数理解析研究所講究録
第 1725 巻 2011 年 106-117

On the complexity of the binary expansions of algebraic numbers

京都大学理学研究科　金子 元 (Kaneko Hajime)
Department of Mathematics, Kyoto University

1 Known results on the binary expansions of algebraic numbers

The binary expansions of rational numbers are ultimately periodic. However, we know only little about the binary expansions of algebraic irrational numbers. Let ξ be a positive real number. We write the n-th digit in the binary expansion of ξ as

$$s(\xi;n)=\lfloor\xi\cdot 2^{-n}\rfloor-2\lfloor\xi\cdot 2^{-n-1}\rfloor\in\{0,1\},$$

where $\lfloor x\rfloor$ denotes the integral part of a real number x. Moreover, let $R(\xi)$ be the largest integer such that $S(\xi;R(\xi))\neq 0$. Then the binary expansion of ξ is denoted by

$$\xi=\sum_{n=-\infty}^{R(\xi)}2^{n}\cdot s(\xi;n).$$

It is widely believed that each algebraic irrational number ξ is normal in base 2 (for instance, see [2]). Namely, let w be any finite word on the alphabet $\{0,1\}$ and $|w|$ its length. Then it is conjectured that w occurs in the binary expansion of ξ with average frequency tending to $2^{-|w|}$. In particular, it is believed that the word 11 appears in the binary expansion of ξ with average frequency tending to $1/4$. However, it is still unknown whether 11 appears infinitely many times in the binary expansions of ξ or not. There is no algebraic irrational number whose normality has been proven.

In this paper we study the complexity of the sequence

$$(s(\xi;n))_{n=-\infty}^{R(\xi)}$$

where ξ is an algebraic irrational number. Let N be a positive integer. First we consider the number $\beta(\xi; N)$ of distinct blocks of N digits in the binary expansion of ξ. Namely,

$$\beta(\xi; N) = \mathrm{Card}\{s(\xi; i)s(\xi; i-1)\dots s(\xi; i-N+1) \mid i \leq R(\xi)\},$$

where Card denotes the cardinality. If ξ is a normal number in base 2, then we have $\beta(\xi; N) = 2^N$ for any positive integer N. Let δ be a positive number less than $1/11$. Then Bugeaud and Evertse [4] showed for all algebraic irrational numbers ξ that

$$\limsup_{N\to\infty} \frac{\beta(\xi; N)}{N(\log N)^\delta} = \infty.$$

However, it is still unknown whether there exists an algebraic irrational number ξ with $\beta(2; \xi) = 3$.

Next, let w be any finite word on the alphabet $\{0, 1\}$. For any integer N, put

$$\begin{aligned}&f(\xi, w; N) := \\ &\mathrm{Card}\{R(\xi) - |w| + 1 \geq n \geq -N \mid s(\xi; n + |w| - 1) \cdots s(\xi; n) = w\}.\end{aligned}$$

The main purpose of this paper is to estimate lower bounds of $f(\xi, w; N)$ in the case of $|w| \leq 2$. In this paper, O denotes the Landau symbol and $\ll, \gg$ mean the Vinogradov symbols. Namely $f = O(g), f \ll g$ and $g \gg f$ imply that

$$|f| \leq Cg$$

for some constant C. Moreover, $f \sim g$ means that the ratio of f and g tends to 1. Suppose again that ξ is a positive algebraic irrational number. By the definition of normal number, ξ is normal in base 2 if and only if, for any word w,

$$f(\xi, w; N) \sim \frac{N}{2^{|w|}}$$

as N tends to infinity. Bailey, Borwein, Crandall, and Pomerance [1] gave lower bounds of $f(\xi, w; N)$ in the case of $w = 1$ as follows: Let $D(\geq 2)$ be the degree of ξ. Then

$$f(\xi, 1; N) \gg N^{1/D}. \tag{1.1}$$

Take a positive integer M such that $2^M > \xi$. Then, using (1.1), we get

$$f(\xi, 0; N) = f(2^M - \xi, 1; M) + O(1) \gg N^{1/D}$$

for all sufficiently large N. Now we consider the case of $|w| = 2$. Let $\gamma(\xi, N)$ be the number of digit changes in the binary expansions of ξ, that is,

$$\gamma(\xi; N) = \mathrm{Card}\{n \in \mathbb{Z} \mid n \geq -N, s(\xi; n) \neq s(\xi; n+1)\}.$$

