On the number of squares in a finite word

S. Brlek¹ and S. Li¹

Laboratoire de Combinatoire et d’Informatique Mathématique, Université du Québec à Montréal,
CP 8888 Succ. Centre-ville, Montréal (QC) Canada H3C 3P8
brlek.srecko@uqam.ca, shuo.li@lacim.ca

Abstract. A square is a word of the form uu. In this paper we prove that for a given finite word w, the number of distinct square factors of w is bounded by |w| − |Alph(w)| + 1, where |w| denotes the length of w and |Alph(w)| denotes the number of distinct letters in w. This result answers a conjecture of Fraenkel and Simpson stated in 1998.

1 Introduction

The study of patterns in a word is related to several topics and it has various applications in several research domains, ranging from practical applications to theoretical considerations. Among these patterns, we can mention palindromes and repetitions such as squares, cubes, periods, overlaps, etc. They appear in different contexts in computer science such as data compression (LZW overlap), searching algorithms, structure of indexes [11], digital geometry [4], in number theory about Diophantine approximation and transcendence statements [1], and in physics in connection with Schrödinger operators [2], among several others.

Palindromic complexity has received noticeable attention and a comprehensive survey was provided by Allouche et al. [2]. In particular, Droubay, Justin and Pirillo established that the number of distinct palindromic factors of a word is bounded by its length plus one and that finite Sturmian (and even episturmian) words realize it [5].

For the square factors the situation seems to be significantly harder to handle. Indeed, Fraenkel and Simpson conjectured in [8] that the number of distinct non-empty squares of a finite word w is bounded by its length |w| and they proved that this number is bounded by 2|w|. After that Ilie [9] strengthened this bound to 2|w| − Θ(log(|w|)); Lam [10] improved this result to 35|w|; Deza, Franek and Thierry [5] achieved a bound of 113|w|; Thierry [13] refined this bound to 2/3|w|.

We remark that the Fraenkel and Simpson’s conjecture implies that the square complexity of a finite word is also bounded by its length plus one by counting the empty word. In this article, we prove the following theorem:

Theorem 1 For any finite word w, let S(w) denote the number of its distinct square factors, |w| denote the length of w and |Alph(w)| denote the number of

* with the support of NSERC (Canada)
distinct letters in \( w \), then we have
\[
S(w) \leq |w| - |\text{Alph}(w)| + 1.
\]

This result is a stronger version of the conjecture of Fraenkel and Simpson stated in [5].

The strategy of the proof is as follows: for a given word \( w \), we first recall the definition of Rauzy graph and define small circuits in it; we then prove that the total number of small circuits in the union of the Rauzy graphs of \( w \) is bounded by \(|w| - |\text{Alph}(w)|\); finally we conclude by proving that there exists an injection from the set of distinct nonempty squares of \( w \) to the set of small circuits in the union of the Rauzy graphs of \( w \).

2 Preliminaries

Let us recall the basic terminology about words. By \textit{word} we mean a finite concatenation of symbols \( w = w_1w_2\cdots w_n \), with \( n \in \mathbb{N} \). The \textit{length} of \( w \), denoted \(|w|\), is \( n \) and we say that the symbol \( w_i \) is at the \textit{position} \( i \). The set \( \text{Alph}(w) = \{w_i | 1 \leq i \leq n\} \) is called the \textit{alphabet} of \( w \) and its elements are called \textit{letters}. Let \(|\text{Alph}(w)|\) denote the cardinality of \( \text{Alph}(w) \). A word of length 0 is called the \textit{empty word} and it is denoted by \( \epsilon \). For any word \( u \), we have \( u = \epsilon u = u \epsilon \).

A word \( u \) is called a \textit{factor} of \( w \) if \( w = pus \) for some words \( p, s \). The set of all factors of \( w \) is denoted by \( \text{Fac}(w) \). For any integer \( i \) satisfying \( 1 \leq i \leq |w| \), let \( L_w(i) \) be the set of all length-\( i \) factors of \( w \) and let \( C_w(i) \) denote the cardinality of \( L_w(i) \).

