Sierk W. ROSEMA

Substitutions on two letters, cutting segments and their projections


<http://jtnb.cedram.org/item?id=JTNB_2007__19_2_523_0>
Substitutions on two letters, cutting segments and their projections

par Sierk W. Rosema

Résumé. Dans cet article on considère la structure des projections des segments de coupure correspondant aux substitutions unimodulaires sur un alphabet binaire. On montre qu’une telle projection est un bloc de lettres si et seulement si la substitution est sturmienne. Une double application de ce procédé à une substitution de Christoffel donne la substitution originelle. On obtient ainsi une dualité sur l’ensemble des substitutions de Christoffel.

Abstract. In this paper we study the structure of the projections of the finite cutting segments corresponding to unimodular substitutions over a two-letter alphabet. We show that such a projection is a block of letters if and only if the substitution is Sturmian. Applying the procedure of projecting the cutting segments corresponding to a Christoffel substitution twice results in the original substitution. This induces a duality on the set of Christoffel substitutions.

1. Introduction

The history of Sturmian words goes back to J. Bernoulli in 1772 and Christoffel [2] (1875). The first in depth study of Sturmian words was made by Morse and Hedlund [6], [7] in 1938 and 1940. A Sturmian word induces a broken half-line, the so-called cutting line, which approximates a half-line through the origin quite well. See Series [14] (1985). We call a substitution \( \sigma \) Sturmian if \( \sigma \) maps every Sturmian word to a Sturmian word. In 1991 Séébold [13] showed that Sturmian substitutions that have a fixed point are exactly those substitutions that have Sturmian words as fixed points. For further information on Sturmian words and substitutions we refer to Lothaire [5], Ch. 2 and Pytheas Fogg [8], Ch. 6.

In 1982 Rauzy [9] introduced a fractal which is defined as the closure of the projection of the cutting line corresponding to the Tribonacci substitution \( 0 \rightarrow 01, \ 1 \rightarrow 02, \ 2 \rightarrow 0 \). The analogues of this so-called Rauzy fractal have been studied for many other substitutions, see [5], [8]. An important question is whether the projection of the cutting line generates a tiling or

Manuscrit reçu le 24 mai 2006.
not. This question was the motivation for the author and Tijdeman [12] to have a closer look at the structure of the projections of the finite cutting segments corresponding to $\sigma^n(0)$ in case $\sigma$ is the Fibonacci or Tribonacci substitution. They found in the Fibonacci case that the projections of the integer points of the cutting line generate a two-sided Fibonacci word. In the Tribonacci case they found a close connection with number systems. The latter connection was generalized by Fuchs and Tijdeman in [3]. In the present paper we generalize the former property to unimodular substitutions defined over two letters.

We examine for which substitutions the projected points form a (doubly-infinite) word and which properties these words have. In Section 2 we start with some notation and definitions. Next in Section 3 we give some properties of the points that we get after projecting the cutting segment corresponding to a substitution. We show that the order of the projected points of $\sigma^n(0)$ is preserved in the projection of $\sigma^{n+1}(0)$. Then in Section 4 we define Sturmian substitutions, Sturmian matrices and prove some of their properties.

In Section 5 we consider substitutions for which the incidence matrix is unimodular, and we show that the projected points form a central word if and only if the substitution is Sturmian. We show how the number of 0’s and 1’s in these central words can be calculated from the incidence matrix of the original substitution.

In the final Section 6 we consider a special class of Sturmian substitutions, that we call Christoffel substitutions. We show that when one starts with a Christoffel substitution, the projected points form Christoffel words, and that the relation between these words is again given by a Christoffel substitution. Moreover, if one applies the procedure of projecting the cutting segment corresponding to these Christoffel words again, the result will be the original substitution. This induces a duality on the set of Christoffel substitutions.

### 2. Notations and definitions

An alphabet $\mathcal{A}$ is a finite set of elements that are called letters. In this article we always assume $\mathcal{A} = \{0, 1\}$. A word is a function $u$ from a finite or infinite block of integers to $\mathcal{A}$. If this block of integers contains 0 we call $u$ a central word. If $a \in \mathcal{A}$ and $u(k) = a$ we say $u$ has the letter $a$ at position $k$, denoted by $u_k = a$. If the block of integers is finite we call $u$ a finite word, otherwise it is an infinite word. If $v = v_0 \ldots v_m$ is a finite word and if $u = u_0 u_1 \ldots$ is a finite or infinite word, and there exists a $k$ such
Substitutions, cutting segments, projections

Figure 1. The cutting segment corresponding to $u = 01001$.

that $v_l = u_{k+l}$ for $l = 0, \ldots, m$, then $v$ is called a subword of $u$. If a word $u$ is finite, we denote by $|u|$ the number of letters in $u$, and by $|u|_a$ the number of occurrences of the letter $a$ in $u$.

A substitution $\sigma$ is an application from an alphabet $A$ to the set of finite words. It extends to a morphism by concatenation, that is, $\sigma(uv) = \sigma(u)\sigma(v)$. It also extends in a natural way to a map over infinite words $u$. A fixed point of a substitution $\sigma$ is an infinite word $u$ with $\sigma(u) = u$.

A substitution over the alphabet $A$ is primitive if there exists a positive integer $k$ such that, for every $a$ and $b$ in $A$, the letter $a$ occurs in $\sigma^k(b)$.

We denote the largest integer $y$ such that $y \leq x$ by $\lfloor x \rfloor$, the smallest integer $y$ such that $y \geq x$ by $\lceil x \rceil$ and we put $\{x\} = x - \lfloor x \rfloor$.

**Definition.** Let $u = u_0 \ldots u_{m-1}$ be a finite word. The cutting segment in the $x$-$y$-plane corresponding to $u$ consists of $m+1$ integer points $p_i$ given by $p_i = (|u_0 \ldots u_{i-1}|_0, |u_0 \ldots u_{i-1}|_1)$ for $i = 0, \ldots, m$, connected by line segments of lengths 1.

In Figure 1 we show the cutting segment corresponding to $u = 01001$.

Let $u = u_0 \ldots u_{m-1}$ be a finite word containing at least one zero. Consider the cutting segment corresponding to $u$, and draw the line through the
origin and the end point of the segment, given by $y = \frac{|u_1|}{|u_0|} x$. We project each integer point $p_i$ on the cutting segment parallel to this line to the $y$-axis. By $P(p_i)$ we denote the second coordinate of the projection of $p_i$. It is clear that $P(p_0) = P(p_m)$. See Figure 2 for an example.

**Lemma 2.1.** Let $u = u_0 \ldots u_{m-1}$ be a finite word containing at least one zero and let $P(p_i)$ for $i = 0, \ldots, m$ be defined as above. Then for every $i = 0, \ldots, m$ we have

$$P(p_i) = \left(\frac{|u_0 \ldots u_{i-1}| |u_0| - |u_0 \ldots u_{i-1}| |u_1|}{|u_0|}\right)/|u_0| \in \mathbb{Z}/|u_0|.$$ 

**Proof.** We use induction on $i$. Obviously $P(p_0) = 0$. Assume the lemma is valid for $i \geq 0$. If $u_i = 0$ then $P(p_{i+1}) = P(p_i) - |u_1|/|u_0| = (|u_0 \ldots u_i| |u_0| - |u_0 \ldots u_i| |u_1|)/|u_0|$, and if $u_i = 1$ then $P(p_{i+1}) = P(p_i) + 1 = (|u_0 \ldots u_i| |u_0| - |u_0 \ldots u_i| |u_1|)/|u_0|$. □

The following lemma says that when the numbers of 0’s and 1’s in $u$ are relatively prime, the points $p_i$ are projected to distinct points.

**Lemma 2.2.** Let $u = u_0 \ldots u_{m-1}$ be a finite word containing at least one zero, let $|u_1| > 0$ if $m > 1$, let $\gcd(|u_0|, |u_1|) = 1$ and let $P(p_i)$ for $i = 0, \ldots, m$ be defined as above. Then for $i, j \in \{0, \ldots, m-1\}$ and $i \neq j$ we have $P(p_i) \neq P(p_j)$. 

**Figure 2.** Projecting the cutting segment corresponding to $u = 01001$. 

[Figure showing the projection of a cutting segment corresponding to a word with zeros and ones, illustrating the projection of integer points $p_i$ onto the $y$-axis and the calculation of $P(p_i)$ for different values of $i$.]