Then we have

$$f(\xi, 01; N) = \frac{1}{2}\gamma(\xi; N) + O(1) \tag{1.2}$$

and

$$f(\xi, 10; N) = \frac{1}{2}\gamma(\xi; N) + O(1). \tag{1.3}$$

Thus, using (1.2), (1.3), and lower bounds by Bugeaud and Evertse [4], we deduce the following: There exist an effectively computable positive absolute constant C_1 and effectively computable positive constant $C_2(\xi)$ depending only on ξ such that

$$f(\xi, 01; N) \geq C_1 \frac{(\log N)^{3/2}}{(\log(6D))^{1/2}(\log\log N)^{1/2}}, \tag{1.4}$$

$$f(\xi, 10; N) \geq C_1 \frac{(\log N)^{3/2}}{(\log(6D))^{1/2}(\log\log N)^{1/2}} \tag{1.5}$$

for all $N \geq C_2(\xi)$, where D is the degree of ξ. In Section 2 we improve (1.4) and (1.5) for certain classes of algebraic irrational numbers ξ. Moreover, we give lower bounds of the function

$$f(\xi, 00; N) + f(\xi, 11; N).$$

In Sections 3 and 4, we give proofs of the main results.

2 Main results

In this section we give lower bounds of the function $f(\xi, w; N)$ in the case of $|w| = 2$. First, we consider the SSB expansions of real numbers which was introduced by Dajani, Kraaikamp, and Liardet [5]. They proved the following: Let ξ be a real number. Then there exist an integer R and a sequence $(x_i)_{i=-\infty}^{R}$ with $x_i \in \{-1, 0, 1\}$ such that, for any $i \leq R$,

$$x_i x_{i-1} = 0$$

and that

$$\xi = \sum_{i=-\infty}^{R} x_i 2^i =: x_R x_{R-1} \ldots x_0 . x_{-1} x_{-2} \ldots . \tag{2.1}$$

We call (2.1) the SSB expansion of ξ. In a sequence of signed bits, we write -1 by $\bar{1}$. For instance,

$$15 = 1000\bar{1}.000\ldots .$$

The SSB expansion of a real number is not always unique. In fact, we have

$$\frac{1}{3} = 0.(01)^{\omega} = 0.1(0\bar{1})^{\omega},$$

where V^{ω} denotes the right-infinite word $VVV\ldots$ for each nonempty finite word V. Note that the SSB expansion of a rational number ξ is ultimately periodic. Moreover, let r be the period of the ordinary binary expansion of ξ, then r is also the period of ξ (see Lemma 2.2 of [6]). Combining (1.2) and (1.3), we obtain the following:

THEOREM 2.1. *Let ξ be a positive algebraic irrational number with minimal polynomial $A_D X^D + A_{D-1} X^{D-1} + \cdots + A_0 \in \mathbb{Z}[X]$, where $A_D > 0$. Assume that there exists a prime number p which divides all coefficients $A_D, A_{D-1}, \ldots, A_1$, but not the integer $2A_0$. Let σ be the number of nonzero digits in the period of the SSB expansion of A_0/p. Let ε be an arbitrary positive number less than 1 and r the minimal positive integer such that p divides $(2^r - 1)$. Then there exists an effectively computable positive constant $C_3(\xi, \varepsilon)$ depending only on ξ and ε such that*

$$f(\xi, 01; N) \geq \frac{1-\varepsilon}{2} \left(\frac{\sigma p}{r A_D} \right)^{1/D} N^{1/D} \tag{2.2}$$

and that

$$f(\xi, 10; N) \geq \frac{1-\varepsilon}{2} \left(\frac{\sigma p}{r A_D} \right)^{1/D} N^{1/D}, \tag{2.3}$$

where N is any integer with $N \geq C_3(\xi, \varepsilon)$.

