Available online at www.sciencedirect.com
ScienceDirect
Theoretical Computer Science 380 (2007) 377–387
Theoretical Computer Science
www.elsevier.com/locate/tcs

Transposition invariant words

Arto Lepistö[a], Francesco Pappalardi[b], Kalle Saari[a,c,*]

[a] *Department of Mathematics, University of Turku, 20014 Turku, Finland*
[b] *Dipartimento di Matematica, Universita' degli studi Roma TRE, Largo S. L. Murialdo, 1, I-00146, Rome, Italy*
[c] *Turku Centre for Computer Science, University of Turku, 20014 Turku, Finland*

Abstract

We define an operation called transposition on words of fixed length. This operation arises naturally when the letters of a word are considered as entries of a matrix. Words that are invariant with respect to transposition are of special interest. It turns out that transposition invariant words have a simple interpretation by means of elementary group theory. This leads us to investigate some properties of the ring of integers modulo n and primitive roots. In particular, we show that there are infinitely many prime numbers p with a primitive root dividing $p+1$ and infinitely many prime numbers p without a primitive root dividing $p+1$. We also consider the orbit of a word under transposition.

Keywords: Transposition invariant words; Partition generated by a subgroup; Primitive roots; Favorable prime numbers

1. Introduction

Let us consider a word w of length pq where p and q are positive integers. Construct a $p \times q$ matrix A by filling the entries with consecutive letters of w row by row, and then transpose it. The entries of A^{T} read row by row correspond to another word, which we will denote by w^{T}. The process of transposing a word to obtain a new word is the inspiration of this paper. If w is invariant with respect to the transposition, we express this by saying that w is $p \times q$-invariant. Words that are $p \times q$-invariant for every appropriate p and q are called *transposition invariant*. These words are the main topic and inspiration of this paper.

In Section 2 we introduce the formal definitions and give some examples. Section 3 contains some introductory results, such as the fact that the power-of-2 length prefixes of the infinite Thue–Morse word are transposition invariant. We also show that any word with at least two different letters can be extended periodically so that the resulting word is nontrivially transposition invariant. In Section 4 we switch to a more number theoretic aspect of the topic and give a characterization of transposition invariant words. Section 5 considers two questions: How many distinct letters can a transposition invariant word have? How long an orbit does a word travel when we iterate the transposition operation with respect to a fixed $p \times q$ matrix? The last part of this paper, Section 6, considers primitive roots modulo a prime

* Corresponding author at: Department of Mathematics, University of Turku, 20014 Turku, Finland.
E-mail addresses: alepisto@utu.fi (A. Lepistö), pappa@mat.uniroma3.it (F. Pappalardi), kasaar@utu.fi (K. Saari).

0304-3975/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2007.03.029

number. Namely, the characterization of transposition invariant words gives rise to a classification of prime numbers into two disjoint sets that we call favorable and unfavorable prime numbers. We show that both sets are infinite.

2. Definitions

Let $w = w_0 w_1 \cdots w_n$ be a word, that is, a string of symbols over some alphabet Σ. The length of w is denoted by $|w|$, so that $|w| = n + 1$. Assume then that $|w| = n + 1 = pq$ for some integers $p, q > 0$, and consider the $p \times q$ matrix

$$A = \begin{pmatrix} w_0 & w_1 & \cdots & w_{q-1} \\ w_q & w_{q+1} & \cdots & w_{2q-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{(p-1)q} & w_{(p-1)q+1} & \cdots & w_{pq-1} \end{pmatrix}.$$

By reading the entries of this matrix row by row starting from the upper left corner, we obtain the word w. When reading the entries column by column, we get another word

$$w^{\mathrm{T}} = w_0 w_q \cdots w_{(p-1)q}\, w_1 w_{q+1} \cdots w_{(p-1)q+1} \cdots w_{q-1} w_{2q-1} \cdots w_{pq-1}.$$

Equivalently, we obtain w^{T} by reading the entries in the transpose matrix A^{T} row by row.

If $w^{\mathrm{T}} = w$, we say that w is *$p \times q$-invariant*. The word w is *transposition invariant* if it is $p \times q$-invariant for all integers $p, q > 0$ such that $pq = |w|$. If the subword $w_1 w_2 \cdots w_{n-1}$ of w is unary or if $|w|$ is a prime number, then w is trivially transposition invariant. In the former case, we say that w is *trivial*.

The Finnish word *möhömahat* – the people with a big belly – is a 3×3-invariant word. Examples of the same length in English are *Malayalam* and *votometer*. Note that, as 9 has only one proper factorization, $3 \cdot 3$, these words are transposition invariant. A more complicated instance of transposition invariant words in natural language is given by the Latin sentence below.

S	A	T	O	R
A	R	E	P	O
T	E	N	E	T
O	P	E	R	A
R	O	T	A	S

This translates roughly as “Seed man Arepo holds wheels in his work”. Our last example comes from classic cryptography. Namely, transposition invariant words are the messages that cannot be encrypted using the rail fence cipher without padding.

Sometimes it is more convenient to write $w = w(0)w(1)\cdots w(n)$ instead of $w = w_0 w_1 \cdots w_n$; we will use both notations. We conclude this section with the following lemma, which could have been taken as a formal definition of $p \times q$-invariance. The proof is immediate, so we omit it.

