Finding binary words with a given number of subsequences

Radosław Żak

February 18, 2022

Abstract

We relate binary words with a given number of subsequences to continued fractions of rational numbers with a given denominator. We deduce that there are binary strings of length $O(\log n \log \log n)$ with exactly $n$ subsequences; this can be improved to $O(\log n)$ under assumption of Zaremba’s conjecture.

Keywords: subsequences, combinatorics of words, continued fractions

1 Introduction

The number of subsequences of a binary word was investigated so far mainly from the probabilistic point of view. Collins in [1] proved that a random binary string of length $n$ has $2 \left( \frac{3}{2} \right)^n - 1$ subsequences on average, while Biers-Ariel, Godbole and Kelley in [2] generalized this result to the case where the probabilities of occurrence of particular letters are distinct. Flaxman, Harrow and Sorkin proved in [3] that the string maximizing the number of subsequences consists of cyclically repeating letters.

Here our main subject of interest is the problem of finding a binary word with exactly $n$ subsequences, as short as possible. We exhibit a relation between binary strings, Euclidean algorithm and continued fractions. Using results of Rukavishnikova ([4]), we can deduce that there are words with $n$ subsequences and length $O(\log n \log \log n)$. If Zaremba’s conjecture is true, we can even find such a word with length $\Theta(\log n)$.

We also derive two interesting facts. Theorem 3 states that if we have a word $s$ and we want to add $n$ letters at the end, so that the resulting string has as many
subsequences as possible, then ABAB... or BABA... is an optimal choice for the letters added (depending on the last letter of s). Theorem 4 relates good approximations of an irrational number with restricted partial quotients by a rational with denominator N to short words with N-1 subsequences.

For a clear distinction between letters, numbers and words we use alphabet \{A, B\}, and we denote words with Fraktur, eg. as s, t. We also use the following notations:

- 0 – the empty string.
- s ◦ t – the concatenation of s and t.
- s^k is simply s ◦ s ◦ ... ◦ s – k copies of s concatenated.
- P(s) – the number of subsequences of s.
- s^* – the word created by replacing in s all letters A with B and vice versa.
- |s| – the length of string s.
- ϕ(·) – the Euler function.

## 2 Words and the Euclidean algorithm

The following notion characterizes words with a given number of subsequences in a surprising way.

**Definition 1.** For two coprime integers a, b ≥ 1 we construct the word gen(a, b) recursively:

\[
\text{gen}(a, b) = \begin{cases} 
0 & \text{if } a = b = 1, \\
A \circ \text{gen}(a - b, b) & \text{if } a > b, \\
B \circ \text{gen}(a, b - a) & \text{if } b > a.
\end{cases}
\]

This is, in some sense, the description of the Euclidean algorithm for numbers a, b (in particular this algorithm implies that words gen(a, b) are well-defined). As it turns out, we have a large control over number of subsequences of this word.

**Theorem 1.** P(gen(a, b)) = a + b - 1.

Before proving the theorem, let us introduce an additional notation.

**Definition 2.** If s is a binary word, denote as \(P_A(s)\) the number of subsequences of s starting with A, including the empty one, and as \(P_A\) the number of subsequences ending with A (empty string also included). Similarly, \(P_B(s)\) and \(P_B\) are the numbers of subsequences of s respectively starting and ending with B.

This way \(P(s) = P_A(s) + P_B(s) - 1\) (the -1 corresponds to the empty subsequence counted two times).
Proof. We will be proving inductively that $P^A(\text{gen}(a, b)) = a$. Then the claim follows easily, as similarly we get $P^B(\text{gen}(a, b)) = b$. For $a = b = 1$ the empty word is the only subsequence of $\text{gen}(1, 1)$.

If $a < b$, the first letter of $\text{gen}(a, b)$ is $B$. It cannot be contained in any subsequence starting with $A$, so deleting it does not change the value of $P^A$. But $\text{gen}(a, b) = B \circ \text{gen}(a, b - a)$, and by induction assumption $\text{gen}(a, b - a)$ has exactly $a$ subsequences starting with $A$.

