



HAL
open science

Completing a Combinatorial Proof of the Rigidity of Sturmian Words Generated by Morphisms

Gwenaël Richomme, Patrice Séébold

► **To cite this version:**

Gwenaël Richomme, Patrice Séébold. Completing a Combinatorial Proof of the Rigidity of Sturmian Words Generated by Morphisms. [Research Report] RR-10030, Lirmm. 2010. lirmm-00512187

HAL Id: lirmm-00512187

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-00512187>

Submitted on 27 Aug 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Completing a combinatorial proof of the rigidity of Sturmian words generated by morphisms

Gwénaél Richomme, Patrice Séébold
LIRMM (CNRS, Univ. Montpellier 2)
UMR 5506 - CC 477,
161 rue Ada,
34095 Montpellier Cedex 5, France

and

Université Paul-Valéry Montpellier 3,
UFR IV, Dpt MIAP,
Route de Mende,
34199 Montpellier Cedex 5, France

gwenael.richomme@lirmm.fr, patrice.seebold@lirmm.fr

August 27, 2010

Abstract

In [8], Séébold announced that Sturmian words generated by morphisms are all rigid. There was a gap in the proof. This gap is corrected here to complete a combinatorial proof of this result.

1 Introduction

An infinite word generated by a morphism is *rigid* if all the morphisms which generate this word are powers of a unique morphism.

In [8], Séébold claimed the following.

Theorem 1.1 ([8], Theorem 7) *Sturmian words generated by morphisms are all rigid.* ■

Séébold's proof is entirely combinatorial. However, recently [6], Rao and Wen published a paper in which they give a geometrical proof of Theorem 1.1 based on Rauzy fractals, saying moreover that they “have sought for a combinatorial proof but did not succeed. It would be interesting to know a combinatorial proof (*sic*)”.

While they did not pointed out Séébold's result, they know it because, when preparing their paper, they noticed in Séébold's proof a part which was not complete and hard to retrieve [1]. Even if Rao and Wen were unable to succeed in finding a combinatorial proof of Theorem 1.1 (in fact in correcting the gap in Séébold's proof), such a proof really exists since Séébold's proof can be completed.

The aim of the present note is therefore to correct the gap in Séébold's proof with only combinatorial arguments, thus completing an entirely (correct) combinatorial proof of Theorem 1.1. The gap is described in Section 3 and corrected in Section 4. In order to be self-contained, and to correct some other imprecisions in Séébold's proof, a combinatorial proof of Theorem 1.1, based on Séébold's original proof (see [8]), is given in Section 5.

2 Preliminaries

Before pointing out the gap and solving it, we recall some definitions and notations, and useful results (for references and details, readers are invited to refer to [8]). For general notions about combinatorics on words, we refer to [5].

Let A be the two-letter alphabet $A = \{a, b\}$.

Sturmian words are infinite aperiodic words over A that contain exactly $n+1$ different factors of length n for each integer $n \geq 0$. *Sturmian morphisms* are those morphisms which preserve Sturmian words: a morphism f on A is Sturmian if $f(s)$ is a Sturmian word whenever s is a Sturmian word.

The set St of all Sturmian morphisms is generated by the three morphisms

$$E(a \mapsto b, b \mapsto a), G(a \mapsto a, b \mapsto ab), \tilde{G}(a \mapsto a, b \mapsto ba).$$

This means that every Sturmian morphism f is a composition of a certain number of these three morphisms in a certain order. Considering such a decomposition as a word over the alphabet $\{E, G, \tilde{G}\}$, we write $St = \{E, G, \tilde{G}\}^*$ and a given decomposition of f is the word f over St .

The set St has the presentation

$$\begin{aligned} E^2 &= Id_A \\ GEG^k E\tilde{G} &= \tilde{G}E\tilde{G}^k EG, k \geq 0 \end{aligned}$$

where Id_A is the identity morphism over A . Note that when $k = 0$, $G\tilde{G} = \tilde{G}G$.

In all the following, since $E^2 = Id_A$, we will without restriction consider only *reduced words*, i.e., decompositions of morphisms with no two consecutive E . This is in particular allowed by the following important lemma which summarizes results proved in [8].

Lemma 2.1 ([8]) *If two Sturmian morphisms f and g are such that $f = g$ then there exists an integer $n \geq 0$ such that $f = f_1 \circ \dots \circ f_n$ and $g = g_1 \circ \dots \circ g_n$ with, for all integers i , $1 \leq i \leq n$, $f_i \in \{E, G, \tilde{G}\}$, $g_i \in \{E, G, \tilde{G}\}$ and, $g_i \in \{G, \tilde{G}\}$ if and only if $f_i \in \{G, \tilde{G}\}$, $g_i = E$ if and only if $f_i = E$. ■*

(In other words, in all decompositions of two equal Sturmian morphisms letter E occurs exactly at the same index.)