Lemma 1. *The word w is $p \times q$-invariant if and only if*

$$w(ip + j) = w(jq + i) \tag{1}$$

for all $0 \le i < q$ and $0 \le j < p$.

3. Motivating results

First we show that any prefix of length 2^k of the celebrated Thue–Morse word (see [1] or [7]) is transposition invariant. The Thue–Morse word, denoted by $\mathbf{t}$, is defined as the limit of an infinite iteration of the morphism $\mu : 0 \mapsto 01, 1 \mapsto 10$ on the letter 0. Thus

$$\mathbf{t} = \lim_{n\to\infty} \mu^n(0) = 01101001100101101001\cdots.$$

Proposition 2. *For all integers $k \ge 1$, the prefix of length 2^k of the Thue–Morse word is transposition invariant.*

Proof. Let us denote $\mathbf{t} = t(0)t(1)t(2)\cdots$. It can be proved that $t(i)$ is the number of occurrences of the letter 1 in the binary expansion of i modulo 2 (see [7]). Using this property it is easy to see that, for all integers $e, i \geq 0$ and $0 \leq j < 2^e$, we have

$$t(i2^e + j) = t(i) + t(j) \bmod 2.$$

Here – as well as later in this paper – "mod 2" denotes the operation of taking the least nonnegative integer modulo 2; when dealing with congruences, we use " (mod 2)" instead.

Let u be the prefix of $\mathbf{t}$ of length 2^k. We have to show that u is $p \times q$-invariant whenever $pq = |u| = 2^k$, that is, $p = 2^e$ and $q = 2^f$ with $e + f = k$. To do this, assume $0 \leq i < q = 2^f$ and $0 \leq j < p = 2^e$. Then

$$u(ip + j) = t(i2^e + j) = t(i) + t(j) \bmod 2 = t(j2^f + i) = u(jq + i).$$

By Lemma 1, the word u is $p \times q$-invariant. Since this is true for all appropriate p and q, the word u is transposition invariant. □

As a simple corollary we get the following result, which could easily be proved directly as well.

Corollary 3. *There exist infinitely many nontrivial transposition invariant words of composite length.*

Note that the requirement that the length be a composite number is essential since the statement is trivial for prime number lengths.

Next we will show that any non-unary word can be extended to a transposition invariant word of composite length. Again, we want the length to be composite; otherwise the problem is trivial.

Suppose $\alpha = a/b$ is a rational number in its lowest terms. Suppose furthermore that w is a word such that b divides $|w|$. Then w^α denotes the word $w^k w'$, where $k = \lfloor \alpha \rfloor$, $w^k = ww\cdots w$ (k times), and w' is a prefix of w such that $|w^k w'| = \alpha|w|$. A word u is a *prefix* of w if $w = uv$ for some word v.

Proposition 4. *For any non-unary word w, there exists a rational number $\alpha \geq 1$ such that w^α is a nontrivial transposition invariant word of composite length.*

Proof. Assume $|w| = m$. Choose two positive integers k and p such that p is prime and $km + 1 = p$. There exist such integers by Dirichlet's theorem on primes in arithmetic progressions (see [2]). In fact, we can choose $p = O(m^{5.5})$ by a result of Heath-Brown [4].

Now set $\alpha = p^2/m$, so that $|w^\alpha| = \alpha|w| = p^2$. We show that w^α is $p \times p$-invariant. To do so, assume $0 \leq i, j < p$. Using the fact that w^α has a period m, we get

$$w^\alpha(ip + j) = w^\alpha(ikm + i + j) = w^\alpha(i + j) = w^\alpha(jkm + j + i) = w^\alpha(jp + i).$$

By Lemma 1, w^α is $p \times p$-invariant and, moreover, transposition invariant since p is prime. The word w^α is nontrivial because w is not unary and $\alpha \geq 2$. Finally, the proof is completed by observing that $|w^\alpha|$ is a composite integer. □

4. A characterization of transposition invariant words

In this section we prove a number theoretic criterion for $p \times q$-invariance, which then allows us to give a characterization of transposition invariant words. But let us first fix some further notation for this and forthcoming sections.

We define $w = w_0 w_1 \cdots w_n$ and $|w| = n + 1 = pq$, where $p, q \geq 1$ are integers. We will be working in $\mathbf{Z}_n$, the ring of integers modulo n. Integers $0, 1, \ldots, n-1$ are considered both as positions of letters in w and as elements of $\mathbf{Z}_n$. For a subset $S \subseteq \mathbf{Z}_n^*$, where $\mathbf{Z}_n^*$ denotes the unit group of $\mathbf{Z}_n$, $\langle S \rangle$ denotes the multiplicative subgroup of $\mathbf{Z}_n^*$ generated by S. If $S = \{p\}$, we will leave the braces out and simply write $\langle p \rangle$. Note that $\langle p \rangle = \langle q \rangle$ because $p = q^{-1}$ in $\mathbf{Z}_n^*$. Note also that the last position of w, namely n, is not included in $\mathbf{Z}_n$, and thus will be left out from our considerations. However, it is not a problem since w_n maps to itself in transposition. We define

$$k\langle p \rangle = \{\, ka : a \in \langle p \rangle \,\}$$

for all $k \in \mathbf{Z}_n$. Note that $k\langle p \rangle$ is a generalization of the usual definition; see, e.g., the example and its tables in the end of the next section.