Suppose \( P(p_i) = P(p_j) \). Put \( x = |u_0 \ldots u_{i-1}|_1, y = |u_0 \ldots u_{i-1}|_0 \) and \( x' = |u_0 \ldots u_{j-1}|_1, y' = |u_0 \ldots u_{j-1}|_0 \). Then \( P(p_i) = (x|u_0 - y|u_1)/|u_0| \) and \( P(p_j) = (x'|u_0 - y'|u_1)/|u_0| \), hence \( x|u_0 - y|u_1 = x'|u_0 - y'|u_1 \). Since \( \gcd(|u_0|, |u_1|) = 1 \) and \( |x - x'| \leq |u_1|, |y - y'| \leq |u_0| \) with at least one strict inequality, we have \( x = x', y = y' \), hence \( i = j \).

Let \( D = \{-|u_0|P(p_i)| i \in \{0, \ldots, m - 1\}\} \), hence \( D \) is a subset of \( \mathbb{Z} \) containing \( m \) elements under the hypotheses of Lemma 2.2. We define the central function \( w : D \to \{0, \ldots, m - 1\} \) as follows. If \( P(p_i) = k/|u_0| \) then \( w(-k) = i \). We say \( w \) has number \( i \) at position \( -k \). If \( k_1 < k_2 < k_3 \) are integers and \( w \) has numbers at positions \( k_1, k_3 \) but not at \( k_2 \), we say \( w \) has a gap at \( k_2 \). If the central function \( w \) has no gap we call \( w \) a central block. Note that a central function always has the number 0 at position 0. By \( |w| \) we mean the number of positions on which \( w \) is defined, hence \( |w| = |u| \) if \( w \) is the central function corresponding to \( u \). The following lemma shows that \( w(k + 1) - w(k) \) is constant modulo \( |u| \).

**Lemma 2.3.** Let \( u \) be a finite word with \( \gcd(|u_0|, |u_1|) = 1 \) and \( w \) the central function corresponding to \( u \). If \( w \) has a number at position \( k \), then \( w(k) = k/|u_1|^{-1} \pmod{|u|} \), where the inverse is taken modulo \( |u| \).

**Proof.** Suppose \( w \) has the number \( i \) at position \( k \). Then we obtain successively from \( |u_0| + |u_1| = |u| \) that
\[
|u_0 \ldots u_{i-1}|_0|u_1| - |u_0 \ldots u_{i-1}|_1|u_0| = k,
\]
\[
|u_0 \ldots u_{i-1}|_0|u_1| + |u_0 \ldots u_{i-1}|_1|u_1| \equiv k \pmod{|u|},
\]
\[
i|u_1| \equiv k \pmod{|u|}.
\]

**Remark.** If \( w(k) = i \) then \( w(k + |u_1|) = i + 1 \) in case \( u_i = 0 \), and \( w(k - |u_0|) = i + 1 \) in case \( u_i = 1 \). We say that to move from number \( i \) to \( i + 1 \) in \( w \) we either "jump" \( |u_1| \) positions to the right or \( |u_0| \) positions to the left. It follows that the \( |w| \) positions on which \( w \) is defined, represent exactly the cosets modulo \( |w| \).

**Example 1.** If \( u = 01001 \), the central function \( w \) associated with \( u \) is a central block given by \( w = 20314 \), where we have underlined the number at position 0. See Figure 2.

### 3. The central functions \( w_n \)

In this section for every \( n \) we define a central function \( w_n \) corresponding to \( u_n = \sigma^n(0) \), where \( \sigma \) is a substitution. We give conditions on \( \sigma \) so that the construction of \( w_n \) is well-defined, and we show that the order of the numbers in \( w_n \) is preserved in \( w_{n+1} \).
Let \( \sigma \) be a primitive substitution that has a fixed point. Without loss of generality we may assume the fixed point starts with 0. Let \( M_\sigma = \begin{pmatrix} |\sigma(0)|_0 & |\sigma(0)|_1 \\ |\sigma(1)|_0 & |\sigma(1)|_1 \end{pmatrix} \) be its incidence matrix. Define \( u_n = \sigma^n(0) \) for \( n \in \mathbb{Z}_{\geq 0} \) where we use the convention that \( \sigma^0(v) = v \) for every word \( v \). We assume \( \gcd(|u_n|_0, |u_n|_1) = 1 \) for every \( n \in \mathbb{Z}_{\geq 0} \) and consider for each \( u_n \) the corresponding central function \( w_n \).

Example 2. Let \( \phi \) be the substitution defined by \( \phi(0) = 01001 \), \( \phi(1) = 01 \).

If we start with 0 and repeatedly apply \( \phi \) we get successively

\[
\begin{align*}
  u_0 &= 0 \\
  u_1 &= 01001 \\
  u_2 &= 0100101010010100101 \ldots
\end{align*}
\]

This yields the following table of central functions \( w_n \), where we have underlined the number at position 0. Note that the central functions are central blocks, that is, have no gap.

\[
\begin{array}{c|cccccccccccccccc}
  n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & \ldots
\end{array}
\]

We use the following lemmas to derive conditions on the incidence matrix \( M_\sigma \) under which the central functions \( w_n \) exist for all \( n \).

**Lemma 3.1.** If \( M \) is a \( 2 \times 2 \)-matrix with integer coefficients and \( \det(M) \neq 0 \), then \( \text{trace}(M^n) - (\text{trace}(M))^n \) is divisible by \( \det(M) \) for every \( n > 0 \).

**Proof.**

\[
\text{trace}(M^n) - (\text{trace}(M))^n = \lambda_1^n + \lambda_2^n - (\lambda_1 + \lambda_2)^n = -\lambda_1\lambda_2 \sum_{k=1}^{n-1} \binom{n}{k} \lambda_1^{k-1} \lambda_2^{n-k-1}
\]

with \( \det(M) = \lambda_1\lambda_2 \). \( \square \)

**Lemma 3.2.** Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be a matrix with \( a, b, c, d \in \mathbb{R} \). Then \( M^n = (a + d)M^{n-1} - (ad - bc)M^{n-2} \) for \( n \geq 2 \).

**Proof.** We have \( M^2 = (a + d)M - (ad - bc)M^0 \). \( \square \)

**Proposition 3.1.** Let \( \sigma \) be a primitive substitution with a fixed point starting with 0, let \( M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be its incidence matrix and let \( u_n = \sigma^n(0) \).
Then \( \gcd(|u_n|_0, |u_n|_1) = 1 \) for every \( n \in \mathbb{Z}_{\geq 0} \) if and only if \( \gcd(a, b) = \gcd(a + d, ad - bc) = 1 \).

**Proof.** Assume \( \gcd(|u_n|_0, |u_n|_1) = 1 \) for every \( n \in \mathbb{Z}_{\geq 0} \). We define \( a_n, b_n, c_n, d_n \) by \( M^n = \left( \begin{array}{cc} a_n & b_n \\ c_n & d_n \end{array} \right) \) for \( n \in \mathbb{Z}_{\geq 0} \). Since \( M^n = M^n \), we have \( |u_n|_0 = a_n, |u_n|_1 = b_n \). Hence \( \gcd(a, b) = \gcd(|u_1|_0, |u_1|_1) = 1 \). By the previous lemma, \( |u_2|_0 = (a + d)a - (ad - bc), |u_2|_1 = (a + d)b \). Since \( \gcd(|u_2|_0, |u_2|_1) = 1 \), we have \( \gcd(a + d, ad - bc) = 1 \).

