J. Aust. Math. Soc. **89** (2010), 233–244
doi:10.1017/S1446788710001503

ON THE BINARY DIGITS OF ALGEBRAIC NUMBERS

HAJIME KANEKO

(Received 5 January 2010; accepted 5 June 2010)

Communicated by I. E. Shparlinski

Abstract

Borel conjectured that all algebraic irrational numbers are normal in base 2. However, very little is known about this problem. We improve the lower bounds for the number of digit changes in the binary expansions of algebraic irrational numbers.

2000 *Mathematics subject classification*: primary 11K16; secondary 11J71, 11K60.
Keywords and phrases: algebraic numbers, binary expansions, nonadjacent form.

1. Introduction

Borel [3] proved that almost all positive numbers ξ are normal in every integral base α (where $\alpha \geq 2$). That is, 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 little is known about this problem, which was first formulated by Borel [4]. For instance, it is still unknown whether the word 11 occurs infinitely often in the binary 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 $\mathbb{Z}^+$ the set of positive integers. Denote the integral and fractional parts of a real number ξ by $\lfloor \xi \rfloor$ and $\{\xi\}$, respectively. Moreover, let $\lceil \xi \rceil$ be the smallest integer not less than ξ. Then the binary expansion of a positive number ξ is written

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

where

$$s(\xi, n) = \lfloor 2^{-n}\xi \rfloor - 2\lfloor 2^{-n-1}\xi \rfloor \in \{0, 1\}. \tag{1.1}$$

This work was supported by a JSPS fellowship.

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,

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

where Card denotes the cardinality. If ξ is normal in base 2, then $\beta(\xi, N) = 2^N$ for any $N \in \mathbb{Z}^+$. Suppose that ξ is an algebraic irrational number. Bugeaud and Evertse [7] showed for any δ in $(0, 1/11)$ that

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

Secondly, we estimate the number of nonzero digits in the binary expansion of ξ. For each integer N, let

$$\lambda(\xi, N) = \mathrm{Card}\{n \in \mathbb{Z} \mid n \geq -N, s(\xi, n) \neq 0\}.$$

Bailey *et al.* [1] showed that, for any algebraic irrational ξ of degree D (so $D \geq 2$), there exists a positive computable constant $C_0(\xi)$, depending only on ξ, such that

$$\lambda(\xi, N) \geq C_0(\xi) N^{1/D}$$

for all sufficiently large integers N. Rivoal [17] improved the constant $C_0(\xi)$ for certain classes of algebraic irrational ξ. For example, let $\xi' = 0.558\ldots$ be the unique positive zero of the polynomial $8X^3 - 2X^2 + 4X - 3$ and ε be an arbitrary real number in $(0, 1)$. Theorem 7.1 in [1] implies, for any sufficiently large $N \in \mathbb{N}$, that

$$\lambda(\xi', N) \geq (1 - \varepsilon) 16^{-1/3} N^{1/3}.$$

On the other hand, using [17, Corollary 2], we obtain

$$\lambda(\xi', N) \geq (1 - \varepsilon) N^{1/3}$$

for all sufficiently large $N \in \mathbb{N}$.

Now 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 [6], is defined by

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

Note that $\gamma(\xi, N) < \infty$ because $s(\xi, n) = 0$ for all sufficiently large $n \in \mathbb{N}$. Suppose again that ξ is an algebraic irrational number of degree $D \geq 2$. Bugeaud [6] proved, using Ridout's theorem [16], that

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

In the same paper, using a quantitative version of Ridout's theorem [12], he showed that

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

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

for every sufficiently large $N \in \mathbb{N}$. Moreover, improving the quantitative parametric subspace theorem from [9], Bugeaud and Evertse [7] verified that there exist an effectively computable absolute constant $C_1 > 0$ and an effectively computable constant $C_2(\xi) > 0$, depending only on ξ, such that

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

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

Note that if ξ is normal, then the word 10 occurs in the binary expansion of ξ with frequency tending to $1/4$. 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. We now state the main results.

THEOREM 1.1. *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 an odd prime number p that divides the coefficients $A_D, A_{D-1}, \ldots, A_1$, but not the constant term A_0. Let ε be an arbitrary number in $(0, 1)$, and r be the smallest 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 integer N greater than $C(\xi, \varepsilon)$.