Proposition 5. *The word w is $p \times q$-invariant if and only if*

$$w(h) = w(k) \tag{2}$$

for all $k \in \mathbf{Z}_n$ and $h \in k\langle p\rangle$.

Proof. We only need to prove the implication

$$k = jq + i \qquad \Longrightarrow \qquad ip + j = kp \bmod n \tag{3}$$

whenever $0 \le i < q$, $0 \le j < p$, and $0 \le k < n$. For if (3) holds true, then by applying it repeatedly we easily obtain an equivalence between (2) and Lemma 1. For future reference, observe that (3) tells us that the letter at the position k is mapped to the position $pk \bmod n$ in transposition.

To prove the implication in (3), we note that $pq \equiv 1 \pmod n$, and hence

$$k = jq + i \quad \Longrightarrow \quad k \equiv jq + i \pmod n \quad \Longrightarrow \quad kp \equiv j + ip \pmod n.$$

Since we have $k < n$, it follows that $j + ip < n$, and so the last congruence gives $ip + j = kp \bmod n$. This completes the proof. □

Now we are ready to establish a number theoretic characterization for transposition invariant words. With the same trouble we can prove a somewhat more general result that goes as follows.

Let S_n be the set of all positive divisors of $n + 1$, that is,

$$S_n = \{\, d \ge 1 : d \mid (n + 1) \,\}.$$

Let $S \subseteq S_n$. We say that the word w is *S-invariant* if it is $p \times (n + 1)/p$-invariant for all $p \in S$. Then the concepts $p \times q$-invariant and transposition invariant coincide with $\{p\}$-invariant and S_n-invariant, respectively.

Theorem 6. *Let $S \subseteq S_n$. Then the word w is S-invariant if and only if, for every $k \in \mathbf{Z}_n$, all letters at positions indicated by the set $k\langle S\rangle$ are the same.*

Proof. Suppose w is S-invariant, that is, w is $p \times (n+1)/p$-invariant for every $p \in S$. Let $r, s \in S$. Using the condition (2), we see that $kr^i s^j \in kr^i\langle s\rangle$ implies $w(kr^i s^j) = w(kr^i)$, and moreover, $kr^i \in k\langle r\rangle$ implies $w(kr^i) = w(k)$. Thus, for all elements $h \in k\langle r\rangle\langle s\rangle = k\langle r, s\rangle$, we have $w(h) = w(k)$. Using this argument repeatedly, we see that, for every $h \in k\langle S\rangle$, $w(h) = w(k)$.

Conversely, assume that $w(h) = w(k)$ for every $h \in k\langle S\rangle$. Then, because $\langle p\rangle \subseteq \langle S\rangle$ for all $p \in S$, it certainly holds that $w(h) = w(k)$ for every $h \in k\langle p\rangle$. According to Proposition 5, the word w is $p \times (n + 1)/p$-invariant for every $p \in S$, that is, S-invariant. □

5. Maximum number of letters and the orbit of a word

It is natural to ask how many distinct letters a transposition invariant word can have. To answer this question, we need the following auxiliary observation which can be proved in a standard manner.

Lemma 7. *Let $S \subseteq \mathbf{Z}_n^*$ and $k, h \in \mathbf{Z}_n$. Then either*

$$k\langle S\rangle = h\langle S\rangle \qquad \text{or} \qquad k\langle S\rangle \cap h\langle S\rangle = \emptyset.$$

Hence every subset $S \subseteq \mathbf{Z}_n^*$ induces a partition of $\mathbf{Z}_n$ by means of the subgroup $\langle S\rangle$. More precisely, there exist integers $k_1, k_2, \ldots, k_r \in \mathbf{Z}_n$ such that

$$\mathbf{Z}_n = \bigcup_{1 \le i \le r} k_i\langle S\rangle$$

and the sets $k_i\langle S\rangle$ and $k_j\langle S\rangle$ are disjoint if $i \ne j$. We denote this partition generated by the set S by $\mathrm{Part}_n(S)$, that is,

$$\mathrm{Part}_n(S) = \{k_1\langle S\rangle, \ldots, k_r\langle S\rangle\}.$$

It follows from Theorem 6 that the maximal number of distinct letters in an S-invariant word is the number of elements in $\#\mathrm{Part}_n(S) + 1$ (remember that the position of the last letter of w is not in $\mathrm{Part}_n(S)$).

Assume that $S \subseteq \mathbf{Z}_n^*$, and let $d \geq 1$ be a divisor of n. In what follows, we use the notation $\langle S\rangle_d$ for the subgroup generated by S in the group $\mathbf{Z}_d^*$, when the elements of S are viewed as elements of $\mathbf{Z}_d^*$. The order of the quotient group $\mathbf{Z}_d^*/\langle S\rangle_d$ is denoted by $\left[\mathbf{Z}_d^* : \langle S\rangle_d\right]$.

