On the binary digits of algebraic numbers*

Hajime Kaneko

Abstract

Let ξ be a positive algebraic irrational number with binary representation $\sum_{n=-\infty}^{\infty} s(\xi,n)2^n,\ s(\xi,n)\in\{0,1\}$. We derive new, improved lower bounds of the number $\gamma(\xi,N)$ of digit changes defined by

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

where Card denotes the cardinality. Let ε be an arbitrary positive number. Our main results show, for instance, that

$$\gamma\left(\frac{1}{\sqrt{3}},N\right)\geq \frac{1-\varepsilon}{\sqrt{2}}\sqrt{N}$$

for any integer N with $N\geq C(1/\sqrt{3},\varepsilon)$, where $C(1/\sqrt{3},\varepsilon)$ is an effectively computable positive constant depending only on ε.

1 Introduction

Borel [2] proved that almost all positive number ξ are normal in every integral base $\alpha\geq 2$. Namely, every string of l consecutive base-α digits occurs with average frequency tending to $1/\alpha^l$ in the α-ary expansion of such ξ. It is widely believed that all algebraic irrational numbers are normal in each integral base. However, very few is known on this problem, which was first formulated by Borel [3]. For instance it is still unknown whether, for $\alpha\geq 3$, the letter 1 occurs infinitely often in the α-ary expansion of $\sqrt{2}$.

In this paper we study the binary expansions of algebraic irrational numbers. In what follows, let $\mathbb{N}$ be the set of nonnegative integers and $\mathbb{Z}_{\geq 1}$ the set of positive integers. Denote the integral and fractional parts of a real number ξ by $[\xi]$ and $\{\xi\}$, respectively. Moreover, let $\lceil\xi\rceil$ be the minimal integer not less than ξ. Then the binary expansion of a positive number ξ is written by

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

where

$$s(\xi,n)=[2^{-n}\xi]-2[2^{-n-1}\xi]\in\{0,1\}.$$

There are several ways to measure the complexity of the binary expansions of real numbers. First we introduce the block complexity. Let $\beta(\xi,N)$ be the total number of distinct blocks of N digits in the binary expansion of ξ, that is,

$$\beta(\xi,N)=\mathrm{Card}\{(s(\xi,i+1),\ldots,s(\xi,i+N))\in\{0,1\}^N|i\in\mathbb{Z}\},$$

*2000 Mathematics Subject Classification : 11J71, 11K16, 11K60 where Card denotes the cardinality. If ξ is normal in base 2, then $\beta(\xi, N) = 2^N$ for any $N \in \mathbb{Z}_{\geq 1}$. Suppose that ξ is an algebraic irrational number. Bugeaud and Evertse [5] showed for any positive δ with $\delta < 1/11$ that

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

Secondly, we consider the asymptotic behaviour of the number of digit changes in the binary expansions of real numbers ξ. Let N be an integer. The number $\gamma(\xi, N)$ of digit changes, introduced in [4], is defined by

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

Note that $\gamma(\xi, N) < \infty$ since $s(\xi, n) = 0$ for all sufficiently large $n \in \mathbb{N}$. Suppose again that ξ is an algebraic irrational number of degree $D \geq 2$. In [4] Bugeaud proved that

$$\lim_{N\to\infty} \frac{\gamma(\xi, N)}{\log N} = \infty$$

by using Ridout's theorem [8]. In the same paper, by using a quantitative version of Ridout's theorem [7], he showed that

$$\gamma(\xi, N) \geq 3(\log N)^{6/5}(\log\log N)^{-1/4}$$

for every sufficiently large $N \in \mathbb{N}$. Moreover, by improving the quantitative parametric subspace theorem from [6], Bugeaud and Evertse [5] verified the following: There exist an effectively computable absolute constant $C_1 > 0$ and an effectively computable constant $C_2(\xi) > 0$, depending only on ξ, satisfying

$$\gamma(\xi, N) \geq C_1 \frac{(\log N)^{3/2}}{(\log(6D))^{1/2}(\log\log N)^{1/2}}$$

for any N with $N \geq C_2(\xi)$.

Note that if ξ is normal, then the word 10 occurs in the binary expansion of ξ with frequency $1/4$. Thus, it is widely believed that the function $\gamma(\xi, N)$ should grow linearly in N. The main purpose of this paper is to improve lower bounds of the function $\gamma(\xi, N)$ for certain classes of algebraic irrational numbers. Now we state the main results.