This implies in particular that the length $|f|$ (the number of occurrences of single morphisms E, G and \tilde{G} in f) is a well-defined number because, under the assumption that E^2 never appear in the decomposition of a morphism, all decompositions of a given morphism have the same length. We will also use the notation $|f|_x$ to denote, in a given decomposition of the morphism f , the number of occurrences of x in this decomposition of f ($x \in \{E, G, \tilde{G}\}$). From what precede, for a given Sturmian morphism f the number $|f|_E$ is the same for all decompositions of f .

Now, if we consider the infinite set of relations of the previous presentation of St as a symmetric rewriting system S then S is locally confluent: every two elements with a common ancestor share a common descendant (this is because each relation is invertible). This implies that, at each step, we can always choose to apply any of the possible rewriting rules to go from one decomposition to another without changing the result.

In the following, we will work with the rewriting system S , considering that if two Sturmian morphisms f and g are equal ($f = g$) then the reduced words f and g (in $St \setminus StE^2St$) are S -equivalent ($f \equiv g$). In particular, from Lemma 2.1, if $f \equiv g$ then $|f| = |g|$ and $f_i = E$ if and only if $g_i = E$, $1 \leq i \leq |f|$.

To end these preliminaries, we recall that the set St is *left and right cancellative* [7], i.e., if f, g and h are Sturmian morphisms then $f \circ g = f \circ h$ implies $g = h$ and $f \circ g = h \circ g$ implies $f = h$. From what precedes, this implies that if $f \circ g \equiv f \circ h$ then $g \equiv h$ and if $f \circ g \equiv h \circ g$ then $f \equiv h$.

69 3 The gap

70 Before indicating the gap in Séébold's proof, we need to recall precisely the meaning of "a
71 morphism generates an infinite word".

72 Let f be a morphism on A . If there exist a letter $c \in A$ and a word $u \in A^+$ such that
73 $f(c) = cu$ and, for every non-negative integer n , $|f^{n+1}(c)| > |f^n(c)|$ then f generates an infinite
74 word, $x = \lim_{n \rightarrow \infty} f^n(c)$. Notice that if f generates an infinite word x then x is a fixed point
75 of f , i.e., $x = f(x)$ (of course the converse is false since, for example, $Id_A(x) = x$ for every
76 word x but the identity morphism never generates any word). To end, it is noteworthy that,
77 since A is a two-letter alphabet then either f or f^2 generates an infinite word, or no power of f
78 generates an infinite word.

79 In his proof of Theorem 1.1 given in [8], Séébold considers two morphisms f and g generating
80 the same Sturmian word and concludes that $f \circ g = g \circ f$ and $f^n = g^m$ for some integers n, m .
81 Then he writes (this is the end of the proof): " $f^n = g^m$ and $fg = gf$ imply that the words
82 f and g are powers of the same word and thus that the morphisms f and g are powers of the
83 same morphism." The gap is here because, due to the presentation of St , the set of all Sturmian
84 morphisms, the decomposition of one particular morphism is generally not unique, consequently
85 what is true for words can be wrong for morphisms.

86 Therefore the proof needs to be completed by showing that, in this case, what is true for
87 words remains true in the rewriting system S .

88 4 The complement

89 The solution is given by the following proposition.

90 **Proposition 4.1** *If f and g are two Sturmian morphisms such that $f \circ g = g \circ f$ and $f^n = g^m$,
91 for some integers $n \leq m$, then there exists a Sturmian morphism h such that $f = g \circ h$.*

92 With this proposition, the gap is ruled out by Corollary 4.3 below which should replace the
93 end of Séébold's proof in [8]. The proof of this corollary needs an intermediate useful lemma.

94 **Lemma 4.2** *Let f be a Sturmian morphism. Then $f \circ E = E \circ f$ if and only if $f = Id_A$ or
95 $f = E$.*

96 *Proof.* The "if" part is trivial.

97 For the "only if" part, let us remark that if f is a Sturmian morphism then $|f(a)|_a + |f(b)|_a \neq$
98 $|f(a)|_b + |f(b)|_b$, except if $f = Id_A$ or $f = E$.

99 Now, $|f \circ E(a)|_a + |f \circ E(b)|_a = |f(a)|_a + |f(b)|_a$ when $|E \circ f(a)|_a + |E \circ f(b)|_a = |f(a)|_b + |f(b)|_b$.
100 Consequently, the only possibility to have $f \circ E = E \circ f$ is that $f = Id_A$ or $f = E$. ■

101 **Corollary 4.3** *Let f and g be Sturmian morphisms generating the same Sturmian word, such
102 that $f \circ g = g \circ f$ and $f^n = g^m$, n, m integers. Then there exist integers k and ℓ , and a Sturmian
103 morphism h such that $f = h^k$ and $g = h^\ell$.*

104 *Proof.* Here, because G and \tilde{G} do not generate any Sturmian word, we use morphisms φ and $\tilde{\varphi}$.
105 It is well known (and immediate since $\varphi = G \circ E$ and $\tilde{\varphi} = \tilde{G} \circ E$) that $St = \{\varphi, \tilde{\varphi}, E\}^*$.

