sciendo

uniform distribution theory

DOI: 10.2478/UDT-2025-0005
Unif. Distrib. Theory **20** (2025), no.1, 44-67

ARITHMETIC INDEPENDENCE OF CERTAIN UNIFORM SETS OF ALGEBRAIC INTEGERS

ASAKI SAITO[1], JUN-ICHI TAMURA[2] AND SHIN-ICHI YASUTOMI[3]

[1]Department of Complex and Intelligent Systems, Future University Hakodate, Hakodate, JAPAN

[2]Institute for Mathematics and Computer Science, Tsuda College, Kodaira, JAPAN

[3]Faculty of Science, Toho University, Funabashi, JAPAN

ABSTRACT. We study four (families of) sets of algebraic integers of degree less than or equal to three. Apart from being simply defined, we show that they share two distinctive characteristics: almost uniformity and arithmetic independence. Here, "almost uniformity" means that the elements of a finite set are distributed lmost equidistantly in the unit interval, while "arithmetic independence" means that the number fields generated by the elements of a set do not have a mutual inclusion relation each other. Furthermore, we reveal to what extent the algebraic number fields generated by the elements of the four sets can cover quadratic or cubic fields.

Communicated by Shigeki Akiyama

1. Introduction

Saito and Yamaguchi have proposed to use the binary sequence $\{\epsilon_i\}_{i=1,2,\ldots}(\epsilon_i \in \{0,1\})$ obtained from the binary expansion $\alpha = \sum_{i=1}^{\infty} \epsilon_i 2^{-i}$ of an irrational algebraic integer α in the open unit interval $(0,1)$ as a pseudorandom binary sequence [1, 2]. As a set of seeds α for pseudorandom number generation, they introduced two sets, $I_n^{2,r}$ and $I_{m,n}^{3,ntr}$: For any integer n satisfying either $n \geq 1$ or $n \leq -3$, a set $I_n^{2,r}$ of real algebraic integers of degree two over $\mathbb{Q}$ is defined by

$$I_n^{2,r} := \begin{cases} \{\alpha \in (0,1) \mid \alpha^2 + n\alpha + c = 0, c \in \mathbb{Z}, -n \leq c \leq -1\} & \text{if } n \geq 1, \\ \{\alpha \in (0,1) \mid \alpha^2 + n\alpha + c = 0, c \in \mathbb{Z}, 1 \leq c \leq -n-2\} & \text{if } n \leq -3. \end{cases} \tag{1}$$

2020 Mathematics Subject Classification: Primary 11R16, Secondary 11J71, 11R11.
Keywords: algebraic integer, quadratic and cubic fields, arithmetic independence, almost uniformity.

Likewise, for any integers m, n satisfying $m^2 - 3n \leq 0$ and $m + n \geq 1$, a set $I_{m,n}^{3,ntr}$ of real algebraic integers of degree three over $\mathbb{Q}$ is defined by

$$I_{m,n}^{3,ntr} := \{\alpha \in (0,1) \mid \alpha^3 + m\alpha^2 + n\alpha + d = 0, d \in \mathbb{Z}, -(m+n) \leq d \leq -1\}. \quad (2)$$

Note that any $\alpha \in I_{m,n}^{3,ntr}$ is not totally real, that is, α has two complex conjugates (see [2]). Both $I_n^{2,r}$ and $I_{m,n}^{3,ntr}$ have some desirable properties as a set of seeds, such as almost uniform distribution of their elements in the unit interval. For definition of almost uniformity, see end of this section. In particular, they have been observed to have a remarkable property — arithmetic independence— from computer experiments [1, 2]. Here, we say that a set $S \subset \mathbb{C}$ is *arithmetically independent* if $\alpha \notin \mathbb{Q}(\beta)$ and $\beta \notin \mathbb{Q}(\alpha)$ hold for any $\alpha \neq \beta \in S$. If α, β are algebraic numbers of prime degrees, then $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ is equivalent to $\alpha \notin \mathbb{Q}(\beta)$ and $\beta \notin \mathbb{Q}(\alpha)$.

When generating multiple pseudorandom sequences, it is desirable that they are as different from each other as possible. For example, it is undesirable that a certain binary sequence $\{\epsilon_i\}_{i=1,2,...}$. and its complement $\{1 - \epsilon_i\}_{i=1,2,...}$ are generated simultaneously. One can guarantee that such a case does not occur if a seed set I is arithmetically independent. (Note that $\alpha \in I$ implies $1 - \alpha \notin I$.) However, the arithmetic independence of $I_n^{2,r}$ or $I_{m,n}^{3,ntr}$ was only presented as conjectures and no proofs have been given yet. Moreover, algebraic and number theoretical properties, other than the arithmetic independence, of $I_n^{2,r}$ and $I_{m,n}^{3,ntr}$ still remain to be elucidated.

In this paper in addition to the above-mentioned sets $I_n^{2,r}$ and $I_{m,n}^{3,ntr}$, we introduce two sets, $I_n^{2,I}$ and $I_{m,n}^{3,tr}$: A set $I_n^{2,I}$ of imaginary algebraic integers of degree two is defined for any integer $n \geq 1$ as follows:

$$I_n^{2,i} := \begin{cases} \left\{\frac{1+\sqrt{1-4c}}{2} \in \mathbb{C} \setminus \mathbb{R} \,\middle|\, c \in \mathbb{Z}, \left(\frac{n-1}{2}\right)^2 + 1 \leq c \leq \left(\frac{n+1}{2}\right)^2\right\} \\ \text{if } n \text{ is odd,} \\ \left\{\sqrt{-c} \in \mathbb{C} \setminus \mathbb{R} \mid c \in \mathbb{Z}, \left(\frac{n}{2}\right)^2 < c < \left(\frac{n}{2} + 1\right)^2\right\} \text{ if } n \text{ is even.} \end{cases} \quad (3)$$

Note that $(1 + \sqrt{1 - 4c})/2$ is a root of the polynomial $X^2 - X + c$ and $\sqrt{-c}$ is that of $X^2 + c$. Likewise, a set $I_{m,n}^{3,tr}$ of real algebraic integers of degree at most three is defined for any integers m, n satisfying $n \leq -m - 3$ as follows:

$$I_{m,n}^{3,tr} := \{\alpha \in (0,1) \mid \alpha^3 + m\alpha^2 + n\alpha + d = 0, d \in \mathbb{Z}, 1 \leq d \leq -m - n - 2\}. \quad (4)$$

All elements of $I_{m,n}^{3,tr}$ are algebraic integers of degree three, except for at most one algebraic integer of degree two, which is specified in Theorem 14. For these four (families of) sets of algebraic integers, we show that they share two distinctive characteristics: the almost uniformity and the arithmetic independence. Moreover, we show that certain unions of $I_n^{2,r}$ (resp. $I_n^{2,i}$, $I_{m,n}^{3,ntr}$, and $I_{m,n}^{3,tr}$) are *full generative* with respect to real quadratic fields (resp. imaginary quadratic fields except $\mathbb{Q}(\sqrt{-1})$, real cubic fields which are not totally real, and totally real cubic fields) in the sense that it contains a primitive element of any real quadratic field (resp. imaginary quadratic field except $\mathbb{Q}(\sqrt{-1})$, real cubic field which is not totally real, and totally real cubic field). For an algebraic number field K, we say that $\alpha \in K$ is a primitive element of K if $K = \mathbb{Q}(\alpha)$.

To the best of our knowledge, $I_n^{2,r}$, $I_n^{2,i}$, $I_{m,n}^{3,ntr}$, and $I_{m,n}^{3,tr}$ are the simplest sets guaranteed to be arithmetically independent, consisting of algebraic integers of degree two or three. In number theory, it is often the case that the difference in discriminants is used to indicate the difference in fields. However, this is hardly simple as a way of defining sets; in particular it requires further number-theoretic discussion when dealing with fields of degree three or higher with the same discriminant (for details on handling the cubic case, see, e.g., [3,4]). Apart from sets defined using nth roots of appropriately chosen integers, which typically have elements with larger heights than $I_n^{2,r}$, $I_n^{2,i}$, $I_n^{2,i}$, and $I_n^{2,i}$ (for background on heights, see, e.g., [5]), there seem to be almost no other sets of algebraic numbers, or families of algebraic number fields, known to be arithmetically independent. The exception is the one-parameter family of totally real cubic fields K_a generated by $x^3 - ax^2 - (a+3)x - 1$ with $a \in \mathbb{Z}$. The field K_a is called a simplest cubic field [6], and necessary and sufficient conditions are given for K_a and K_b with $a \neq b$ to be isomorphic [7]. (The problem of determining whether wo fields belonging to a specific family are isomorphic is sometimes called field isomorphism problem; see, e.g., [8].) Okazaki showed that all K_a in this family are distinct from each other, except for the obvious coincidence of $K_a = K_{-a-3}$, and a few exceptions: $K_{-1} = K_5 = K_{12} = K_{1259}$, $K_0 = K_3 = K_{54}$, $K_1 = K_{66}$, and $K_2 = K_{2389}$ for $a \geq -1$. Hoshi gave another proof of this result [8, Theorem 1.4], and also showed a similar result for a one-parameter family of totally real sextic fields [9], as well as for a one-parameter family of totally real fields of degree 24 and 12 [10].