THEOREM 1.1. *Let $\xi > 0$ be an 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 an odd prime number p which divides all coefficients $A_D, A_{D-1}, \ldots, A_1$, but not the constant term A_0. Let ε be an arbitrary positive number with $\varepsilon < 1$ and r the minimal positive integer such that p divides $(2^r - 1)$. Then there exists an effectively computable positive constant $C(\xi, \varepsilon)$ depending only on ξ and ε such that*

$$\gamma(\xi, N) \geq (1-\varepsilon)p^{1/D}r^{-1/D}A_D^{-1/D}N^{1/D}$$

for any integers N with $N \geq C(\xi, \varepsilon)$.

For instance, let A and D be positive integers such that $A^{-1/D}$ is an irrational number of degree D. Assume that there is an odd prime p which divides A. Let ε be any positive number with $\varepsilon < 1$ and r defined as in Theorem 1.1. Then, since the minimal polynomial of $A^{-1/D}$ is $AX^D - 1$, by Theorem 1.1 we obtain

$$\gamma(A^{-1/D}, N) \geq (1-\varepsilon)p^{1/D}r^{-1/D}A^{-1/D}N^{1/D}$$

for every integer $N \geq C(A^{-1/D}, \varepsilon)$. In the case where $A = 3$ and $D = 2$, we get $p = 3$ and $r = 2$. Hence

$$\gamma\left(\frac{1}{\sqrt{3}}, N\right) \geq \frac{1-\varepsilon}{\sqrt{2}}\sqrt{N}$$

for each integer $N \geq C(1/\sqrt{3}, \varepsilon)$.

2 The number of nonzero digits

Let n be a nonnegative integer. Let $\mu(n)$ be the number of nonzero digits in the binary expansion of n. For instance, $\mu(0) = 0$ and $\mu(2^l) = 1$, for $l \in \mathbb{N}$. Bailey, Borwein, Crandall, and Pomerance [1] proved the convexity relations of the function $\mu(n)$. Namely, for any nonnegative integers m and n, we have

$$\begin{aligned} \mu(m+n) &\leq \mu(m) + \mu(n), \\ \mu(mn) &\leq \mu(m)\mu(n). \end{aligned} \tag{2.1}$$

Let h be a positive integer and S a subset of $\mathbb{Z}$. Then put

$$\begin{aligned} \overline{S} &= S \cup \{-s | s \in S\}, \\ hS &= \{s_1 + \cdots + s_h | s_1, \ldots, s_h \in S\}. \end{aligned}$$

For convenience, let $0S = \{0\}$. We consider the set Λ defined by

$$\Lambda = \{0\} \cup \{2^l | l \in \mathbb{N}\}.$$

For each integer n, put

$$\nu(n) = \min\{h \in \mathbb{N} | n \in h\overline{\Lambda}\}.$$

Then we have the following:

LEMMA 2.1. *Let n be a nonzero integer and $\lambda_1, \ldots, \lambda_{\nu(n)} \in \overline{\Lambda}$. Assume that*

$$\lambda_1 + \ldots + \lambda_{\nu(n)} = n.$$

Then, for any i with $1 \leq i \leq \nu(n)$,

$$1 \leq |\lambda_i|.$$

Moreover, for any i and j with $1 \leq i < j \leq \nu(n)$,

$$|\lambda_i| \neq |\lambda_j|.$$

Proof. If $\lambda_i = 0$ for some i, then

$$n = \sum_{\substack{k=1 \\ k \neq i}}^{\nu(n)} \lambda_k \in (-1 + \nu(n))\overline{\Lambda},$$

which contradicts to the definition of $\nu(n)$. Next, assume that $|\lambda_i| = |\lambda_j|$ for some i and j with $1 \leq i < j \leq \nu(n)$. Observe that

$$\lambda_i + \lambda_j \in \overline{\Lambda}.$$

Thus

$$n = \lambda_i + \lambda_j + \sum_{\substack{k=1 \\ k \neq i,j}}^{\nu(n)} \lambda_k \in (-1 + \nu(n))\overline{\Lambda},$$

which is a contradiction. $\square$

Suppose that $n \in \mathbb{N}$. Then, by the definition of the function $\nu(n)$, we get

$$0 \leq \nu(n) = \nu(-n) \leq \mu(n) \leq n.$$

For instance, if $n \geq 2$, then

$$\mu(2^n - 1) = n, \nu(2^n - 1) = 2.$$

We now prove the convexity relations of the function $\nu(n)$.