106 First of all, let us remark that f and g are not Id_A nor E because the identity morphism
107 Id_A and the exchange morphism E do not generate any infinite word.

108 The proof is by induction on $\max(|f|, |g|)$.

109 If $\max(|f|, |g|) = 0$ then f and g are the empty morphisms which do not generate any word.
110 Therefore $|f| \geq 1$ and $|g| \geq 1$.

111 If $\max(|f|, |g|) = 1$ then $f = \varphi$ or $f = \tilde{\varphi}$ and g must be equal to f .

112 Suppose $|f| \geq |g|$. From Proposition 4.1, there exists a Sturmian morphism h such that
 113 $f = g \circ h$. Since $f \circ g = g \circ f$, one has $g \circ h \circ g = g \circ g \circ h$ from which we obtain $h \circ g = g \circ h$
 114 because St is left cancellative. If $h = Id_A$ then $f = g$. Otherwise $|h| \geq 1$ and, from Lemma 4.2,
 115 $h \neq E$ (otherwise $g = Id_A$ or $g = E$, a contradiction). Consequently $|f| > \max(|g|, |h|)$ (thus
 116 $n < m$).

117 Since $f^n = g^m$ and $h \circ g = g \circ h$, $g^n \circ h^n = g^m$, thus $h^n = g^{m-n}$. By induction, there exist
 118 integers k, ℓ and a Sturmian morphism h' such that $g = h'^k$ and $h = h'^\ell$. Thus $f = h'^{k+\ell}$. ■

119 Before proving Proposition 4.1 we need to establish some intermediate lemmas.

120 **Lemma 4.4** *Let f, α, β be three Sturmian morphisms.*

- 121 • *If f has a decomposition $f \equiv G\alpha\tilde{G}\beta$ with $|\alpha|_{\tilde{G}} = 0$ and $|\alpha|_E$ odd, then all decompositions*
 122 *of f begin with G .*
- 123 • *If f has a decomposition $f \equiv \tilde{G}\alpha G\beta$ with $|\alpha|_G = 0$ and $|\alpha|_E$ odd, then all decompositions*
 124 *of f begin with \tilde{G} .*

125 Note that, on the other hand, if f has a decomposition $f \equiv G\alpha\tilde{G}\beta$ with $|\alpha|_{\tilde{G}} = 0$ and $|\alpha|_E$ even,
 126 then there exists a decomposition of f beginning with \tilde{G} (and the same is true, exchanging G
 127 and \tilde{G}).

128 *Proof.* We prove the first assertion (the proof of the second one is exactly the same, exchanging
 129 G and \tilde{G}).

130 So, let f, α, β be three Sturmian morphisms such that f has a decomposition $f \equiv G\alpha\tilde{G}\beta$
 131 with $|\alpha|_{\tilde{G}} = 0$ and $|\alpha|_E$ odd.

132 First note that, from Lemma 2.1, no decomposition of f can begin with E .

133 We proceed by induction on $|f|$. Necessarily $|f| \geq 3$ and when $|f| = 3$, $f = GE\tilde{G}$ has a
 134 unique decomposition over $\{G, E, \tilde{G}\}$ (without factor EE) and in this case the result holds.

135 Assume now that $|f| > 3$.

136 Consider first that $|\alpha|_E = 1$. Then $\alpha \equiv G^{k_1}EG^{k_2}$, $k_1, k_2 \geq 0$ and $f \equiv G^{k_1+1}EG^{k_2}\tilde{G}\beta$.
 137 From the presentation of St , f admits a factorization beginning with \tilde{G} only if $\tilde{G}\beta$ admits a
 138 factorization $\tilde{G}\beta \equiv G^{k_3}E\tilde{G}\gamma$ with $k_3 > 0$, and $\gamma \in \{G, \tilde{G}, E\}^*$. But, since $|G^{k_3}E\tilde{G}\gamma| = |\tilde{G}\beta| <$
 139 $|f|$, by induction, this is not possible.