Two finite words \( u \) and \( v \) are \textit{conjugate} when there exist words \( x, y \) such that \( u = xy \) and \( v = yx \). The conjugacy class of a word \( w \) is denoted by \([w]\). Let \( w = w_1w_2\cdots w_t \) be a finite word, for any integer \( i \) satisfying \( 1 \leq i \leq t \), let us define \( w_s(i) = w_iw_{i+1}\cdots w_t \) and \( w_p(i) = w_1w_2\cdots w_{i-1} \) and let \( w_s(1) = w \) and \( w_p(1) = \epsilon \). Thus, \([w] = \{w(i)|w(i) = w_s(i)w_p(i), i = 1, 2, \ldots t\} \).

For any natural number \( k \), we define the \( k \)-power of a finite word \( u \) to be the concatenation of \( k \) copies of \( u \), and it is denoted by \( u^k \). Particularly, a \textit{square} is a word \( w \) of the form \( w = uu \). A word \( w \) is said to be \textit{primitive} if it is not a power of another word. Let \( \text{Prim}(w) \) denote the set of primitive factors of \( w \). For any word \( u \) and any rational number \( \alpha \), the \( \alpha \)-power of \( u \) is defined to be \( u^\alpha \) where \( u_0 \) is a prefix of \( u \), \( a \) is the integer part of \( \alpha \), and \(|u^au_0| = \alpha |u| \). The \( \alpha \)-power of \( u \) is denoted by \( u^\alpha \). Let \( \alpha \) be a positive rational number larger than 1, the word \( w \) is said to be of the \textit{period} \( \alpha \) if there exists a word \( u \) such that \( w = u^\alpha \).

Here we recall some basic lemmas concerning repetitions:

\textbf{Lemma 1 (Fine and Wilf [7]).} Let \( w \) be a word having \( k \) and \( l \) for periods. If \(|w| \geq k + l - \gcd(k, l)\) then \( \gcd(k, l) \) is also a period of \( w \).
Lemma 2 (Lyndon and Schützenberger [12]). Let $x$ and $y$ be two words such that $xy = yx$. Then there exist a primitive $p$ and two non-negative integers $i, j$ such that $x = p^i$ and $y = p^j$.

Lemma 3 (Lyndon and Schützenberger [12]). Let $x, y, z$ be three words such that $xy = yz$ and $|y| \neq 0$. Then there exist two words $u, v$ with $|u| \neq 0$ and some positive integer $i$ such that $x = uv, y = (uv)^i u, z = vu$.

Here we recall some elementary definitions and properties concerning graphs from Berge [3].

A (non-oriented) graph consists of a nonempty set of vertices $V$ and a set of edges $E$. A vertex $a$ represents an endpoint of an edge and an edge joins two vertices $a, b$. A chain is a sequence of edges $e_1, e_2, \ldots, e_k$, in which each edge $e_i$ $(1 < i < k)$ has one vertex in common with $e_{i-1}$ and the other vertex in common with $e_{i+1}$. A cycle is a finite chain which begins with a vertex $x$ and ends at the same vertex. A graph is called connected if for any couple of vertices $a, b$ in this graph, there exists a chain which begins at $a$ and ends at $b$.

A graph is called oriented if its edges are oriented from one endpoint to the other. An oriented graph is called weakly connected if it is connected as a non-oriented graph.

Let $G$ be a connected graph and let $\{e_1, e_2, \ldots, e_l\}$, $\{v_1, v_2, \ldots, v_k\}$ denote respectively the edge set and the vertex set of $G$. The number $\chi(G) = l - s + 1$ is called the cyclomatic number of $G$.

Let $C$ be a cycle in $G$. A vector $\mu(C) = (e_1, e_2, \ldots, e_l)$ in the $l$-dimensional space $\mathbb{R}^l$ is called the vector-cycle corresponding to $C$ if $e_i$ is the number of visits of the edge $e_i$ in the cycle $C$ for all $i$ satisfying $1 \leq i \leq l$. The cycle $C_1, C_2, \ldots, C_k, \ldots$ are said to be independent if their corresponding vectors are linearly independent.