LEMMA 2.2. *Let m and n be integers. Then*

$$\nu(m+n) \leq \nu(m) + \nu(n), \tag{2.2}$$
$$\nu(mn) \leq \nu(m)\nu(n). \tag{2.3}$$

Proof. (2.2) is obvious by the definition of the function $\nu(n)$. We check (2.3). Put

$$a = \nu(m),\ b = \nu(n).$$

Without loss of generality we may assume that $mn \neq 0$. Namely, $a, b \geq 1$. Then there exist $\lambda_1, \ldots, \lambda_a, \lambda'_1, \ldots, \lambda'_b \in \overline{\Lambda}$ such that

$$m = \sum_{i=1}^{a} \lambda_i,\ n = \sum_{j=1}^{b} \lambda'_j.$$

Note that, for any i and j with $1 \leq i \leq a$ and $1 \leq j \leq b$, $\lambda_i \lambda'_j \in \overline{\Lambda}$. Thus

$$mn = \sum_{i=1}^{a} \sum_{j=1}^{b} \lambda_i \lambda'_j \in ab\overline{\Lambda},$$

which implies (2.3). $\square$

COROLLARY 2.3. *Let m and n be integers. Then*

$$|\nu(m+n) - \nu(m)| \leq |n|.$$

Proof. By Lemma 2.2, we get

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

and

$$\nu(m) - \nu(m+n) \leq \nu(-n) \leq |n|.$$

□

We represent the function $\nu(n)$ by using $\mu(n)$.

LEMMA 2.4. *Let n be an integer. Then*

$$\nu(n) = \min_{x \in \mathbb{N}} (\mu(|n| + x) + \mu(x)). \tag{2.4}$$

Proof. We denote the right-hand side of (2.4) by $\overline{\nu}(n)$. In the case of $n = 0$, (2.4) is trivial. Without loss of generality, we may assume that $n \geq 1$ since $\nu(n) = \nu(-n)$ for any $n \in \mathbb{Z}$. There exist $b \in \mathbb{Z}_{\geq 1}$ with $b \leq \nu(n)$ and $\lambda_1, \ldots, \lambda_{\nu(n)} \in \Lambda$ such that

$$n = \lambda_1 + \cdots + \lambda_b - \lambda_{b+1} - \cdots \lambda_{\nu(n)}.$$

Let $y = \lambda_{1+b} + \cdots + \lambda_{\nu(n)}$. Note that if $b = \nu(n)$, then $y = 0$. By Lemma 2.1 we get

$$\mu(y) = \nu(n) - b$$

and

$$\mu(n+y) = \mu(\lambda_1 + \cdots + \lambda_b) = b.$$

Hence

$$\nu(n) = \mu(n+y) + \mu(y) \geq \overline{\nu}(n).$$

On the other hand, there exists $x_0 \in \mathbb{N}$ such that

$$\mu(n + x_0) + \mu(x_0) = \overline{\nu}(n).$$

By using

$$n + x_0 \in \mu(n + x_0)\Lambda$$

and

$$x_0 \in \mu(x_0)\Lambda = (\overline{\nu}(n) - \mu(n + x_0))\Lambda,$$

we obtain

$$n = (n + x_0) - x_0 \in \overline{\nu}(n)\overline{\Lambda},$$

consequently,

$$\nu(n) \leq \overline{\nu}(n).$$

Therefore we verified the Lemma 2.4. □

Let w be an integer and p an odd prime number. In the rest of this section, we give lower bounds of the value $\nu([(2^N w)/p])$ for each $N \in \mathbb{N}$. We start with some simple observations about the number of nonzero digits of binary expansion. Let N, a, b be nonnegative integers with $a \leq b$. Put

$$\mu(a, b; N) = \mathrm{Card}\{i \in \mathbb{N} | s(N, i) \neq 0, a \leq i \leq b\}.$$

Then we have the following.