140 Consider now that $|\alpha|_E \geq 3$, that is, $\alpha \equiv G^{k_1}EG^{k_2}EG^{k_3}E\delta$ with $k_1 \geq 0$, $k_2, k_3 \geq 1$,
 141 $\delta \in \{G, E\}^*$, and $f \equiv GG^{k_1}EG^{k_2}EG^{k_3}E\delta\tilde{G}\beta$. Observe that $|E\delta|_E = |\alpha|_E - 2$ is odd and
 142 $|G^{k_3}E\delta\tilde{G}\beta| < |f|$. Therefore by induction $G^{k_3}E\delta\tilde{G}\beta$ has no decomposition beginning with \tilde{G} ,
 143 which implies this also holds for f because $k_2 \geq 1$. ■

144 **Lemma 4.5** *If a Sturmian morphism has two decompositions $G^{k+1}E\alpha \equiv \tilde{G}^{k+1}E\beta$ then $k = 0$.*

145 *Proof.* Let $f \equiv G^{k+1}E\alpha \equiv \tilde{G}^{k+1}E\beta$ for a non-negative integer k . We first remark that α must
 146 contain at least one occurrence of \tilde{G} otherwise no decomposition of $G^{k+1}E\alpha$ can start with \tilde{G} .

147 If α begins with $G^{k'}\tilde{G}$ for some integer k' then, from Lemma 4.4, no decomposition of $G^{k+1}E\alpha$
 148 can begin with \tilde{G} . Therefore $\alpha \equiv G^{k'}E\alpha'$ with $k' \geq 1$. In this case the only possibility for f
 149 to have a decomposition beginning with \tilde{G} is that α' has a decomposition beginning with \tilde{G} .
 150 Consequently, a decomposition of f begins with $G^{k+1}EG^{k'}E\tilde{G} \equiv G^k\tilde{G}E\tilde{G}^{k'}EG \equiv \tilde{G}^kE\tilde{G}^{k'}EG$.

151 Let γ be such that $f \equiv \tilde{G}G^kE\tilde{G}^{k'}EG\gamma$. Since $f \equiv \tilde{G}^{k+1}E\beta$, $\tilde{G}G^kE\tilde{G}^{k'}EG\gamma \equiv \tilde{G}^{k+1}E\beta$ from
 152 which $G^kE\tilde{G}^{k'}EG\gamma \equiv \tilde{G}^kE\beta$ (because St is left cancellative) which is impossible from Lemma
 153 4.4 if $k \neq 0$. ■

154 **Lemma 4.6** *Let f be a Sturmian morphism.*

155 • *If f has a decomposition $f \equiv \alpha G E G^k$ with $k \geq 1$, then all decompositions of f end with*
 156 *$E G^k$.*

157 • *If f has a decomposition $f \equiv \alpha \tilde{G} E \tilde{G}^k$ with $k \geq 1$, then all decompositions of f end with*
 158 *$E \tilde{G}^k$.*

159 *Proof.* We prove the second assertion (the proof of the first one is exactly the same, exchanging
 160 G and \tilde{G}).

161 The property is true if $\alpha \equiv G^p \tilde{G}^q$ ($p, q \geq 0$) or $\alpha \equiv G^{p_1} \tilde{G}^{q_1} E G^{p_0} \tilde{G}^{q_0}$ ($p_0, q_0, p_1, q_1 \geq 0$), i.e.,
 162 if $|\alpha|_E = 0$ or $|\alpha|_E = 1$.

163 Arguing by induction on $|\alpha|_E$, let us suppose that $\alpha \equiv \alpha' E G^{p_1} \tilde{G}^{q_1} E G^{p_0} \tilde{G}^{q_0}$. If $\alpha' = \varepsilon$ then it
 164 is again straightforward that all decompositions of f end with $E \tilde{G}^k$. Otherwise, $\alpha' \equiv \alpha'' G^{p_2} \tilde{G}^{q_2}$
 165 therefore $f \equiv \alpha'' G^{p_2} \tilde{G}^{q_2} E G^{p_1} \tilde{G}^{q_1} E G^{p_0} \tilde{G}^{q_0} \tilde{G} E \tilde{G}^k$ with $p_0, q_0, p_1, q_1, p_2, q_2 \geq 0$ and $p_1 + q_1 \geq 1$,
 166 $p_2 + q_2 \geq 1$.

167 Two cases have to be considered.

168 1) $q_1 = 0$. In this case, f has a decomposition $f \equiv \alpha'' G^{p_2} \tilde{G}^{q_2} E G^{p_1} E G^{p_0} \tilde{G}^{q_0} \tilde{G} E \tilde{G}^k$.

169 • If $q_0 \geq 1$ then every decomposition of f ends with $E \tilde{G}^k$ because only one occurrence
 170 of \tilde{G} in the block $G^{p_0} \tilde{G}^{q_0} \tilde{G}$ can be changed in G , implying that no rewriting rule
 171 using E can be applied to the end of the decomposition of f .