Before proceeding we explain what finite sets in the closed unit interval $[0,1]$ are called uniform or almost uniform in this paper. Let N be a positive integer. Let $S = S_N = \left\{x_i = x_i^{(N)} \mid i = 1,2,\dots,N\right\}$ be a finite set with N elements in $[0,1]$. Without loss of generality, we may assume that the elements are ordered increasingly, i.e., $0 \leq x_1 < x_2 < \cdots < x_N \leq 1$. Let $\Delta_i := x_{i+1} - x_i (i \in \{1,2,\dots,N-1\})$ be a distance between two neighboring elements.

We say that the elements of a finite set $S \subset [0,1]$ are distributed uniformly in the unit interval if $\Delta_i = 1/N$ holds for all $i \in \{1,2,\dots,N-1\}$. This definition of uniformity is based on the minimality of the discrepancy D_N, given by

$$D_N = \sup_{0 \leq a < b \leq 1} \left|\frac{A([a,b);S)}{N} - (b-a)\right|,$$

where $A([a,b);S)$ is the number of elements in S that fall into $[a,b)$ [11]. Using [11, theorem 2.7], we see that a finite sequence $\{y_1, y_2, \dots, y_N\}$ in $[0,1]$ gives the minimum value $1/N$ of D_N if and only if there exists $\delta \in [0,1/N]$ such that $y_1, y_2, \dots, y_N$ are the numbers $1/N - \delta, 2/N - \delta, \dots, N/N - \delta$ in some order.

Next we explain the concept of almost uniformity. Let $S_1, S_2, \dots$ be a family of finite sets in $[0,1]$. Assume that there exists a constant c independent of N such that

$$\max_{i \in \{1,2,\dots,N-1\}} \left|\Delta_i - \frac{1}{N}\right| \leq \frac{c}{N^2}$$

holds for all N. We say that the elements of S_N are distributed almost uniformly in the unit interval, or simply that S_N is almost uniform, if $N \geq 2c$. Note that one can impose a condition on N stricter than $N \geq 2c$ in order to avoid less uniform S_N, but such differences in conditions do not affect the subsequent discussion. For simplicity, without explicitly specifying the constant c (and thus the condition $N \geq 2c$), we say that the elements of S_N are distributed almost uniformly in the unit interval for sufficiently large N. Obviously, S_N is almost uniform for sufficiently large N if

$$\max_{i \in \{1,2,\ldots,N-1\}} \left|\Delta_i - \frac{1}{N}\right| = O\left(\frac{1}{N^2}\right) \tag{5}$$

holds, where O is Landau's Big O notation. We can see from [11, theorem 2.7] that the discrepancy D_N of S_N satisfying (5) satisfies $D_N = O(1/N)$.

2. Properties of $I^{2,r}$

In this section, we investigate properties of the sets $I_n^{2,r}$ of real algebraic integers of degree two, which are defined in (1). Concerning the uniformity of $I_n^{2,r}$ in the unit interval, we have the following result.

Proposition 1 *([1]). The elements of $I_b^{2,r}$ are distributed almost uniformly in the unit interval for sufficiently large $|b|$.*

We note that the number of elements in $I_b^{2,r}$, denoted by $|I_b^{2,r}|$, is given by

$$|I_b^{2,r}| = \begin{cases} |b| & \text{if } b \geq 1, \\ |b| - 2 & \text{if } b \leq -3, \end{cases}$$

see (1).

In terms of pseudorandom number generation, this characteristic of $I_n^{2,r}$ is desirable for unbiased sampling of seeds.

As mentioned in the introduction, however, another characteristic of $I_n^{2,r}$, namely the arithmetic independence, was only presented as a conjecture in [1]. Here, we give a proof of the conjecture.

Theorem 2. *Let b be an integer other than $0, -1$ and -2. Then, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ holds for all $\alpha, \beta \in I_b^{2,r}$ with $\alpha \neq \beta$.*

Proof. Assume that there are $\alpha, \beta \in I$^{2,r}_{b} such that $\alpha \neq \beta$ and $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Set $K := \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Let α_1 and α_2 be the conjugates of α. We may assume that $\alpha_1 = \alpha$. Then, $\alpha_2 = -b - \alpha_1$. Similarly, let $\beta 1$ and $\beta 2$ be the conjugates of β, and assume that $\beta_1 = \beta$ and $\beta_2 = -b - \beta_1$. Then, we have

$$|\alpha_2 - \beta_2| = |\alpha_1 - \beta_1| < 1,$$

where the inequality follows from $\alpha_1, \beta_1 \in (0,1)$. The above gives

$$|(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)| < 1. \tag{6}$$

Since $(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)$ is the norm of $\alpha_1 - \beta_1$ as an element of K, it is a rational number, but it is obviously an algebraic integer. Thus, $(\alpha_1 - \beta_1) \times (\alpha_2 - \beta_2)$ is an integer. From (6), we obtain

$$(\alpha_1 - \beta_1)(\alpha_2 - \beta_2) = 0,$$

which implies $\alpha = \beta$. This contradicts the assumption $\alpha \neq \beta$.

We now see the diversity of the quadratic fields generated by the elements in $I_n^{2,r}$ from another viewpoint. Let $S^{2,r}$ be the union of $I_n^{2,r}$ with positive n, namely

$$S^{2,r} := \bigcup_{n \geq 1} I_n^{2,r} \tag{7}$$

It turns out that $S^{2,r}$ includes a primitive element of any real quadratic field, that is, $S^{2,r}$ is full generative with respect to real quadratic fields. We can see this from two stronger properties of $S^{2,r}$ and $I_n^{2,r}$ (see Theorems 3 and 4 below).

In preparation for the next statement, we introduce some notation. Let S be a set of complex numbers. We put

$$+S := S, \quad -S := \{-\alpha \mid \alpha \in S\}.$$

For an integer n, we further put

$$S + n := \{\alpha + n \mid \alpha \in S\}, \quad S - n := \{\alpha - n \mid \alpha \in S\}$$

We put $\langle x \rangle \coloneqq x - \lfloor x \rfloor$, where $\lfloor x \rfloor$ is the greatest integer which does not exceed a real number x. In what follows, we call an algebraic integer of degree two over $\mathbb{Q}$ a quadratic algebraic integer. We also need the following equality:

$$I_{-n-2}^{2,r} = \{1 - \alpha \mid \alpha \in I_n^{2,r}\} \quad n \in \mathbb{Z} \setminus \{0, -1, -2\} \tag{8}$$

This equality follows from the fact that α is a root of $X^2 + bX + c$ if and only if $1 - \alpha$ is a root of $X^2 + (-b - 2)X + b + c + 1$.

Theorem 3. *The followings hold:*

(i) The set of all quadratic algebraic integers in ℝ is expressed as

$$\biguplus_{\substack{n \in \mathbb{Z} \\ \varepsilon \in \{-1, +1\}}} (\varepsilon S^{2,r} + n) \tag{9}$$

where ⊎ denotes disjoint union.

(ii) In particular, $S^{2,r}$ includes a primitive element of any real quadratic field.

Proof. We prove (i). We know that the set of all quadratic algebraic integers in the open unit interval $(0,1)$ is given by

$$\bigcup_{n \in \mathbb{Z} \setminus \{0, -1, -2\}} I_n^{2,r}$$

(see [1]). Using (8), we express this set as $S^{2,r} \cup (-S^{2,r} + 1)$. Let now α be an arbitrary quadratic algebraic integer in $\mathbb{R}$. Then, $\langle \alpha \rangle$ is contained in $S^{2,r} \cup (-S^{2,r} + 1)$. This implies

$$\alpha \in \cup_{n \in \mathbb{Z}} [\{S^{2,r} \cup (-S^{2,r} + 1)\} + n].$$

It is easy to see that the family $\{S^{2,r} + n \mid n \in \mathbb{Z}\} \cup \{-S^{2,r} + n \mid n \in \mathbb{Z}\}$ is mutually disjoint.

To prove (ii), it suffices, by (i), to note that any real quadratic field, denoted by K, includes real quadratic algebraic integers, any of which is a primitive element of K.