We now prove the other implication. Assume that \( \gcd(a, b) = \gcd(a + d, ad - bc) = 1 \). From Lemma 3.1 and our assumption that \( \gcd(\text{trace}(M^n), \det(M^n)) = 1 \) it follows that

\[
\gcd(a_n + d_n, a_1 d_1 - b_1 c_1) = \gcd(\text{trace}(M^n), \det(M^n)) = 1 \quad \text{for every } n > 0.
\]

We prove by induction on \( n \) that \( \gcd(a_n, b_n) = 1 \). We know that \( \gcd(a_1, b_1) = 1 \). Assume \( \gcd(a_m, b_m) = 1 \) for \( m = 1, \ldots, n \). Note that

\[
M^n_{n+1} = \left( \begin{array}{cc} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{array} \right) = \left( \begin{array}{cc} a_n & b_n \\ c_n & d_n \end{array} \right) \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) = \left( \begin{array}{cc} aa_n + cb_n & ba_n + db_n \\ ac_n + cd_n & bc_n + dd_n \end{array} \right).
\]

Assume \( p \) is prime and \( p|a_{n+1} \) and \( p|b_{n+1} \). Then \( p|ab_{n+1} - ba_{n+1} = ab + adb_n - aba_n - bcb_n = b_n(ad - bc) \). Hence \( p|b_n \) or \( p|(ad - bc) \). Suppose \( p|b_n \). From \( p|b_{n+1} = ba_n + db_n \) it follows that \( p|b \) and from \( p|a_{n+1} = aa_n + cb_n \) that \( p|a \), but \( \gcd(a, b) = 1 \). Thus \( p \nmid b_n \) and

\[
p|(ad - bc) = \det(M).
\]

By (3.2) this gives \( p \nmid a_{n+1} + d_{n+1} \), hence \( p \nmid d_{n+1} \). By (3.3) we have \( p|\det(M^n) = a_n d_n - b_n c_n \). Thus \( p|b(a_n d_n - b_n c_n) \) and because \( p|d_n b_{n+1} = ba_n d_n + db_n d_n \) we obtain \( p|d_n b_{n+1} = b_n d_{n+1} \). This contradiction implies that \( \gcd(a_{n+1}, b_{n+1}) = 1 \). \( \square \)

Consider the sequence of words \( w_n \) in (3.1) from Example 2. We see that the numbers \( 0, \ldots, 4 \) in \( w_1 \) are ordered in the same way as the numbers \( 0, 5, 7, 12, 17 \) in \( w_2 \) directly below them. This observation illustrates the following proposition.

**Proposition 3.2.** Let \( \sigma \) be a primitive substitution with incidence matrix \( M_\sigma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \) and a fixed point starting with 0, let \( \gcd(a, b) = \gcd(a + d, ad - bc) = 1 \) and let \( w_n \) be the corresponding central functions for \( n \in \mathbb{Z}_{\geq 0} \). If \( w_n \) has numbers at positions \( k \) and \( l \) then \( w_{n+1} \) has numbers at positions \( \det(M_\sigma) \cdot k \) and \( \det(M_\sigma) \cdot l \). If the number at position \( k \) of \( w_n \) is larger than
the number at position $l$ of $w_n$ then the number at position $\det(M_\sigma) \cdot k$ of $w_{n+1}$ is larger than the number at position $\det(M_\sigma) \cdot l$ of $w_{n+1}$.

**Proof.** First note that since 
\[
|u_{n+1}|_0 = a|u_n|_0 + c|u_n|_1 \\
|u_{n+1}|_1 = b|u_n|_0 + d|u_n|_1
\]
we have $a|u_{n+1}|_1 - b|u_{n+1}|_0 = (ad - bc)|u_n|_1 = \det(M_\sigma)|u_n|_1$, and similarly $c|u_{n+1}|_1 - d|u_{n+1}|_0 = -\det(M_\sigma)|u_n|_0$. We prove the proposition by induction. Since the first letter of $u_n$ is a 0, the first jump in $w_n$ starting at position 0 is to the right and places the number 1 at position $|u_n|_1$. When going from $u_n$ to $u_{n+1}$ this 0 is replaced by a 0’s and b 1’s. Therefore the number $a + b$ in $w_{n+1}$ is placed at position $a|u_{n+1}|_1 - b|u_{n+1}|_0 = \det(M_\sigma)|u_n|_1$.

We see that the statements of the proposition hold for the positions of the numbers 0 and 1 in $w_n$. Assume that in $w_n$ the number $m$ is placed at position $k$ and in $w_{n+1}$ the number $m'$ is placed at position $\det(M_\sigma)k$. The next jump is either to the right or to the left, depending on the value of the $(m+1)$-th letter in $u_n$. If the next jump in $w_n$ is to the right, then the number $m + 1$ is placed at position $k + |u_n|_1$ in $w_n$, and it follows that the number $m' + a + b$ is placed at position $\det(M_\sigma)(k + |u_n|_1)$ in $w_{n+1}$. If the next jump in $w_n$ is to the left, then the number $m + 1$ is placed at position $k - |u_n|_0$ in $w_n$, and it follows that the number $m' + c + d$ is placed at position $\det(M_\sigma)(k - |u_n|_0)$ in $w_{n+1}$. The assertions of the proposition follow now easily. \qed

**Example 3.** Let the substitution $\sigma$ be given by $\sigma(0) = 011$, $\sigma(1) = 0$ so that it has incidence matrix $M_\sigma = \left( \begin{array}{cc} 1 & 2 \\ 1 & 0 \end{array} \right)$ and $\det(M_\sigma) = -2$. We get the following table for $u_n = \sigma^n(0)$:

\[
\begin{array}{l}
  u_0 = 0 \\
  u_1 = 011 \\
  u_2 = 01100 \\
  u_3 = 01100011011 \\
  \ldots \\
\end{array}
\]

This gives the following sequence of $w_n$’s, where $\square$ indicates a gap.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$w_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>1</td>
<td>(0) 2 1</td>
</tr>
<tr>
<td>2</td>
<td>3 (\square) 4 2 0 (\square) 1</td>
</tr>
<tr>
<td>3</td>
<td>3 (\square) (\square) (\square) 0 2 4 (\square) 8 10 1 (\square) 5 7 9 (\square) (\square) (\square) 6</td>
</tr>
</tbody>
</table>

\[\ldots\]

Comparing $w_2$ with $w_3$ illustrates Proposition 3.2.
4. Sturmian matrices and Sturmian substitutions

In this section we define Sturmian matrix, Sturmian substitution, reduced matrix, dual matrix and we list some properties of these objects.

A word $u$ is called balanced if $||v|_0 - |w|_0| < 2$ for all subwords $v, w$ of equal length. A finite word $u$ is called strongly balanced if $u^2$ is balanced. Here $u^2$ is the concatenation of $u$ with $u$. It is easy to see that a finite word $u$ is strongly balanced if and only if $u^n$ is balanced for some $n \geq 2$. A one-sided infinite word is Sturmian if it is balanced and not ultimately periodic. We call a $2 \times 2$-matrix Sturmian if it has determinant equal to $\pm 1$ and has entries in $\mathbb{Z}_{\geq 0}$. We call a substitution $\sigma$ over two letters Sturmian if $\sigma(u)$ is a Sturmian word for every Sturmian word $u$. [5] Th 2.3.7 says that a substitution $\sigma$ is Sturmian if and only if there exists a Sturmian word $v$ such that $\sigma(v)$ is Sturmian. It follows that a primitive substitution $\sigma$ is Sturmian if and only if its fixed point is Sturmian.

**Lemma 4.1.** A Sturmian substitution maps every finite balanced word to a finite balanced word.

**Proof.** See [10] Cor.9. □

The set of Sturmian substitutions is generated by the following three substitutions, cf. [5] Th 2.3.7.

$$E : \begin{cases} 0 \rightarrow 1 \\ 1 \rightarrow 0 \end{cases} \quad \phi : \begin{cases} 0 \rightarrow 01 \\ 1 \rightarrow 0 \end{cases} \quad \tilde{\phi} : \begin{cases} 0 \rightarrow 10 \\ 1 \rightarrow 0 \end{cases}.$$  

Their incidence matrices are $M_E = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $M_\phi = M_{\tilde{\phi}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, respectively. From this it follows that each Sturmian substitution has a Sturmian matrix as incidence matrix. On the other hand we have the following result.

**Theorem 4.1.** If $M$ is a Sturmian matrix then there exists a Sturmian substitution that has $M$ as its incidence matrix.

**Proof.** Let $M$ be a Sturmian matrix. It can be written as a product of factors $M_E$ and $M_\phi$, cf. [8] Sec.6.5.5. By replacing each matrix with the corresponding substitution the composition of these substitutions is a Sturmian substitution that has $M$ as incidence matrix. □

**Lemma 4.2.** Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Sturmian matrix.

(i) If $a + b = c + d$, then $M$ is the identity matrix or $M_E$.

(ii) If $a > c$ and $b < d$, then $M$ is equal to the identity matrix.

(iii) If $a < c$ and $b > d$, then $M = M_E$. 

Proof. (i) Assume $a + b = c + d$. Then $M = \begin{pmatrix} a & b \\ a - \delta & b + \delta \end{pmatrix}$ for some $\delta \in \mathbb{Z}$. Since $\det(M) = (a + b)n = \pm 1$ we have $a + b = 1$ and $\delta = \pm 1$. It follows that $M$ is of the form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Since $\det(M) = (a + b)\delta = \pm 1$ we have $a + b = 1$ and $\delta = \pm 1$. It follows that $M$ is of the form $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. 