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 that divides A. Take any ε in $(0, 1)$, and r as defined in Theorem 1.1. Then, since the minimal polynomial of $A^{-1/D}$ is $AX^D - 1$, it follows from Theorem 1.1 that

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

for every integer N larger than $C(A^{-1/D}, \varepsilon)$. 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 larger than $C(1/\sqrt{3}, \varepsilon)$.

2. Signed binary representations

In this section we study signed binary expansions of a nonzero integer n of the form

$$n = \sum_{i=0}^{l-1} a_i 2^i, \tag{2.1}$$

where $a_i \in \{-1, 0, 1\}$ and $a_{l-1} \neq 0$ when $0 \leq i \leq l-1$. The sequence of signed bits is usually written with the most significant digits a_{l-1} first. In a sequence of

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

signed bits, $\overline{1}$ denotes -1. Thus, $1000\overline{1}$ is a signed bit representation of 15. We are interested in finding a representation of n of minimal Hamming weight, that is, number of nonzero digits. Note that the minimality of a Hamming weight does not determine a unique representation in general, as, for example, $19 = 2^4 + 2 + 1 = 2^4 + 2^2 - 1$. Reitwiesner [15] proved that for each integer n there exists a unique signed expansion (2.1) satisfying

$$a_i a_{i+1} = 0$$

for all $i \geq 0$. We will call this representation the signed separated binary (SSB) expansion of n. We write the Hamming weight of the SSB expansion of n as

$$\nu(n) = \sum_{i=0}^{l-1} |a_i|.$$

For instance, if $l \geq 2$, then $\nu(2^l - 1) = 2$. For convenience, let $\nu(0) := 0$. It is known for every integer n that $\nu(n)$ is the minimal Hamming weight among the signed binary expansions of n (for instance, see [5]). In particular, since

$$n = 1 + \cdots + 1$$

with n summands, or

$$n = -1 - \cdots - 1$$

with $|n|$ summands, we see that

$$\nu(n) \leq |n|. \tag{2.2}$$

SSB expansions have applications in the optimal design of arithmetical hardware [2, 15], in coding theory [13], and in cryptography [14]. For detailed information about the SSB expansions of integers, see [5, 8, 10, 11].

We now show that the function ν satisfies convexity relations, which are analogues of [1, Theorem 4.2].

LEMMA 2.1. *Let m and n be integers. Then*

$$\nu(m + n) \leq \nu(m) + \nu(n) \tag{2.3}$$

and

$$\nu(mn) \leq \nu(m)\nu(n). \tag{2.4}$$

PROOF. It is easy to check (2.3) and (2.4) in the case where $mn = 0$. Thus, we may assume that $mn \neq 0$. Let

$$\Lambda := \{\pm 2^l \mid l \in \mathbb{N}\}.$$

Then there exist $\lambda_1, \ldots, \lambda_{\nu(m)}, \lambda'_1, \ldots, \lambda'_{\nu(n)} \in \Lambda$ such that

$$m = \sum_{k=1}^{\nu(m)} \lambda_k \quad \text{and} \quad n = \sum_{h=1}^{\nu(n)} \lambda'_h. \tag{2.5}$$

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

Then

$$m+n=\sum_{k=1}^{\nu(m)}\lambda_k+\sum_{h=1}^{\nu(n)}\lambda'_h$$

and

$$mn=\sum_{k=1}^{\nu(m)}\sum_{h=1}^{\nu(n)}\lambda_k\lambda'_h.$$

Observe that $\lambda_k\lambda'_h\in\Lambda$ for any k and h. Hence, using the minimality of the Hamming weights of SSB expansions, we obtain (2.3) and (2.4). □

Note that the SSB expansion (2.5) of an integer m satisfies

$$|\lambda_i|\neq|\lambda_j| \quad \text{whenever } 1\le i<j\le\nu(m). \tag{2.6}$$

In fact, if $|\lambda_i|=|\lambda_j|$ for some such i and j, then

$$m=\begin{cases}2\lambda_i+\sum_{k=1,k\neq i,j}^{\nu(m)}\lambda_k & \text{if } \lambda_i=\lambda_k,\\ \sum_{k=1,k\neq i,j}^{\nu(m)}\lambda_k & \text{if } \lambda_i=-\lambda_k.\end{cases}$$