Moreover, we can show that for any given finite combination of real quadratic fields, there exists $I_n^{2,r}$ some of whose elements can generate the given fields over $\mathbb{Q}$:

Theorem 4. *Let k be a positive integer. Let $K_1, K_2, \dots, K_k$ be distinct real quadratic fields. Then, there exists a positive integer n such that $I_n^{2,r}$ contains a primitive element of every $K_i (i \in \{1,2, \dots, k\})$.*

Proof. For each K_i, there exists a positive integer j_i such that $K_i = \mathbb{Q}(\sqrt{j_i})(i \in \{1,2, \dots, k\})$. Clearly, 1, $\sqrt{j_1}, \dots, \sqrt{j_k}$ are linearly independent over $\mathbb{Q}$, and so are $1, -\frac{1}{\sqrt{j_1}}, \dots, -\frac{1}{\sqrt{j_k}}$. Let ϵ be a positive number such that $\epsilon\sqrt{j_i} < 1$ for all $i \in \{1,2, \dots, k\}$. By Kronecker's theorem [12], there exist integers $n > 0, m_1, m_2, \dots, m_k$ such that

$$0 < -\frac{n}{\sqrt{j_i}} + m_i < \epsilon \quad (i \in \{1,2, \dots, k\}).$$

Thus, we have $0 < -n + m_i\sqrt{j_i} < \epsilon\sqrt{j_i} < 1 (i \in \{1,2, \dots, k\})$. Set $\alpha_i := -n + m_i\sqrt{j_i} (i \in \{1,2, \dots, k\})$. Obviously, α_i is a quadratic algebraic integer in $(0, 1)$, as well as a primitive element of K_i. Let α_i^σ be the conjugate of αi that is different from α_i, namely $\alpha_i^\sigma = -n - m_i\sqrt{j_i}$. Since $\alpha_i + \alpha_i^\sigma = -2n$, we see that all $\alpha_i (i \in \{1,2, \dots, k\})$ are included in $I_{2n}^{2,r}$.

We note here the following point. One can obtain, in a trivial manner, a family of sets of quadratic algebraic integers in (0, 1), which has the properties described in Theorems 2 and 4. One example is the family $I_n^{2,p} (n \in \mathbb{Z} > 0)$ defined by

$$I_n^{2,p} := \{\langle\sqrt{p_1}\rangle, \langle\sqrt{p_2}\rangle, \dots, \langle\sqrt{p_n}\rangle\},$$

where $p_1, p_2, \dots, p_n$ are the first n prime numbers. The uniformity of $I_n^{2,p}$, however, is inferior to that of $I_n^{2,r}$. For example, $I_8^{2,p}$ consists of five elements less than $1/2$ and three elements greater than $1/2$. Similarly, $I_{32}^{2,p}$ consists of 19 elements less than $1/2$ and 13 elements greater than $1/2$. This is in contrast with the fact that for $I_n^{2,r}$ with even n, the number of elements less than 1/2 is the same as the number of elements greater than $1/2$, and for $I_n^{2,r}$ with odd positive (resp. negative) n, the number of elements less than 1/2 is exactly one less (resp. more) than the number of elements greater than $1/2$. Likewise, there is no expression involving $S^{2,p} := \cup_{n \geq 1} I_n^{2,p}$, which is as simple as (9) and which can cover the set of all quadratic algebraic integers in $\mathbb{R}$. Thus, what makes $I_n^{2,r}$ distinctive is not only the properties described in Theorems 2 and 4 but also other properties such as those described in Proposition 1 and Theorem 3 (i), in addition to its simple definition. In the next section we will see that $I_n^{2,i}$ occupies an equivalent position in the imaginary quadratic domain.

In preparation for the next section, we give the following lemma.

Lemma 5. *Let n be a positive integer. The followings hold:*

(i) For even n, we have

$$I_n^{2,r} + \frac{n}{2} = \left\{\sqrt{-c} \in \mathbb{R} \mid c \in \mathbb{Z}, -\left(\frac{n}{2}+1\right)^2 < c < -\left(\frac{n}{2}\right)^2\right\}.$$

(ii) For odd n, we have

$$I_n^{2,r} + \frac{n+1}{2} = \left\{\frac{1+\sqrt{1-4c}}{2} \in \mathbb{R} \middle| c \in \mathbb{Z}, -\frac{n^2+4n+3}{4} < c < -\frac{n^2-1}{4}\right\}.$$

Proof. We prove (i). Since $n > 0, \alpha \in (0,1)$ satisfying $\alpha^2 + n\alpha + c = 0$ is given by $\alpha = \left(-n + \sqrt{n^2 - 4c}\right)/2$ (cf. (1)). Thus, $\alpha + n/2$ can be written as $\alpha + n/2 = \sqrt{-c'}$, where $c' = -(n/2)^2 + c$. As easily verified, $c \in \mathbb{Z}$ satisfies $-n \leq c \leq -1$ if and only if $c' \in \mathbb{Z}$ satisfies $-(n/2+1)^2 < c' < -(n/2)^2$.

We can prove (ii) in the same way as (i).

3. Properties of $I_n^{2,i}$

In this section, we consider the imaginary quadratic case, which is the counterpart of the real quadratic case considered in Section 2. For $z = x + \sqrt{-1}y (x, y \in \mathbb{R})$, we put $\Re(z) := x, \Im(z) := y$, and $\bar{z} := x - \sqrt{-1}y$, as usual. For a subset S of $\mathbb{C}\backslash\mathbb{R}$, we denote by $\Im(S)$ the set $\{\Im(\alpha) \mid \alpha \in S\}$, and by $\langle\Im(S)\rangle$ the set $\{\langle\Im(\alpha)\rangle \mid \alpha \in S\}$. In this paper, we identify the uniformity of a set $S \subset \mathbb{C} \setminus \mathbb{R}$ as the uniformity of the set $\langle\Im(S)\rangle$ in the unit interval.

We obtain the following result concerning the uniformity of $I_n^{2,i}$ (see (3) for the definition of $I_n^{2,i}$).

Theorem 6. *The elements of $\langle\Im(I_n^{2,i})\rangle$ are distributed almost uniformly in the unit interval for sufficiently large n.*

We note that, from (3), the number of elements in $\langle\Im(I_n^{2,i})\rangle$ is equal to n.

Proof. For even n, it follows from (3) and Lemma 5 (i) that

$$\Im(I_n^{2,i}) = I_n^{2,r} + \frac{n}{2}.$$

The uniformity of $I_n^{2,i}$ then follows from Proposition 1

For odd n, we see that $\Im((1+\sqrt{1-4c})/2)=\sqrt{c-1/4}$. Let $m:=(n-1)/2$. Since $m^2+1 \leq c \leq (m+1)^2$, we see that $m < \sqrt{c-1/4} < m+1$. We assume from now on that $n \neq 1$. The distances $\Delta_i (i \in \{1,2,\ldots,2m\})$ between two neighboring elements of $\langle \Im(I_n^{2,i}) \rangle$ are given by $\Delta_i = \sqrt{(m^2+i+1)-1/4} - \sqrt{(m^2+i)-1/4}$. By the mean value theorem, there exists γ_i in the interval (m^2+i, m^2+i+1) such that $\Delta_i = \left(2\sqrt{\gamma_i - 1/4}\right)^{-1}$. Thus, we have

$$\frac{1}{2m+2} < \frac{1}{2\sqrt{(m^2+2m+1)-1/4}} < \Delta_i < \frac{1}{2\sqrt{(m^2+1)-1/4}} < \frac{1}{2m}$$

for every $i \in \{1,2,\ldots,2m\}$, so that

$$\frac{1}{n+1} - \frac{1}{n} < \Delta_i - \frac{1}{n} < \frac{1}{n-1} - \frac{1}{n},$$

which implies

$$\max_{i \in \{1,2,\ldots,n-1\}} \left|\Delta_i - \frac{1}{n}\right| < \frac{1}{n(n-1)}.$$

Thus, the elements of $\langle \Im(I_n^{2,i}) \rangle$ are distributed in the unit interval almost uniformly for sufficiently large n.

It follows from (10) together with the fact stated before Lemma 5 that for even n, $\langle \Im(I_n^{2,i}) \rangle$ contains an equal number of elements less and greater than $1/2$. Also for odd n, it is easy to verify that the number of elements less than $1/2$ is exactly one less than the number of elements greater than $1/2$, similarly as in $I_n^{2,r}$ with $n \geq 1$.

Next we show that $I_n^{2,i}$ is also arithmetically independent.