(ii) Assume $a > c$ and $b < d$. Using that $ab - bc = \pm 1$ we get $bc \leq (d - 1)(a - 1) \leq bc - (a + d) + 2$. It follows that $a + d \leq 2$, hence $a = d = 1$ and $b = c = 0$. 

(iii) The proof is similar to the proof of (ii). \qed

Corollary 4.1. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Sturmian matrix. If $M$ is an upper matrix then $a \geq c$ and $b \geq d$ with at least one of the two inequalities strict. If $M$ is a lower matrix then $a \leq c$ and $b \leq d$ with at least one of the two inequalities strict.

Proof. This follows immediately from Lemma 4.2. \qed

Definition. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Sturmian matrix. If $a + b > c + d$, then we call $M$ an upper matrix, if $a + b < c + d$ a lower matrix.

Corollary 4.2. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a Sturmian matrix with $ab \neq 0$.

Then there exists a non-negative integer $k$ such that $\begin{pmatrix} a & b \\ c - ka & d - kb \end{pmatrix}$ is an upper matrix.

Proof. Let $k = \min(\lfloor c/a \rfloor, \lfloor d/b \rfloor)$ and let $N = \begin{pmatrix} a & b \\ c - ka & d - kb \end{pmatrix}$. Then $\det N = \det M$ hence $N$ is Sturmian. Since $c - ka < a$ or $d - kb < b$ it follows from Lemma 4.2 that $N$ is an upper matrix. \qed

Definition. We call the upper matrix that is constructed from $M$ as described in Corollary 4.2 the reduced matrix of $M$.

It follows directly from Corollary 4.1 that this definition of reduced matrix is unique.

Lemma 4.3. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an upper matrix. Then there exists a unique upper matrix $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ such that $\det(N) = \det(M)$, $\alpha + \beta = a + b$ and $\alpha = c + d$. Moreover $\gamma + \delta = a$ and $\text{trace}(M) = \text{trace}(N)$.

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an upper matrix. We assume $\det(M) = 1$, the case for $\det(M) = -1$ is similar. We define $N := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} =$
\[
\begin{pmatrix}
(c + d & a + b - (c + d) \\
c & a - c
\end{pmatrix}.
\]
We have to show that \( N \) has nonnegative entries. This is clear for \( \alpha, \beta, \gamma \). Assume \( a < c \). Then \( b = (ad - 1)/c < d \). This implies \( c + d \leq a + b - 1 < c + d \). It follows that \( \delta \geq 0 \). Next we show that \( N \) is unique. Because \( \alpha + \beta = a + b \) and \( \alpha = a + b \), the variables \( \alpha \) and \( \beta \) are uniquely defined. It is well known from number theory that the equation \( \alpha x - \beta y = 1 \) in unknowns \( x, y \) has a unique solution in nonnegative integers \( x, y \) with \( x + y < \alpha + \beta \). Therefore \( \gamma \) and \( \delta \) are also uniquely defined. For \( \alpha + \beta > \gamma + \delta \), observe that if \( b = 0 \) then \( a = d = 1 \), hence \( a + b = 1 \leq c + d \). The other properties are obvious.

\[\square\]

**Definition.** For an upper matrix \( M \) we call the matrix \( N \) as defined in the previous lemma the dual matrix of \( M \). If \( N = M \) we say that \( M \) is self-dual.

It follows directly from the proof of Lemma 4.3 that if \( N \) is the dual matrix of \( M \), then \( M \) is the dual matrix of \( N \), and that an upper Sturmian matrix \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) is self-dual if and only if \( a = c + d \).

**Lemma 4.4.** Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be a Sturmian matrix with \( a, b > 1 \). Then \( [c/a] = [d/b] \).

**Proof.** From \( ad - bc = \pm 1 \) it follows that \( d/b - c/a = \pm \frac{1}{ab} \). From \( c + \frac{1}{a} = \frac{d}{b} \) and \( b > 1 \) we get \( \lfloor c/a \rfloor = \lfloor d/b \rfloor \). From \( \frac{d + 1}{b} = \frac{c}{a} \) and \( a > 1 \) we also get \( \lfloor c/a \rfloor = \lfloor d/b \rfloor \). \( \square \)

The statement of Lemma 4.4 is not valid if \( a = 1 \) and \( ad - bc = -1 \) and if \( b = 1, \ ad - bc = 1 \).

**Lemma 4.5.** Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be a Sturmian matrix with \( ab \neq 0 \) and let \( k = \min([c/a], [d/b]) \). Put
\[
M^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \quad \text{and} \quad N_n = \begin{pmatrix} a_n & b_n \\ c_n - ka_n & d_n - kb_n \end{pmatrix}
\]
for \( n > 0 \). Then \( N_n \) is the reduced matrix of \( M^n \).

**Proof.** The case where \( n = 1 \) has been proven in Corollary 4.2. Assume \( N_n \) is an upper matrix for \( n > 1 \). Then it follows from Corollary 4.1 that \( c_n \leq (k + 1)a_n, \ d_n \leq (k + 1)b_n \) with at least one of the inequalities strict. From this we derive \( ac_n + cd_n \leq (k + 1)(aa_n + cb_n) \) and \( bc_n + dd_n \leq (k + 1)(ba_n + db_n) \). Since \( M^{n+1} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_an + cb_n & ba_n + db_n \\ ac_n + cd_n & bc_n + dd_n \end{pmatrix} \) it follows that \( N_{n+1} \) is an upper matrix. \( \square \)
5. Unimodular substitutions

We call a substitution $\sigma$ over 2 letters unimodular if its incidence matrix is Sturmian. We assume that all substitutions that we consider are unimodular, primitive and have a fixed point starting with 0. Note that for a unimodular substitution $\gcd(a, b) = \gcd(a + d, ad - bc) = 1$, so that it follows from Proposition 3.1 that the construction of $w_n$ is well-defined for all $n > 0$.

Lemma 5.1. Let $u = 0u_1u_2 \ldots$ be the fixed point of a primitive unimodular substitution. Then $u$ is not eventually periodic.

Proof. Let $\psi$ be the primitive unimodular substitution with fixed point $u$. Then $\psi$ has a Sturmian incidence matrix $M$. It follows from Theorem 4.1 that there exists a Sturmian substitution $\sigma$ with incidence matrix $M$. Let $u_n = \psi^n(0)$ and $u'_n = \sigma^n(0)$. Because the numbers of 0’s and 1’s in $u_n$ and $u'_n$ are completely determined by $M$, we have $|u_n|_0 = |u'_n|_0$ and $|u_n|_1 = |u'_n|_1$ for every $n \in \mathbb{Z}_{\geq 0}$. Therefore $\lim_{n \to \infty} |u_n|_0/|u_n|_1 = \lim_{n \to \infty} |u'_n|_0/|u'_n|_1$ and this limit is irrational since it is the fixed point of a Sturmian substitution ([5] Sec.2.1.1). It follows that $u$ is not eventually periodic. \hfill $\Box$

For a finite word $u$ we denote by $f^a_u = |u|_a/|u|$ the frequency of the letter $a$ in $u$.

Lemma 5.2. Let $u$ be a finite word that is not balanced. Then $u$ has a subword $v$ with $2|v| \leq |u|$ such that $|v|_0 > \lceil |v||f^0_u| \rceil$ or $|v|_1 > \lceil |v||f^1_u| \rceil$.

Proof. Since $u$ is not balanced, it has subwords $v, w$ of equal length such that $|v|_0 - |w|_0 \geq 2$. Without loss of generality we may assume that $v$ and $w$ are disjoint, so that $|v| = |w| \leq |u|/2$. Assume $|v|_0 \leq \lceil |v||f^0_u| \rceil$. Then $|w|_1 = |w| - |w|_0 \geq |w| + 2 - |v|_0 \geq |w| + 2 - \lceil |v||f^0_u| \rceil = |w| + 2 - \lceil |w|(1 - f^1_u) \rceil \geq 1 + \lceil |w||f^1_u| \rceil$. \hfill $\Box$

Lemma 5.3. Let $u$ be a finite word with $\gcd(|u|_0, |u|_1) = 1$. Then $u$ is strongly balanced if and only if for every subword $v$ of $u$ we have $|v|_0 = \lceil |v||f^0_u| \rceil$ or $|v|_0 = \lceil |v||f^1_u| \rceil$.