The equality above contradicts the minimality of the Hamming weights of SSB expansions. Combining (2.2) and (2.3), we see that, for all integers m and n,

$$|\nu(m+n)-\nu(m)|\le|n|. \tag{2.7}$$

In fact, we get

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

and

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

The SSB expansions of real numbers were also introduced in [8]. Let V be a nonempty finite word on the alphabet $\{0,1,\overline{1}\}$. We write the right-infinite word $VVV\cdots$ by V^ω. Let

$$\mathcal{K}:=\{\mathbf{x}=x_{-1}x_{-2}x_{-3}\cdots\in\{0,1,\overline{1}\}^{\mathbb{N}}\mid x_{-i}x_{-i-1}=0 \text{ whenever } i\ge1\}.$$

Endowed with the weak topology, $\mathcal{K}$ is a nonempty compact subset of $\{0,1,\overline{1}\}$, so two points are close if they agree on a sufficiently large initial block. Dajani *et al.* [8] introduced the continuous map f from $\mathcal{K}$ onto the interval $[-2/3,2/3]$ given by

$$f(\mathbf{x})=\sum_{i=-\infty}^{-1}x_i2^i=:0.x_{-1}x_{-2}\cdots.$$

We will call this representation the SSB expansion of $f(\mathbf{x})$. Note that f is not injective, that is, the SSB expansion of a given real number $\eta\in[-2/3,2/3]$ is not unique. For instance,

$$\tfrac{1}{3}=0.(01)^\omega=0.1(0\overline{1})^\omega.$$

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

Let ξ be any real number. We take a sufficiently large positive integer R such that

$$\eta := 2^{-R}\xi \in [-\tfrac{2}{3}, \tfrac{2}{3}].$$

Using the SSB expansion of $\eta = \sum_{i=-\infty}^{-1} x_i 2^i$, we define the SSB expansion of ξ as follows:

$$\begin{aligned}\xi &= 2^R \sum_{i=-\infty}^{-1} x_i 2^i \\ &=: \sum_{i=-\infty}^{R-1} y_i 2^i = y_{R-1}\cdots y_0.y_{-1}y_{-2}\cdots ,\end{aligned}$$

where $y_i = x_{i-R}$ for $i \le R-1$. Dajani *et al.* [8] identified $\mathcal{K}$, up to a countable set, with the interval $[-2/3, 2/3]$. They studied the dynamical properties of $\mathcal{K}$, equipped with its Borel σ-algebra $\mathcal{B}_{\mathcal{K}}$ both under the shift σ and the odometer τ. We now give the SSB expansions of rational numbers.

LEMMA 2.2. *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 the SSB expansion of ξ.*

PROOF. Without loss of generality, we may assume that $\xi > 0$. In fact, let $\sum_{i=-\infty}^{R} a_i 2^i$ be the SSB expansion of ξ. Then the SSB expansion of $-\xi$ is $\sum_{i=-\infty}^{R}(-a_i)2^i$. Moreover, we may assume that $\xi < 1/2$. Since ξ is a rational number, its ordinary binary expansion is ultimately periodic. That is,

$$\xi = 0.0UV^{\omega},$$

where U and V are words on the alphabet $\{0, 1\}$ and the length of V is r. Put

$$\xi_k := 0.0UV\cdots V, \tag{2.8}$$

where V appears k times. It is easy to obtain the SSB expansion of ξ_k from its ordinary binary expansion (2.8): apply the following rule repeatedly, working from right to left (that is, least significant first):

replace any sequence $01\cdots 1$, with l consecutive entries 1 (where $l \ge 2$),
by the sequence $10\cdots 0\overline{1}$, with $l-1$ consecutive entries 0.

Hence, the SSB expansion of ξ_k satisfies

$$\xi_k = 0.U'V_1V_2\ldots V_2V_3,$$

where U', V_i are words on the alphabet $\{0, 1, \overline{1}\}$, the word V_2 appears $k-2$ times, and the length of V_i is r when $i = 1, 2, 3$. Therefore, we deduce that the SSB expansion of ξ is

$$\xi = 0.U'V_1V_2^{\omega},$$

which implies Lemma 2.2. □

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

LEMMA 2.3. *Let b be an integer and p be an odd prime number. Assume that p does not divide b. Let r be the minimal positive integer such that p divides $2^r - 1$. Then, for each $N \in \mathbb{N}$,*

$$\nu\left(\left\lfloor \frac{2^N b}{p} \right\rfloor\right) \geq \frac{N}{r} - 4.$$