Theorem 7. *Let n be a positive integer. Then, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ holds for all $\alpha, \beta \in I_n^{2,i}$ with $\alpha \neq \beta$.*

Proof. We first consider the case where n is even. We see that $\mathbb{Q}(\sqrt{-c}) \neq \mathbb{Q}(\sqrt{-c'})$ holds if c and c' are positive integers satisfying $\mathbb{Q}(\sqrt{c}) \neq \mathbb{Q}(\sqrt{c'})$. Thus, the assertion for even n follows from Theorem 2 together with (3) and Lemma 5 (i).

Now consider the case where n is odd. Assume that there are $\alpha, \beta \in I_n^{2,i}$ such that $\alpha \neq \beta$ and $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Set $K := \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. From the proof of Theorem 6 we have

$$\alpha = \frac{1}{2} + (m + \langle \Im(\alpha) \rangle)\sqrt{-1}, \quad \beta = \frac{1}{2} + (m + \langle \Im(\beta) \rangle)\sqrt{-1},$$

where $m = (n-1)/2$. This gives $|\alpha - \beta| = |\langle \Im(\alpha) \rangle - \langle \Im(\beta) \rangle| < 1$, so that $|(\alpha - \beta)\overline{(\alpha - \beta)}| < 1$. Since $(\alpha - \beta)\overline{(\alpha - \beta)}$ is an algebraic integer as well as the norm of $\alpha - \beta$ as an element of K, it is an integer. Thus, $(\alpha - \beta)\overline{(\alpha - \beta)} = 0$, which implies $\alpha = \beta$. Since $\alpha \neq \beta$, we get a contradiction.

We now turn to consider to what extent the union of $I_n^{2,i}$ or a single $I_n^{2,i}$ can cover the imaginary quadratic fields in the sense of Theorems 3 and 4. We let

$$S^{2,i} := \bigcup_{n\geq 1} I_n^{2,i}.$$

Since $4c-1$ with $c \in \mathbb{Z}_{>0}$ cannot be a square number, we have $S^{2,i} \cap \mathbb{Q}(\sqrt{-1}) = \emptyset$. Set

$$\hat{S}^{2,i} := S^{2,i} \cup \{n\sqrt{-1} \mid n \in \mathbb{Z}_{>0}\}. \tag{11}$$

We will see below that $\hat{S}^{2,i}$ thus defined is full generative with respect to imaginary quadratic fields, and therefore $S^{2,i}$ is full generative with respect to imaginary quadratic fields except $\mathbb{Q}(\sqrt{-1})$ (see Theorems 8 and 9).

To simplify the exposition below, we set

$$(b,c)_+ := \left(-b+\sqrt{b^2-4c}\right)/2, \quad (b,c)_- := \left(-b-\sqrt{b^2-4c}\right)/2.$$

From (3) and (11), we see that

$$\begin{aligned} \hat{S}^{2,i} &= \{(b,c)_+ \mid b \in \{0,-1\}, c \in \mathbb{Z}_{>0}\}, \\ -\hat{S}^{2,i} &= \{(b,c)_- \mid b \in \{0,1\}, c \in \mathbb{Z}_{>0}\}. \end{aligned}$$

The set of all quadratic algebraic integers in $\mathbb{C}\setminus\mathbb{R}$ is given by

$$\{(b,c)_\pm \mid (b,c) \in \mathbb{Z}^2, c > b^2/4\}.$$

An easy calculation shows that for any integer n, we have

$$(b,c)_\pm + n = (-2n+b, n^2-bn+c)_\pm.$$

Theorem 8. *The followings hold:*

(i) The set of all quadratic algebraic integers in $\mathbb{C}\setminus\mathbb{R}$ is expressed as

$$\biguplus_{\substack{n\in\mathbb{Z} \\ \varepsilon\in\{-1,+1\}}} \left(\varepsilon\hat{S}^{2,i}+n\right).$$

The set of all quadratic algebraic integers in $\mathbb{C}\setminus\mathbb{R}$ except those in $\mathbb{Q}(\sqrt{-1})$ is expressed as

$$\biguplus_{\substack{n\in\mathbb{Z} \\ \varepsilon\in\{-1,+1\}}} \left(\varepsilon S^{2,i}+n\right).$$

(ii) In particular, $\hat{S}^{2,i}$ includes a primitive element of any imaginary quadratic field; $S^{2,i}$ includes a primitive element of any imaginary quadratic field except $\mathbb{Q}(\sqrt{-1})$.

Proof. We have

$$\begin{aligned} \hat{S}^{2,i}+n &= (\{(0,c)_+ \mid c \in \mathbb{Z}_{>0}\}+n) \cup (\{(-1,c)_+ \mid c \in \mathbb{Z}_{>0}\}+n), \\ &= \{(-2n, n^2+c)_+ \mid c \in \mathbb{Z}_{>0}\} \cup \{(-2n-1, n^2+n+c)_+ \mid c \in \mathbb{Z}_{>0}\}. \end{aligned}$$

Considering that $(-2n)^2/4 = n^2, (-2n-1)^2/4 = n^2 + n + 1/4$, and $\cup_{n\in\mathbb{Z}} \{-2\mathrm{n}, -2\mathrm{n}-1\} = \mathbb{Z}$, we obtain

$$\cup_{n\in\mathbb{Z}} \left(\hat{S}^{2,i} + n\right) = \{(b,c)_+ \mid (b,c) \in \mathbb{Z}^2, c > b^2/4\}.$$

By a similar argument, we obtain

$$\cup_{n\in\mathbb{Z}} \left(-\hat{S}^{2,i} + n\right) = \{(b,c)_- \mid (b,c) \in \mathbb{Z}^2, c > b^2/4\}.$$

Therefore

$$\{(b,c)_\pm \mid (b,c) \in \mathbb{Z}^2, c > b^2/4\} = \left(\cup_{n\in\mathbb{Z}} \left(\hat{S}^{2,i} + n\right)\right) \cup \left(\cup_{n\in\mathbb{Z}} \left(-\hat{S}^{2,i} + n\right)\right).$$

It is easy to see that the family $\{\hat{S}^{2,i} + n \mid n \in \mathbb{Z}\} \cup \{-\hat{S}^{2,i} + n \mid n \in \mathbb{Z}\}$ is mutually disjoint. The second statement of (i) is derived from the first statement by considering the fact that for $n \in \mathbb{Z}, (b,c)_\pm + n \in \mathbb{Q}(\sqrt{-1})$ if and only if $(b,c)_\pm \in \mathbb{Q}(\sqrt{-1})$.

As in the proof of Theorem 3, (ii) follows from (i).

The following theorem is the imaginary counterpart of Theorem 4.

Theorem 9. *Let k be a positive integer. Let $K_1, K_2, \dots, K_k$ be distinct imaginary quadratic fields other than $\mathbb{Q}(\sqrt{-1})$. Then, there exists a positive integer n such that $I_{2n}^{2,i}$ contains a primitive element of every $K_i (i \in \{1,2,\dots,k\})$.*

Proof. For each K_i, there exists a square-free integer $j_i \geq 2$ such that $K_i = \mathbb{Q}\left(\sqrt{-j_i}\right) (i \in \{1,2,\dots,k\})$. We define the real quadratic fields $K_i' (i \in \{1,2,\dots,k\})$ by $K_i' := \mathbb{Q}\left(\sqrt{j_i}\right)$. By Theorem 4, there exists a positive integer n such that $I_{2n}^{2,r}$ contains a primitive element of every K_i'. Obviously, $I_{2n}^{2,r} + n$ also contains a primitive element of every K_i'. Using Lemma 5 (i), we express this set as

$$I_{2n}^{2,r} + n = \left\{\sqrt{c} \in \mathbb{R} \mid c \in \mathbb{Z}, n^2 < c < (n+1)^2\right\}.$$

Thus, for each j_i, there exists an integer ci in the range $n^2 < c_i < (n+1)^2$ such that $c_i = m_i^2 j_i$ for some integer m_i. By (3) we have

$$I_{2n}^{2,i} = \left\{\sqrt{-c} \in \mathbb{C} \setminus \mathbb{R} \mid c \in \mathbb{Z}, n^2 < c < (n+1)^2\right\},$$

and we find that $\sqrt{-c_i} \in I_{2n}^{2,i}$ is a primitive element of $K_i = \mathbb{Q}\left(\sqrt{-j_i}\right)$.