Now consider case $a > b$. The first letter of $\text{gen}(a, b)$ is $A$. Observe that if we choose letters from $\text{gen}(a, b)$ in order to form a subsequence starting with $A$, we may use the first letter as a start – the only exception is the empty sequence. Therefore, as $\text{gen}(a, b) = A \circ \text{gen}(a - b, b)$ we have a correspondence between nonempty subsequences of $\text{gen}(a, b)$ starting with $A$ and subsequences of $\text{gen}(a - b, b)$. By induction assumption there are $a - 1$ of the latter, which along with the empty word form $a$ subsequences of $\text{gen}(a, b)$ starting with $A$. This ends the proof.

Example. Take $a = 11$, $b = 7$. Then $\text{gen}(11, 7) = A \circ \text{gen}(4, 7) = AB \circ \text{gen}(4, 3) = ABA \circ \text{gen}(1, 3) = ABAB \circ \text{gen}(1, 2) = ABABB$. We can check that $ABABB$ has 10 nonempty subsequences starting with $A$, and 6 starting with $B$.

The proof of Theorem 1 says that the inverse function of $\text{gen}$ is $s \mapsto (P^A(s), P^B(s))$. As it is not hard to see that any binary word can be written as $\text{gen}(a, b)$ for some $a$, $b$, this gives a bijection between binary words and pairs of coprime positive integers, which allows us to form the following corollary (insignificant for our later reasonings, but interesting on its own).

Proposition 1. There are exactly $\varphi(N + 1)$ binary words with $N$ subsequences.

Proof. All of them have form $\text{gen}(a, b)$, where $b = N + 1 - a$ and $\gcd(a, b) = 1$. The latter is equivalent to $\gcd(a, N + 1) = 1$, so there are exactly $\varphi(N + 1)$ possible choices for $a$. 

2.1 Concatenation theorem

Before we proceed further, it is important to state the formula for the number of subsequences of two words’ concatenation.

Theorem 2. 

$$P(s \circ t) = P^A(s)P^B(t) + P_B(s)P^A(t) - 1.$$ 

Proof. We prove inductively on $|s|$. For $s = 0$ the claim is clear. Suppose $s$ is nonempty. Without loss of generality $s = u \circ A$ for some $u$. Then $P^A(s) = P_A(u) + P_B(u)$ and $P_B(s) = P_B(u)$. Therefore:
\[ P_A(s)P_B(t) + P_B(s)P_A(t) = \]
\[ (P_A(u) + P_B(u))P_B(t) + P_B(u)P_A(t) = \]
\[ P_A(u)P_B(t) + P_B(u)(P_B(t) + P_A(t)) = \]
\[ P_A(u)P_B(A \circ t) + P_B(u)P_A(A \circ t). \]

\[ \square \]

3 Short words

Define string \( z_n \) by \( z_0 = 0, z_{n+1} = A \circ z_n^* \). In other words, \( z_n \) is a string \( ABABA \ldots \) with \( n \) letters.

**Theorem 3.** Let \( s \) be a word ending with \( B \) (or an empty one), and \( n \) a nonnegative integer. Then

\[ \max_{|t|=n} P(s \circ t) = P(s \circ z_n). \]

Moreover if \( s \neq 0 \), the maximum is attained only by \( z_n \).

**Proof.** We will be proving inductively on \( n \). For \( n = 0 \) it is clear. Suppose \( n > 0 \) and let \( t \) be the \( n \)-letter word for which \( P(s \circ t) \) is maximal. When \( t \) starts with \( A \), we get the claim by applying inductive hypothesis to \( (s \circ A)^* \) and \( n-1 \). When \( t \) starts with \( B \), by applying inductive hypothesis to \( s \circ B \) and \( n-1 \) we can replace \( t \) with \( z_n^* \). Hence we just need to check that \( P(s \circ z_n) \geq P(s \circ z_n^*) \) (and that the inequality is strict whenever \( s \) is nonempty).