Lemma 4 (Theorem 2, Chapter 4 in [3]). the cyclomatic number of a graph is the maximum number of independent cycles in this graph.

3 Rauzy graph and small circuits

We first recall the definition of Rauzy graph. Let $w$ be a word of length $k$. For any integer $n$ such that $1 \leq n \leq k$, let the Rauzy graph $\Gamma_n(w)$ be an oriented graph whose set of vertices is $L_w(n)$ and the set of edges is $L_w(n+1)$; an edge $e \in L_w(n+1)$ starts at the vertex $u$ and ends at the vertex $v$, if $u$ is a prefix and $v$ is a suffix of $e$. We remark that $\Gamma_n(w)$ is a weakly connected graph for any $n$.

Let us define $\Gamma(w) = \bigcup_{n=1}^k \Gamma_n(w)$.

Let $\Gamma(w)$ be a Rauzy graph of $w$. A sub-graph in $\Gamma(w)$ is called an elementary circuit if there are $j$ distinct vertices $v_1, v_2, \ldots, v_j$ and $j$ distinct edges $e_1, e_2, \ldots, e_j$ for some integer $j$, such that for each $k$ with $1 \leq k \leq j - 1$, the edge $e_k$ starts at $v_k$ and ends at $v_{k+1}$, and for the edge $e_j$, it starts at $v_j$ and ends at $v_1$, further, $j$ is called the size of the circuit. We let this circuit be denoted by
The small circuits in the graph $\Gamma_i(w)$ are those elementary circuits whose sizes are no larger than $i$.

**Lemma 5.** Let $w$ be a finite word and let $\Gamma_r(w)$ be a Rauzy graph of $w$ for some $r$. Then for any small circuit $C$ on $\Gamma_r(w)$, there exists a unique primitive word $q$, up to conjugacy, such that $|q| \leq r$ and the vertex set of $C$ is $\{p^{|p|}|p \in [q]\}$ and its edge set is $\{p^{r-|p|}+1|p \in [q]\}$.

**Proof.** Let $C$ be a small circuit on $\Gamma_r(w)$ of size $l$, then it contains $l$ distinct vertices, say $v_1, v_2, ..., v_l$, and $l$ distinct edges, say $e_1, e_2, ..., e_l$. For each $i$ satisfying $1 \leq i \leq l$, let us define $p_i$ to be a word by concatenating consecutively the last letter of words $e_i, e_{i+1}, ..., e_{i+l-1}$ with $e_r = e_{r-l}$ if $r \geq l+1$. The words $p_1, p_2, ..., p_l$ are pairwisely conjugate. Further, for each $i$ satisfying $1 \leq i \leq l$, from the fact that the edges in the order of $e_i, e_{i+1}, ..., e_{i+l-1}$ form a circuit, we can deduce that $v_i$ is a suffix of $v_i p_i$. Thus, there exists a word $p'_i$ of length $l$ such that $v_i p_i = p'_i v_i$. From Lemma 3 there exists two words $u_i, t_i$ with $|u_i| \neq 0$ and a nonnegative integer $j$ such that $p'_i = u_i t_i, p_i = t_i u_i$ and $v_i = (u_i t_i)^j u_i$. Consequently, $v_i = (p'_i)^j$. Further, as $p'_i$ and $p_i$ are conjugate, the words $p'_1, p'_2, ..., p'_l$ are also pairwisely conjugate. Thus, the vertex set of $C$ is $\{p^{|p|}|p \in [p_1]\}$ and its edge set is $\{p^{r-|p|}+1|p \in [p_1]\}$.

Here we prove the primitivity of $p_1$. If $p_1$ is not primitive, then there are two distinct integers $r, s$ satisfying $1 \leq r, s \leq l$ such that $p'_r = p'_s$, and further, $v_r = v_s$. This contradicts the hypothesis that $C$ contains $l$ distinct vertices.

From the previous lemma, each small circuit can be uniquely identified by two parameters: a primitive word $p$ defined in the lemma and an integer $i$ such that $\Gamma_w(i)$ is the Rauzy graph in which the circuit is located. Let all small circuits be denoted by $C(p, i)$ with the parameters defined as above.