Lastly in this section, it is worth noting that as in the real quadratic case, one can define a set $\tilde{I}_n^{2,i}$ which is twin to $I_n^{2,i}$ by

$$\tilde{I}_n^{2,i} := \left\{1 - \alpha \mid \alpha \in I_n^{2,i}\right\} \quad n = 1,2,\dots, \tag{12}$$

see (8). By using (3), we obtain explicit formulae for $\tilde{I}_n^{2,i}$:

$$\tilde{I}_n^{2,i} = \begin{cases} \left\{(-1,c)_- \in \mathbb{C}\setminus\mathbb{R} \mid c \in \mathbb{Z}, \left(\frac{n-1}{2}\right)^2 + 1 \le c \le \left(\frac{n+1}{2}\right)^2\right\} \\ \text{if } n \text{ is odd,} \\ \left\{(-2,c)_- \in \mathbb{C}\setminus\mathbb{R} \mid c \in \mathbb{Z}, \left(\frac{n}{2}\right)^2 + 1 < c < \left(\frac{n}{2}+1\right)^2 + 1\right\} \\ \text{if } n \text{ is even.} \end{cases}$$

Due to definition (12), $\tilde{I}_n^{2,i}$ has the properties described in Theorems 7 and 9.

Also the uniformity of $\tilde{I}_n^{2,i}$ is as good as that of $I_n^{2,i}$ since

$$\langle \Im(\tilde{I}_n^{2,i}) \rangle = \{1 - \beta \mid \beta \in \langle \Im(I_n^{2,i}) \rangle\}$$

holds.

4. Properties of $I_{m,n}^{3,ntr}$

In this section, we investigate properties of the sets $I_{m,n}^{3,ntr}$ of real cubic algebraic integers that are not totally real (see (2) for the definition of $I_{m,n}^{3,ntr}$). As for the uniformity of $I_{m,n}^{3,ntr}$ in the unit interval, we have the following result.

Proposition 10 *([2]). Let b be a fixed integer. Then, the elements of $I_{b,c}^{3,ntr}$ are distributed almost uniformly in the unit interval for sufficiently large c.*

We note that, from (2), the number of elements in $I_{b,c}^{3,ntr}$ is equal to $b + c$.

Moreover, we can easily see that similarly to $I_n^{2,r} (n \ge 1)$ and $I_n^{2,i} (n \ge 1)$ discussed in the previous sections, the following holds for $I_{m,n}^{3,ntr}$ with $m \in \{0, -1\}$, namely $I_{0,n}^{3,ntr} (n \ge 1)$ and $I_{-1,n}^{3,ntr} (n \ge 2)$: If $I_{0,n}^{3,ntr}$ (or $I_{-1,n}^{3,ntr}$) consists of even number of elements, then the elements less than $1/2$ and those greater than 1/2 are equal in number. If $I_{0,n}^{3,ntr}$ (or $I_{-1,n}^{3,ntr}$) consists of odd number of elements, then the number of elements less than $1/2$ is exactly one less than the number of elements greater than $1/2$. From the fact that α is a root of $X^3 + bX^2 + cX + d$ if and only if $1 - \alpha$ is a root of $X^3 + (-b - 3)X^2 + (2b + c + 3)X + (-b - c - d - 1)$, we obtain

$$I_{-b-3,2b+c+3}^{3,ntr} = \{1 - \alpha \mid \alpha \in I_{b,c}^{3,ntr}\}. \tag{13}$$

Thus, we see that the elements of $I_{-2,n}^{3,ntr} (n \ge 3)$ (or $I_{-3,n}^{3,ntr} (n \ge 4)$) are also divided into the intervals $(0, 1/2)$ and $(1/2, 1)$ as equally as possible (i.e., the number of elements in $(0, 1/2)$ is equal to or exactly one more than the number of elements in $(1/2, 1)$). On the other hand, for m other than $0, -1, -2$, and -3, uniformity in this sense is inferior. In fact, it is not difficult to see that even if $I_{m,n}^{3,ntr}$ with $m \in \mathbb{Z}\,\{0, -1, -2, -3\}$ consists of even number of elements, the elements less than $1/2$ and those greater than $1/2$ are not equal in number (i.e., the difference between the number of elements in $(0, 1/2)$ and the number of elements in $(1/2, 1)$ is greater than or equal to two). Thus, we will specialise to $I_{m,n}^{3,ntr}$ with $m \in \{0, -1, -2, -3\}$ below.

We now show the arithmetic independence of $I_{m,n}^{3,ntr}$ with $m \in \{0,-1,-2,-3\}$, which was originally conjectured in [2, Conjecture 1].

Theorem 11. *Let b, c be integers satisfying $-3 \leq b \leq 0$ and $c \geq -b+1$. Then, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ holds for all $\alpha, \beta \in I_{b,c}^{3,ntr}$ with $\alpha \neq \beta$.*

Note that if b and c satisfy $-3 \leq b \leq 0$ and $c \geq -b+1$, then $b^2 \leq 3_c$ holds (cf. definition (2)).

Proof. Assume that $\alpha, \beta \in I_{b,c}^{3,ntr}$ with $\alpha \neq \beta$ satisfy $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Let $\alpha_i (i \in \{1,2,3\})$ (resp. $\beta_i (i \in \{1,2,3\})$) be the conjugates of α (resp. β). We may assume that $\alpha_1 = \alpha$, $\beta_1 = \beta$, and $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_i) (i \in \{1,2,3\})$. Note that α_i and β_i with $i > 1$ are imaginary numbers, and that α_3 (resp. β_3) is the complex conjugate of α_2 (resp. β_2). We assume that α_2 is in the upper half of the complex plane (β_2 can be in the upper or lower half plane).

We divide the proof into four cases: (i) $b=0$, $c \geq 1$, (ii) $b=-1$, $c \geq 2$, (iii) $b=-2$, $c \geq 3$, (iv) $b=-3$, $c \geq 4$.

Case (i): For calculational convenience, we temporarily assume that $c \geq 10$. By the relation between roots and coefficients, we have

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \qquad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = c.$$

Thus, we have

$$\alpha_1(\alpha_2 + \alpha_3) + \alpha_2\alpha_3 = c, \qquad \alpha_2\alpha_3 = c + \alpha_1^2, \qquad |\alpha_2| (= |\alpha_3|) = \sqrt{c + \alpha_1^2}.$$

Therefore, we obtain $\alpha_2 = -\frac{\alpha_1}{2} + \sqrt{c + \frac{3\alpha_1^2}{4}}\, i$, where we denote for simplicity $\sqrt{-1}$ by i. In a similar manner, we have (P) $\beta_2 = -\frac{\beta_1}{2} + \sqrt{c + \frac{3\beta_1^2}{4}}\, i$ or (M) $\beta_2 = -\frac{\beta_1}{2} - \sqrt{c + \frac{3\beta_1^2}{4}}\, i$.

First, assume (P). Then we have

$$\alpha_2 - \beta_2 = -\frac{\alpha_1 - \beta_1}{2} + \left(\sqrt{c + \frac{3\alpha_1^2}{4}} - \sqrt{c + \frac{3\beta_1^2}{4}} \right) i,$$

which means that

$$\begin{aligned} |\alpha_2 - \beta_2| &\leq \frac{|\alpha_1 - \beta_1|}{2} + \left| \sqrt{c + \frac{3\alpha_1^2}{4}} - \sqrt{c + \frac{3\beta_1^2}{4}} \right| \\ &= \frac{|\alpha_1 - \beta_1|}{2} + \left| \frac{\frac{3(\alpha_1^2 - \beta_1^2)}{4}}{\sqrt{c + \frac{3\alpha_1^2}{4}} + \sqrt{c + \frac{3\beta_1^2}{4}}} \right| \\ &< \frac{1}{2} + \frac{\frac{3}{4}}{2\sqrt{c}} \leq \frac{1}{2} + \frac{3}{8\sqrt{10}} < 1. \end{aligned}$$

Since $\alpha_3 - \beta_3 = \overline{\alpha_2 - \beta_2}$, we also have $|\alpha_3 - \beta_3| < 1$. Thus, we see that $|(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)(\alpha_3 - \beta_3)| < 1$. Since $(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)(\alpha_3 - \beta_3) \in \mathbb{Z}$, we have $(\alpha_1 - \beta_1)(\alpha_2 - \beta_2)(\alpha_3 - \beta_3) = 0$, which implies $\alpha_1 = \beta_1$. This contradicts $\alpha \neq \beta$.