We consider the case where w is 00 or 11. However, it is difficult to give lower bounds of $f(\xi, 00; N)$ and $f(\xi, 11; N)$. In fact, we can not prove that the functions $f(\xi, 00; N)$ and $f(\xi, 11; N)$ are unbounded. We give lower bounds of $f(\xi, 00; N) + f(\xi, 11; N)$ for certain classes of algebraic irrational numbers ξ.

THEOREM 2.2. *Let ξ be a positive algebraic irrational number with minimal polynomial $A_D X^D + A_{D-1}X^{D-1} + \cdots + A_0 \in \mathbb{Z}[X]$, where $A_D > 0$. Assume that there exists a prime number p which divides all coefficients $A_D, A_{D-1}, \ldots, A_1$, but not the integer $6A_0$. Let σ' be the number of nonzero digits in the period of the SSB expansion of $(3^D A_0)/p$. Let ε be an arbitrary positive number less than 1 and r the minimal positive integer such that p divides $(2^r - 1)$. Then there exists an effectively computable positive constant $C_4(\xi, \varepsilon)$ depending only on ξ and ε such that*

$$f(\xi, 00; N) + f(\xi, 11; N) \geq \frac{1-\varepsilon}{6}\left(\frac{\sigma' p}{r A_D}\right)^{1/D} N^{1/D} \tag{2.4}$$

for any integer N with $N \geq C_4(\xi, \varepsilon)$.

Note that the assumptions about ξ in Theorem 2.2 is stronger than the ones in Theorem 2.1. We give numerical examples. We consider the case of $\xi = 1/\sqrt{5}$. The minimal polynomial of ξ is

$$A_2 X^2 + A_1 X + A_0 = 5X^2 - 1.$$

Thus, ξ satisfies the assumptions in Theorems 2.1 and 2.2. We have $p = 5$ and $r = 4$. Since the SSB expansion of A_0/p is written as

$$\frac{A_0}{p} = -\frac{1}{5} = 0.(0\bar{1}01)^{\omega},$$

we get $\sigma = 2$. Let ε be an arbitrary positive number less than 1. Then, by Theorem 2.1, we obtain

$$\begin{aligned} f\left(\frac{1}{\sqrt{5}}, 01; N\right) &\geq \frac{1-\varepsilon}{2\sqrt{2}}\sqrt{N}, \\ f\left(\frac{1}{\sqrt{5}}, 10; N\right) &\geq \frac{1-\varepsilon}{2\sqrt{2}}\sqrt{N} \end{aligned}$$

for all sufficiently large N. Similarly, using

$$\frac{3^D A_0}{p} = -\frac{9}{5} = \bar{1}0.(010\bar{1})^{\omega},$$

we get $\sigma' = 2$. Hence, Theorem 2.2 implies that

$$f\left(\frac{1}{\sqrt{5}}, 00; N\right) + f\left(\frac{1}{\sqrt{5}}, 11; N\right) \geq \frac{1-\varepsilon}{6\sqrt{2}}\sqrt{N}$$

for any sufficiently large N.

3 Hamming weights of the SSB expansions of integers

In the previous section we introduced the SSB expansions of real numbers. Let n be an integer. Then the SSB expansion of n is finite, that is,

$$n = x_R x_{R-1} \dots x_0.0^\omega, \tag{3.1}$$

where $x_R \neq 0$ if $n \neq 0$. For simplicity, we denote the SSB expansion (3.1) by

$$n = x_R x_{R-1} \dots x_0.$$

Reitwiesner [7] proved that the representation (3.1) is unique. Let us define the Hamming weight of the SSB expansion of n by

$$\nu(n) = \sum_{i=0}^{R} |x_i|.$$

In this section we introduce lemmas about the Hamming weights of integers in [6]. It is known for each integer n that $\nu(n)$ is the minimal Hamming weight among the signed binary expansions of n (for instance, see [3]). Namely, assume that

$$n = \sum_{i=0}^{M} a_i 2^i,$$

where M and $a_0, a_1, \dots, a_M$ are integers. Then

$$\nu(n) \leq \sum_{i=0}^{M} |a_i|.$$

In particular, since

$$n = \underbrace{1 + \cdots + 1}_{n} \text{ or } n = \underbrace{-1 - \cdots - 1}_{n},$$

we get

$$\nu(n) \leq |n|. \tag{3.2}$$

The function ν satisfies the convexity relations which are analogues of Theorem 4.2 in [1].