Proof. Assume $u$ is not strongly balanced. Put $u = u_0 \ldots u_m$. Since $u^2$ is not balanced, there exists a subword $v$ of $u^2$ with $|v| \leq |u|$ and $|v|_0 > \lceil |v||f^0_u| \rceil$ or $|v|_1 > \lceil |v||f^1_u| \rceil$, according to the previous lemma. It is obvious that $|v| \neq |u|$. If $v$ is a subword of $u$ we are done. Otherwise $v$ is of the form $u_p \ldots u_m u_0 \ldots u_q$ with $q < p - 1$. Without loss of generality we assume $|v|_1 > \lceil |v||f^1_u| \rceil$, hence $-|v|_0 > -\lceil |v||f^0_u| \rceil$. Define $v' = u_{q+1} \ldots u_{p-1}$. This is a subword of $u$ with $|v| + |v'| = |u|$. We get

$$|v'|_0 = |u|_0 - |v|_0 > \lceil |u|_0 - |v||f^0_u| \rceil = \lceil |v'||f^0_u| \rceil.$$
Assume there is a subword $v$ of $u = u_0 \ldots u_m$ with $|v| < |u|$ and $|v|_0 < \lfloor |v|f_u^0 \rfloor$ or $|v|_0 > \lceil |v|f_u^0 \rceil$. We assume the second case, the proof for the first case is similar. Put $n = |v|$, hence $n < |u| = m + 1$. Consider the $m + 1$ subwords of $u^2$ of length $n$ that start with the letters $u_0, u_1, \ldots, u_m$. Each letter of $u$ occurs in exactly $n$ of these subwords, hence on average each of these subwords contains $nf_u^0$ zeros. Because $\gcd(|u|_0, |u|_1) = 1$ we know $nf_u^0 \notin \mathbb{Z}$. Assume all these subwords contain $\lceil nf_u^0 \rceil$ or more zeros. Then $|u|_0 \geq (m + 1) \lceil nf_u^0 \rceil / n > (m + 1)f_u^0 = |u|_0$. This contradiction implies that there exists a subword $v'$ of $u^2$ of length $n$ with fewer than $\lceil nf_u^0 \rceil$ zeros, and it follows that $u^2$ is not balanced.

□

Proposition 5.1. Let $u$ be a finite word with $\gcd(|u|_0, |u|_1) = 1$ and let $w$ be the corresponding central function. Then $w$ forms a central block if and only if $u$ is strongly balanced.

Proof. Assume that $u$ is not strongly balanced. Then using the previous lemma we may assume without loss of generality that there exists a subword $v$ of $u$ with $|v|_0 > \lceil |v|f_u^0 \rceil$, since if $|v|_0 < \lceil |v|f_u^0 \rceil$ then $|v|_1 > \lceil |v|f_u^0 \rceil$. Because of the way $w$ is defined, there are two letters in $w$ at positions that are $|u|_1|v|_0 - |u|_0|v|_1$ apart. We get

$$|u|_1|v|_0 - |u|_0|v|_1 \geq |u|_1 \left( \lceil f_u^0|v| \rceil + 1 \right) - |u|_0 \left( |v| - \lceil f_u^0|v| \rceil - 1 \right) \geq |u|f_u^0|v| + |u| - |u|_0|v| = |u|.$$ 

Hence $w$ contains a gap.

Assume $w$ contains a gap. Then $w$ has two numbers at positions that are $|w|$ or more apart. Call the smallest of these two numbers $a$ and the largest $b$. Let $v$ be the subword of $u$ that starts at the $(a + 1)$-th letter and ends with the $b$-th letter. There are two possibilities, $|u|_0|v|_1 - |u|_1|v|_0 \geq |u|$ or $|u|_1|v|_0 - |u|_0|v|_1 \geq |u|$, depending on whether the position of $a$ in $w$ is left or right of the position of $b$. We will assume the second inequality holds; the proof for the first case is similar. We get, successively,

$$|u|_1|v|_0 \geq |u| + |u|_0(|v| - |v|_0),$$

$$|v|_0 \geq 1 + f_u^0|v| > \lceil f_u^0|v| \rceil .$$ 

It follows from the previous lemma that $u_n$ is not strongly balanced. □

Remark. If we replace the condition in Proposition 5.1 that $u$ is strongly balanced by the condition that $u$ is balanced the statement does not hold. Take for example $u = 0010100$ so that $\gcd(|u|_0, |u|_1) = 1$, $u$ is balanced (but $u^2$ is not balanced). Then $w = 5 \sqcup 6 3 0 4 1 \sqcup 2$ contains gaps.

Theorem 5.1. Let $\sigma$ be a primitive unimodular substitution with fixed point starting with 0. Then $\sigma$ is Sturmian if and only if $w_n$ forms a central block for every $n > 0$. 

Substitutions, cutting segments, projections
Proof. Because $\sigma^n$ is a Sturmian substitution it follows from Corollary 4.1 that $u_n^2 = \sigma^n(00)$ is balanced. Applying Proposition 5.1 gives that $w_n$ has no gap for any $n > 0$.

Assume $w_n$ has no gap for any $n > 0$. Proposition 5.1 implies that $u_n$ is balanced for every $n$, and therefore the fixed point of $\sigma$ is balanced. Because it is not eventually periodic according to Lemma 5.1, it is a Sturmian word. Hence $\sigma$ is a Sturmian substitution. □

Example 2 (continued). For $n > 0$ we define $v_n$ as follows. Let $g_n$ be the number at position $-1$ of $w_n$. Then $v_n$ is obtained by replacing every number in $w_n$ that is smaller than $g_n$ by 0, and every other number by 1. We get the following table of central words over a two-letter alphabet.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$v_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1 0 1</td>
</tr>
<tr>
<td>2</td>
<td>1 0 1 1 0 1 0 1 0 1 1 0 1 1 0 1</td>
</tr>
</tbody>
</table>

This example illustrates the following definition. Let $\sigma$ be a primitive unimodular substitution with fixed point starting with 0. For $n > 0$ put $g_n = -\det^n(M_\sigma)|u_n|_1^{-1}$ (mod $|u_n|$), where the inverse is taken with respect to $|u_n|$. Let $w'_n = w_n$ for each $n$ if $\det(M_\sigma) = 1$, otherwise let $w'_n = w_n$ and reflect each $w'_n$ in the origin for $n$ odd. Note that it follows from Lemma 2.3 that $g_n$ is the number at position $-1$ of $w'_n$ if there is one.

Definition. Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0 and $g_n$, $w'_n$ as defined above. Then for $n > 0$ we get the central word $v_n$ by replacing every number in $w'_n$ that is smaller than $g_n$ by 0, and every other number by 1.

We already noted in Section 2 that $w_n$ has in each coset modulo $|w_n|$ exactly one position on which it is defined. This means we can extend $w'_n$ to a bi-infinite central block $\hat{w}'_n$ with period $|w_n|$. It follows from the definition of $v_n$ that $\hat{w}'_n(i) < \hat{w}'_n(i + 1) \iff \hat{w}'_n(i) < \hat{w}'_n(-1) \iff v_n(i) = 0$. The next corollary follows directly from Proposition 3.2.

Corollary 5.1. Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0 and assume that $v_p$ has a letter at position $-1$. Then for $n \geq p$ if $v_n$ has a letter at position $k$ then $v_{n+1}$ has the same letter at position $k$.

We see that in this case $v := \lim_{n \to \infty} v_n$ is an infinite central word. The only primitive Sturmian substitutions with fixed point starting with 0 for which there does not exist an integer $p$ such that $v_p$ has a letter at position $-1$ are the Christoffel substitutions defined in Section 6.
**Example 4.** Let the primitive Sturmian substitution $\psi$ be given by $\psi(0) = 01$, $\psi(1) = 011$. Then the statement of Corollary 5.1 does not hold since $v_1(1) = 1$ and $v_2(1) = 0$, as we see in the table below. Note that there is no letter at position $-1$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$u_n$</th>
<th>$w_n = w'_n$</th>
<th>$v_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0 1</td>
<td>0 1</td>
</tr>
<tr>
<td>1</td>
<td>0 1</td>
<td>0 1 1</td>
<td>2 4 1</td>
</tr>
<tr>
<td>2</td>
<td>0 1</td>
<td>0 1 0 1 1</td>
<td>0 0 1</td>
</tr>
</tbody>
</table>

**Theorem 5.2.** Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0. If $v_n$ has a letter at position $i$ then it equals 0 if $\{-i g_n/|v_n|\} \in [0, g_n/|v_n|)$ and 1 otherwise. Moreover, $v_n$ is strongly balanced for every $n > 0$.