Second, assume (M). Then we have

$$\alpha_2 + \beta_2 = -\frac{\alpha_1+\beta_1}{2} + \left(\sqrt{c + \frac{3\alpha_1^2}{4}} - \sqrt{c + \frac{3\beta_1^2}{4}}\right) i,$$

which means that

$$|\alpha_2 + \beta_2| \leq \frac{|\alpha_1+\beta_1|}{2} + \left|\sqrt{c + \frac{3\alpha_1^2}{4}} - \sqrt{c + \frac{3\beta_1^2}{4}}\right|$$
$$< 1 + \frac{\frac{3}{4}}{2\sqrt{c}} \leq 1 + \frac{3}{8\sqrt{10}} < 1.1186.$$

We also have $|\alpha_3 + \beta_3| < 1.1186$. Since $|\alpha_1 + \beta_1| < 2$, we see that $|(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3)| < 2 \times (1.1186)^2 = 2.50253192$. Since $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \in \mathbb{Z}$, we see that $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3)$ is equal to either 0, 1, or 2. Assuming $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) = 0$, we have $\alpha_1 + \beta_1 = 0$, which is a contradiction. Thus, $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3)$ is equal to 1 or 2. We now show that $\alpha_1 + \beta_1 \notin \mathbb{Q}$ (i.e., $\alpha_1 + \beta_1 \notin \mathbb{Z}$). Assuming $r := \alpha_1 + \beta_1 \in \mathbb{Q}$, we have $3r = (\alpha_1 + \beta_1) + (\alpha_2 + \beta_2) + (\alpha_3 + \beta_3) = 0$, which contradicts $r \neq 0$. Thus, $\alpha_1 + \beta_1$ is a cubic algebraic integer. Note that $\alpha_1 + \beta_1$ has negative discriminant

TABLE 1. Numerical roots of irreducible polynomials $x^3 + px - q$ with $|p| \leq 5, q \in \{1,2\}$, and negative discriminant

Polynomial	*Real root*	*Imaginary roots*
$x^3 - 2x - 2$	1.76929	$-0.88465 \pm 0.58974i$
$x^3 - x - 1$	1.32472	$-0.66236 \pm 0.56228i$
$x^3 - x - 2$	1.52138	$-0.76069 \pm 0.85787i$
$x^3 - 2$	1.25992	$-0.62996 \pm 1.09112i$
$x^3 + x - 1$	0.68233	$-0.34116 \pm 1.16154i$
$x^3 + 2x - 1$	0.45340	$-0.22670 \pm 1.46771i$
$x^3 + 2x - 2$	0.77092	$-0.38546 \pm 1.56388i$
$x^3 + 3x - 1$	0.32219	$-0.16109 \pm 1.75438i$
$x^3 + 3x - 2$	0.59607	$-0.29804 \pm 1.80734i$
$x^3 + 4x - 1$	0.24627	$-0.12313 \pm 2.01134i$
$x^3 + 4x - 2$	0.47347	$-0.23673 \pm 2.04160i$

x^3+5x-1	0.19844	$-0.09922 \pm 2.24266i$
x^3+5x-2	0.38829	$-0.19415 \pm 2.26121i$

since α_1 has negative discriminant and $\alpha_1+\beta_1 \in \mathbb{Q}(\alpha_1)$. We have

$$\begin{aligned}
&|(\alpha_1+\beta_1)(\alpha_2+\beta_2)+(\alpha_2+\beta_2)(\alpha_3+\beta_3)+(\alpha_3+\beta_3)(\alpha_1+\beta_1)| \\
&\leq |\alpha_1+\beta_1||\alpha_2+\beta_2|+|\alpha_2+\beta_2||\alpha_3+\beta_3|+|\alpha_3+\beta_3||\alpha_1+\beta_1| \\
&< 2\times 1.1186+(1.1186)^2+1.1186\times 2 \\
&= 5.72566596 < 6.
\end{aligned}$$

Therefore, the minimal polynomial of $\alpha_1+\beta_1$, denoted by x^3+px-q, satisfies $|p| \leq 5$ and $q \in \{1,2\}$. We numerically found the roots of x^3+px-q which is irreducible and whose discriminant is negative, and we show the results in Table 1. We can see from the above argument that the absolute value of the imaginary part of $\alpha_2+\beta_2$ is less than 0.1186, but there is no polynomial having such an imaginary root in Table 1. So again we arrive at a contradiction.

Consequently, we have proved the assertion for $c \geq 10$ in Case (i). The assertion for $1 \leq c < 10$ has already been confirmed by direct computation in [2].

Case (ii): As in the proof of Case (i), we temporarily assume that $c \geq 10$. Using

$$\alpha_1+\alpha_2+\alpha_3=1, \qquad \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1=c,$$

we have

$$\begin{aligned}
&\alpha_1(\alpha_2+\alpha_3)+\alpha_2\alpha_3=c, \qquad \alpha_2\alpha_3=c-\alpha_1(1-\alpha_1), \\
&|\alpha_2|(=|\alpha_3|)=\sqrt{c-\alpha_1(1-\alpha_1)},
\end{aligned}$$

and we obtain $\alpha_2=\frac{1-\alpha_1}{2}+\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}\,i$. Similarly, we have (P)$\beta_2=\frac{1-\beta_1}{2}+\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\,i$ or (M) $\beta_2=\frac{1-\beta_1}{2}-\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\,i$.

First, assume (P). Then we have

$$\alpha_2-\beta_2=-\frac{\alpha_1-\beta_1}{2}+\left(\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}-\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\right)i,$$

which means that

$$\begin{aligned}
|\alpha_2-\beta_2| &\leq \frac{|\alpha_1-\beta_1|}{2}+\left|\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}-\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\right| \\
&= \frac{|\alpha_1-\beta_1|}{2}+\left|\frac{\frac{(\alpha_1-\beta_1)\{3(\alpha_1+\beta_1)-2\}}{4}}{\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}+\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}}\right|.
\end{aligned}$$

Since $3x^2-2x-1=3(x-1/3)^2-4/3$, we have

$$|\alpha_2-\beta_2|<\frac{1}{2}+\frac{1}{2\sqrt{c-\frac{1}{3}}}\le\frac{1}{2}+\frac{1}{2\sqrt{\frac{29}{3}}}<1.$$

We also have $|\alpha_3-\beta_3|<1$. Thus, we see that $|(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3)|<1$, and we have $(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3)=0$. This contradicts $\alpha\neq\beta$.

Second, assume (M). Then we have

$$\alpha_2+\beta_2=1-\frac{\alpha_1+\beta_1}{2}+\left(\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}-\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\right)i,$$

which means that

$$|\alpha_2+\beta_2|\le\left|1-\frac{\alpha_1+\beta_1}{2}\right|+\left|\sqrt{c+\frac{3\alpha_1^2-2\alpha_1-1}{4}}-\sqrt{c+\frac{3\beta_1^2-2\beta_1-1}{4}}\right|$$
$$<1+\frac{1}{2\sqrt{c-\frac{1}{3}}}\le1+\frac{1}{2\sqrt{\frac{29}{3}}}<1.1609.$$

We also have $|\alpha_3+\beta_3|<1.1609$. Thus, $|(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3)|<2\times(1.1609)^2=2.69537762$. Since $\alpha_1+\beta_1>0$, we have $(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3)>0$. Thus, $(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3)$ is equal to 1 or 2. We now show that $\alpha_1+\beta_1\notin\mathbb{Q}$, namely $\alpha_1+\beta_1\notin\mathbb{Z}$. Assuming $z:=\alpha_1+\beta_1\in\mathbb{Z}$, we have $3z=(\alpha_1+\beta_1)+(\alpha_2+\beta_2)+(\alpha_3+\beta_3)=2$, which gives the contradiction

TABLE 2. Numerical roots of irreducible polynomials x^3-2x^2+px-q with $|p|\le 5, q\in\{1,2\}$, and negative discriminant

Polynomial	*Real root*	*Imaginary roots*
x^3-2x^2-4x-2	3.36523	$-0.68262\pm0.35826i$
x^3-2x^2-3x-1	3.07960	$-0.53980\pm0.18258i$
x^3-2x^2-3x-2	3.15276	$-0.57638\pm0.54968i$
x^3-2x^2-2x-1	2.83118	$-0.41559\pm0.42485i$
x^3-2x^2-2x-2	2.91964	$-0.45982\pm0.68817i$
x^3-2x^2-x-1	2.54682	$-0.27341\pm0.56382i$
x^3-2x^2-x-2	2.65897	$-0.32948\pm0.80225i$
x^3-2x^2-1	2.20557	$-0.10278\pm0.66546i$
x^3-2x^2-2	2.35930	$-0.17965\pm0.90301i$
x^3-2x^2+x-1	1.75488	$0.12256\pm0.74486i$
x^3-2x^2+2x-2	1.54369	$0.22816\pm1.11514i$

$x^3 - 2x^2 + 3x - 1$	0.43016	$0.78492 \pm 1.30714i$
$x^3 - 2x^2 + 4x - 1$	0.28477	$0.85761 \pm 1.66615i$
$x^3 - 2x^2 + 4x - 2$	0.63890	$0.68055 \pm 1.63317i$
$x^3 - 2x^2 + 5x - 1$	0.21676	$0.89162 \pm 1.95409i$
$x^3 - 2x^2 + 5x - 2$	0.46682	$0.76659 \pm 1.92266i$

$z = 2/3$. Thus, $\alpha_1 + \beta_1$ is a cubic algebraic integer. Note that $\alpha_1 + \beta_1$ has negative discriminant since α_1 has negative discriminant and $\alpha_1 + \beta_1 \in \mathbb{Q}(\alpha_1)$.