**Example 6.** Let us consider the word $u = aababa$, here we draw $\Gamma_u(1), \Gamma_u(2), \Gamma_u(3)$ as follows:
We conclude.

Let us consider two other conjugates of \( q \) to prove that \( (p) \) exists a prefix \( \{a, b\} \) and \( \{ab, ba\} \). With the notation defined as above, these circuits are denoted respectively by \( C(a, 1), C(ab, 2) \) and \( C(ab, 3) \). We remark that, in \( \Gamma(u) \), there exists a circuit \( \{a, b\} \) which is not small.

Let \( \prec \) be a lexicographic order over \( \text{Fac}(w) \), for a given small circuit, let us define the maximal edge of this circuit to be the lexicographically greatest element in its edge set.

**Lemma 7.** Each small circuit contains exactly one maximal edge. Further, the maximal edges of the small circuits in the same Rauzy graph are pairwisely distinct.

**Proof.** From Lemma 5, the edge set of any small circuit is of the form \( \{p' | p \in [q]\} \) such that \( t > 1 \) and \( q \) is primitive. Thus, \( u' \) is the lexicographically greatest element in \( \{p' | p \in [q]\} \) if and only if \( u \) is the lexicographically greatest element in \( [q] \). Hence the maximal edge of each small circuit is unique.

For the second part, let us suppose that \( v \) is the maximal edge of two distinct small circuits \( C(p, r) \) and \( C(q, r) \). From Lemma 5, there are two positive integers \( i \geq 1, j \geq 1 \) and two words \( p', q' \) which are respectively a prefix of \( p, q \) such that \( v = p'^j = q'^j \), where \( p', q' \) can be \( \varepsilon \). First we state that \( |p'| \neq |q'| \). Otherwise, \( p' = q' \). However, in this case, from Lemma 4, \( p \) and \( q \) can not be both primitive. Without loss of generality, let us suppose \( |p'| > |q'| \), thus \( |p^i| < |q^i| \). Then there exists a prefix \( p'' \) of \( p \) such that \( |p''| < |p| \) and \( q^j = p'' p'' \). However, \( p'' \) is also a prefix of \( p' \). Thus, there exists a word \( w \) such that \( q^j = p'' wp'' \) and \( p' = p'' wp'' \).

Now let us prove that \( v \) cannot be the maximal edge of \( C(q, r) \). It is enough to prove that \( q^j = p'' wp'' \) is not the lexicographically greatest element in \([q^j]\). Let us consider two other conjugates of \( q^j \): \((p'')^2 w \) and \( w(p'')^2 \). We claim that \((p'')^2 w \neq p'' wp'' \). Otherwise, from Lemma 2, there exists a primitive \( a \) and two positive integers \( t_2 > t_1 > 0 \) such that \( p'' = a^{t_1}, p'' w = a^{t_2} \). However, in this case, \( p' = p'' w = a^{t_2} \) and \( |a| < |p| \). Once more from Lemma 4, \( p \) and \( a \) can not be both primitive. If \((p'')^2 w < p'' wp'' \), then \( p'' w < wp'' \), but if so, \( p'' wp'' < w(p'')^2 \). We conclude.

Now let us define the Circuit Arrangement Order \( \prec_{\text{CAO}} \) for the small circuits on \( \Gamma(w) \). Let \( C_1 \) and \( C_2 \) be two small circuits in a same Rauzy graph \( \Gamma(w) \),

There are three small circuits in these graphs: \( \{\{a\}, \{aa\}\}, \{\{ab, ba\}, \{aba, bab\}\} \) and \( \{\{aba, bab\}, \{abab, bab\}\} \) with the notation defined as above, these circuits are denoted respectively by \( C(a, 1), C(ab, 2) \) and \( C(ab, 3) \). We remark that, in \( \Gamma(u) \), there exists a circuit \( \{a, b\} \) which is not small.

Let \( \prec \) be a lexicographic order over \( \text{Fac}(w) \), for a given small circuit, let us define the maximal edge of this circuit to be the lexicographically greatest element in its edge set.