172 • If $q_0 = 0$ then $f \equiv \alpha'' G^{p_2} \tilde{G}^{q_2} E G^{p_1} E G^{p_0} \tilde{G} E \tilde{G}^k$.

173 If $p_2 = 0$ then no rewriting rule using $E \tilde{G}^k$ can be applied to the end of the decom-
 174 position of f .

175 Otherwise, $p_2 \geq 1$ and $f \equiv \alpha'' G^{p_2-1} \tilde{G}^{q_2} G E G^{p_1} E \tilde{G} G^{p_0} E \tilde{G}^k$
 $\equiv \alpha'' G^{p_2-1} \tilde{G}^{q_2+1} E \tilde{G}^{p_1} E G^{p_0+1} E \tilde{G}^k$.

176 By induction hypothesis, every decomposition of $\alpha'' G^{p_2-1} \tilde{G}^{q_2+1} E \tilde{G}^{p_1}$ ends with $E \tilde{G}^{p_1}$.
 177 Therefore, no rewriting rule using $E \tilde{G}^k$ can be applied to the end of the decomposition
 178 of f .

179 2) $q_1 \geq 1$. Then $f \equiv \alpha'' G^{p_2} \tilde{G}^{q_2} E G^{p_1} \tilde{G}^{q_1} E \tilde{G} G^{p_0} \tilde{G}^{q_0} E \tilde{G}^k$.

180 Again, by induction hypothesis, every decomposition of $\alpha'' G^{p_2} \tilde{G}^{q_2} E G^{p_1} \tilde{G}^{q_1} E \tilde{G}$ ends with
 181 $E \tilde{G}$, therefore no rewriting rule using $E \tilde{G}^k$ can be applied to the end of the decomposition
 182 of f . ■

183 We are now ready to prove Proposition 4.1.

184 *Proof of Proposition 4.1.* Let f and g be two Sturmian morphisms such that $f \circ g = g \circ f$ and
 185 $f^n = g^m$, for some integers $n \leq m$. This implies $|f| \geq |g|$, so all decompositions of f are longer
 186 (as words) than all decompositions of g .

187 Since f and g are Sturmian, $f \in \{E, G, \tilde{G}\}^*$ and $g \in \{E, G, \tilde{G}\}^*$. From Lemma 2.1, equality
 188 $f^n = g^m$ implies that for all decompositions of f and g , and for each integer i , $1 \leq i \leq n \cdot |f|$
 189 ($= m \cdot |g|$), $(f^n)_i = E$ if and only if $(g^m)_i = E$, and $(f^n)_i \in \{G, \tilde{G}\}$ if and only if $(g^m)_i \in \{G, \tilde{G}\}$.
 190 In particular, for all decompositions of f and g , and for each integer j , $1 \leq j \leq |g|$, $f_j = E$ if
 191 and only if $g_j = E$, and $f_j \in \{G, \tilde{G}\}$ if and only if $g_j \in \{G, \tilde{G}\}$.

192 Now, let us suppose that for all decompositions of f and g there exists an index $i \leq |g|$ such
 193 that $f_i \neq g_i$. This implies in particular that $2 \leq n \leq m$ (otherwise $n = 1$, so $f = g^m$).

194 Let $f \equiv uf_{|u|+1}v_1$ and $g \equiv ug_{|u|+1}v_2$ be decompositions of f and g where $|u|$ is the greatest
195 possible such that $f_{|u|+1} \neq g_{|u|+1}$. Possibly exchanging f and g , we can assume that $f_{|u|+1} = G$,
196 $g_{|u|+1} = \tilde{G}$, i.e., $f \equiv uGv_1$ and $g \equiv u\tilde{G}v_2$.

197 If $|v_1|_{\tilde{G}} \neq 0$ then there exist α_1, β_1 such that $|\alpha_1|_{\tilde{G}} = 0$ and $f \equiv uG\alpha_1\tilde{G}\beta_1$. The fact that $|u|$
198 is maximal implies that $|\alpha_1|_E$ is odd. But, in this case $f^n \equiv uG\alpha_1\tilde{G}\beta_1f^{n-1}$ and $g^m \equiv u\tilde{G}v_2g^{m-1}$
199 and, since St is left cancellative, $f^n = g^m$ implies $G\alpha_1\tilde{G}\beta_1f^{n-1} \equiv \tilde{G}v_2g^{m-1}$. But, since $|\alpha_1|_E$ is
200 odd, from Lemma 4.4 each decomposition of $G\alpha_1\tilde{G}\beta_1f^{n-1}$ begins with G , a contradiction.