We have

$$\begin{aligned}
&|(\alpha_1+\beta_1)(\alpha_2+\beta_2)+(\alpha_2+\beta_2)(\alpha_3+\beta_3)+(\alpha_3+\beta_3)(\alpha_1+\beta_1)| \\
&\leq |\alpha_1+\beta_1||\alpha_2+\beta_2|+|\alpha_2+\beta_2||\alpha_3+\beta_3|+|\alpha_3+\beta_3||\alpha_1+\beta_1| \\
&< 2\times 1.1609 + (1.1609)^2 + 1.1609\times 2 \\
&= 5.99128881 < 6.
\end{aligned}$$

Therefore, the minimal polynomial of $\alpha_1 + \beta_1$, denoted by $x^3 - 2x^2 + px - q$, satisfies $|p| \leq 5$ and $q \in \{1,2\}$. Table 2 shows numerical roots of $x^3 - 2x^2 + px - q$ which is irreducible and whose discriminant is negative. From the above argument, the absolute value of the imaginary part of $\alpha_2 + \beta_2$ is less than 0.1609, but there is no such imaginary root in Table 2. So again we arrive at a contradiction.

Consequently, we have proved the assertion for $c \geq 10$ in Case (ii). The assertion for $2 \leq c < 10$ has already been confirmed in [2].

By (13), proofs for Cases (iii) and (iv) follow from Cases (ii) and (i), respectively.

Note that in contrast to the one-parameter families $\{I_n^{2,r}\}$ and $\{I_n^{2,i}\}$ discussed in the previous sections, the two-parameter family $\{I_{m,n}^{3,ntr}\}$ with m unrestricted includes a set which has more than one element belonging to an identical field. For example, the two elements $\sqrt[3]{2} - 1$ and $\sqrt[3]{2^2} - 1$ of $I_{3,3}^{3,ntr}$ belong to the same cubic field $\mathbb{Q}(\sqrt[3]{2})$.

We now move on to consider to what extent some unions of $I_{m,n}^{3,ntr}$ can cover the cubic fields. For each integer m in $\{0,-1,-2,-3\}$, we define the set $S_m^{3,ntr}$ by

$$S_m^{3,ntr} := \bigcup_{n \geq -m+1} I_{m,n}^{3,ntr}$$

As noted before, if m and n satisfy $-3 \leq m \leq 0$ and $n \geq -m + 1$, then $m^2 \leq 3n$ holds. For the cubic sets $S_m^{3,ntr}$ with $m = 0$ and -3 (i.e., $S_0^{3,ntr}$ and $S_{-3}^{3,ntr}$), we prove a result weaker than Theorems 3, 4, 8, and 9 for the quadratic counterparts. That is, we just show their full generation with respect to real cubic fields which are not totally real.

Theorem 12. The set $S_0^{3,ntr}$ includes a primitive element of any real cubic field which is not totally real. The same is true of $S_{-3}^{3,ntr}$.

Proof. By (13), it suffices to prove the statement for $S_0^{3,ntr}$. Let K be a real cubic field with two complex embeddings. Let O_K be the ring of algebraic integers of K. We denote by $\sigma_i, i = 1,2,3$, the three embeddings of K into $\mathbb{C}$, where we may assume that σ_1 is the identity map on K. Let ϕ be the embedding of K into $\mathbb{R} \times \mathbb{C}$ defined by $\phi(\alpha) := (\sigma_1(\alpha), \sigma_2(\alpha))$ for $\alpha \in K$. For a real number $\lambda > 0$, we define the set $D(\lambda) \subset \mathbb{R} \times \mathbb{C}$ by

$$D(\lambda) := \{(u, s + ti) \in \mathbb{R} \times \mathbb{C} | |u|, |s| \leq 1/4, |t| \leq \lambda\}.$$

This $D(\lambda)$ is a convex set which is symmetric with respect to the origin. We choose λ sufficiently large so that there exists $\alpha \in O\_\{K\}$ such that $\alpha \neq 0$ and $\phi(\alpha) \in D(\lambda)$, by Minkowski's theorem [12]. Due to the symmetry of $D(\lambda)$, we can assume that $\alpha > 0$. Note that α is not a rational number (i.e., $\alpha \notin \mathbb{Z}$) since $|\alpha| \leq 1/4$. We denote the minimal polynomial of α by $X^3 + bX^2 + cX + d$. As before, we put $\alpha_1 := \alpha, \alpha_2 := \sigma_2(\alpha)$, and $\alpha_3 := \sigma_3(\alpha)$. Since $|\alpha_1| \leq 1/4$, we see that $0 < \alpha_1 \leq 1/4$. Likewise, we have $|\Re(\alpha_2)| \leq 1/4$. Thus,

$$|\alpha_1 + \alpha_2 + \alpha_3| = |\alpha_1 + 2\Re(\alpha_2)| < 1.$$

Since $\alpha_1 + \alpha_2 + \alpha_3 \in \mathbb{Z}$, we see that $\alpha_1 + \alpha_2 + \alpha_3 = 0$, which implies $b = 0$. We also see that $\alpha_1\alpha_2\alpha_3 \in \mathbb{Z}$ is nonzero. This means that $|\alpha_1\alpha_2\alpha_3| \geq 1$, and therefore $\alpha_2\alpha_3 \geq 4$. Then, we have

$$c = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = \alpha_1\big(2\Re(\alpha_2)\big) + \alpha_2\alpha_3 \geq 4 - 1/8 > 0.$$

Let $f: \mathbb{R} \to \mathbb{R}$ be a function given by $f(x) = x^3 + bx^2 + cx + d$. Since $b = 0$ and $c > 0$, we see that f is strictly monotonically increasing. Since $f(\alpha) = 0$ and $0 < \alpha < 1$, we have $f(0) < 0$ and $f(1) > 0$, which implies $-c - 1 < d < 0$. Thus, we have $\alpha \in I_{0,c}^{3,ntr} \subset S_0^{3,ntr}$.

In contrast with $S_0^{3,ntr}$ and $S_{-3}^{3,ntr}$, the other sets, $S_{-1}^{3,ntr}$ and $S_{-2}^{3,ntr}$, are not full generative with respect to real cubic fields which are not totally real. For example, any algebraic integer in $\mathbb{Q}(\sqrt[3]{2})$ has a multiple of three as its trace, and therefore it does not belong to $S_{-1}^{3,ntr}$ and $S_{-2}^{3,ntr}$, which consist of algebraic integers whose traces are one and two, respectively.

5. Properties of $I_{m,n}^{3,tr}$

This section deals with the sets $I_{m,n}^{3,tr}$, which are defined in (4). By definition, $I_{m,n}^{3,tr}$ consists of real algebraic integers of degree at most three. Since the open unit interval $(0, 1)$ contains no integer, any $\alpha \in I_{m,n}^{3,tr}$ is irrational. Let $f(x) = x$^{3} $+ mx$^{2} $+ nx + d$ for $m, n, d \in \mathbb{Z}$ satisfying $n \leq -m - 3$ and $1 \leq d \leq -m - n - 2$. Since f is a monic cubic polynomial satisfying $f(0) > 0$ and $f(1) < 0$, f has three real roots, only one of which is in $(0, 1)$. Thus, if $\alpha \in I_{m,n}^{3,tr}$ is cubic, then α is totally real, that is, all conjugates of α are real. We will show that $I_{m,n}^{3,tr}$ contains at most one, if any, quadratic integer, and all other elements are totally real cubic (cf. Theorem 14).

As in (13), we have

$$I_{-b-3,2b+c+3}^{3,tr} = \{1 - \alpha \mid \alpha \in I_{b,c}^{3,tr}\}. \tag{14}$$

We obtain the following result concerning the uniformity of $I_{b,c}^{3,tr}$.

Theorem 13. *Let b be a fixed integer. Then, the elements of $I_{b,c}^{3,tr}$ are distributed almost uniformly in the unit interval for any negative integer c whose absolute value is sufficiently large.*

We note that, from (4), the number of elements in $I_{b,c}^{3,tr}$ is equal to $-b-c-2$.