If \( s = 0 \), this is clear. Suppose \( |s| > 0 \). By Theorem 2 we know that \( P(s \circ t) + 1 = P_A(s)P_B(t) + P_B(s)P_A(t) \). We know that \( P_A(z_n) = P_A(z_n^*) \) and \( P_B(z_n) = P_A(z_n^*) \). Since \( s \) ends with \( B \), we have \( P_B(s) > P_A(s) \). Moreover \( P_A(z_n) > P_A(z_n^*) \), therefore by rearrangement inequality \( P(s \circ z_n) > P(s \circ z_n^*) \).

\[ \square \]

This theorem allows us to replicate the result from [3] for binary strings:

**Proposition 2.** The words \( z_n \) and \( z_n^* \) (and only them) have the maximal number of subsequences among binary words on \( n \) letters.

**Proof.** For \( n = 0 \) it is clear; for \( n > 0 \) by using Theorem 3 for \( s = B \) we get that \( z_n^* \) has more subsequences than any string starting with \( B \); for \( z_n \) it is symmetric.

Using induction we can enumerate \( P(z_n) = F_{n+3} - 1 \), where \( F_m \) is the \( m \)-th Fibonacci number. Indeed,

\[ P(z_n) + 1 = P(A \circ z_n^* - 1) + P_B(AB \circ z_n - 2) = (1 + P(z_n^* - 1)) + (1 + P(z_n - 2)) \]

(being careful for the empty subsequence), which by inductive assumption is equal to \( F_{n+2} + F_{n+1} = F_{n+3} \).
Since \( F_n \approx \frac{1}{\sqrt{5}} \phi^n \), where \( \phi = \frac{1 + \sqrt{5}}{2} \) is the golden ratio, we get that a word with \( n \) subsequences has to have length \( \Omega(\log n) \). The following conjecture seems natural:

**Conjecture.** For any \( n \geq 1 \) there is a binary word with length \( O(\log n) \) and exactly \( n \) subsequences.

### 3.1 Continued fractions

To arrive at our main results, we observe the following duality:

**Proposition 3.** Let \( a, b \) be coprime positive integers and \( \theta = \frac{a}{b} \). If the continued fraction of \( \theta \) is \([c_0; c_1, c_2, \ldots, c_k + 1]\), then \( \text{gen}(a, b) = A^{c_0} B^{c_1} A^{c_2} \ldots \).

**Proof.** We proceed by induction. If \( a = b = 1 \), then \( \theta = 1 \) and \( \text{gen}(a, b) = \theta^0 = 0 \). If \( b > a \), \( c_0 = 0 \). We can swap these numbers, so that \( \theta \) becomes \( \theta^{-1} = [c_1; c_2, c_3, \ldots] \) and proceed further. Finally if \( a > b \), let \( a' := a - b \). Then \( \text{gen}(a, b) = \text{gen}(a', b) \).

It is tempting to look for short strings with \( N - 1 \) subsequences among those words which start with long segment of form \( \frac{1}{N} \). For that, take \( a \approx \frac{1}{N} \) and \( b = N - a \); then \( \frac{a}{b} \approx \phi \). Theorem 4 captures the same idea for an arbitrary irrational number, such that the terms of its continued fraction are bounded.

Choose an integer \( C \geq 1 \). We say that a number \( \theta \) has partial quotients bounded by \( C \) if the continued fraction of \( \theta = [c_0; c_1, c_2, \ldots] \) has \( c_i \leq C \) for all \( i \). Denote by \( S_C \) the set of irrational numbers with partial quotients bounded by \( C \). It is clearly closed under operation \( \theta \mapsto \theta^{-1} \) and if \( \theta \in S_C \), \( \theta > 1 \), then also \( \theta - 1 \in S_C \).

**Theorem 4.** Take \( \xi \in (0, 1) \cap S_C \). If \( \xi \) can be approximated by an irreducible fraction \( \frac{a}{b} \) with error \( |\xi - \frac{a}{b}| = \delta \), then \( \text{gen}(a, N - a) \) is a binary word with \( N - 1 \) subsequences and length

\[
O(C \log N + N \sqrt{\delta C^3}).
\]

**Proof.** Let \( \theta = \frac{1}{\xi} - 1 \). Since \( \xi \leq 1 \), \( \theta \) is positive, moreover \( \xi \in S_C \) implies \( \theta \in S_C \).

