ON THE FROBENIUS CONJECTURE

Mélodie Lapointe[1]
Université de Paris, CNRS, IRIF, Paris, France
lapointe@irif.fr

Christophe Reutenauer
Département de mathématiques, Université du Québec à Montréal, Montréal, Québec, Canada
Reutenauer.Christophe@uqam.ca

Received: 4/1/21, Accepted: 6/7/21, Published: 6/14/21

Abstract

A Markoff number is a component of a solution of the Diophantine equation $x^2 + y^2 + z^2 = 3xyz$. One way to obtain a Markoff number is to associate it with a Christoffel word. The Frobenius conjecture claims that each Markoff number is associated with a unique Christoffel word. The map returning the Markoff number associated with a Christoffel word is well-defined on any binary word. We propose the following generalization of the Frobenius conjecture: the map from the set of finite Sturmian words (a set of binary words containing Christoffel words) to the set of natural numbers is injective. We prove particular cases of this generalized conjecture. This map restricted to the set of circular factors of a Christoffel word is injective, and it is also injective on the language of a Sturmian sequence.

1. Introduction

Markoff numbers were introduced to describe minima of indefinite real binary quadratic forms [9, 10]. A Markoff number is a component of a Markoff triple, which is a positive integer solution of the Markoff equation

$$x^2 + y^2 + z^2 = 3xyz.$$

A well-known recursive rule for generating all Markoff triples results in an infinite binary tree labeled by Markoff triples. There are only two Markoff triples with repeated values, $(1, 1, 1)$ and $(1, 1, 2)$. All other Markoff triples, called proper Markoff

[1]We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), [funding reference number BP–545242–2020] and the support of the Fonds de Recherche du Québec en Science et Technologies.

triples, have a maximal value. The Frobenius conjecture, also called the Markoff injectivity conjecture, states that each Markoff number is the maximum value of a unique Markoff triple [6].

Many other combinatorial objects are generated using an infinite binary tree, like Farey numbers, Christoffel words, and Cohn matrices. Each of them can be used to generate Markoff numbers. Moreover, the Frobenius conjecture has an equivalent formulation using those labelings. In this paper, we label Markoff numbers with Christoffel words. This labelling was introduced by Cohn [5], by defining a certain matrix function from the set of binary words to the set of Markoff numbers. It was used by Bombieri [2] and the second author [14].

This function is the upper right corner entry of a representation of the free monoid by 2 by 2 matrices over $\mathbb{Z}$. It is defined on all binary words, not only on Christoffel words. We propose to extend the Frobenius conjecture to a larger set of words. We will also prove some special cases of the generalized conjecture.

Recently, some progress has been made towards proving the Frobenius conjecture. Instead of labeling Markoff numbers with Christoffel words, we can label them with Farey numbers. Three conjectures on the growth of Markoff numbers on subsets of Farey numbers were presented in Aigner [1]. These conjectures have been proved in [12, 18], but they are not sufficient to prove the Frobenius conjecture. Even in [18], a generalization of Aigner's conjectures is also proposed, on the set of conjugates and powers of Christoffel words.

Our conjecture is on a larger set of words, the set of finite Sturmian words. The conjugates and powers of Christoffel words are Sturmian words but there exists Sturmian words which are not conjugates or powers of Christoffel words.

This paper is organized as follows. In section 2, we present the Frobenius conjecture and his relationship with Christoffel words. In section 3, we discuss a generalization of the Frobenius conjecture on the set of finite Sturmian words. On section 4, we prove the conjecture on two subsets of finite Sturmian words, namely the circular factors of a Christoffel word and the language of a Sturmian sequence.

2. The Frobenius Conjecture Through Christoffel Words

Before recalling the Frobenius conjecture, let us introduce Christoffel words. A *Christoffel word* is a word on the free monoid $\{a, b\}^*$ that discretizes from below a segment from $[0, 0]$ to $[l, m]$ in the plane, as shown in Figure 1; here l, m are two relatively prime nonnegative integers. More precisely, the path represented by the Christoffel word never crosses the segment, and the polygon formed by the segment and the path contains no integral interior point. Note: These are usually named lower Christoffel words.

The slope of a Christoffel word is the slope of the path discretized by the word.