LEMMA 2.5. *Let $x, y \in \mathbb{N}$. Suppose that $s(x, a) = 0$ and $s(x, b) = 1$ for some $a, b \in \mathbb{N}$ with $a < b$. Then*

$$\mu(a, b; x + y) + \mu(a, b; y) \geq 1.$$

Proof. Assume the contrary, namely, that

$$\mu(a, b; x + y) = \mu(a, b; y) = 0.$$

Let

$$x' = \sum_{i=0}^{b} s(x, i) 2^i, \; y' = \sum_{i=0}^{b} s(y, i) 2^i.$$

Since $x' + y' \equiv x + y \bmod 2^{1+b}$ and since $y' \equiv y \bmod 2^{1+b}$,

$$\mu(a, b; x' + y') = \mu(a, b; y') = 0. \tag{2.5}$$

Then, by $s(x, a) = 0$, $s(x, b) = 1$ and (2.5), we get

$$2^b \leq x' \leq \sum_{i=0}^{b} 2^i - 2^a < 2^{1+b} - 2^a \tag{2.6}$$

and

$$0 \leq y' = \sum_{i=0}^{a-1} s(y, i) 2^i < 2^a.$$

Hence, by combining (2.5) and $x' + y' < 2^{1+b}$, we obtain

$$x' + y' \leq \sum_{i=0}^{a-1} 2^i < 2^a < 2^b$$

which contradicts to (2.6). □

LEMMA 2.6. *Let w be an integer and p an odd prime number. Assume that p does not divide w. Let r be the minimal positive integer such that p divides $(2^r - 1)$. Then*

$$\nu\left(\left[\frac{2^N w}{p}\right]\right) \geq \frac{N}{r} - 3$$

for each $N \in \mathbb{N}$ with $N \geq 2r$.

Proof. Let $\eta = w/p$. First we consider the case of $w \geq 0$. Since p divides $(2^r - 1)$, there exist $F, G \in \mathbb{N}$ with $0 \leq G \leq 2^r - 2$ such that

$$\eta = F + \frac{G}{2^r - 1}.$$

Since p does not divide w, we have $G \geq 1$. Let us denote the binary expansion of G by

$$G = 2^{r-1} g_{-1} + \cdots + 2 g_{-r+1} + g_{-r},$$

where $g_{-1}, \ldots, g_{-r+1}, g_{-r} \in \{0, 1\}$. Since $1 \leq G \leq 2^r - 2$, $g_{-i} = 1$ for some i with $1 \leq i \leq r$ and $g_{-j} = 0$ for some j with $1 \leq j \leq r$. The binary expansion of η is given by

$$\begin{aligned} \eta &= F + \sum_{i=0}^{\infty} 2^{-(i+1)r} \sum_{j=1}^{r} g_{-j} 2^{r-j} \\ &= F + \sum_{i=0}^{\infty} \sum_{j=1}^{r} g_{-j} 2^{-ir-j}. \end{aligned}$$

Namely, for any i, j with $1 \leq j \leq r$, we have

$$s(\eta, -ir - j) = g_{-j}.$$

In particular, let m and n be positive integers such that $m \equiv n \bmod r$. Then

$$s(\eta, -m) = s(\eta, -n). \tag{2.7}$$

Let

$$\begin{aligned} e &= \min\{n \geq 1 | s(\eta, -n) = 1\}, \\ f &= \min\{n \geq e + 1 | s(\eta, -n) = 0\}. \end{aligned}$$

Then, by (2.7) we get

$$e \leq r,\ f \leq e + r - 1. \tag{2.8}$$

Let $N \in \mathbb{N}$ with $N \geq 2r$ and

$$j_0 = \left[\frac{N - e + 1}{r}\right] \geq 1.$$

Note that

$$[2^N \eta] = \sum_{i=0}^{\infty} s(\eta, i - N) 2^i$$

and that, for any j with $1 \leq j \leq j_0$,

$$N - e + 1 - jr \geq 0.$$

Let y be a nonnegative integer. Then

$$\begin{aligned}
&\mu([2^N\eta]+y)+\mu(y) \\
&\geq \sum_{j=1}^{j_0}\Big(\mu\big(N-e+1-jr, N-e-(j-1)r; [2^N\eta]+y\big) \\
&\qquad\qquad +\mu\big(N-e+1-jr, N-e-(j-1)r; y\big)\Big)
\end{aligned} \tag{2.9}$$