201 Consequently $v_1 \in \{G, E\}^*$ and, with the same reasoning, $v_2 \in \{\tilde{G}, E\}^*$.

202 From $f^n = g^m$, $n, m \geq 2$, we have

$$Gv_1uGv_1f^{n-2} \equiv \tilde{G}v_2u\tilde{G}v_2g^{m-2} \quad (1)$$

203 and from $f \circ g = g \circ f$, we have

$$Gv_1u\tilde{G}v_2 \equiv \tilde{G}v_2uGv_1. \quad (2)$$

204 Now, four cases have to be considered following the value of v_1 .

205 1) $v_1 = \varepsilon$

206 In this case, since $|v_1| \geq |v_2|$ (because $|f| \geq |g|$), $v_2 = \varepsilon$. Therefore $f = uG$ and $g = u\tilde{G}$.
207 In particular $|f| = |g|$, so $n = m$.

208 Two cases are possible:

209 • $|u|_E = 0$. In this case, $u \equiv G^r\tilde{G}^s$ for some non-negative integers r, s and then
210 $f^n \equiv (G^r\tilde{G}^sG)^n \equiv G^{n(r+1)}\tilde{G}^{ns}$ and $g^m \equiv G^{mr}\tilde{G}^{m(s+1)}$, a contradiction with $f^n = g^m$.

211 • $|u|_E \geq 1$. In this case, $u \equiv G^r\tilde{G}^sEu'$ for some non-negative integers r, s and u' does
212 not begin with E .

213 Equation (1) gives $G^r\tilde{G}^sEu'GG^r\tilde{G}^sEu'Gf^{n-2} \equiv G^r\tilde{G}^sEu'\tilde{G}G^r\tilde{G}^sEu'\tilde{G}g^{n-2}$. Since
214 St is left cancellative, this means $GEu'Gf^{n-2} \equiv \tilde{G}Eu'\tilde{G}g^{n-2}$. But, from Lemma 4.4,
215 if u' begins with G then all decompositions of $\tilde{G}Eu'\tilde{G}g^{n-2}$ begins with \tilde{G} and if u'
216 begins with \tilde{G} then all decompositions of $GEu'Gf^{n-2}$ begins with G .

217 Consequently, $u' = \varepsilon$ and Equation (2) gives $GE\tilde{G} \equiv \tilde{G}EG$, a contradiction.

218 2) $v_1 = G^{\ell_0}$ for some integer $\ell_0 \geq 1$

219 In this case, since $|v_1| \geq |v_2|$ and from Equation (1), $v_2 = \tilde{G}^{k_0}$, $k_0 \leq \ell_0$.

220 • If $|u|_E = 0$ then $u \equiv G^r\tilde{G}^s$ for some non-negative integers r, s and Equation (1) gives
221 $G^{n(r+\ell_0+1)}\tilde{G}^{ms} \equiv G^{mr}\tilde{G}^{m(s+k_0+1)}$ which is impossible because $m \geq n \geq 2$ implies
222 $m(s+k_0+1) > ns$.

223 • If $|u|_E \geq 1$ then $u \equiv G^r\tilde{G}^sEu'$ for some non-negative integers r, s and Equation (2)
224 gives $G^{\ell_0+1}Eu'\tilde{G}^{k_0+1} \equiv \tilde{G}^{k_0+1}Eu'G^{\ell_0+1}$ which implies, from Lemma 2.1, $\ell_0 = k_0$ and
225 then, from Lemma 4.5, $\ell_0 = k_0 = 0$, a contradiction.

226 3) $v_1 = G^{\ell_0}E$ for some integer $\ell_0 \geq 0$

227 In this case $f \equiv uG^{\ell_0+1}E$ and then $v_2 = \tilde{G}^{\ell_0}E$. For if not, from Lemma 2.1 and Equa-
228 tion (1), and since $|v_1| \geq |v_2|$, $v_2 = \tilde{G}^{k_0}$ for some integer $k_0 \leq \ell_0$, which implies g^m ends
229 with \tilde{G} when f^n ends with E , a contradiction with Equation (1) and Lemma 2.1.

Since $v_1 \equiv G^{\ell_0} E$ and $v_2 \equiv \tilde{G}^{\ell_0} E$, Equation (1) gives

$$G^{\ell_0+1} E u G^{\ell_0+1} E f^{n-2} \equiv \tilde{G}^{\ell_0+1} E u \tilde{G}^{\ell_0+1} E g^{m-2}.$$

230 Again, from Lemma 4.5, $\ell_0 = 0$.

231 Therefore, $v_1 = v_2 = E$, and Equation (1) gives $G E u G E f^{n-2} \equiv \tilde{G} E u \tilde{G} E g^{m-2}$.

- 232 • If $u = \varepsilon$, then the left part of this equivalence contains only occurrences of G when
- 233 its right part contains only occurrences of \tilde{G} , a contradiction.
- 234 • If u begins with G then, from Lemma 4.4, each decomposition of $\tilde{G} E u \tilde{G} E g^{m-2}$ begins
- 235 with \tilde{G} , a contradiction.
- 236 • If u begins with \tilde{G} then, from Lemma 4.4, each decomposition of $G E u G E f^{n-2}$ begins
- 237 with G , a contradiction.