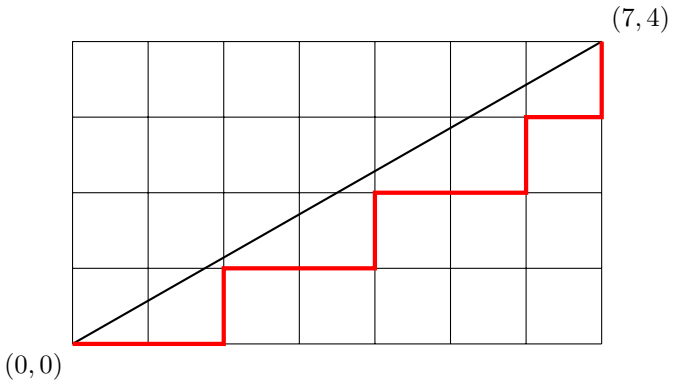

Figure 1: The Christoffel word *aabaabaabab* of slope 4/7

The number of occurrences of the letter a (resp. b) of the Christoffel word of slope m/l (reduced fraction) is l (resp. m). In particular, its length is $m+l$. The slope of a Christoffel word is therefore $m/l = |w|_b/|w|_a$. The Christoffel words a and b have slope 0 and ∞ respectively. The other Christoffel words are called *proper*.

Denote by $\widetilde{w}$ the *reversal* of the word $w = a_1 \dots a_n$, that is $\widetilde{w} = a_n a_{n-1} \dots a_1$. Recall that w is called a *palindrome*, if $\widetilde{w} = w$.

A proper Christoffel word has the form amb where m is a palindrome. A word m over the alphabet $\{a, b\}$, is called *central* if amb is a Christoffel word. Recall that a central word is also a palindrome [16].

A *Markoff number* is a component of some positive solution of the *Markoff equation*

$$x^2 + y^2 + z^2 = 3xyz.$$

Let μ be the monoid homomorphism $\{a, b\}^* \to SL_2(\mathbb{Z})$ defined by

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

It is known that each Markoff number is equal to $\mu(w)_{1,2} = (1/3)Tr(\mu(w))$ for some Christoffel word w ([5, 2, 1, 13]; see also [16] Chapter 3). We call $\mu(w)_{1,2}$ the *Markoff number associated with the Christoffel word* w.

Conjecture 1. (Frobenius 1913) The mapping $w \mapsto \mu(w)_{1,2}$ is injective on the set of Christoffel words.

3. Extension of the Conjecture to Finite Sturmian Words

The mapping $w \mapsto \mu(w)_{1,2}$ is clearly defined on each word $w \in \{a,b\}^*$. It is not injective, since $\mu(aabbab)_{1,2} = 1130 = \mu(abaabb)_{1,2}$. The Frobenius conjecture asks for the injectivity of the restriction to the set of Christoffel words. It is therefore natural to search for larger sets for which the mapping is injective.

A conjugate of a word w is a word of the form vu for some factorization $w = uv$. A *factor* of a word w is a word y such that $w = xyz$ for some words x, z; if x is the empty word, the factor y is called a *prefix* of w. A *circular factor* of a word w is a factor of length at most $|w|$ of ww; equivalently, it is a prefix of a conjugate of w.

We need to mention *Sturmian sequences*. All we need to know is that the set of finite factors of all Sturmian sequences coincides with the set of circular factors of all Christoffel words. See [7] Chapter 2, for details. Such a finite word will be called a *finite Sturmian word*.

We propose the following generalization of the Frobenius conjecture. It is stronger than the latter, since each Christoffel word is a finite Sturmian word.

Conjecture 2. The mapping $w \mapsto \mu(w)_{1,2}$ is injective on the set of finite Sturmian words.

Here is the list of the first values obtain by the mapping $w \mapsto \mu(w)_{1,2}$ from the set of finite Sturmian words into $\mathbb{N}$:

$$\underline{1}, \underline{2}, 3, \underline{5}, 7, 8, 12, \underline{13}, 17, 19, 21, \underline{29}, 31, \underline{34}, 41, 44, 46, 50, 55, 70, 75, 81, \underline{89}, 99, \ldots$$

where we have underlined the Markoff numbers. We have tested using a computer this conjecture for finite Sturmian words up to length 500. To enumerate all finite Sturmian words up to a given length, we used the *left normal form* of a finite Sturmian word introduced in [15].

We shall prove particular cases of the Conjecture 2.

4. Circular Factors of a Christoffel Word

We order the free monoid as follows: first by length, then lexicographically. This order is called the *military order*.