Let \( b = N - a \), \( x = \xi N \), \( y = (1 - \xi)N \). Now \( \frac{a}{b} = \theta \), \( x + y = N \) and \( \varepsilon := |y - b| = |x - a| = N|\xi - \frac{1}{\xi}| = N\delta \).

We can apply Euclidean algorithm to pairs \((x, y)\) and \((a, b)\). They go the same way, until the total error \( |x - a| + |y - b| \) is greater than (or equal to) \(|x - y|\) (when \( |x - a| + |y - b| \geq |x - y| \) the equivalence \( a < b \leftrightarrow x < y \) holds). Let \( s \) be the part of \( \text{gen}(a, b) \) corresponding to that interval of time.

Observe that the error \((x - a, y - b)\) starts at \((\pm \varepsilon, \mp \varepsilon)\), and while we execute the Euclidean algorithm, taking a difference between \( x \) and \( y \) corresponds to adding absolute value of one of these errors to another. Therefore the errors after we have the word \( s \) are \((\pm P_A(s), \mp P_B(s))\varepsilon\), and the sum of their absolute values is \( (P(s) + 1)\varepsilon \).
Let \((z, w)\) be the values of \((x, y)\) after we execute on them part of the Euclidean algorithm corresponding to \(s\). Since \((\max(z, w), \max(z, w)) \geq (z, w)\) (coordinate-wise), by reversing the algorithm (adding one coordinate to another, the choice of coordinate is indicated by \(s\)), which preserves inequalities (it consists only of adding) we get \((\max(z, w)P^A(s), \max(z, w)P^B(s)) \geq (x, y)\), thus \(\max(z, w) \geq \frac{x + y}{P(s) + 1} = \frac{N}{P(s) + 1}\).

The value of \(\frac{\max(x, y)}{\min(x, y)}\) in one step of the Euclidean algorithm changes either by \(\theta \to \theta - 1\) or \(\theta \to \frac{1}{\theta - 1}\). In both cases it stays inside \(S_C\). Now

\[
|z - w| = \left(1 - \frac{\min(z, w)}{\max(z, w)}\right) \max(z, w)
\]

and the fraction lies in \((0, 1) \cap S_C\) (\(z \neq w\), since \(\xi\) is irrational). The maximum of \((0, 1) \cap S_C\) is not greater than \(\frac{1}{\sqrt{C + 2}} = \frac{\sqrt{1}}{\sqrt{C + 2}}\), so

\[
|z - w| \geq \frac{\max(z, w)}{C + 2} \geq \frac{N}{(C + 2)(P(s) + 1)}.
\]

Since \(|z - w|\) is not greater than the total error \(\varepsilon(P(s) + 1)\) (if it was, we could continue the algorithm), we obtain

\[
P(s) + 1 \geq \sqrt{\frac{N}{(C + 2)\varepsilon}}.
\]

We can write \(\text{gen}(a, b)\) as \(s \circ t\) for some word \(t\). Let us say that \(t\) starts with \(B\) (the other case is analogous). By Theorem \([2]\)

\[
N = P(\text{gen}(a, b)) + 1 \geq P_A(s)P^B(t) \geq P_A(s)|t|
\]

(the last inequality follows from the fact that we have subsequences of \(t\) starting with \(B\) with all possible lengths).

Since \(s\) comes from the continued fraction of \(\theta\), which lies in \(S_C\), each letter can repeat at most \(C\) times in a row. By easy induction, if \(\nu\) is any word with exactly \(k\) letters \(B\) at the end, then \(P^A(\nu) \geq \frac{1}{k + 2}(P(\nu) + 1)\) (equivalently \(P^B(\nu) \leq (k + 1)P^A(\nu)\); for \(k = 0\) it works, and step \(k \to k + 1\) changes both sides of the equation by \(P^A(\nu)\)). Therefore

\[
N \geq P_A(s)|t| \geq \frac{1}{C + 2}(P(s) + 1)|t| \geq \sqrt{\frac{N}{(C + 2)^3\varepsilon}}|t|,
\]

and so, putting \(\varepsilon = N\delta\),

\[
N\sqrt{\delta(C + 2)^3} \geq |t|.
\]