LEMMA 3.1. *Let m and n be integers. Then we have*

$$\nu(m+n) \leq \nu(m) + \nu(n)$$

and

$$\nu(mn) \leq \nu(m)\nu(n).$$

Combining (3.2) and Lemma 3.1, we obtain

$$|\nu(m+n) - \nu(m)| \leq |n|. \tag{3.3}$$

Finally, we introduce lower bounds of Hamming weight denoted in Remark 3.1 in [6]

LEMMA 3.2. *Let b be an integer and p a prime number. Assume that p does not divide $2b$. Let r be the minimal positive integer such that p divides $(2^r - 1)$. Moreover, let σ be the nonzero digits in the period of the SSB expansion of b/p. Then we have*

$$\nu\left(\left\lfloor -\frac{A_0}{p} 2^N \right\rfloor\right) \geq \frac{\sigma}{r} N - 2\sigma - 2.$$

4 Proof of Theorem 2.2

We use the same notation as in Section 1. Put

$$\begin{aligned} F(\xi; N) &:= f(\xi, 00; N) + f(\xi, 11; N) \\ &= \mathrm{Card}\{R(\xi) - 1 \geq n \geq -N \mid s(\xi; n+1) = s(\xi; n)\}. \end{aligned}$$

We give lower bounds of $F(\xi; N)$ by the Hamming weight of the SSB expansions of integers.

LEMMA 4.1. *Let h be a positive integer and N a nonnegative integer. Then*

$$\nu(\lfloor 3^h 2^N \xi^h \rfloor) \leq (6F(\xi; N) + 2)^h + 6^{h+1} \max\{1, \xi^h\}.$$

Proof. We show for any nonnegative integer N that

$$\nu(3\lfloor 2^N\xi\rfloor) \leq 6f(\xi;N)+2. \tag{4.1}$$

We write the fractional part of a real number x by $\{x\}$. Let v be a word of length L on the alphabet $\{0,1\}$. For nonnegative real number x, put

$$v^x = \underbrace{vv\ldots v}_{\lfloor x\rfloor}v',$$

where v' is the prefix of v with length $\lfloor L\{x\}\rfloor$. For instance, if $v=101$, then

$$v^2 = 101101,\ v^{8/3} = 10110110.$$

The ordinary binary expansion of $\lfloor \xi 2^N\rfloor$ is written as

$$\lfloor \xi 2^N\rfloor = v_1^{x_1}w_1^{y_1}v_2^{x_2}w_2^{y_2}\ldots v_{l-1}^{x_{l-1}}w_{l-1}^{y_{l-1}}v_l^{x_l} \tag{4.2}$$

or

$$\lfloor \xi 2^N\rfloor = v_1^{x_1}w_1^{y_1}v_2^{x_2}w_2^{y_2}\ldots v_{l-1}^{x_{l-1}}w_{l-1}^{y_{l-1}}v_l^{x_l}w_l^{y_l}, \tag{4.3}$$

where $v_i\in\{01,10\}, w_i\in\{0,1\}$, and $2x_i, y_i\in\mathbb{Z}$ for each i. Note that

$$F(\xi;N) = \sum_{i\geq 1} y_i.$$

First we assume that $\lfloor \xi 2^N\rfloor$ is written as (4.2). Then, for any i, the ordinary binary expansion of $3v_i^{x_i}$ is denoted as

$$3v_i^{x_i} = 11\ldots 1 \text{ or } 11\ldots 10,$$

and so,

$$\nu(3v_i^{x_i}) \leq 2.$$

Thus, using Lemma 3.1 and

$$\nu(3w_i^{y_i}) \leq \nu(3)\nu(w_i^{y_i}) \leq 4,$$

we obtain

$$\begin{aligned}
\nu(3\lfloor \xi 2^N\rfloor) &\leq \sum_{i=1}^{l}\nu(3v_i^{x_i}) + \sum_{i=1}^{l-1}\nu(3w_i^{y_i}) \\
&\leq 2l + 4(l-1) = 6(l-1)+2 \\
&\leq 6\sum_{i=1}^{l-1} y_i + 2 = 6F(\xi;N)+2.
\end{aligned}$$