238 Henceforth, $u = E u'$ and, since $v_1 = v_2 = E$, $f \equiv E u' G E$, $g = E u' \tilde{G} E$. Since $E^2 = Id_A$,

239 $f^n \equiv E (u' G)^n E$ and $g^m = E (u' \tilde{G})^m E$. Let $f' = u' G$ and $g' = u' \tilde{G}$. From $f^n = g^m$ we

240 obtain $f'^m = g'^m$, and from $f \circ g = g \circ f$ we obtain $f' \circ g' = g' \circ f'$. Therefore, we are in

241 the previous case $v_1 = v_2 = \varepsilon$ for $f' = u' G v_1$, $g' = u' \tilde{G} v_2$.

242 4) $v_1 = G^{\ell_0} E G^{\ell_1} v'_1$ for some integers $\ell_0 \geq 0, \ell_1 \geq 1$, and a word $v'_1 \in \{G, E\}^*$

243 Then $f \equiv u G^{\ell_0+1} E G^{\ell_1} v'_1$ and Equation (2) gives

$$G^{\ell_0+1} E G^{\ell_1} v'_1 u \tilde{G} v_2 \equiv \tilde{G} v_2 u G^{\ell_0+1} E G^{\ell_1} v'_1. \quad (3)$$

244 If v'_1 ends with E then, as previously, v_2 ends with E and Equation (3) remains the same

245 without this last occurrence of E .

246 Thus our assuming that $G^{\ell_1} v'_1$ ends with G (and then $\tilde{G} v_2$ ends with \tilde{G}). In this case, since

247 $v'_1 \in \{G, E\}^*$ and $v_2 \in \{\tilde{G}, E\}^*$, there exist v''_1 and v'_2 such that $G^{\ell_0+1} E G^{\ell_1} v'_1 = v''_1 G E G^{\ell'}$

248 with $\ell' \geq 1$, and $\tilde{G} v_2 = v'_2 \tilde{G}$.

249 Then Equation (3) becomes $G^{\ell_0+1} E G^{\ell_1} v'_1 u v'_2 \tilde{G} \equiv \tilde{G} v_2 u v''_1 G E G^{\ell'}$, which is impossible from

250 Lemma 4.6.

251 In the four cases, the assumption that $f_i = G$ and $g_i = \tilde{G}$ for some index i , $1 \leq i \leq |g|$, leads to

252 a contradiction.

253 This implies that there exist one decomposition of f and one decomposition of g such that

254 $f_i = g_i$, $1 \leq i \leq |g|$. Then $f = g \circ h$ and h is a Sturmian morphism because $f_j \in \{E, G, \tilde{G}\}$,

255 $|g| + 1 \leq j \leq |f|$. ■

256 5 A combinatorial proof of Theorem 1.1

257 Before starting the proof of Theorem 1.1, we need to define some terminology and to recall some

258 results from [8].

259 **Result 5.1 ([8], Theorem 2)** *Let $f : A^* \rightarrow A^*$ be a morphism. The following three conditions*

260 *are equivalent:*

261 (i) $f \in St$;

262 (ii) f is Sturmian;

263 (iii) there exists at least one Sturmian word s such that $f(s)$ is Sturmian. ■

264 A Sturmian word x is *characteristic* if both ax and bx are Sturmian words. A morphism f
 265 is *standard* if $f \in \{E, \phi\}^*$. Standard morphisms generating Sturmian words are called *charac-*
 266 *teristic morphisms*.

267 A morphism g is a *conjugate* of a morphism f if there exists $s \in A^*$ such that $sg(ab) = f(ab)s$
 268 and $|g(a)| = |f(a)|$ (which of course implies that $|g(b)| = |f(b)|$). In what follows, *good conjugates*
 269 of a standard morphisms are all its conjugates that are Sturmian morphisms. Notice that each
 270 Sturmian morphism is a conjugate of one standard morphism.

271 **Result 5.2 ([8], Lemma 8)** *Let $g \in St$ be a morphism which generates a Sturmian word x .*
 272 *Then g is a conjugate of a characteristic morphism f which generates a word y having the same*
 273 *set of factors as x . ■*

274 A morphism is *primitive* if it is not a power of another morphism.

275 **Result 5.3 ([8], Theorem 6)** *Let f be a characteristic morphism and x be the characteristic*
 276 *word generated by f . Then there exists a primitive characteristic morphism h such that*

- 277 1. $f = h^n$ for an integer n ;
- 278 2. a morphism $g : A^* \rightarrow A^*$ generates an infinite word having the same set of factors as x if
 279 and only if g is a good conjugate of a power of h . ■

280 **Result 5.4 ([8], Lemma 7)** *Let f be a characteristic morphism. Then any primitive mor-*
 281 *phism g on A , such that f is a power of g , is standard. ■*

282 **Result 5.5 ([8], Proposition 6)** *A morphism $g \in St$ is a good conjugate of a power of a*
 283 *standard morphism f if and only if g is a composition of good conjugates of f . ■*

284 Let us recall that two words u and v are *conjugates* (of each other) if there exists $s \in A^*$
 285 such that $su = vs$.