Proposition 8. *Let $S \subseteq \mathbf{Z}_n^*$. Then*

$$\#\mathrm{Part}_n(S) = \sum_{d|n} \left[\mathbf{Z}_d^* : \langle S\rangle_d\right] = \sum_{d|n} \frac{\varphi(d)}{\#\langle S\rangle_d},$$

where φ denotes the Euler totient function.

Proof. For all $k_i\langle S\rangle \in \mathrm{Part}_n(S)$, write $k_i = a_i d_i$, where $d_i = \gcd(k_i, n)$ and $a_i = k_i/d_i$, so that

$$\mathrm{Part}_n(S) = \{a_1 d_1\langle S\rangle, \ldots, a_r d_r\langle S\rangle\}.$$

We need a few auxiliary results to prove the claim. They are numbered accordingly.

If $\gcd(a, n) = 1$, then $adi \equiv adj \pmod n$ if and only if $di \equiv dj \pmod n$, and thus

(1) $\#ad\langle S\rangle = \#d\langle S\rangle$.

Consider next the mapping $d\langle S\rangle \longrightarrow \langle S\rangle_{n/d}$ defined by $di \mapsto i$. Firstly, this mapping is well defined because $\gcd(i, n) = 1$ implies $\gcd(i, n/d) = 1$. Moreover, it is injective, which is easily seen by using the equivalence $di \equiv dj \pmod n$ if and only if $i \equiv j \pmod{n/d}$. Consequently,

(2) $\#d\langle S\rangle \leq \#\langle S\rangle_{n/d}$.

Now, let ψ be the mapping

$$\psi : \mathrm{Part}_n(S) \longrightarrow \bigcup_{d\,|\,n} \mathbf{Z}_{n/d}^*/\langle S\rangle_{n/d}, \qquad ad\langle S\rangle \mapsto a\langle S\rangle_{n/d},$$

so that ψ associates the elements of $\mathrm{Part}_n(S)$ with conjugacy classes of the quotient groups $\mathbf{Z}_{n/d}^*/\langle S\rangle_{n/d}$, where $d \,|\, n$. We leave it to the reader to verify that ψ is both well defined and injective. Next, consider the number α_d of the sets in $\mathrm{Part}_n(S)$ of the form $ad\langle S\rangle$ with $\gcd(a, n) = 1$. Clearly

$$\alpha_d = \#\{i : d = \frac{k_i}{a_i}\},$$

so that

$$\sum_{d|n} \alpha_d = \#\mathrm{Part}_n(S). \tag{4}$$

It follows from the definition and injectivity of ψ that α_d is at most the number of elements in the quotient group $\mathbf{Z}_{n/k}^*/\langle S\rangle_{n/d}$, that is to say,

(3) $\alpha_d \leq [\mathbf{Z}_{n/d}^* : \langle S\rangle_{n/d}]$.

Now we are ready to employ these observations. Recall that $\mathrm{Part}_n(S)$ is a partition of $\mathbf{Z}_n$, and hence

$$\begin{aligned} n &= \sum_{ad\langle S\rangle \in \mathrm{Part}(S)} \#ad\langle S\rangle \overset{1)}{=} \sum_{ad\langle S\rangle \in \mathrm{Part}(S)} \#d\langle S\rangle \\ &= \sum_{d\,|\,n} \alpha_d \,\#d\langle S\rangle \overset{2),3)}{\leq} \sum_{d\,|\,n} [\mathbf{Z}_{n/d}^* : \langle S\rangle_{n/d}]\,\#\langle S\rangle_{n/d} \\ &= \sum_{d\,|\,n} \varphi\left(\frac{n}{d}\right) = n. \end{aligned} \tag{5}$$

(For the last equality, see [2, Th. 2.2].) Thus the inequality in (5) is actually an equality. Consequently, also inequalities in (2) and (3) are equalities. Hence $\alpha_d = [\mathbf{Z}_{n/d}^* : \langle S\rangle_{n/d}]$, and this together with (4) proves the claim. □

Let us introduce the notation

$$\iota_n(S) = \sum_{d|n} \frac{\varphi(d)}{\#\langle S\rangle_d}.$$

So by Proposition 8, $\iota_n(S)$ denotes the number of elements in the partition of $\mathbf{Z}_n^*$ induced by S.

By combining the previous considerations and Theorem 6, we can sum up our discussion about S-invariant words as follows:

Theorem 9. *Let $S \subseteq S_n$. A word w of length $n+1$ is S-invariant if and only if, for every set $P \in \mathrm{Part}_n(S)$, the letters occupying the positions in P are the same. Hence there exists, up to renaming the letters, a unique alphabetically maximal S-invariant word, and it has $\iota_n(S)+1$ distinct letters.*

Next we discuss the behavior of the function $\iota_n(S_n)$. The following result tells us that its values fluctuate heavily.

Theorem 10. *We have*

$$\liminf_{n\longrightarrow\infty} \frac{\iota_n(S_n)}{n} = 0 \qquad \text{and} \qquad \limsup_{n\longrightarrow\infty} \frac{\iota_n(S_n)}{n} = 1.$$

Proof. The value $\liminf_{n\longrightarrow\infty} \frac{\iota_n(S_n)}{n} = 0$ follows immediately from the fact that there exist infinitely many prime numbers n with a primitive root that divides $n+1$. We will prove this fact in Theorem 17.