Next, we consider the case where $\lfloor \xi 2^N \rfloor$ is written as (4.3). By Lemma 3.1

$$\begin{aligned}\nu(3\lfloor \xi 2^N \rfloor) &\le \sum_{i=1}^{l} \nu(3v_i^{x_i}) + \sum_{i=1}^{l} \nu(3w_i^{y_i}) \\ &\le 6l \le 6\sum_{i=1}^{l} y_i = 6F(\xi; N).\end{aligned}$$

Therefore, we proved (4.1).

Recall that the ordinary binary expansion of ξ is

$$\xi = \sum_{n=-\infty}^{\infty} s(\xi, n)2^n.$$

Put

$$\xi_1 := \sum_{n=-N}^{\infty} s(\xi, n)2^n, \; \xi_2 := \sum_{n=-\infty}^{-N-1} s(\xi, n)2^n.$$

Then we have

$$\begin{aligned}3^h 2^N \xi^h &= 3^h 2^N (\xi_1 + \xi_2)^h \\ &= 3^h 2^N \xi_1^h + 3^h 2^N \sum_{i=1}^{h} \binom{h}{i} \xi_1^{h-i} \xi_2^i,\end{aligned}$$

and so

$$\left| \lfloor 3^h 2^N \xi^h \rfloor - \lfloor 3^h 2^N \xi_1^h \rfloor \right| \le 1 + \left\lfloor 3^h 2^N \xi_1^h + 3^h 2^N \sum_{i=1}^{h} \binom{h}{i} \xi_1^{h-i} \xi_2^i \right\rfloor.$$

Hence, using (3.3) and Lemma 3.1, we obtain

$$\begin{aligned}&\nu\left(\lfloor 3^h 2^N \xi^h \rfloor\right) \\ &\le \nu\left(\lfloor 3^h 2^N \xi_1^h \rfloor\right) + 1 + \left\lfloor 3^h 2^N \xi_1^h + 3^h 2^N \sum_{i=1}^{h} \binom{h}{i} \xi_1^{h-i} \xi_2^i \right\rfloor \\ &\le \nu\left(\lfloor 3^h 2^N \xi_1^h \rfloor\right) + 1 + 3^h \sum_{i=0}^{h} \binom{h}{i} \max\{1, \xi^h\} \\ &\le \nu\left(\lfloor 3^h 2^N \xi_1^h \rfloor\right) + 1 + 6^h \max\{1, \xi^h\}. \qquad (4.4)\end{aligned}$$

Note that

$$\nu(3^h 2^{hN} \xi_1^h) \le \nu(3 \cdot 2^N \xi_1)^h = \nu(3\lfloor 2^N \xi \rfloor)^h.$$

Write the SSB expansion of $3^h 2^{hN} \xi_1^h$ by

$$3^h 2^{hN} \xi_1^h = \sum_{i=0}^{t} \sigma_i 2^i.$$

Then we have

$$\sum_{i=0}^{t} |\sigma_i| \le \nu(3\lfloor 2^N \xi \rfloor)^h. \tag{4.5}$$

Let

$$\theta_1 := \sum_{i=(h-1)N}^{t} \sigma_i 2^{i-(h-1)N},\ \theta_2 := \sum_{i=0}^{(h-1)N-1} \sigma_i 2^{i-(h-1)N}.$$

Since $\theta_1 \in \mathbb{Z}$, $|\theta_2| < 1$, and since

$$\theta_1 + \theta_2 = 3^h 2^N \xi_1^h,$$

we get

$$\left| \lfloor 3^h 2^N \xi_1^h \rfloor - \theta_1 \right| \le 1$$

By (4.5)

$$\begin{aligned} \nu\left(\lfloor 3^h 2^N \xi_1^h \rfloor\right) &\le \nu(\theta_1) + 1 \\ &= 1 + \sum_{i=(h-1)N}^{t} |\sigma_i| \le 1 + \nu(3\lfloor 2^N \xi \rfloor)^h. \end{aligned} \tag{4.6}$$