*Proof.* The first statement follows directly from the definition of $v_n$ and from Lemma 2.3 which says $w_n(i) = i|u_n|_1^{-1} \pmod{|u_n|}$. It follows from [5] Sec.2.1.2. that words defined in this way are strongly balanced (so-called rotation words). □

**Remark.** The central words $v_n$ need not be balanced if we would not require that $g_n$ is the number at position 1 or $-1$ in $w_n$. We illustrate this using the substitution $\phi$ from Example 2 and choosing in $w_2$ the number at position $-2$ as $g_2$. Then

$$v_2 = 0010000100100001001.$$  

Clearly $v_2$ is not balanced, since it contains subwords of length 4 that contain two 0’s and subwords of length 4 that contain four 0’s.

**Theorem 5.3.** Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0 and $M_\sigma$ as its incidence matrix. Then $|v_n|_0$ and $|v_n|_1$ are given by the top left and top right entry, respectively, of the dual matrix of the reduced matrix of $M_\sigma^n$ for $n > 0$.

*Proof.* We know that $M_\sigma^n = \begin{pmatrix} |u_n|_0 & |u_n|_1 \\ c_n & d_n \end{pmatrix}$ with $c_n, d_n \in \mathbb{Z}_{\geq 0}$ for $n > 0$.  

We call its reduced matrix $\begin{pmatrix} |u_n|_0 & |u_n|_1 \\ c'_n & d'_n \end{pmatrix}$. It follows from the definition of $w_n$ that $w'_n(-1) = x_n + y_n$ where $(x_n, y_n)$ is the unique solution of the equation $|u_n|_0 x - |u_n|_1 y = \det(M_\sigma^n)$ with $0 \leq x_n \leq |u_n|_1$ and $0 \leq y_n \leq |u_n|_0$. Therefore we must have that $(c'_n, d'_n) = (y_n, x_n)$. From the definition of $v_n$ we get immediately that $|v_n|_0 = t_n = w'_n(-1) = x_n + y_n$. This means that the dual matrix of the reduced matrix of $M_\sigma^n$ has $|v_n|_0$ as top left entry, and because the sum of the elements of the top row is the same for the dual matrix, it has $|v_n|_1$ as top right entry. □
Corollary 5.2. Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0, $M_n$ its incidence matrix and let $v_n$ be the central word corresponding to $u_n$ for some $n > 0$. Shift $v_n$ a number of positions to the right so that the left most letter is at position 0. In the same way as before we can project the cutting segment constructed from the shifted word $v_n$ to form the central block $t_n$. By looking at the incidence matrix of $M_\sigma$ we get $t'_n$ from $t_n$ in the same way as we construct $w'_n$ from $w_n$. Finally we construct a new central word $z_n$ from $t'_n$. Then $|z_n|_0 = |u_n|_0$ and $|z_n|_1 = |u_n|_1$.

Proof. Let $N_n$ be the reduced matrix of the dual matrix of $M^n_\sigma$. We know from the previous theorem that $N_n$ is of the form \[
\begin{pmatrix}
|v_n|_0 & |v_n|_1 \\
c_n & d_n
\end{pmatrix}
\] for some $c_n, d_n \in \mathbb{Z}_{\geq 0}$ and it is an upper matrix. This means that the solution $(x_n, y_n)$ of the equation $|v_n|_0x - |v_n|_1y = \det(M^n_\sigma)$ is given by the bottom entries of $N_n$. Therefore $|z_n|_0$ and $|z_n|_1$ are given by the top left and top right entry of the dual matrix of $N_n$, respectively, which is the reduced matrix of $M^n_\sigma$, since the dual matrix of the dual matrix is the original matrix. Of course the reduced matrix of $M^n_\sigma$ has the same top row as $M^n_\sigma$ itself. \[\square\]

Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0 and $M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ its incidence matrix. For $n > 0$ we define $(x_n, y_n)$ as the unique solution of the equation $|u_n|_0x - |u_n|_1y = \det(M^n_\sigma)$ satisfying $0 \leq x_n \leq |u_n|_1$ and $0 \leq y_n \leq |u_n|_0$. Since $M^n_\sigma = \begin{pmatrix} |u_n|_0 & |u_n|_1 \\ c_n & d_n \end{pmatrix}$, it follows that $|u_n|_0d_n - |u_n|_1c_n = \det(M^n_\sigma)$. Hence $x_n = d_n - k|u_n|_1$, $y_n = c_n - k|u_n|_0$ for some suitable $k \in \mathbb{Z}_{\geq 0}$. From Lemma 4.5 we know that the value of $k$ is independent of $n$. Since according to Lemma 3.2 both $(c_n), (d_n)$ and $(|u_n|_0), (|u_n|_1)$ satisfy the recurrence relation $p_n = (a + d)p_{n-1} - (a + b)c_p_{n-2}$ it follows that $(x_n)$ and $(y_n)$ satisfy the same recurrence relation. By going backwards we define $x_0$ and $y_0$. Since $|u_0|_0x_0 - |u_0|_1y_0 = 1$ and $|u_0|_0 = 1, |u_0|_1 = 0$, we see that $x_0 = 1$, but $y_0$ is not determined by this equation.

We mentioned in the proof of Theorem 5.3 that $|v_n|_0 = x_n + y_n$. Hence we see that $(|v_n|_0)$ and $(|v_n|_1)$ satisfy the same recurrence relation. By going backwards we can now define $|v_0|_0$ and $|v_0|_1$, and we see that also $|v_0|_0 = x_0 + y_0$. Note that $v_0$ has no meaning in terms of projecting a cutting sequence, and is only formally defined. We will see that $|v_0|_0$ and $|v_0|_1$ can take negative values, but their sum is $|v_0|_0 = 1$. Theorem 5.3 can be used to find $|v_n|_0$ and $|v_n|_1$ for $n > 0$. In order to calculate $|v_0|_0$ and $|v_0|_1$ we prove the following lemma.
Lemma 5.4. Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0 and $M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ its incidence matrix. Let $k$ be the non-negative integer such that $\begin{pmatrix} a & b \\ c - ka & d - kb \end{pmatrix}$ is an upper matrix. Then $|v_0|_1 = k$ and $|v_0| = 1 - |v_0|_1 = 1 - k$.

Proof. The reduced matrix of $M_\sigma$ equals $\begin{pmatrix} a & b \\ c' & d' \end{pmatrix}$ where $c' = c - ka, d' = d - kb$ and $ad' - bc' = \det M_\sigma$. Recall $\det M_\sigma = \pm 1$. In the table below we know $|u_0|_1 = 1, |u_0| = 0, |u_1|_1 = a, |u_1| = b$. Using the recurrence relation on $(|u_n|_0), (|u_n|_1)$ we compute $|u_2|_0 = a(a + d) \mp 1, |u_2|_1 = b(a + d)$. We know that $x_0 = 1, x_1 = d'$ and $y_1 = c'$. Next we get $x_2 = (a + d)d' \mp 1$ from the recurrence relation on $(x_n)$. Recall that $a + d \neq 0$ and $b \neq 0$. We use the equation $|u_2|_0 x_2 - |u_2|_1 y_2 = 1$ to find $y_2$ as follows.

$$b(a + d)y_2 = a(a + d)^2d' \mp a(a + d) \mp (a + d)d';$$
$$by_2 = a(a + d)d' \mp (a + d') = (bc' \pm 1)(a + d) \mp (a + d') = bc'(a + d) \pm kb;$$
$$y_2 = c'(a + d) \pm k.$$

Finally we find $y_0 = -k$ from the recurrence relation on $(y_n)$ and then $|v_0|_1 = x_0 + y_0 = 1 - k, |v_0| = 1 - |v_0|_1 = k$. See the table below.

| $n$ | $|u_n|_0$ | $|u_n|_1$ | $x_n$ | $y_n$ | $|v_n|_0$ | $|v_n|_1$ |
|-----|-----------|-----------|------|------|--------|--------|
| 0   | 1         | 0         | 1    | $-k$ | 1 - $k$ | $k$    |
| 1   | $a$       | $b$       | $d'$ | $c'$ | $c'(a + d) \pm k$ |
| 2   | $a(a + d) \mp 1$ | $b(a + d)$ | $(a + d)d' \mp 1$ | $c'(a + d) \pm k$ |

\[ \square \]

Consider a primitive Sturmian substitution $\sigma$ with fixed point starting with 0, with incidence matrix $M_\sigma$ and $u_n, v_n$ defined as before. As mentioned before we have for $(|v_n|_0)$ and $(|v_n|_1)$ the same recurrence relation as for $(|u_n|_0)$. The following theorem shows that there is a Sturmian matrix that we call $M_\tau$ such that $(|v_n|_0, |v_n|_1) \cdot M_\tau = (|v_{n+1}|_0, |v_{n+1}|_1)$ for every $n \in \mathbb{Z}_{\geq 0}$. Thus $M_\tau$ has the same trace and determinant as $M_\sigma$.