**Lemma 7.** Each small circuit contains exactly one maximal edge. Further, the maximal edges of the small circuits in the same Rauzy graph are pairwisely distinct.

**Proof.** From Lemma 5, the edge set of any small circuit is of the form \( \{p' | p \in [q]\} \) such that \( t > 1 \) and \( q \) is primitive. Thus, \( u' \) is the lexicographically greatest element in \( \{p' | p \in [q]\} \) if and only if \( u \) is the lexicographically greatest element in \( [q] \). Hence the maximal edge of each small circuit is unique.

For the second part, let us suppose that \( v \) is the maximal edge of two distinct small circuits \( C(p, r) \) and \( C(q, r) \). From Lemma 5, there are two positive integers \( i \geq 1, j \geq 1 \) and two words \( p', q' \) which are respectively a prefix of \( p, q \) such that \( v = p'^j = q'^j \), where \( p', q' \) can be \( \varepsilon \). First we state that \( |p'| \neq |q'| \). Otherwise, \( p' = q' \). However, in this case, from Lemma 4, \( p \) and \( q \) can not be both primitive. Without loss of generality, let us suppose \( |p'| > |q'| \), thus \( |p^i| < |q^i| \). Then there exists a prefix \( p'' \) of \( p \) such that \( |p''| < |p| \) and \( q^j = p'' p'' \). However, \( p'' \) is also a prefix of \( p' \). Thus, there exists a word \( w \) such that \( q^j = p'' wp'' \) and \( p' = p'' wp'' \).

Now let us prove that \( v \) cannot be the maximal edge of \( C(q, r) \). It is enough to prove that \( q^j = p'' wp'' \) is not the lexicographically greatest element in \([q^j]\). Let us consider two other conjugates of \( q^j \): \((p'')^2 w \) and \( w(p'')^2 \). We claim that \((p'')^2 w \neq p'' wp'' \). Otherwise, from Lemma 2, there exists a primitive \( a \) and two positive integers \( t_2 > t_1 > 0 \) such that \( p'' = a^{t_1}, p'' w = a^{t_2} \). However, in this case, \( p' = p'' w = a^{t_2} \) and \( |a| < |p| \). Once more from Lemma 4, \( p \) and \( a \) can not be both primitive. If \((p'')^2 w < p'' wp'' \), then \( p'' w < wp'' \), but if so, \( p'' wp'' < w(p'')^2 \). We conclude.
we define $C_1 \prec_{C_{AO}} C_2$ if $e_1 \prec e_2$, where $e_i$ is the maximal edge of the cycle $C_i$. From Lemma 7 the small circuits in the same Rauzy graph are well-ordered under $\prec_{C_{AO}}$.

**Lemma 8.** Let $w$ be a finite word and let $\Gamma_r(w)$ be a Rauzy graph of $w$ for some $r$. Then the small circuits in $\Gamma_r(w)$ are independent.

**Proof.** Let $C_1, C_2, \ldots, C_k$ be the small circuits in $\Gamma_r(w)$ satisfying

$$C_1 \prec_{C_{AO}} C_2 \prec_{C_{AO}} \cdots \prec_{C_{AO}} C_k.$$

If there exist some real numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $\sum_{i=1}^k \alpha_i \mu(C_i) = 0$, where $\mu(C_i)$ is the vector-cycle corresponding to $C_i$, then we claim that $\alpha_k = 0$. In fact, if we let $e(C_k)$ be the maximal edge of $C_k$, then from Lemma 7 the coefficient $c(C_k)$ in $\mu(C_i)$ is 1 if $i = k$ and 0 if $i < k$. Thus, $\alpha_k = 0$. Doing this argument recurrently, we prove that $\alpha_i = 0$ for all $i$. Consequently, $C_1, C_2, \ldots, C_k$ are independent.