Denote the right-hand side of (2.9) by $\sum_{j=0}^{j_0}\Phi(j)$. Let j be an integer with $1 \leq j \leq j_0$. Put

$$a = N-f-(j-1)r,\ b = N-e-(j-1)r.$$

By (2.7) we get

$$s([2^N\eta], a) = s(\eta, a-N) = s(\eta, -f) = 0 \tag{2.10}$$

and

$$s([2^N\eta], b) = s(\eta, b-N) = s(\eta, -e) = 1. \tag{2.11}$$

By using (2.10), (2.11), and Lemma 2.5, and $a \geq N-e+1-jr$, we obtain

$$\Phi(j) \geq \mu(a, b; [2^N\eta]+y)+\mu(a, b; y) \geq 1.$$

Therefore, by combining the inequality above and (2.9), we conclude that

$$\mu([2^N\eta]+y)+\mu(y) \geq j_0 \geq \frac{N}{r}-2.$$

Since y is an arbitrary nonnegative integer,

$$\nu([2^N\eta]) \geq \frac{N}{r}-2$$

by Lemma 2.4.

Next, we assume that $\eta < 0$. Then, since $2^N\eta \notin \mathbb{Z}$, we have

$$[2^N\eta] = -[-2^N\eta]-1.$$

Thus, by using Corollary 2.3 and lower bounds in the case of $\eta \geq 0$, we obtain

$$\begin{aligned}
\nu([2^N\eta]) &\geq \nu(-[-2^N\eta])-1 \\
&= \nu([-2^N\eta])-1 \geq \frac{N}{r}-3.
\end{aligned}$$

□

3 Proof of Theorem 1.1

First we check the following.

LEMMA 3.1. *Let η_1, η_2 be real numbers.*
(1)

$$|[\eta_1 + \eta_2] - ([\eta_1] + [\eta_2])| \leq 1.$$

(2)

$$|[\eta_1 - \eta_2] - ([\eta_1] - [\eta_2])| \leq 1.$$

Proof. We have

$$[\eta_1 + \eta_2] - ([\eta_1] + [\eta_2]) = -\{\eta_1 + \eta_2\} + \{\eta_1\} + \{\eta_2\}.$$

Thus we may assume that $0 \leq \eta_1, \eta_2 < 1$. Hence

$$[\eta_1 + \eta_2] - ([\eta_1] + [\eta_2]) = \eta_1 + \eta_2 - \{\eta_1 + \eta_2\} = [\eta_1 + \eta_2] \in \{0, 1\},$$

which implies the first statement. Since

$$|[\eta_1 - \eta_2] - ([\eta_1] - [\eta_2])| = |[\eta_1] - ([\eta_1 - \eta_2] + [\eta_2])|,$$

the second statement follows from the first. $\square$

We study the relations between the number $\gamma(\xi, N)$ of digit changes and the value $\nu([2^N \xi^h])$ for $h \in \mathbb{Z}_{\geq 1}$ and $N \in \mathbb{N}$.

LEMMA 3.2. *Let ξ be a positive number. Then, for any $h \in \mathbb{Z}_{\geq 1}$ and $N \in \mathbb{N}$,*

$$\nu([2^N \xi^h]) \leq \big(\gamma(\xi, N) + 1\big)^h + 2^{h+1} \max\{1, \xi^h\}.$$

Proof. First we prove

$$\nu([2^N \xi]) \leq \gamma(\xi, N) + 1. \tag{3.1}$$

Since

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

we get

$$\gamma(\xi, N) = \gamma(\xi 2^N, 0).$$

We denote this number by τ. Let

$$\{n \in \mathbb{N} | s(\xi, n - N) \neq s(\xi, 1 + n - N)\} =: \{0 \leq t_1 < t_2 < \cdots < t_\tau\}.$$

Then

$$\begin{aligned} [2^N \xi] &= \sum_{n=0}^{t_\tau} s(\xi, n - N) 2^n \\ &= s(\xi, t_1 - N) \sum_{n=0}^{t_1} 2^n + \sum_{i=2}^{\tau} s(\xi, t_i - N) \sum_{n=1+t_{i-1}}^{t_i} 2^n. \end{aligned}$$