Proposition 1. *Let w be a Christoffel word and H be the set of its circular factors. The mapping $H \to \mathbb{N}, u \mapsto \mu(u)_{1,2}$ is strictly increasing for the military order; in particular it is injective on H.*

See Figure 2 for an illustration of this result: in the figure are written all the conjugates of the Christoffel word $w = aaabaab$, lexicographically ordered from top to bottom, and on the right side, for each prefix u of a conjugate of w, the number

a	a	a	b	a	a	b	1	3	8	34	115	311	1325
a	a	b	a	a	a	b	1	3	13	44	119	313	1327
a	a	b	a	a	b	a	1	3	13	44	119	507	1715
a	b	a	a	a	b	a	1	5	17	46	121	513	1735
a	b	a	a	b	a	a	1	5	17	46	196	663	1793
b	a	a	a	b	a	a	2	7	19	50	212	717	1939
b	a	a	b	a	a	a	2	7	19	81	274	741	1949

Figure 2: The circular factors and the conjugates of a Christoffel word, and their values under the function $\mu(-)_{1,2}$

$\mu(u)_{1,2}$ replaces the last letter of u; the matrix of numbers thus obtained grows along the columns, and from left to right, in accordance with the Proposition 1 (since the circular factors of a word are the prefixes of its conjugates).

The array at the left of Figure 2 is related to the *Burrows-Wheeler transform*. This array is defined for each w as follows: write the conjugates of w in lexicographical order from top to bottom. Then the Burrows-Wheeler transform of w is the word obtained by reading the last column from top to bottom (in the figure, it is b^2a^5). It was proved by Mantaci, Restivo and Sciortino that $w \in \{a, b\}^*$ is the conjugate of a Christoffel word if and only if it Burrows-Wheeler transform is of the form $b^j a^i$ [8]. Note that the values of the function $\mu(-)_{1,2}$ on the set of conjugates of a Christoffel word have several number-theoretical interpretations. In particular, they are the n smallest values of the Markoff quadratic form associated to w, with $n = |w|$, whereas the associated Markoff number (which is $\mu(w)_{1,2}$) is the minimum of this quadratic form, see [17].

For the proof of the proposition, we need some preparation.

Lemma 1. *Let w be a Christoffel word and $w = w_1 < w_2 < \cdots < w_n$ be the conjugates of w in lexicographical order. If u is a prefix of w_i and v is a prefix of w_{i+1} such that $|u| = |v|$, $u \neq v$ and $i \in \{1, \ldots, n-1\}$, then $\mu(u)_{1,2} < \mu(v)_{1,2}$.*

Proof. It is known that if w_i and w_{i+1} are two successive conjugates of w, then for some words p and s, one has $w_i = pabs$, $w_{i+1} = pbas$ (see [4] for details). Moreover, sp is the palindrome which is the central word of w (see [16], Theorem 15.2.4 and its proof). Since $u \neq v$, we have two cases:

(i) $u = pa, v = pb$;

(ii) $u = pabs_1, v = pbas_1$ with $s = s_1 s_2$.

In case (i), we have

$$\mu(u)_{1,2} = \mu(p)_{1,1} + \mu(p)_{1,2} < 2\mu(p)_{1,1} + \mu(p)_{1,2} = \mu(v)_{1,2},$$

since $\mu(p)_{1,1} > 0$.

In case (ii), we have to distinguish between the two cases: $|p| \leq |s_1|$ or the opposite inequality.

Suppose that $|p| \leq |s_1|$; since $s_1 s_2 p$ is a palindrome, we have $s_1 = \tilde{p}t$. Thus $u = pab\tilde{p}t$ and $v = pba\tilde{p}t$. We prove that the right corner entry of the square matrix $\mu(v) - \mu(u)$ is a positive value. Note that $\mu(\tilde{p})$ is the transpose of $\mu(p)$ since $\mu(a)$ and $\mu(b)$ are symmetric matrices. Let

$$\mu(p) = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \quad \text{and} \quad \mu(t) = \begin{pmatrix} i' & j' \\ k' & l' \end{pmatrix}.$$

Also, we have that

$$\begin{aligned} \mu(ba) - \mu(ab) &= \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 12 & 7 \\ 5 & 3 \end{pmatrix} - \begin{pmatrix} 12 & 5 \\ 7 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}. \end{aligned}$$

It follows that

$$\begin{aligned} \mu(v) - \mu(u) &= \mu(p)(\mu(ba) - \mu(ab))\mu(\tilde{p})\mu(t) \\ &= \begin{pmatrix} i & j \\ k & l \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} \mu(\tilde{p})\mu(t) \\ &= \begin{pmatrix} -2j & 2i \\ -2l & 2k \end{pmatrix} \begin{pmatrix} i & k \\ j & l \end{pmatrix} \mu(t) \\ &= \begin{pmatrix} 0 & -2jk + 2il \\ -2li + 2kj & 0 \end{pmatrix} \mu(t) \\ &= \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix} \begin{pmatrix} i' & j' \\ k' & l' \end{pmatrix} \\ &= \begin{pmatrix} 2k' & 2l' \\ -2i' & -2j' \end{pmatrix}, \end{aligned}$$

since $il - jk = \det(p) = 1$. Moreover $l' > 0$, thus we have $\mu(u)_{1,2} < \mu(v)_{1,2}$.