**Example 9.** Let us consider the word $v = abaaabaabaaaba$, the $\Gamma_5(v)$ is drown as follows:

![Diagram](attachment:image.png)

In this graph, there exist three small circuits: $C(aaaba, 5)$, $C(aaab, 5)$, $C(abaa, 5)$. If we define $b \prec a$, the maximal edges of these circuits are respectively $aaaba$, $aaabaa$ and $aabaab$. We can check that $aaaba$ is only in $C(aaaba, 5)$ and $aabaab$ is only in $C(abaa, 5)$, thus, the three circuits in the graph are independent.
Lemma 10. Let \( w \) be a finite word, then for any Rauzy graph \( \Gamma_r(w) \), the number of small circuits in this graph, which is denoted by \( sc_r \), satisfies that

\[
sc_r \leq C_w(r + 1) - C_w(r) + 1.
\]

Proof. It is a direct consequence of Lemma 4, Lemma 8 together with the facts that \( \Gamma_r(w) \) is weakly-connected and the number of edges and vertices in \( \Gamma_r(w) \) are respectively \( C_w(r + 1) \) and \( C_w(r) \).

Lemma 11. Let \( w \) be a finite word, then the total number of small circuits on \( \Gamma(w) \) is bounded by \( |w| - |\text{Alph}(w)| \).

Proof. Let \( sc(w) \) denote the total number of small circuits on \( \Gamma(w) \), then from the previous lemma, we have:

\[
sc(w) = \sum_{i=1}^{|w|} sc_i \\
\leq \sum_{i=1}^{|w|} C_w(i + 1) - C_w(i) + 1 \\
\leq |w| + C_w(|w| + 1) - C_w(1) \\
\leq |w| - |\text{Alph}(w)|.
\]

4 Injection from nonempty squares to small circuits

Let \( w \) be a finite word. For any square \( u^2 \in \text{Fac}(w) \), there exists a primitive word \( v \in \text{Prim}(w) \) and a positive integer \( n \) such that \( u^2 = v^{2n} \). Thus, we can gather the squares in terms of their smallest period. Let \( v \in \text{Prim}(w) \), a square \( u^2 \in \text{Fac}(w) \) is called in the class of \( v \) if there is a primitive word \( t \in [v] \) and a positive integer \( n \) such that \( u^2 = t^{2n} \). Let \( \text{Class}(v) \) be the set of all squares in the class of \( v \). Two classes \( \text{Class}(u) \) and \( \text{Class}(v) \) are equal only if \( u \) and \( v \) are conjugate.

Now, given a class \( \text{Class}(v) \), let us define its index to be an integer \( \text{Index}(v) \) such that \( \text{Index}(v) = \max \{ n | n \in \mathbb{N}^+, \exists u \in [v], \text{such that } u^{2n} \in \text{Fac}(w) \} \). Without loss of generality, a class is denoted by \( \text{Class}(v) \) if \( v \) is a primitive such that \( v^{2n} \) is in the class where \( n \) is the index of this class. In other words, \( v^{2\text{Index}(v)} \in \text{Class}(v) \). From the definition, the elements in \( \text{Class}(v) \) are all of the form \( v_s(i) v^{2j-1} v_p(i) \) with \( 1 \leq i \leq |v| \) and \( 1 \leq j \leq \text{Index}(v) \), let \( v(i,j) \) denote the square \( v_s(i) v^{2j-1} v_p(i) \).

Example 12. Let \( r = abcabcabcabca \). The squares \( (abc)^2, (bca)^2, (cab)^2, (abc)^4, (bca)^4 \) are in the same class. The index of this class is 4 and this class can be denoted by \( \text{Class}(abc) \) or \( \text{Class}(bca) \). However, it cannot be denoted by \( \text{Class}(cab) \), because \( (cab)^4 \notin \text{Fac}(r) \).
Lemma 13. Let $v$ be a primitive factor of a finite word $w$ such that $|v| = l$ and that $\text{Class}(v)$ is nonempty. If $\text{Index}(v) \geq 2$, then for any couple of integers $(i, j)$ satisfying $1 \leq i \leq l$ and $1 \leq j \leq \text{Index}(v)$, there exists a small circuit $C(v, jl + i - 1)$ in $\Gamma_{j+1}(w)$. Further, there exists an injective function $f_v$ which associates each square $v(i, j)$ in $\text{Class}(v)$ to the small circuit $C(v, jl + i - 1)$ in \{ $C(v, jl + i - 1) | 1 \leq i \leq l, 1 \leq j \leq \text{Index}(v)$ \}.