Theorem 5.4. Let $\sigma$ be a primitive Sturmian substitution with fixed point starting with 0, with incidence matrix $M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and let $(v_n)_{n=0}^\infty$ be the corresponding central words. Let $k$ be the non-negative integer such that $\begin{pmatrix} a & b \\ c - ka & d - kb \end{pmatrix}$ is an upper matrix. Then $(|v_n|_0, |v_n|_1) \cdot M_\tau = (|v_{n+1}|_0, |v_{n+1}|_1)$ for every $n \in \mathbb{Z}_{\geq 0}$ where $M_\tau = M'_\tau + k \begin{pmatrix} a' - c' & b' - d' \\ a' - c' & b' - d' \end{pmatrix}$ and $M_\tau = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ is the dual matrix of the reduced matrix of $M_\sigma$. 
Proof. Let $\sigma$ be a Sturmian substitution. We write its incidence matrix as $M_\sigma = \begin{pmatrix} a & b \\ c + ak & d + bk \end{pmatrix}$ so that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the reduced matrix of $M_\sigma$. Then $M_\tau = \begin{pmatrix} c + d(k+1) & a + b - (c + d) + k(b - d) \\ c + kd & a - c + k(b - d) \end{pmatrix}$. Using the previous lemma we see that $|v_0|_1$ is $k$ and we can make the following table.

| $n$ | $u_n|_0$ | $u_n|_1$ | $x_n$ | $y_n$ | $|v_n|_0$ | $|v_n|_1$ |
|-----|----------|----------|------|------|----------|----------|
| 0   | 1        | 0        | 1    | $-k$ | 1 - $k$  | $k$      |
| 1   | $a$      | $b$      | $c$  | $d$  | $c + d$  | $a + b - (c + d)$ |

We see that $$(|v_0|_0, |v_0|_1) \cdot M_\tau = (1 - k, k) \cdot \begin{pmatrix} c + d(k+1) & a + b - (c + d) + k(b - d) \\ c + kd & a - c + k(b - d) \end{pmatrix} = (c + d, a + b - (c + d)) = (|v_1|_0, |v_1|_1).$$

Straightforward calculations show that $\text{trace}(M_\tau) = a + d + bk = \text{trace}(M_\sigma)$ and $\det(M_\tau) = ad - bc = \det(M_\sigma)$. Since $(|v_n|_0)$ and $(|v_n|_1)$ satisfy the same recurrence relation $p_n = \text{trace}(M_\tau)p_{n-1} - \det(M_\tau)p_{n-2}$ as $(|u_n|_0)$, $(|u_n|_1)$ and since $\text{trace}(M)M - \det(M)I = M^2$ for any matrix $M$, it follows that $(|v_n|_0, |v_n|_1) \cdot M_\tau = (|v_{n+1}|_0, |v_{n+1}|_1)$ for every $n \in \mathbb{Z}_{\geq 0}$. □

6. Christoffel substitutions

In this section we consider a special class of unimodular substitutions that we will call Christoffel substitutions.

Let $u$ be a finite word. We call $u$ a Lyndon word if $u = vw$ implies $u < vw$ in the lexicographical order. Let $0 < p < q$ and $\text{gcd}(p, q) = 1$. The finite word $u = u_0u_1\ldots u_{q-1}$ is called a lower Christoffel word or just Christoffel word if

$$u_i = \left\lfloor \frac{(i + 1)p}{q} \right\rfloor - \left\lfloor \frac{ip}{q} \right\rfloor,$$

cf. [5] Sect.2.1.2. Note that $p$ equals the number of 1’s in $u$. It follows from the definition that for each $a, b \in \mathbb{Z}_{>0}$ with $\text{gcd}(a, b) = 1$ there exists a unique Christoffel word containing $a$ zeros and $b$ ones. We also see that every Christoffel word starts with 0 and ends with 1.

Lemma 6.1. A finite non-constant word is a Christoffel word if and only if it is a balanced Lyndon word.

Proof. See [1] Sec.4. □

This means Christoffel words are the finite balanced words in which the 0’s are placed 'as far as possible' to the left.
Definition. Let \( M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be a Sturmian matrix with determinant 1 and \( abcd \neq 0 \). We call the unique substitution \( \sigma \) that has \( M \) as incidence matrix and for which \( \sigma(0) \) and \( \sigma(1) \) are Christoffel words the Christoffel substitution corresponding to \( M \).

**Lemma 6.2.** Let \( \sigma \) be a substitution with \( \sigma(0), \sigma(1) \) Lyndon words, and \( \sigma(0) < \sigma(1) \) in the lexicographical order, and let \( u \) be a Lyndon word. Then \( \sigma(u) \) is a Lyndon word.

**Proof.** See [11]. \( \square \)

Let \( M \) be a matrix with determinant 1. \( M \) can be written in a unique way as the product of some occurrences of the matrices \( X_0 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \) and \( X_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). We associate to each occurrence of \( X_0 \) the substitution \( \psi_0 : \{ 0 \rightarrow 0, 1 \rightarrow 1 \} \) and to each occurrence of \( X_1 \) the substitution \( \psi_1 : \{ 0 \rightarrow 01, 1 \rightarrow 1 \} \). Let \( \sigma \) be the inverse product of the associated substitutions. It is clear that \( \psi_0 \) and \( \psi_1 \) are Sturmian substitutions, therefore \( \sigma \) is a Sturmian substitution. Hence \( \sigma(0) \) and \( \sigma(1) \) are balanced. Also it follows from Lemma 6.2 that they are Lyndon words. Now we conclude from Lemma 6.1 that \( \sigma \) is a Christoffel substitution.

Since for each matrix with determinant 1 and positive integer entries there exists a unique Christoffel substitution, we get the following result.

**Lemma 6.3.** Christoffel substitutions are Sturmian substitutions.

**Lemma 6.4.** Let \( M_\sigma \) be a Sturmian matrix with positive entries and determinant equal to 1 and let \( \sigma \) be the Christoffel substitution belonging to \( M_\sigma \). If \( M_\sigma \) is an upper matrix there exist possibly empty words \( u \) and \( v \) such that \( \sigma(0) = u0v \) and \( \sigma(1) = u1 \). If \( M_\sigma \) is a lower matrix there exist possibly empty words \( u \) and \( v \) such that \( \sigma(0) = u0v \) and \( \sigma(1) = (u0v)^k u1 \) for some positive integer \( k \).

**Proof.** If \( M_\sigma \) can be written as the product of two matrices \( X_0, X_1 \), we have either \( M_\sigma = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \), \( \sigma : \{ 0 \rightarrow 01, 1 \rightarrow 1 \} \) or \( M_\sigma = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \), \( \sigma : \{ 0 \rightarrow 01, 1 \rightarrow 01 \} \) and we see that the statement holds. Assume the statement of the lemma is true for incidence matrices that can be written as the product of \( n \) matrices \( X_0, X_1 \). Let \( M_\tau \) be a Sturmian matrix with positive entries and determinant equal to 1 that can be written as the product of \( n + 1 \) matrices \( X_0, X_1 \), and let \( \tau \) be the Christoffel substitution belonging
to $M_\tau$. Then $\tau = \sigma'\psi_0$ or $\tau = \sigma'\psi_1$, where $\sigma'$ is of the form stated in the lemma. It is easy to check that $\tau$ is also of this form. \qed

**Corollary 6.1.** Let $\sigma$ be a Christoffel substitution. Then $\sigma^n(0)$ is a Christoffel word for every $n > 0$.