Note that

$$\nu\left(\sum_{n=0}^{t_1} 2^n\right) = \nu(2^{1+t_1} - 1) \le 2 \tag{3.2}$$

and that, for any i with $2 \le i \le \tau$,

$$\nu\left(\sum_{n=1+t_{i-1}}^{t_i} 2^n\right) = \nu(2^{1+t_i} - 2^{1+t_{i-1}}) \le 2. \tag{3.3}$$

By using (3.2), (3.3) and Lemma 2.2, we obtain

$$\nu([2^N\xi]) \le 2\sum_{i=1}^{\tau} s(\xi, t_i - N).$$

By the definition of $t_1, \ldots, t_\tau$, we have

$$(s(\xi, t_i - N), s(\xi, t_{1+i} - N)) \in \{(0,1), (1,0)\}.$$

Hence

$$\nu([2^N\xi]) \le 2\left[\frac{\tau}{2}\right] \le \tau + 1,$$

which implies (3.1).

Next suppose that $h \ge 2$. Put

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

Note that $2^N\xi_1 \in \mathbb{Z}$. We have

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

and so, by Lemma 3.1,

$$[2^N\xi^h] \le [2^N\xi_1^h] + \left[2^N\sum_{i=1}^{h}\binom{h}{i}\xi_1^{h-i}\xi_2^i\right] + 1.$$

Hence by Corollary 2.3, we get

$$\nu([2^N\xi^h]) \le \nu([2^N\xi_1^h]) + \left[2^N\sum_{i=1}^{h}\binom{h}{i}\xi_1^{h-i}\xi_2^i\right] + 1. \tag{3.4}$$

In what follows we estimate upper bounds of the right-hand side of (3.4). By (3.1) and Lemma 2.2,

$$\nu(2^{hN}\xi_1^h) \le \nu(2^N\xi_1)^h = \nu([2^N\xi])^h \le (\tau+1)^h.$$

By the inequality above and Lemma 2.1, there exist $a, b \in \mathbb{N}$ with $a+b \leq (\tau+1)^h$ and $l_1, \ldots, l_a, k_1, \ldots, k_b \in \mathbb{N}$ satisfying the following:

$$l_1 < \cdots < l_a,\ k_1 < \cdots < k_b; \tag{3.5}$$
$$2^{hN}\xi_1^h = \sum_{i=1}^{a} 2^{l_i} - \sum_{j=1}^{b} 2^{k_j}.$$

Let

$$\begin{aligned}
\theta_1 &= \sum_{\substack{1\leq i\leq a \\ l_i \geq (h-1)N}} 2^{l_i-(h-1)N} - \sum_{\substack{1\leq j\leq b \\ k_j \geq (h-1)N}} 2^{k_j-(h-1)N}, \\
\theta_2 &= \sum_{\substack{1\leq i\leq a \\ l_i < (h-1)N}} 2^{l_i-(h-1)N} - \sum_{\substack{1\leq j\leq b \\ k_j < (h-1)N}} 2^{k_j-(h-1)N}.
\end{aligned}$$

Then $\theta_1 \in \mathbb{Z}$ and

$$\theta_1 + \theta_2 = 2^N \xi_1^h. \tag{3.6}$$

By (3.5) we have

$$\sum_{\substack{1\leq i\leq a \\ l_i < (h-1)N}} 2^{l_i-(h-1)N} < \sum_{i=1}^{\infty} 2^{-i} = 1$$

and

$$\sum_{\substack{1\leq j\leq b \\ k_j < (h-1)N}} 2^{k_j-(h-1)N} < 1.$$

Thus

$$|\theta_2| < 1. \tag{3.7}$$

By combining (3.6) and (3.7), we obtain

$$|[2^N\xi_1^h] - \theta_1| \leq 1.$$

Hence by Corollary 2.3

$$\begin{aligned}
\nu([2^N\xi_1^h]) &\leq \nu(\theta_1) + 1 \\
&\leq a + b + 1 \leq (\tau+1)^h + 1. \qquad (3.8)
\end{aligned}$$