Suppose now that $|p| > |s_1|$; since $s_1 s_2 p$ is a palindrome, we have $p = t\widetilde{s_1}$. Thus $u = t\widetilde{s_1}abs_1$ and $v = t\widetilde{s_1}bas_1$. We prove that the right corner entry of the square matrix $\mu(v) - \mu(u)$ is a positive value. Let $\mu(t)$ as above and

$$\mu(s_1) = \begin{pmatrix} i & j \\ k & l \end{pmatrix}.$$

We have

$$\begin{aligned}\mu(v) - \mu(u) &= \mu(t)\mu(\widetilde{s_1})(\mu(ba) - \mu(ab))\mu(s_1) \\ &= \begin{pmatrix} -2j' & 2i' \\ -2l' & 2k' \end{pmatrix},\end{aligned}$$

by a similar computation as above. Therefore, $\mu(u)_{1,2} < \mu(v)_{1,2}$, since $i' > 0$. □

To prove that the values increase from left to right, we need to know that some linear combinations of values in the matrices are positive.

Lemma 2. *Let* $\mu(w) = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ *be in the monoid* $\mu(A^*)$. *Then* $p-q+r > 0$ *and* $2p - 3q + r - s > 0$.

Proof. Since the matrices $\mu(a)$ and $\mu(b)$ are positive, so are the coefficients of the matrices in $\mu(A^*)$, except for the identity matrix, for which nevertheless $p = s = 1 > 0$ and $q = r = 0$. We prove the two inequalities by induction on the length of w. If w is the empty word, then the inequalities are clear.

Let $w' = wa$ and $\mu(w') = \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix}$. Then

$$\mu(w') = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2p+q & p+q \\ 2r+s & r+s \end{pmatrix}.$$

Thus $p' - q' + r' = 2p + q - p - q + 2r + s = p + 2r + s > 0$ and

$$2p' - 3q' + r' - s' = 4p + 2q - 3p - 3q + 2r + s - r - s = p - q + r > 0$$

by induction.

Let $w' = wb$ and $\mu(w')$ as above. Then

$$\mu(w') = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5p+2q & 2p+q \\ 5r+2s & 2r+s \end{pmatrix}.$$

Thus $p' - q' + r' = 5p + 2q - 2p - q + 5r + 2s = 3p + q + 5r + 2s > 0$ and

$$2p' - 3q' + r' - s' = 10p + 4q - 6p - 3q + 5r + 2s - 2r - s = 4p + q + 3r + s > 0.$$

Hence, we have proved that $p - q + r > 0$ and $2p - 3q + r - s > 0$. □

Lemma 3. *Let* w *be a Christoffel word and* w_n *be its largest conjugate. If* u *is a prefix of length* k *of* w_n *and* v *is a prefix of length* $k+1$ *of* w, *then* $\mu(u)_{1,2} < \mu(v)_{1,2}$.

Proof. By Pirillo theorem[11], we have that $w = w_1 = ahb, w_n = bha$, where h is the central word of w. We may assume that $k \geq 1$. Thus, we have $u = bz$ and $v = azx$ for some prefix z of h and some letter x. We show that $\mu(bz)_{1,2} < \mu(azx)_{1,2}$,

and actually $\mu(bz)_{1,2} < \mu(aza)_{1,2}$ will be enough, since the matrix $\mu(a) \leq \mu(b)$ coefficientwise. One has

$$\mu(bz) = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} * & 5q+2s \\ * & * \end{pmatrix}$$

and

$$\begin{aligned} \mu(aza) &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} * & 2p+r+2q+s \\ * & * \end{pmatrix}. \end{aligned}$$

Thus $\mu(aza)_{1,2} - \mu(bz)_{1,2} = 2p + r + 2q + s - 5q - 2s = 2p - 3q + r - s > 0$ by Lemma 2. □

Proof of Proposition 1. Consider the sequence of words obtained as follows: let $w_1 < w_2 < \ldots < w_n$ be the conjugates of w lexicographically ordered; then take the empty word, the prefixes of length one of $w_1, \ldots, w_n$, followed by the prefixes of length 2, and so on, until the prefixes of length n, which are the w_i themselves. Then clearly this sequence of n^2 words is the set of circular factors of w militarily ordered, with possible repetitions (see Figure 2).