The latter equality is trivial: Consider the values $n = p-1$ with p a prime number. Now, $\langle S_n\rangle_d = \langle 1\rangle$ for all $d \mid n$, so

$$\iota_n(S_n) = \sum_{d|n} \frac{\varphi(d)}{\#\langle S_n\rangle_d} = \sum_{d|n} \varphi(d) = n,$$

and hence $\limsup_{n\longrightarrow\infty} \iota_n(S_n)/n = 1$. The proof is now complete. □

The last topic of this section was inspired by a question of J. Cassaigne at the WORDS'05 conference. So far we have only considered words that are invariant under transposition. But it is also natural to consider the orbit that a word w makes when the transposition operation is iterated with respect to some fixed $p \times q$ matrix. More precisely, if $f_{p,q}\colon \Sigma^{n+1} \to \Sigma^{n+1}$ is defined by $f_{p,q}(w) = w^{\mathrm{T}}$, where transposition is carried out in a $p \times q$ matrix, then the orbit we are interested in is the set

$$\mathrm{Orb}_{p,q}(w) = \left\{ f_{p,q}^i(w) : i \geq 0 \right\}.$$

We will characterize the possible sizes of these orbits in Theorem 12, but first we need the following lemma.

Lemma 11. *Let G be a subgroup of $\mathbf{Z}_n^*$. Then for any $a \in \mathbf{Z}_n$, the order of the set $aG = \{ax : x \in G\}$ divides the order of G.*

Proof. Note that, for $a \in \mathbf{Z}_n^*$, the claim is Lagrange's theorem on orders of subgroups. Let us define

$$\mathrm{Fix}_a(G) = \{ x \in G : ax = a \}.$$

Clearly, $\mathrm{Fix}_a(G)$ is a subgroup of G, so we can form the quotient group $G/\mathrm{Fix}_a(G)$. Let $\Psi\colon G/\mathrm{Fix}_a(G) \to aG$ be the mapping defined by $b \cdot \mathrm{Fix}_a(G) \mapsto ab$. It is easy to show that Ψ is well defined and bijective. Hence

$$|G| = \#\mathrm{Fix}_a(G) \cdot \#aG,$$

and the claim follows. □

Now we are ready for the last result of this section.

Theorem 12. *Let w be a word of length $n+1$, and suppose $n+1 = pq$. Then $\#\mathrm{Orb}_{p,q}(w)$ divides $\#\langle p\rangle$. Conversely, if $d \geq 1$ divides $\#\langle p\rangle$, then there exists a word w such that $\#\mathrm{Orb}_{p,q}(w) = d$.*

Proof. As was seen in the proof of Proposition 5, the letter at the position k moves to the position $kp \bmod n$ in transposition. Hence, the letters at positions $k\langle p\rangle$ travel on an independent orbit, and therefore $\#\mathrm{Orb}_{p,q}(w)$ equals the least common multiple of the sizes of orbits of letters occupied at positions $k\langle p\rangle$ for all $k \in \mathbf{Z}_n$.

Now consider the orbit $k\langle p\rangle$, and let $r = \#k\langle p\rangle$. Let $a_1, a_2, \ldots, a_r$ denote the letters of w at positions $k, kp, kp^2, \ldots, kp^{r-1}$ modulo n, respectively. After each iteration of $f_{p,q}$ on w, the mutual arrangement of these letters in the positions $k\langle p\rangle$ changes as follows:

$$a_1a_2\cdots a_{r-1}a_r \to a_ra_1a_2\cdots a_{r-1} \to \cdots \to a_2a_3\cdots a_ra_1 \to a_1a_2\cdots a_{r-1}a_r.$$

Hence when the orbit of these letters is full, the corresponding words give rise to the word equation $uv = vu$, where $u = a_1a_2\cdots a_i$ and $v = a_{i+1}a_{i+2}\cdots a_r$. One of the fundamental theorems of combinatorics on words (see [7]) says that two words commute if and only they are powers (repetitions) of some common word. Hence the length of the orbit of the letters at positions $k\langle p\rangle$,$|u|$, divides $\#k\langle p\rangle$ (=$|uv|$), and so by Lemma 11, it divides $\#\langle p\rangle$. Since $\#\mathrm{Orb}(w)$ is the least common multiple of $\#k\langle p\rangle$ with $k \in \mathbf{Z}_n$, it follows that also $\#\mathrm{Orb}(w)$ divides $\#\langle p\rangle$.

Conversely, suppose d divides $\#\langle p\rangle = \#\langle q\rangle$. Define a word $w = w_0w_1\cdots w_n$ as follows:

$$w_i = \begin{cases} 1 & \text{if } i \text{ is of the form } i = q^{dj} \bmod n \text{ for some } j \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then, by the construction, the orbit of w consists of exactly d distinct words. The proof is now complete. □