Proof. For a given couple of integers $(i, j)$, it is enough to prove that

$$\left\{ u^{1+i} | u \in [v] \right\} \subset \text{Fac}(w).$$

If it is the case, then there exists a circuit in $\Gamma_u (jl + i - 1)$ such that its edge set is $\left\{ u^{1+i} | u \in [v] \right\}$, further, it can be identified by $C(v, jl + i - 1)$. From the hypothesis that $\text{Index}(v) \geq 2$ and $v^{\text{Index}(v)} \in \text{Fac}(w)$, we have $v^{i+2} \in \text{Fac}(w)$ for all $j$ satisfying $1 \leq j \leq \text{Index}(v)$ and easily check that $\left\{ u^{1+i} | u \in [v] \right\} \subset \text{Fac}(v^{i+2})$.

The injectivity of the function is from the fact that the circuits $C(v, jl + i - 1)$ are pairwisely distinct. In fact, if there are two pairs of integers $(j_1, i_1), (j_2, i_2)$ satisfying $1 \leq i_1, i_2 \leq l, j_1 \geq j_2$ and $j_1l + i_1 - 1 = j_2l + i_2 - 1$, then $(j_1 - j_2)l = i_1 - i_2$. However, $i_1 - i_2 < l$, hence $0 \leq j_1 - j_2 < 1$. Thus, $j_1 = j_2$ and $i_1 = i_2$.

Lemma 14. Let $v$ be a primitive factor of a finite word $w$ such that $|v| = l$ and that the size of $\text{Class}(v)$ is $t$. If $\text{Index}(v) = 1$, then for each integer $i$ such that $1 \leq i \leq t$, there exists a small circuit $C(v, l + i - 1)$ in $\Gamma_{i+1}(w)$. Thus, there exists a bijective function $f_v$ which associates each square in $\text{Class}(v)$ to one of the small circuits in \{ $C(v, l + i - 1) | 1 \leq i \leq t$ \}.

Proof. It is enough to prove that for any positive integer $i$ satisfying $1 \leq i \leq t$,

$$S_i = \left\{ u^{1+i} | u \in [v] \right\} \subset \text{Fac}(w).$$

If so, there exists a circuit in $\Gamma_{i+1}(w)$ such that its edge set is exactly $S_i$. Let us first consider the elements in $\text{Class}(v)$. Under the hypothesis that $\text{Index}(v) = 1$, the elements in $\text{Class}(v)$ are all conjugates of $v^2$, thus they are all of the form $v_s(j)v_p(j)$ for some $j$. Consequently, the size of $\text{Class}(v)$ is no larger than the number of conjugates of $v$, thus, $t \leq l$. Now let us consider the elements in $S_i$.

For any given $i$ satisfying $1 \leq i \leq t$ and any $u^{1+i} \in S_i$, there exists a couple of integers $(r, s)$ satisfying $s \equiv r + i \pmod{l}$ and $u^{1+i} = v_s(r)v_p(s)$. For any $v_s(j)v_p(j) \in \text{Class}(v)$, a word $v_s(r)v_p(s) \in S_i$ is not a factor of $v_s(j)v_p(j)$ if and only if $s < j < r$. Further, from the relation $s \equiv r + i \pmod{l}$, we have $r - s = i$. Thus, for any $v_s(r)v_p(s) \in S_i$, there are at most $i - 1$ distinct words $v_s(j)v_p(j) \in \text{Class}(v)$ which do not contain $v_s(r)v_p(s)$ as a factor. However, from the hypothesis, there are exactly $t \geq i$ elements in $\text{Class}(v)$. Hence there exists at least one word in $\text{Class}(v)$ such that $v_s(r)v_p(s)$ is a factor of this word. Thus, all elements in $S_i$ are factors of $w$. 

S. Brlek, S. Li
Lemma 15. There exists an injective function \( f \) from the set of nonempty squares of \( w \) to the set of small circuits in \( \Gamma(w) \).