Therefore, it is enough to prove the two following properties:

1. If u, v are prefixes of the same length of two conjugates x, y of w, which are successive in the lexicographical order, and if $u \neq v$, then $\mu(u)_{1,2} < \mu(v)_{1,2}$.

2. If u is a prefix of length k of w_n and v the prefix of length $k+1$ of w_1, then $\mu(u)_{1,2} < \mu(v)_{1,2}$.

These two properties follow from Lemma 1 and Lemma 3. Hence, the map $u \mapsto \mu(u)_{1,2}$ is injective on the set of circular factors of a Christoffel word. □

This implies another particular case of the Conjecture 2.

Corollary 1. *Let F be the set of finite factors of a given Sturmian sequence s, that is, the language of the sequence s. Then the mapping $u \mapsto \mu(u)_{1,2}$ is strictly increasing for the military order; in particular, it is injective on F.*

Proof. Let $u, v \in F$ be such that $u < v$ for the military order. By Proposition 2.1.18 in [7], we may assume that s is equal to a mechanical word of the form $s_{\alpha,0}$ for some irrational $\alpha \in (0,1)$ (see terminology and notations in [7] pp. 53-54). In other words, s is an infinite Christoffel word in the sense of [3]; thus, s has infinitely many prefixes which are Christoffel words ([3] Definitions p. 33). This implies that u, v are factors of some Christoffel word w. In view of Proposition 1, we deduce that $\mu(u)_{1,2} < \mu(v)_{1,2}$. □

References

[1] M. Aigner, *Markov's Theorem and 100 Years of the Uniqueness Conjecture*, Springer International Publishing, Switzerland, 2013.

[2] E. Bombieri, Continued fractions and the Markoff tree, *Expo. Math.* **25** (2007), 187-213.

[3] J.-P. Borel, F. Laubie, Quelques mots sur la droite projective réelle, *J. Théor. Nombres Bordeaux* **5** (1993), 23-51.

[4] J.-P. Borel, C. Reutenauer, On Christoffel classes, *RAIRO Theor. Inform. Appl.* **40** (2006), 15-27.

[5] H. Cohn, Growth types of Fibonacci and Markoff, *Fibonacci Quart.* **17** (1979), 178-183.

[6] G.F. Frobenius, Über die Markoffschen Zahlen, *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* **26** (1913), 458-487.

[7] M. Lothaire, *Combinatorics on Words*, Cambridge University Press, 2002.

[8] S. Mantaci, A. Restivo, M. Sciortino, Burrows–Wheeler transform and Sturmian words, *Inform. Process. Lett.* **86** (2001), 241–246.

[9] A. Markoff, Sur les formes quadratiques binaires indéfinies, *Math. Ann.* **15** (1879), 381-496.

[10] A. Markoff, Sur les formes quadratiques binaires indéfinies (second mémoire), *Math. Ann.* **17** (1880), 379-399.

[11] G. Pirillo, A new characteristic property of the palindrome prefixes of a standard Sturmian word, *Sém. Lothar. Combin.* **43** (1999), B43f.

[12] M. Rabideau, R. Schiffler, Continued fractions and orderings on the Markov numbers, *Adv. Math.* **370** (2020), 107231.

[13] C. Reutenauer, Mots de Lyndon généralisés, *Sém. Lothar. Combin.* **54** (2006), B54h.

[14] C. Reutenauer, Christoffel words and Markoff triples, *Integers* **9** (2009), 327-332.

[15] C. Reutenauer, Studies on finite Sturmian words, *Theoret. Comput. Sci.* **591** (2015), 106-133.

[16] C. Reutenauer, *From Christoffel Words to Markoff Numbers*, Oxford University Press, 2019.

[17] C. Reutenauer, On quadratic numbers and forms, and Markoff theory, to appear in *J. of Number Theory*.

[18] C. Lagisquet, E. Pelantová, S. Tavenas, L. Vuillon, On the Markov numbers: Fixed numerator, denominator, and sum conjectures, *Adv. in Appl. Math.* **130** (2021), 102227.