Moreover, since $\xi_1 \leq \xi$ and since $\xi_2 \leq 2^{-N}$,

$$\begin{aligned}
\left[2^N \sum_{i=1}^{h} \binom{h}{i} \xi_1^{h-i}\xi_2^i \right] &\leq \sum_{i=0}^{h} \binom{h}{i} \max\{1, \xi^h\} \\
&= 2^h \max\{1, \xi^h\}. \qquad (3.9)
\end{aligned}$$

By combining (3.4), (3.8), and (3.9), we conclude that

$$\begin{aligned}
\nu([2^N\xi^h]) &\leq (\tau+1)^h + 2^h \max\{1, \xi^h\} + 2 \\
&\leq (\tau+1)^h + 2^{1+h} \max\{1, \xi^h\}.
\end{aligned}$$

□

Now we verify Theorem 1.1. Let $A'_i = A_i/p$ for $i = 1, 2, \ldots, D$. Then we have

$$\sum_{h=1}^{D} A'_h 2^N \xi^h = -\frac{2^N A_0}{p}$$

for each $N \in \mathbb{N}$. By Lemma 2.6 we get

$$\nu\left(\left[-\frac{2^N A_0}{p}\right]\right) \geq \frac{N}{r} - 3. \tag{3.10}$$

On the other hand, by Lemma 3.1

$$\left|\left[\sum_{h=1}^{D} A'_h 2^N \xi^h\right] - \sum_{h=1}^{D} A'_h [2^N \xi^h]\right| \leq \sum_{h=1}^{D} |A'_h|.$$

Hence, by using Corollary 2.3, and Lemmas 2.2 and 3.2, we get

$$\begin{aligned}
\nu\left(\left[-\frac{2^N A_0}{p}\right]\right) &= \nu\left(\left[\sum_{h=1}^{D} A'_h 2^N \xi^h\right]\right) \leq \nu\left(\sum_{h=1}^{D} A'_h [2^N \xi^h]\right) + \sum_{h=1}^{D} |A'_h| \\
&\leq \sum_{h=1}^{D} |A'_h| \Big(\nu([2^N \xi^h]) + 1\Big) \\
&\leq \sum_{h=1}^{D} |A'_h| \Big(\big(\gamma(\xi, N) + 1\big)^h + 2^{h+1} \max\{1, \xi^h\} + 1\Big). \quad (3.11)
\end{aligned}$$

By combining (3.10) and (3.11), we obtain, for every nonnegative integer n,

$$N \leq P(\gamma(\xi, N)), \tag{3.12}$$

where $P(X) \in \mathbb{R}[X]$ is a polynomial of degree D with leading coefficient rA'_D. Thus, for any positive number R, there is an effectively computable positive constant $C'(\xi, R)$ depending only on ξ and R such that

$$\gamma(\xi, N) \geq R$$

for any integer N with $N \geq C'(\xi, R)$. Let ε be an arbitrary positive number with $\varepsilon < 1$. Put

$$\delta := -1 + (1 - \varepsilon)^{-D} > 0.$$

By (3.12), there exists an effectively computable positive constant $C(\xi, \varepsilon)$ depending only on ξ and ε such that, for every integer N with $N \geq C(\xi, \varepsilon)$,

$$N \leq (1 + \delta) r A'_D \gamma(\xi, N)^D,$$

namely,

$$(1 - \varepsilon) p^{1/D} r^{-1/D} A_D^{-1/D} \leq \gamma(\xi, N).$$

Therefore we proved Theorem 1.1.

Acknowledgements

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, Les probabilités dénombrables et leurs applications arithmétiques, Rend. circ. Mat. Palermo **27** (1909), 247-271.

[3] 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.

[4] Y. Bugeaud, On the b-ary expansion of an algebraic number, Rend. Semin. Mat. Univ. Padova **118** (2007), 217-233.

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

[6] J. -H. Evertse and H. P. Schlickewei, A quantitative version of the absolute subspace theorem, J. Reine Angew. Math. **548** (2002), 21-127.

[7] H. Locher, On the number of good approximations of algebraic numbers by algebraic numbers of bounded degree, Acta Arith. **89** (1999), 97-122.

[8] D. Ridout, Rational approximations to algebraic numbers, Mathematika **4** (1957), 125-131.

Department of Mathematics, Kyoto University
Oiwake-tyou
Kitashirakawa
Kyoto-shi, Kyoto, Japan
e-mail: kanekoha@math.kyoto-u.ac.jp