PROOF. Put $\xi := b/p$. We show that the SSB expansion of ξ is

$$\xi =: \sum_{i=-\infty}^{R} a_i 2^i = U \cdot V_1 V_2^{\omega}, \tag{2.9}$$

where U and both V_j are words on the alphabet $\{0, 1, \overline{1}\}$, and the length of V_j is r (when $j = 1, 2$). For the proof of (2.9), we may assume that $\xi > 0$. Observe that

$$\xi = \lfloor \xi \rfloor + \frac{u}{2^r - 1}$$

for some integer u such that $0 \leq u < 2^r - 1$. Thus, the ordinary binary expansion of ξ satisfies

$$\xi = U' \cdot W^{\omega},$$

where U' and W are words on the alphabet $\{0, 1\}$ and the length of W is r. Hence, as in the proof of Lemma 2.2, we obtain (2.9). For each $N \in \mathbb{N}$, let

$$\xi_N := \sum_{i=-N}^{R} a_i 2^i.$$

Then $2^N \xi_N$ is an integer whose SSB expansion is

$$2^N \xi_N = U V_1 \underbrace{V_2 \cdots V_2}\, V',$$

where V_2 appears $\lfloor N/r \rfloor - 1$ times and V' is the prefix of V_2 of length $r\{N/r\}$. By the assumptions of Lemma 2.3, it is clear that the expansion (2.9) is not finite, that is, at least one letter of the word V_2 is not zero. Hence,

$$\nu(2^N \xi_N) \geq \left\lfloor \frac{N}{r} \right\rfloor - 1. \tag{2.10}$$

Observe that

$$|2^N \xi - 2^N \xi_N| = \left| 2^N \sum_{i=-\infty}^{-N-1} a_i 2^i \right| = \left| \sum_{i=-\infty}^{-1} a_{i-N} 2^i \right|.$$

The second statement of [8, Lemma 1] implies that

$$|2^N \xi - 2^N \xi_N| \leq \tfrac{2}{3},$$

and so

$$|\lfloor 2^N \xi \rfloor - 2^N \xi_N| \leq 2.$$

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

Therefore, combining (2.7) and (2.10), we obtain

$$\nu(\lfloor 2^N \xi \rfloor) \geq \nu(2^N \xi_N) - 2 \geq \left\lfloor \frac{N}{r} \right\rfloor - 3,$$

which implies Lemma 2.3. □

3. Proof of Theorem 1.1

We study the relations between the number of digit changes $\gamma(\xi, N)$ and the value $\nu(\lfloor 2^N \xi^h \rfloor)$ where $h \in \mathbb{Z}^+$ and $N \in \mathbb{N}$. Let η_1 and η_2 be any real numbers. Then it is easily seen that

$$|\lfloor \eta_1 + \eta_2 \rfloor - (\lfloor \eta_1 \rfloor + \lfloor \eta_2 \rfloor)| \leq 1 \tag{3.1}$$

and

$$|\lfloor \eta_1 - \eta_2 \rfloor - (\lfloor \eta_1 \rfloor - \lfloor \eta_2 \rfloor)| \leq 1. \tag{3.2}$$

LEMMA 3.1. *Let ξ be a positive real number. Then, for any $h \in \mathbb{Z}^+$ and $N \in \mathbb{N}$,*

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

PROOF. Let $\tau := \gamma(\xi, N)$. We first consider the case where $h = 1$. Using the definition of τ and the observation that

$$1 \cdots 10 \cdots 0 = 2^{k+l} - 2^k,$$

where 1 occurs l times and 0 occurs k times, we obtain

$$\nu(\lfloor 2^N \xi \rfloor) \leq 2 \left\lceil \frac{\tau}{2} \right\rceil \leq \tau + 1 \tag{3.3}$$

because $\nu(\lfloor 2^N \xi \rfloor)$ is the minimal Hamming weight for the signed binary expansions of $\lfloor 2^N \xi \rfloor$.