Consequently, combining (4.1), (4.4), and (4.6), we conclude that

$$\begin{aligned} \nu\left(\lfloor 3^h 2^N \xi^h \rfloor\right) &\le \nu\left(\lfloor 3^h 2^N \xi_1^h \rfloor\right) + 1 + 6^h \max\{1, \xi^h\} \\ &\le \nu(3\lfloor 2^N \xi \rfloor)^h + 2 + 6^h \max\{1, \xi^h\} \\ &\le (6f(\xi; N) + 2)^h + 6^{h+1} \max\{1, \xi^h\}. \end{aligned}$$

□

We now prove Theorem 2.2. By

$$\sum_{h=0}^{D} A_h \xi^h = 0,$$

we get

$$-\frac{3^D A_0}{p}2^N = \sum_{h=1}^{D} \frac{3^{D-h}A_h}{p} 3^h 2^N \xi^h.$$

Lemma 3.2 implies that

$$\nu\left(\left\lfloor -\frac{3^D A_0}{p}2^N \right\rfloor\right) \geq \frac{\sigma'}{r}N - 2\sigma' - 2.$$

Using (3.3)and Lemmas 3.1, 4.1, we obtain

$$\begin{aligned}
&\nu\left(\left\lfloor -\frac{3^D A_0}{p}2^N \right\rfloor\right) = \nu\left(\left\lfloor \sum_{h=1}^{D} \frac{3^{D-h}A_h}{p} 3^h 2^N \xi^h \right\rfloor\right) \\
&\leq \nu\left(\sum_{h=1}^{D} \frac{3^{D-h}A_h}{p} \lfloor 3^h 2^N \xi^h \rfloor\right) + \sum_{h=1}^{D} \frac{3^{D-h}|A_h|}{p} \\
&\leq \sum_{h=1}^{D} \frac{3^{D-h}|A_h|}{p} \left(1 + \nu(\lfloor 3^h 2^N \xi^h \rfloor)\right) \\
&\leq \sum_{h=1}^{D} \frac{3^{D-h}|A_h|}{p} \left(1 + (6f(\xi;N)+2)^h + 6^{h+1}\max\{1,\xi^h\}\right).
\end{aligned}$$

Therefore, there exists a polynomial $P(X) \in \mathbb{R}[X]$ with leading term

$$\frac{6^D r A_D}{\sigma' p} X^D$$

such that, for any nonnegative integer N,

$$N \leq P\Big(F(\xi;N)\Big).$$

Consequently, for any positive real number ε less than 1, there exists a positive computable constant $C_4(\xi,\varepsilon)$ depending only on ξ and ε such that, for each integer N with $N \geq C_4(\xi,\varepsilon)$,

$$F(\xi;N) \geq \frac{1-\varepsilon}{6}\left(\frac{\sigma' p}{r A_D}\right)^{1/D} N^{1/D}.$$

Finally, we showed Theorem 2.2.

Acknowledgements

I would like to thank Prof. Yann Bugeaud for giving me useful advice. I am very grateful to Prof. Shigeki Akiyama for useful suggestions and for giving me fruitful information about the SSB expansions of integers. This work is supported by the JSPS fellowship.

References

[1] D. H. Bailey, J. M. Borwein, R. E. Crandall and C. Pomerance, 'On the binary expansions of algebraic numbers', *J. Théor. Nombres Bordeaux* **16** (2004), 487–518.

[2] É. Borel, 'Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne', *C. R. Acad. Sci. Paris* **230** (1950), 591–593.

[3] W. Bosma, 'Signed bits and fast exponentiation', *J. Théor. Nombres Bordeaux* **13** (2001), 27–41.

[4] Y. Bugeaud and J.-H. Evertse, 'On two notions of complexity of algebraic numbers', *Acta Arith.* **133** (2008), 221–250.

[5] K. Dajani, C. Kraaikamp and P. Liardet, 'Ergodic properties of signed binary expansions', *Discrete Contin. Dyn. Syst.* **15** (2006), 87–119.

[6] H. Kaneko, On the binary digits of algebraic numbers, *J. Aust. Math. Soc.* to appear.

[7] G. W. Reitwiesner, 'Binary arithmetic', *Advances in computers*, **1** (1960), 231–308.