w \in ab^* \implies \gamma = \left\lceil \left(2 - \sqrt{2}\right) m \right\rceil$;
- $w \in a^* b \implies \gamma = \left\lfloor \frac{\sqrt{5}-1}{2} m \right\rfloor$.

Further examples exist, though; for $w = aabab$, e.g., we have
$\gamma = 119 = \left\lfloor \frac{\sqrt{5}-1}{2} 194 \right\rfloor = \left\lfloor \frac{\sqrt{5}-1}{2} m \right\rfloor$.

More Precise Bounds

Theorem

Let $w \in a\mathrm{PAL}b$, $m = \mu(w)_{1,2}$, $\gamma = \mu(w)_{2,2}$. *Then*

$$2m - \sqrt{2m^2 - 1} \leq \gamma \leq \frac{-m + \sqrt{5m^2 - 4}}{2},$$

and the lower (resp. upper) bound is attained if and only if $w \in ab^*$ *(resp.* $w \in a^*b$*).*

Extended Limited Uniqueness Results

Theorem

Let $w = aub, u \in \mathrm{PAL}$ *be such that* $S(w) = 2^h p^k$ *(resp.* $[\mu(u)] = 2^h p^k$*)*[a] *for an odd prime* p *and integers* $h \geq 0, k \geq 1$.
Then for all $w' \in a\mathrm{PAL}b$,

$$w \neq w' \implies S(w) \neq S(w').$$

[a](Here $[M] = M_{1,1} + M_{1,2} + M_{2,1} + M_{2,2}$.)

Remark

It is not known whether there are infinitely many such Markov numbers!

Odd-Indexed Fibonacci & Pell Numbers

Pell numbers are defined by:

- $P_0 = 0$, $P_1 = 1$;
- $P_{n+1} = 2P_n + P_{n-1}$ for $n \geq 1$.

Well-known: for all $n \geq 0$, $\{1, F_{2n+1}, F_{2n+3}\}$ and $\{2, P_{2n+1}, P_{2n+3}\}$ are Markov triples.

Lemma (cf. Gessel 1972)

A natural number n is an odd- (resp. even-) indexed Fibonacci number if and only if $5n^2 - 4$ (resp. $5n^2 + 4$) is a perfect square.
Similarly, n is an odd- (resp. even-) indexed Pell number if and only if $2n^2 - 1$ (resp. $2n^2 + 1$) is a perfect square.

Corresponding Words and Matrices

In particular,

- $\mu(a^n b) = \begin{pmatrix} 2F_{2n+3} + F_{2n+1} & F_{2n+3} \\ 2F_{2n+2} + F_{2n} & F_{2n+2} \end{pmatrix}$,
- $\mu(ab^n) = \begin{pmatrix} P_{2n+2} & P_{2n+1} \\ P_{2n+1} + P_{2n} & P_{2n} + P_{2n-1} \end{pmatrix}$.

Theorem (Bugeaud, Reutenauer, Siksek 2009)

Odd-indexed Fibonacci and Pell numbers > 5 have no intersection. Also, when written in order, they alternate forming a Sturmian sequence.

Specialized Uniqueness

However, it is not even known whether allodd-indexed Fibonacci and Pell numbers are unique Markov numbers in general!

Theorem

Let $w = a^n b$, $w' \in \mathrm{CH} \setminus \{w\}$, *and* $\gamma' = \mu(w')_{2,2}$.
If $\gamma' > F_{2n+2}$ *or* $\gamma' \leq \frac{2(2-\sqrt{2})}{\sqrt{5}-1} F_{2n+2} \approx 0.948\, F_{2n+2}$, *then*

$$S(w') \neq S(w).$$

Corollary

Let $w = a^n b$, $w' \in \mathrm{CH} \setminus \{w\}$, *and* $\gamma' = \mu(w')_{2,2}$.
If $S(w') = S(w) = F_{2n+3}$, *then* γ' *is not a Fibonacci number.*

Sounds Easy?

The Fibonacci case of the uniqueness conjecture can be restated as follows:

Conjecture

Let $x, y, z \in \mathbb{N}$ be such that $x \leq y \leq z$, with

$$x^2 + y^2 + z^2 = 3xyz \quad \text{and} \quad \sqrt{5z^2 - 4} \in \mathbb{N}.$$

Then $x = 1$.

Main References

M. Aigner. *Markov's theorem and 100 years of the uniqueness conjecture*. Springer, 2013.

C. Reutenauer. *From Christoffel words to Markoff numbers*. Oxford University Press, USA, 2019.

Thank You

In loving memory of Aldo (1941–2018)

mentor and friend