Next suppose that $h \geq 2$. Put

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

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

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

and so, by (3.1),

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

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

Hence, by (2.7),

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

In what follows we estimate upper bounds of the right-hand side of (3.4). By (2.4) and (3.3),

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

By the inequality above and (2.6), there exist $a, b \in \mathbb{N}$ such that $a + b \le (\tau + 1)^h$ and $l_1, \dots, l_a, k_1, \dots, k_b \in \mathbb{N}$, which satisfy the following conditions:

$$\begin{aligned} &l_1 < \cdots < l_a \quad \text{and} \quad k_1 < \cdots < k_b; \\ &2^{hN} \xi_1^h = \sum_{i=1}^{a} 2^{l_i} - \sum_{j=1}^{b} 2^{k_j}. \end{aligned} \tag{3.5}$$

Define

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

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

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

By (3.5),

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

and

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

Thus

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

Combining (3.6) and (3.7), we obtain

$$|\lfloor 2^N \xi_1^h \rfloor - \theta_1| \le 1.$$

Hence, by (2.7),

$$\nu(\lfloor 2^N \xi_1^h \rfloor) \le \nu(\theta_1) + 1 \le a + b + 1 \le (\tau + 1)^h + 1. \tag{3.8}$$

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

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

$$2^N \sum_{i=1}^{h} \binom{h}{i} \xi_1^{h-i} \xi_2^i \le \sum_{i=0}^{h} \binom{h}{i} \max\{1, \xi^h\} = 2^h \max\{1, \xi^h\}.$$

Combining (3.4), (3.8), and (3.9), we conclude that

$$\begin{aligned} \nu(\lfloor 2^N \xi^h \rfloor) &\le (\tau+1)^h + 2^h \max\{1, \xi^h\} + 2 \\ &\le (\tau+1)^h + 2^{1+h} \max\{1, \xi^h\}, \end{aligned}$$

as required. □

We now verify Theorem 1.1. Let $A_i' = A_i/p$ when $i = 1, 2, \ldots, D$. Then

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

for each $N \in \mathbb{N}$. By Lemma 2.3,

$$\nu\left(\left\lfloor -\frac{2^N A_0}{p} \right\rfloor\right) \ge \frac{N}{r} - 4. \tag{3.9}$$

On the other hand, by (3.1) and (3.2),

$$\left| \left\lfloor \sum_{h=1}^{D} A_h' 2^N \xi^h \right\rfloor - \sum_{h=1}^{D} A_h' \lfloor 2^N \xi^h \rfloor \right| \le \sum_{h=1}^{D} |A_h'|.$$

Hence, using (2.3), (2.7) and Lemma 3.1, we get

$$\begin{aligned} \nu\left(\left\lfloor -\frac{2^N A_0}{p} \right\rfloor\right) = \nu\left(\left\lfloor \sum_{h=1}^{D} A_h' 2^N \xi^h \right\rfloor\right) &\le \nu\left(\sum_{h=1}^{D} A_h' \lfloor 2^N \xi^h \rfloor\right) + \sum_{h=1}^{D} |A_h'| \\ &\le \sum_{h=1}^{D} |A_h'| (\nu(\lfloor 2^N \xi^h \rfloor) + 1) \qquad (3.10) \\ &\le \sum_{h=1}^{D} |A_h'| ((\gamma(\xi, N) + 1)^h + 2^{h+1} \max\{1, \xi^h\} + 1). \end{aligned}$$

Combining (3.9) and (3.11), we deduce that, for every nonnegative integer N,

$$N \le P(\gamma(\xi, N)), \tag{3.11}$$

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

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

for any integer N greater than $C'(\xi, R)$. Take an arbitrary ε in $(0, 1)$, and put

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

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

By (3.11), there exists an effectively computable positive constant $C(\xi, \varepsilon)$, depending only on ξ and ε, such that, for every integer N greater than $C(\xi, \varepsilon)$,

$$N \le (1+\delta) r A_D' \gamma(\xi, N)^D,$$

that is,

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

We have therefore proved Theorem 1.1.

REMARK 3.1. The constant preceding $N^{1/D}$ in Theorem 1.1 can be improved by considering the number σ of nonzero digits in the period of the SSB expansion of A_0/p. As in the proof of Lemma 2.3, we can show that

$$\nu\left(\left\lfloor -\frac{2^N A_0}{p} \right\rfloor\right) \ge \sigma\left(\left\lfloor \frac{N}{r} \right\rfloor - 1\right) - 2 \ge \frac{\sigma}{r} N - 2\sigma - 2.$$

Let ε be an arbitrary number in $(0, 1)$. Then, by Lemma 3.1, there exists an effectively computable positive constant $C''(\xi, \varepsilon)$, depending only on ξ and ε, such that

$$\gamma(\xi, N) \ge (1-\varepsilon)\left(\frac{\sigma p}{r A_D}\right)^{1/D} N^{1/D} \tag{3.12}$$

for every integer N larger than $C''(\xi, \varepsilon)$, which improves Theorem 1.1.