Proof. Let us consider the function \( f \) satisfying that for any \( \text{Class}(v) \),

\[ f|\text{Class}(v) = f_v, \]

with \( f_v \) defined in the previous lemmas. Here we prove that this function is injective. If \( C(p, i) \) and \( C(q, j) \) are two images of two squares under \( f \) such that \( C(p, i) = C(q, j) \), from Lemma 5, \( p = q \) and \( i = j \). However, if \( p = q \), the pre-image of these two circuits are in the same class, and from the previous lemmas, the function \( f \) over a class is injective. Thus, these two squares are the same. Hence \( f \) is injective.

Proof (of Theorem 1). From Lemma 15 and Lemma 11, the number of distinct nonempty squares, \( S(w) - 1 \), satisfies the equation

\[ S(w) - 1 \leq \text{sc}(w) \leq |w| - |\text{Alph}(w)|. \]

Example 16. Let us consider the word \( w = baababaabbbabbabbbbab \). We can check that \( |w| = 22 \) and there are 14 squares in \( w \):

\( \varepsilon, aa, bb, abab, baba, abab, abab, babbbabb, bbabbbab, baababaaba, aababaabab, bababbabbbab, \)

The nonempty squares are distributed in 8 classes. In the following table we list these classes and their sizes:

| Class | a | b | ab | aba | abb | babb | baaba | babbbab |
|-------|---|---|----|-----|-----|------|-------|---------|
| size  | 1 | 1 | 2  | 1   | 3   | 2    | 2     | 1       |

The images of these squares under the injection \( f \) are listed as follows:

\( C(a, 1), C(b, 1), C(ab, 2), C(ab, 3), C(aba, 3), C(abb, 3), C(abb, 4), C(abb, 5), C(babba, 5), C(baaba, 6), C(babbbab, 7). \)

The Rauzy graphs of \( w \) from \( \Gamma_w(1) \) to \( \Gamma_w(7) \) are provided in Appendix.

References

1. Adamczewski, B., Allouche, J.P.: Reversals and palindromes in continued fractions. Theoretical Computer Science 380(3), 220–237 (2007)
2. Allouche, J.P., Baake, M., Cassaigne, J., Damanik, D.: Palindrome complexity. Theoretical Computer Science 292(1), 9–31 (2003)
3. Berge, C.: The Theory of Graphs and Its Applications. Greenwood Press (1982)
4. Blondin Massé, A., Garon, A., Labbé, S.: Combinatorial properties of double square tiles. Theoretical Computer Science 502, 98–117 (2013)
5. Deza, A., Franek, F., Thierry, A.: How many double squares can a string contain? Discrete Applied Mathematics 180, 52–69 (2015)
6. Droubay, X., Justin, J., Pirillo, G.: Episturmian words and some constructions of de Luca and Rauzy. Theoretical Computer Science 255(1-2), 539–553 (2001)
7. Fine, N.J., Wilf, H.S.: Uniqueness theorems for periodic functions. Proceedings of the American Mathematical Society 16(1), 109–114 (1965)
8. Fraenkel, A.S., Simpson, J.: How many squares can a string contain? J. Comb. Theory, Ser. A 82(1), 112–120 (1998)
9. Ilie, L.: A note on the number of distinct squares in a word. In: Brlek, S., Reutenauer, C. (eds.) Proc. Words2005, 5-th International Conference on Words. vol. 36, pp. 289–294. Publications du LaCIM, Montreal, Canada (13–17 Sep 2005)
10. Lam, N.H.: On the number of squares in a string. AdvOL-Report 2 (2013)
11. Lothaire, M.: Applied Combinatorics on Words. Cambridge University Press, Cambridge (2005)
12. Lyndon, R.C., Schützenberger, M.P.: The equation $a^M = b^N c^P$ in a free group. Michigan Mathematical Journal 9(4), 289 – 298 (1962)
13. Thierry, A.: A proof that a word of length $n$ has less than $1.5n$ distinct squares (2020)
5 Appendix: graphs of $w = baababaabbbabbbab$  

Here we draw the Rauzy graphs of $w$ from $\Gamma_w(1)$ to $\Gamma_w(7)$, they are all the Rauzy graphs containing small cycles.