Here is an example of the situation of the previous theorem. Let us consider a word $w = w_0w_1w_2\cdots w_{45}$ of length 46 in a 2×23 matrix. In this case $n = 45$, $p = 2$, and $q = 23$. The mapping $f_{2,23}$ generates nine separate orbits for letters w_i in w which are obtained from $\langle 2\rangle$ except the trivial one that corresponds to the last symbol w_{45}:

	orbit	corresponding subword
$0\langle 2\rangle$:	0	w_0
$1\langle 2\rangle$:	1, 2, 4, 8, 16, 32, 19, 38, 31, 17, 34, 23	$w_1w_2w_4w_8w_{16}w_{32}w_{19}w_{38}w_{31}w_{17}w_{34}w_{23}$
$3\langle 2\rangle$:	3, 6, 12, 24	$w_3w_6w_{12}w_{24}$
$5\langle 2\rangle$:	5, 10, 20, 40, 35, 25	$w_5w_{10}w_{20}w_{40}w_{35}w_{25}$
$7\langle 2\rangle$:	7, 14, 28, 11, 22, 44, 43, 41, 37, 29, 13, 26	$w_7w_{14}w_{28}w_{11}w_{22}w_{44}w_{43}w_{41}w_{37}w_{29}w_{13}w_{26}$
$9\langle 2\rangle$:	9, 18, 36, 27	$w_9w_{18}w_{36}w_{27}$
$15\langle 2\rangle$:	15, 30	$w_{15}w_{30}$
$21\langle 2\rangle$:	21, 42, 39, 33	$w_{21}w_{42}w_{39}w_{33}$
last symb. :	45	w_{45}

As described in the proof of Theorem 12, the length of the orbit of the letters in $k\langle p\rangle$, say r_k, divides $\#k\langle p\rangle$. More precisely,

$$z_k = z_{k_0}\cdots z_{k_{\#k\langle p\rangle-1}} = u_k^{r_k},$$

where $z_{k_i} = w_{kp^i-1 \bmod n}$ and u_k is the shortest word such that $z_k \in u_k^+$. Thus, by simple combinatorics, we obtain

$$\#\mathrm{Orb}(w) = \operatorname*{lcm}_{k\in\mathbf{Z}_n}(r_k).$$

If we let

$$w = aabbcacabacacbbaabbccbbbbccbcacabbccacbbabbacc,$$

we have

i	x_i	length of period
$0\langle 2\rangle$	$z_0 = a$	1
$1\langle 2\rangle$	$z_1 = abcbabcbabcb$	4
$3\langle 2\rangle$	$z_3 = bccb$	4
$5\langle 2\rangle$	$z_5 = accacc$	3
$7\langle 2\rangle$	$z_7 = abcabcabcabc$	3
$9\langle 2\rangle$	$z_9 = abab$	2
$15\langle 2\rangle$	$z_{15} = ac$	2
$21\langle 2\rangle$	$z_{22} = bbbb$	1

Moreover, by above observation, $\#\mathrm{Orb}(w) = 12$.

6. Favorable prime numbers

In this section we study the lengths, or integers, such that the only transposition invariant words of that length are of the form ab^*c. For example, 4, 6, 12, and 14 are such lengths, as is readily verified.

We begin with an example. Let w be a word of length $n+1$ over four-letter alphabet $A = \{a, b, c, d\}$ defined by

$$w_i = \begin{cases} a & \text{if } i = 0, \\ b & \text{if } \gcd(i, n) = 1, \\ c & \text{if } \gcd(i, n) > 1 \text{ and } i < n, \\ d & \text{if } i = n \end{cases}$$

for all $0 \le i \le n$. Then w is transposition invariant. For if $0 \le i, j \le n$, where $\gcd(i, n) = 1$ and $\gcd(j, n) > 1$, then $i\langle S\rangle \cap j\langle S\rangle = \emptyset$. Moreover, if n is composite, then both letters b and c occur in w, and thus w is nontrivial. We conclude that if a positive integer n is composite, then there always exist nontrivial S-invariant words of length $n+1$ for every $S \subseteq S_n$. This leads us to the next result.

Theorem 13. *Let $S \subseteq S_n$. There exist only trivial S-invariant words of length $n+1$ if and only if n is prime and $\langle S\rangle = \mathbf{Z}_n^*$.*

Proof. Assume there exist only trivial S-invariant words of length $n+1$. This is equivalent to the condition that the partition of $\mathbf{Z}_n$ generated by $\langle S\rangle$ has only two elements, $\{0\}$ and $\{1, 2, \ldots, n-1\}$, which then have to be $0\langle S\rangle$ and $1\langle S\rangle$, respectively. This is equivalent to $\langle S\rangle = \mathbf{Z}_n \setminus \{0\}$, which in turn, happens exactly when n is prime and $\langle S\rangle = \mathbf{Z}_n \setminus \{0\} = \mathbf{Z}_n^*$. □

Motivated by Theorem 13, we say that a prime number n is *favorable* (for the existence of nontrivial transposition invariant words) if there exists a nontrivial transposition invariant word of length $n+1$, that is, if $\langle S_n\rangle \neq \mathbf{Z}_n^*$. Next we will prove that there exist infinitely many favorable primes. This is done with the help of quadratic residues (see [2, 6]). To do that, we need the following lemma.