Now it is left to see that \(|s| = O(C\log N)\). Indeed, every letter in \(s\) comes at most \(C\) times in a row, so \(s\) has \(s_m\) or \(s_m^*\) as a subsequence, where \(m = \lfloor \frac{1}{\varepsilon} |s| \rfloor\). On the other hand, then \(P(s_m) \leq P(s) \leq N\), so \(m = O(\log N)\).
The second summand, seemingly linear in $N$, is actually balanced by $\delta$. If $\delta = O(N^{-2})$ (which is the best possible option), it reduces to $\sqrt{C}$, which is even smaller than the $C \log N$ when $C$ does not exceed $\log^2 N$. Unfortunately without some results on diophantine approximation we cannot give any particular bounds on how small $\delta$ can be.

However, the case of rational $\xi$ seems to be better studied in theory of continued fractions. By Proposition 3, now the correspondence between fractions and words is even clearer. Zaremba conjectured in 1972 that for any $N$ there is an irreducible fraction $\frac{a}{N}$ that has all partial quotients bounded by 5. In our case, this would imply that $\text{gen}(a, N-a)$ is a word with $N-1$ subsequences, and length logarithmic in $N$. Bourgain and Kontorovich ([5]) proved that Zaremba’s hypothesis is true (with bound $C = 50$) for $N$ forming a set of density 1 in $\mathbb{N}$.

If we denote by $S_N(a)$ the sum of partial quotients in $\frac{a}{N}$, by Proposition 3 we have $S_N(a) = |\text{gen}(a, N-a)| + 2$. Rukavishnikova proved in [4] an analog of the law of large numbers for $S_N(a)$, namely that if $g(N)$ is any unboundedly increasing function, such that $g(N) \leq \sqrt{\log N}$, then the fraction of all numbers $S_N(a)$ that fall outside of the interval $|S_N(a) - \frac{12}{\pi^2} \log N \log \log N| \leq g(N) \log N \sqrt{\log \log N}$ grows asymptotically slower than $\frac{1}{g(N)^2}$. Thus we should expect that for most values of $N$, median of all numbers $S_N(a)$ with $\gcd(a, N) = 1$ for general $N$ – the case we are interested in.

Thus we need to use another result by Rukavishnikova, also featured in [4]:

**Theorem 5** (Rukavishnikova). Suppose that $g(d)$ is unboundedly increasing sequence of positive real numbers for which $g(d) \leq (\log d)^2$. Then for $d > 2$

$$\frac{1}{\varphi(d)} \# \{ a \in \mathbb{Z}_N^* : S_d(a) \geq g(d) \log d \log \log d \} = O \left( \frac{1}{g(d)} \right).$$

In particular, the smallest value of $S_N(a)$ among $a \in \mathbb{Z}_N^*$ is $O(\log N \log \log N)$ (as it is growing slower than any function growing faster than $\log N \log \log N$). This implies the following:

**Proposition 4.** For any positive integer $N$ there is a binary word of length $O(\log N \log \log N)$ with exactly $N$ subsequences.

However, our conjecture still remains unproven. It is not obvious if its potential future proof will be a combinatorial one, or one coming from a seemingly unrelated field – theory of continued fractions.

**References**

[1] M. Collins, *The Number of Distinct Subsequences of a Random Binary String*, arXiv:1310.7288
[2] Y. Biers-Ariel, A. Godbole, E. Kelley, *Expected Number of Distinct Subsequences in Randomly Generated Binary Strings*, Discrete Mathematics and Theoretical Computer Science, Vol. 19, No. 2, (2018).

[3] A. Flaxman, A. Harrow and G. Sorkin, Strings with maximally many distinct subsequences and substrings, Electronic Journal of Combinatorics, 11 (1), 2004.

[4] M. G. Rukavishnikova, *A probability estimate for the sum of incomplete partial quotients with fixed denominator*, Mathematical Notes, Vol. 90, No. 3, p. 418–430 (2011).

[5] J. Bourgain, A. Kontorovich, *On Zaremba’s Conjecture*. Annals of Mathematics, Vol. 180, p.137-196 (2014).