**Proof.** Because according to Lemma 6.3 a Christoffel substitution is a Sturmian substitution, $\sigma^n(0)$ is balanced. It follows from Lemma 6.4 that $\sigma(0) < \sigma(1)$ in the lexicographical order, and applying Lemma 6.2 gives that $\sigma^n(0)$ is a Lyndon word. According to Lemma 6.1, $\sigma^n(0)$ is a Christoffel word. \qed

**Proposition 6.1.** Let $u$ be a Christoffel word, let $w' = w$ be the central block that we get after projecting the cutting segment of $u$, and let $v$ be the corresponding central word, as defined in Section 5. Then $v$ is a Christoffel word.

**Proof.** According to [1] Sec.4 the cutting segment of a Christoffel word lies below the line connecting the origin and the endpoint of the cutting segment. It follows that when the integer points on the cutting segment are projected parallel to this line, they all lie below the origin, except the origin which is projected to itself. Since Christoffel words are Sturmian words according to Lemma 6.3, there is no gap by Theorem 5.1. Hence the projected points form the word $w = w(0) \ldots w(|u| - 1)$ with $w(i) = i|u|^{-1} (\text{mod } |u|)$. Put $g = |u|^{-1} (\text{mod } |u|)$. Then

$$v(i) = 0 \iff w(i) < w(i + 1) \iff ig \mod |u| < (i + 1)g \mod |u|$$

and we see that $v$ is a Christoffel word containing $|u|^{-1} (\text{mod } |u|)$ ones. \qed

**Theorem 6.1.** Let $\sigma$ be a Christoffel substitution. Let $(v_n)$ be the words that we get by projecting the cutting segments of $u_n = \sigma^n(0)$ for $n > 0$. Then there exists a Christoffel substitution $\tau$ such that $\tau(v_n) = v_{n+1}$ for $n > 0$ and $\tau$ has $M_\tau$ as defined in Theorem 5.4 as incidence matrix.

**Proof.** It follows from the previous proposition that the words $(v_n)$ are Christoffel words. According to Theorem 5.4 the relation between the number of 0's and 1's in $v_n$ and $v_{n+1}$ is given by $M_\tau$. Define $\tau$ as the Christoffel substitution that has $M_\tau$ as incidence matrix. Because $\tau$ is Sturmian, $\tau(v_n)$ is a balanced word. Because $v_n$ is a Lyndon word, and $\tau$ is a Christoffel substitution with $\tau(0) < \tau(1)$ in the lexicographical order, $\tau(v_n)$ is also a Lyndon word. Thus $\tau(v_n)$ is a Christoffel word. Because there is only one Christoffel word of length $|v_{n+1}|$ that contains $|v_{n+1}|_0$ zeros, it follows that $\tau(v_n) = v_{n+1}$. \qed
Definition. Let $\sigma$ be a Christoffel substitution with incidence matrix $M_\sigma$ that is an upper matrix. Then we call $\tau$ as defined in Theorem 6.1 the dual substitution of $\sigma$.

Corollary 6.2. Let $\tau$ be the dual substitution of $\sigma$. Then $\sigma$ is the dual substitution of $\tau$.

Proof. Let $\sigma$ be a Christoffel substitution and let its incidence matrix be an upper matrix. It follows from Lemma 5.4 that $|v_0|_0 = 1$ and $|v_0|_1 = 0$. Hence according to Theorem 6.1 we have $v_n = \tau^n(0)$. It follows from Theorem 5.4 that $M_\tau$ is an upper matrix. Define $z_n$ as the central word that corresponds to $v_n$, as in Corollary 5.2 (note that the left most letter of $v_n$ is already at position 0, so that $v_n$ doesn’t have to be shifted to the right). Then it follows from this corollary and the fact that $\tau$ is a Christoffel substitution that $z_n = u_n$ for $n \in \mathbb{Z}_{\geq 0}$.

Example 5. The duality relation exists between the following pairs $\sigma$, $\tau$ of Christoffel substitutions.

- $\sigma : \begin{cases} 0 \to 0010101 \\
1 \to 01 \end{cases}$ and $\tau : \begin{cases} 0 \to 01011 \\
1 \to 011 \end{cases}$
- $\sigma : \begin{cases} 0 \to 0010101 \\
1 \to 01 \end{cases}$ and $\tau : \begin{cases} 0 \to 0110111 \\
1 \to 0111 \end{cases}$
- $\sigma : \begin{cases} 0 \to 0101111 \\
1 \to 0111 \end{cases}$ and $\tau : \begin{cases} 0 \to 0001001 \\
1 \to 01 \end{cases}$

The following Christoffel substitutions are self-dual (i.e. $\sigma = \tau$).

- $\sigma : \begin{cases} 0 \to 001 \\
1 \to 01 \end{cases}$
- $\sigma : \begin{cases} 0 \to 0001 \\
1 \to 001 \end{cases}$

The next lemma and theorem are thanks to a suggestion by Julien Cassaigne.

Lemma 6.5. Let $z = z_0z_1 \ldots z_n$ be a finite word with $z_i \in \{0, 1\}$. Put

\[
\begin{pmatrix} a & b \\
c & d \end{pmatrix} = X_{z_0}X_{z_1} \ldots X_{z_n}. \quad \text{Then} \quad X_{z_n} X_{z_{n-1}} \ldots X_{z_0} = \begin{pmatrix} d & b \\
c & a \end{pmatrix}.
\]

Proof. It is easy to check that this holds for $n = 0, 1$. Assume it holds for $n$. Let $z = z_0 \ldots z_{n+1}$ be given. Then $X_{z_0} \ldots X_{z_{n+1}} = \begin{pmatrix} a & b \\
c & d \end{pmatrix} X_{z_{n+1}}$. In case $z_{n+1} = 0$ we get $\begin{pmatrix} a + b & b \\
c + d & d \end{pmatrix}$ and in case $z_{n+1} = 1$ we get $\begin{pmatrix} a & a + b \\
c & c + d \end{pmatrix}$. In the same way we find $X_{z_{n+1}} \ldots X_{z_0}$ equals $\begin{pmatrix} d & b \\
c + d & a + b \end{pmatrix}$ in case $z_{n+1} = 0$. 
and \( \begin{pmatrix} c + d & a + b \\ c & a \end{pmatrix} \) in case \( z_{n+1} = 1 \). We see that the lemma also holds for \( n+1 \). \( \square \)

Let \( \sigma \) be a Christoffel substitution with incidence matrix \( M_\sigma \) that is an upper matrix. Hence there exists a finite word \( z = z_0 z_1 \ldots z_n \) so that \( \sigma = \psi z_0 \ldots \psi z_n \psi_1 \). If we write \( M_\sigma = \begin{pmatrix} a + c & b + d \\ c & a \end{pmatrix} \), we see that \( X_{z_n} \ldots X_{z_0} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Hence using the previous lemma we get \( X_{z_0} \ldots X_{z_n} = \begin{pmatrix} d & b \\ c & a \end{pmatrix} \).

We define the Christoffel substitution \( \phi = \psi z_n \ldots \psi z_0 \psi_1 \) and see that it has incidence matrix \( M_\phi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & b \\ c & a \end{pmatrix} = \begin{pmatrix} c + d & a + b \\ c & a \end{pmatrix} \). We find that \( M_\phi \) is the dual matrix of \( M_\sigma \) and hence \( \phi \) is the dual substitution of \( \sigma \). This gives the following theorem.

**Theorem 6.2.** Let \( \sigma \) be a Christoffel substitution with incidence an upper matrix, so that we can write \( \sigma = \psi z_0 \ldots \psi z_n \psi_1 \), with \( z_i \in \{0, 1\} \).

Then the dual substitution of \( \sigma \) equals \( \psi z_n \ldots \psi z_0 \psi_1 \).

**Example 5 (continued).** If we write the substitutions \( \sigma \) and \( \tau \) from Example 5 as products of \( \psi_0 \) and \( \psi_1 \) we get the following pairs of substitutions.

- \( \sigma = \psi_0 \psi_1 \psi_1 \) and \( \tau = \psi_1 \psi_0 \psi_1 \)
- \( \sigma = \psi_1 \psi_0 \psi_0 \psi_1 \) and \( \tau = \psi_0 \psi_0 \psi_1 \psi_1 \)
- \( \sigma = \tau = \psi_0 \psi_1 \)
- \( \sigma = \tau = \psi_0 \psi_0 \psi_1 \)

**Acknowledgements.** We like to thank Robert Tijdeman and the referee for valuable remarks and suggestions.

**References**


Sierk W. Rosema
Mathematical Institute
Leiden University
P.O. Box 9512, 2300 RA Leiden
The Netherlands
*E-mail: swrosema@math.leidenuniv.nl*