Lemma 14. *If a positive integer n is prime and $n \equiv 7 \pmod 8$, then every integer dividing $n+1$ is a quadratic residue modulo n.*

Proof. Since the product of two quadratic residues modulo n is a quadratic residue, it is enough to show that each prime divisor of $n+1$ is a quadratic residue modulo n. So assume that p is prime and $p \mid n+1$. It is well known that 2 is a quadratic residue modulo prime n exactly when $n \equiv \pm 1 \pmod 8$. Hence the case $p = 2$ is clear. Suppose then that $p > 2$. Now, by using the basic principles of residue calculation, we get

$$\begin{aligned} \left(\frac{p}{n}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{n-1}{2}} \left(\frac{n}{p}\right) \quad \text{(law of quadratic reciprocity)} \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{n}{p}\right) \quad \left(n \equiv 7 \pmod 8 \text{ implies } \frac{n-1}{2} \text{ odd}\right) \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{-1}{p}\right) \quad \left(n \equiv -1 \pmod p\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \quad \left(\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\right). \\ &= 1. \end{aligned}$$

Hence p is a quadratic residue modulo n, and the claim follows. □

Theorem 15. *There exist infinitely many favorable primes.*

Proof. Let n be a prime number with $n \equiv 7 \pmod 8$. Dirichlet's theorem on arithmetic progressions (see [2]) says that there exist infinitely many such primes n. By Lemma 14, every integer in the set S_n is a quadratic residue modulo n. Thus every integer in the set $\langle S_n\rangle$ also is a quadratic residue. But exactly half of all the integers in $\mathbf{Z}_n^*$ are quadratic residues modulo n; the other half is the set of quadratic nonresidues modulo n. Therefore, $\langle S_n\rangle \neq \mathbf{Z}_n^*$, and nontrivial transposition invariant words of length $n+1$ exist, so that n is favorable. □

The other direction, the infinitude of unfavorable primes, is more difficult, and requires some more advanced techniques. We prove that there exist infinitely many primes p with a primitive root dividing $p+1$, which is stronger statement than just unfavorability of p. The proof is a little application of Heath-Brown's [3] ideas. To present the proof, we need some technical definitions and a lemma.

Suppose $\alpha, \delta > 0$ and $\alpha + \delta < \frac{1}{2}$. The notation $n = P_2(\alpha, \delta)$ means that either n is prime, or $n = p_1 p_2$ with p_1, p_2 primes and $n^\alpha \le p_1 \le n^{\frac{1}{2}-\delta}$.

In what follows, p always denotes a prime number. The notation $f(x) \ll g(x)$ means the same as $f(x) = O(g(x))$. Finally, $\exp_p(a)$ denotes $\#\langle a\rangle_p$. The following lemma is proved in [3].

Lemma 16. *Let $k = 1, 2$, or 3, and put $K = 2^k$. Suppose u and v are coprime integers such that $K \mid u-1$, $16 \mid v$, and $\left(\frac{u-1}{K}, v\right) = 1$. Then there exist $\alpha \in (\frac{1}{4}, \frac{1}{2})$ and $\delta \in (0, \frac{1}{2} - \alpha)$ such that the set*

$$S(x) = \left\{ p \le x : p \equiv u \pmod{v}, \frac{p-1}{K} = P_2(\alpha, \delta) \right\},$$

satisfies

$$\#S(x) \gg \frac{x}{\log^2 x}.$$

Theorem 17. *There exist infinitely many primes p with a primitive root that divides $p+1$.*

Proof. By setting $u = 2 \cdot 3 \cdot 7 \cdot 11 - 1 = 461$, $v = 16 \cdot 3 \cdot 7 \cdot 11 = 3696$, and $k = 2$, we can apply Lemma 16, since u, v, and k clearly satisfy its conditions.

We will show that there are infinitely many primes p such that $p \equiv u \pmod{v}$ and either 3, 7, or 11 is a primitive root mod p. This will then attest to the claim because each of 3, 7, 11 is a divisor of $p+1$.

First we show that if $p \in S(x)$, then 4 divides each of $\exp_p(3)$, $\exp_p(7)$, and $\exp_p(11)$. Since $4 \mid p-1$, the law of quadratic reciprocity gives

$$\left(\frac{3}{p}\right) = \left(\frac{7}{p}\right) = \left(\frac{11}{p}\right) = -1.$$

Now, let a denote some primitive root modulo p, and suppose $a^k \equiv 3 \pmod{p}$ for some k. A well-known result (see [2, Lemma 1 on p. 206]) gives

$$\exp_p(3) = \frac{p-1}{\gcd(k, p-1)}.$$

Since 3 is a quadratic nonresidue modulo p, k must be odd. Thus, since $p-1$ is divisible by 4, so is $\exp_p(3)$. The same reasoning applies for 7 and 11.

Next we analyze different possibilities that can occur with $p \in S(x)$. We have either $p = 4q+1$ with q a prime, or $p = 4p_1p_2+1$ with p_1, p_2 primes. If $p = 4q+1$ and $p > 11^4$, then $\mathrm{ord}_p(3) \mid 4q = p-1$ implies $\mathrm{ord}_p(3) = p-1$. Hence if $\lim_{x\to\infty} S(x)$ contains infinitely many primes of the form $4q+1$, we are done.

Therefore we may assume that $S(x)$ has $\gg \frac{x}{\log^2 x}$ primes of the form $p = p_1p_2 + 1$. Let us denote by $S_2(x)$ this subset of primes in $S(x)$.