For instance, we consider the case where $\xi = 1/\sqrt{5}$. Then $A_2 = p = 5$ and $r = 4$. Theorem 1.1 implies that

$$\gamma\left(\frac{1}{\sqrt{5}}, N\right) \ge \frac{1-\varepsilon}{2}\sqrt{N}$$

for each integer N larger than $C(1/\sqrt{5}, \varepsilon)$. Observe that the SSB expansion of $A_0/p = -1/5$ is

$$-\tfrac{1}{5} = 0.(0\bar{1}01)^{\omega}.$$

Hence, the number of nonzero digits in the SSB expansion of A_0/p is 2. Therefore, (3.12) implies that

$$\gamma\left(\frac{1}{\sqrt{5}}, N\right) \ge \frac{1-\varepsilon}{\sqrt{2}}\sqrt{N}$$

for any integer N greater than $C''(1/\sqrt{5}, \varepsilon)$.

Acknowledgements

I would like to express my gratitude to Professor Yann Bugeaud for careful reading of the manuscript and for giving useful advice. I am very grateful to Professor Shigeki Akiyama for useful suggestions and for giving me fruitful information about the references [10, 11]. I would like to thank the referees for their very useful information about the SSB expansions of real numbers and valuable suggestions on Remark 3.1, which improves Theorem 1.1.

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press

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] A. D. Booth, 'A signed multiplication technique', *Quart. J. Mech. Appl. Math.* **4** (1951), 236–240.
[3] É. Borel, 'Les probabilités dénombrables et leurs applications arithmétiques', *Rend. Circ. Mat. Palermo* **27** (1909), 247–271.
[4] 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.
[5] W. Bosma, 'Signed bits and fast exponentiation', *J. Théor. Nombres Bordeaux* **13** (2001), 27–41.
[6] Y. Bugeaud, 'On the b-ary expansion of an algebraic number', *Rend. Sem. Mat. Univ. Padova* **118** (2007), 217–233.
[7] Y. Bugeaud and J.-H. Evertse, 'On two notions of complexity of algebraic numbers', *Acta Arith.* **133** (2008), 221–250.
[8] K. Dajani, C. Kraaikamp and P. Liardet, 'Ergodic properties of signed binary expansions', *Discrete Contin. Dyn. Syst.* **15** (2006), 87–119.
[9] J.-H. Evertse and H. P. Schlickewei, 'A quantitative version of the absolute subspace theorem', *J. Reine Angew. Math.* **548** (2002), 21–127.
[10] P. J. Grabner and C. Heuberger, 'On the number of optimal base 2 representations of integers', *Des. Codes Cryptogr.* **40** (2006), 25–39.
[11] C. Heuberger, 'Minimal expansions in redundant number systems: Fibonacci bases and greedy algorithms', *Period. Math. Hungar.* **49** (2004), 65–89.
[12] H. Locher, 'On the number of good approximations of algebraic numbers by algebraic numbers of bounded degree', *Acta Arith.* **89** (1999), 97–122.
[13] J. L. Massey and O. N. Garcia, 'Error-correcting codes in computer arithmetic', in: *Advances in Information Systems Science,* Vol. 4, (ed. J. Tou) (Plenum Press, New York, 1972), pp. 273–326.
[14] F. Morain and J. Olivos, 'Speeding up the computations on an elliptic curve using addition–subtraction chains', *RAIRO Inform. Théor. Appl.* **24** (1990), 531–543.
[15] G. W. Reitwiesner, 'Binary arithmetic', *Adv. Comput.* **1** (1960), 231–308.
[16] D. Ridout, 'Rational approximations to algebraic numbers', *Mathematika* **4** (1957), 125–131.
[17] T. Rivoal, 'On the bits counting function of real numbers', *J. Aust. Math. Soc.* **85** (2008), 95–111.

HAJIME KANEKO, Department of Mathematics, Kyoto University, Oiwake-tyou, Kitashirakawa, Kyoto-shi, Kyoto 606-8502, Japan
e-mail: kanekoha@math.kyoto-u.ac.jp

https://doi.org/10.1017/S1446788710001503 Published online by Cambridge University Press