286 **Result 5.6 ([8], Corollary 2)** *Let g be a Sturmian morphism (different from Id_A and E) and*
 287 *f the standard morphism of which g is a conjugate then, for all $u \in A^*$, the word $g(u)$ is a*
 288 *conjugate of the word $f(u)$. ■*

289 *Proof of Theorem 1.1.*

290 Let f and g , be two morphisms on A which generate the same Sturmian word x . Since
 291 $f(x) = x = g(x)$, f and g are Sturmian by Result 5.1. From Result 5.2, there exist f' and
 292 g' , two characteristic morphisms of which f and g are respectively good conjugates and which
 293 generate two words¹ with the same set of factors as x . From Results 5.3 and 5.4, and Lemma 2.1,
 294 this implies that f' and g' are two powers of a same primitive characteristic morphism h . Thus
 295 f and g are good conjugates of two powers of h , and there exist two strictly positive integers m
 296 and n such that f is a good conjugate of h^m and g is a good conjugate of h^n . But in this case,
 297 from Result 5.5, f^n and g^m are both conjugates of h^{nm} and $f \circ g$ and $g \circ f$ are both conjugates
 298 of h^{n+m} . Since all these morphisms generate x , one has then $f^n = g^m$ and $f \circ g = g \circ f$ (indeed
 299 for every prefix u of x , by Result 5.6, $|f^n(u)| = |h^{nm}(u)| = |g^m(u)|$, so that words $f^n(u)$ and
 300 $g^m(u)$ are equal since they are both prefixes of x ; similarly $f \circ g(u) = g \circ f(u)$). This implies,
 301 from Corollary 4.3, that the morphisms f and g are powers of a same morphism. ■

¹Notice that, since these two words are characteristic words with the same set of factors, they are equal (see, e.g., [5]). This argument was used in Séébold's original proof [8], but there, this property was not explicitly proved. This is why we choose here to do not use this equality and to show that results explicitly proved in [8] are sufficient to conclude.

302 6 Conclusion

303 In this note, in order to complete an entirely combinatorial proof of Theorem 1.1, we have
304 proved in Proposition 4.1 that if f and g are two Sturmian morphisms such that $f \circ g = g \circ f$
305 and $f^n = g^m$, for some integers $n \leq m$, then there exists a Sturmian morphism h such that
306 $f = g \circ h$. Of course, only the first condition is not sufficient to have the result since, for example,
307 $f = G$ and $g = \tilde{G}$ are such that $f \circ g = g \circ f$ while $f \neq g$. On the contrary, the second condition
308 could perhaps be enough alone because, in the proof of Proposition 4.1, it seems that the first
309 condition could be avoided.

310 On the other hand, let us also point out that, recently, new developments on rigidity were
311 obtained (see, e.g., [4], [2], [3]).

312 References

- 313 [1] V. BERTHÉ, Private communication, 2008.
- 314 [2] V. DIEKERT, D. KRIEGER, Some remarks about stabilizers, *Theoret. Comput. Sci.* **410**
315 (2009), 2935–2946.
- 316 [3] F. DURAND, M. RIGO, Syndeticity and independent substitutions, *Adv. in Applied Math.*
317 **42** (2009), 1–22.
- 318 [4] D. KRIEGER, On stabilizers of infinite words, *Theoret. Comput. Sci.* **400** (2008), 169–181.
- 319 [5] M. LOTHAIRE, *Algebraic Combinatorics on Words, Encyclopedia of Mathematics and its*
320 *Applications* vol. 90, Cambridge University Press, Cambridge, United Kingdom, 2002.
- 321 [6] H. RAO, Z.-Y. WEN, Invertible Substitutions with a Common Periodic Point, *in: J.*
322 *Barral, S. Seuret (eds), Recent Developments in Fractals and Related Fields*, Springer
323 Science+Business Media, Singapour, (2010), 401–409.
- 324 [7] G. RICHOMME, Conjugacy and episturmian morphisms, *Theoret. Comput. Sci.* **302** (2003),
325 1–34.
- 326 [8] P. SÉÉBOLD, On the conjugation of standard morphisms, *Theoret. Comput. Sci.* **195**
327 (1998), 91–109.