If $p \in S_2(x)$ and $p > 11^4$, then

$$\exp_p(3), \exp_p(7), \exp_p(11) \in \{4p_1, 4p_2, p-1\}.$$

In what follows, we will show that for infinitely many $p \in S_2(x)$, one of $\exp_p(3), \exp_p(7), \exp_p(11)$ must equal $p-1$.

Suppose that $p \in S_2(x)$ and $\exp_p(3) = 4p_1$. We make the following auxiliary estimation. Let

$$T(X) = \left\{ p \le x : \exp_p(3) \le 4x^{1/2-\delta} \right\}.$$

Then

$$\#T(x) \le \sum_{e\le 4x^{1/2-\delta}} \#\left\{ p \le x : p \mid 3^e - 1 \right\} \ll \sum_{e\le 4x^{1/2-\delta}} \log(3^e - 1)$$
$$\ll \sum_{e\le 4x^{1/2-\delta}} e \ll x^{1-2\delta}.$$

Since $1-2\delta < 1$, we have $x^{1-2\delta} = o\left(\frac{x}{\log^2 x}\right)$. Now, observe that p is in $T(x)$ because if $p \in S_2(x)$, then $4p_1 \le 4x^{\frac{1}{2}-\delta}$. Hence the number of primes p in $S_2(x)$ with $\exp_p(3) = 4p_1$ is $o\left(\frac{x}{\log^2 x}\right)$. The same estimate holds for 7 and 11.

Therefore there have to be $\gg \frac{x}{\log^2 x}$ primes p in $S_2(x)$ such that

$$\exp_p(3), \exp_p(7), \exp_p(11) \in \{4p_2, p-1\}.$$

If there are infinitely many $p \in S_2(x)$ such that $\exp_p(l) = p-1$ for some $l = 3, 7, 11$, our proof is done. If not, there must be $\gg \frac{x}{\log^2 x}$ primes $p \in S_2(x)$ such that $\exp_p(3) = \exp_p(7) = \exp_p(11) = 4p_2$. We will derive a contradiction by showing that the number of these primes is $o\left(\frac{x}{\log^2 x}\right)$.

The integers $n = 3^e \cdot 7^f \cdot 11^g$ for $0 \le e, f, g \le 2x^{(1-\alpha)/3}$ all satisfy $n^{4p_2} \equiv 1 (\mathrm{mod}\ p)$. Hence by Lagrange's theorem, n can have at most $4p_2$ values. But the number of triples (e, f, g) is at least $8x^{1-\alpha} \ge 8p^{1-\alpha} \ge 8p_2$, so that there are at least two distinct triples that produce the same n mod p. It follows that p divides the numerator N of $3^e \cdot 7^f \cdot 11^g - 1$ for some triple (e, f, g) with $|e|, |f|, |g| \le 2x^{(1-\alpha)/3}$ and $(e, f, g) \ne (0, 0, 0)$. Clearly, $N \ne 0$. It follows that the number of primes p such that $p \in S_2(x)$ and $\exp_p(3) = \exp_p(7) = \exp_p(11) = 4p_2$ is at most the number of different triples (e, f, g) with $|e|, |f|, |g| \le 3x^{(1-\alpha)/3}$ times the number of prime divisors of N. Since

$$\log|N| \ll \max(|e|, |f|, |g|) \ll x^{(1-\alpha)/3},$$

N has $\ll x^{(1-\alpha)/3}$ prime factors. Thus the number of such primes p in $S_2(x)$ is $\ll x^{(1-\alpha)/3} x^{1-\alpha} = o\left(\frac{x}{\log^2 x}\right)$ (observe that $4(1-\alpha)/3 < 1$). This contradiction shows that there are infinitely many primes in $\lim_{x\to\infty} S(x)$ such that either 3, 7, or 11 is a primitive root mod p. The proof is now complete. □

If we denote by $F(x)$ the number of primes p up to x for which there exists a primitive root modulo p dividing $p+1$, then clearly

$$F(x) \ge \#\{p \le x \text{ such that 2 is a primitive root modulo } p\}.$$

Let $N_2(x)$ be the quantity on the right hand side above. A famous result of Hooley [5] states that the Generalized Riemann Hypothesis implies

$$N_2(x) \sim A\frac{x}{\log x},$$

where $A = \prod_{l \text{ prime}} \left(1 - (l^2 - l)^{-1}\right) = 0.3739558136192\cdots$ is Artin's constant. This observation implies immediately that (on GRH) there exists a positive density of primes p with a primitive root dividing $p+1$.

On the other hand numerical evidence suggests that

$$F(x) \sim B\frac{x}{\log x},$$

where $B \ge 0.65$. We believe that the problem of computing the exact value of B can be tackled via the Generalized Riemann Hypothesis.

Acknowledgement

Work of the last author was supported by the Academy of Finland under grant 8203354.

References

[1] J.-P. Allouche, J. Shallit, Automatic Sequences, Cambridge, 2003.
[2] T.M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[3] D.R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford 37 (2) (1986) 27–38.
[4] D.R. Heath-Brown, Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression, Proc. London Math. Soc. 64 (3) (1992) 265–338.
[5] C. Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967) 209–220.
[6] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., in: Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
[7] M. Lothaire, Combinatorics on Words, in: Encyclopedia of Mathematics and its Applications, vol. 17, Addison-Wesley, 1983.