Proof. We first introduce some notation. Let b, c, d be integers satisfying $c \leq -b-3$ and $1 \leq d \leq -b-c-2$. Let $f_d(x) = x^3 + bx^2 + cx + d$, and let α_d be the root of f_d in the open unit interval (0,1). We see easily that $\alpha_{d-1} < \alpha_d$ and $f_d(\alpha_{d-1}) = 1$ hold for $d \in \{2, 3, \dots, -b-c-2\}$. Let $\Delta_d = \alpha_d - \alpha_{d-1} (d \in \{2,3,\dots,-b-c-2\})$. By the mean value theorem, there exists $\beta \in (\alpha_{d-1}, \alpha_d)$ such that $f_d'(\beta) = -\Delta_d^{-1}$.

By (14), it suffices to show the assertion for $b \geq -1$. We consider two cases. If $b = -1$, we easily verify that $c - 1/3 \leq f_d'(x) < c+1$ holds for $x \in (0,1)$. This gives

$$(-c+1/3)^{-1} \leq \Delta_d < (-c-1)^{-1}.$$

We denote by N the number of the elements of $I_{-1,c}^{3,tr}$, namely $N = -c-1$. Then, we have

$$\frac{-4/3}{N(N+4/3)} = \frac{1}{N+4/3} - \frac{1}{N} \leq \Delta_d - \frac{1}{N} < \frac{1}{N} - \frac{1}{N} = 0,$$

which implies

$$\max_{d \in \{2,3,\dots,N\}} \left| \Delta_d - \frac{1}{N} \right| \leq \frac{4/3}{N(N+4/3)}.$$

Thus, for sufficiently large negative c (and therefore sufficiently large N), the elements of $I_{-1,c}^{3,tr}$ are distributed almost uniformly in the unit interval.

If $b \geq 0$, we see that $c < f_d'(x) < 3 + 2b + c$ holds for $x \in (0,1)$. Suppose that $c < -2b-3$. Then, we have

$$(-c)^{-1} < \Delta_d < (-3-2b-c)^{-1}.$$

As above, we denote by N the number of the elements of $I_{b,c}^{3,tr}$, i.e., $N = -b-c-2$. Then, we have

$$\frac{-b-2}{N(N+b+2)} = \frac{1}{N+b+2} - \frac{1}{N} < \Delta_d - \frac{1}{N} < \frac{1}{N-b-1} - \frac{1}{N} = \frac{b+1}{N(N-b-1)},$$

which implies

$$\max_{d \in \{2,3,\dots,N\}} \left| \Delta_d - \frac{1}{N} \right| < \max\left\{ \frac{b+2}{N(N+b+2)}, \frac{b+1}{N(N-b-1)} \right\}.$$

Thus, for sufficiently large negative c (and therefore sufficiently large N), the elements of $I_{b,c}^{3,tr}$ are distributed almost uniformly in the unit interval.

Moreover, for any $I_{m,n}^{3,tr}$ with $m \in \{0,-1,-2,-3\}$ and $n \leq -m-3$, we can how that its elements are divided into the intervals $(0,1/2)$ and $(1/2,1)$ as equally as possible, similarly to $I_n^{2,r}(n \geq 1)$, $I_n^{2,i}(n \geq 1)$, and $I_{m,n}^{3,ntr}$ $(m \in \{0,-1,-2,-3\}, n \geq -m+1)$ (see discussion following Proposition 10).

We now establish the arithmetic independence of $I_{m,n}^{3,tr}$ with $m \in \{0,-1,-2,-3\}$. In addition, we show that such $I_{m,n}^{3,tr}$ contains at most one, if any, real quadratic integer, and all other elements are totally real cubic.

Theorem 14. *Let b, c be integers satisfying $-3 \leq b \leq 0$ and $c \leq -b-3$. Then, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ holds for all $\alpha, \beta \in I_{b,c}^{3,tr}$ with $\alpha \neq \beta$. Moreover, all the elements of $I_{b,c}^{3,tr}$ are totally real cubic if c is of the form $-n^2+(b-1)n-1 (n \in \mathbb{Z}, n \geq \delta_b)$ or $-n^2+bn (n \in \mathbb{Z}, n \geq 1+\epsilon_b-\epsilon_{-3-b})$, where $\delta_b, \epsilon_b (b \in \{0,-1,-2,-3\})$ are integers defined by $\delta_0=\delta_{-1}=1, \delta_{-2}=\delta_{-3}=0, \epsilon_0=1, \epsilon_{-1}=\epsilon_{-2}=\epsilon_{-3}=0$. Otherwise all the elements, except one, are totally real cubic. The exception is the element that is real quadratic. Specifically, for c satisfying $-n^2+(b-1)n-1<c<-n^2+bn (n \in \mathbb{Z}, n \geq 1+\epsilon_b)$ or $-n^2+bn<c<-n^2+(b-1)n-1 (n \in \mathbb{Z}, n \leq -3-\epsilon_{-3-b})$, the unique quadratic element is a root of the polynomial $x^3+bx^2+cx-(n-b)(c+n^2-bn)$, and its minimal polynomial is given by $x^2+nx+c+n^2-bn$.*

Note that every integer $c \leq -b-3$ falls into exactly one of the four cases stated in the statement, namely $c=-n^2+(b-1)n-1 (n \in \mathbb{Z},\ n \geq \delta_b), c=-n^2+bn (n \in \mathbb{Z}, n \geq 1+\epsilon_b-\epsilon_{-3-b}), -n^2+(b-1)n-1<c<-n^2+bn (n \in \mathbb{Z}, n \geq 1+\epsilon_b)$, and $-n^2+bn<c<-n^2+(b-1)n-1 (n \in \mathbb{Z}, n \leq -3-\epsilon_{-3-b})$ To see this, it may be helpful to observe that c satisfies

$$-n^2+bn<c<-n^2+(b-1)n-1$$

for some integer $n \leq -3-\epsilon_{-3-b}$ if and only if

$$-(m+1)^2+b(m+1)<c<-m^2+(b-1)m-1$$

for some integer $m \geq 2+b+\epsilon_{-3-b}$, where $n=-m+b-1$.

Proof. We begin with the case $b=0$ with $c=-n^2-n-1 (n \in \mathbb{Z}, n \geq 1)$. Let $f(x)=x^3+cx+d$ with $d \in \{1,2,\ldots,-c-\ 2\}$. We see that f has three real roots, since $f(0)>0, f(1)<0, f(-n-1)<0, f(-n)>0, f(n)<0$, and $f(n+1)>0$ hold. More specifically, each of three open intervals $(0,1)$, $(-n-1,-n)$, and $(n,n+1)$ contains only one of the three roots. This, together with the fact that f is a monic cubic polynomial with integer coefficients, implies that f is irreducible, and thus all the elements of $I_{0,c}^{3,tr}$ are totally real cubic.

We now assume that $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$ holds for some $\alpha, \beta \in I_{0,c}^{3,tr}$ with $\alpha \neq \beta$. Let $\alpha_i (i \in \{1,2,3\})$ (resp. $\beta_i (i \in \{1,2,3\})$) be the conjugates of α (resp. β). As in the proof of Theorem 11, we assume that $\alpha_1=\alpha, \beta_1=\beta$, and $\mathbb{Q}(\alpha_i)=\mathbb{Q}(\beta_i) (i \in \{1,2,3\})$. Note that $\alpha\_\{i\}$ and $\beta\_\{i\}$ with $i>1$ are in either $(n,n+1)$ or $(-n-1,-n)$. We assume that $\alpha\_\{2\}$ is in $(n,n+1)$ (β_2 can be in $(n,n+1)$ or $(-n-1,-n)$).

First assume that $\beta_2 \in (n,n+1)$. Since $|\alpha_1-\beta_1|<1, |\alpha_2-\beta_2|<1$, and $|\alpha_3-\beta_3|<1$, we have $|(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3)|<1$. Since $(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3) \in \mathbb{Z}$, we see that $(\alpha_1\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3)=0$. This contradicts $\alpha \neq \beta$.

Now assume that $\beta_2 \in (-n-1,-n)$. Then, we have $0 < \alpha_1 + \beta_1 < 2, -1 < \alpha_2 + \beta_2 < 1$, and $-1 < \alpha_3 + \beta_3 < 1$, which give $-2 < (\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) < 2$. Since $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \in \mathbb{Z}$, we see that $(\alpha_1 + \beta_1)(\alpha_2 + \beta_2)(\alpha_3 + \beta_3) \in \{-1,0,1\}$. We now show that $\alpha_1 + \beta_1 \notin \mathbb{Q}$ (i.e., $\alpha_1 + \beta_1 \notin \mathbb{Z}$). Assuming $r := \alpha_1 + \beta_1 \in \mathbb{Q}$, we have $3r = (\alpha_1 + \beta_1) + (\alpha_2 + \beta_2) + (\alpha_3 + \beta_3) = 0$, which contradicts $r \neq 0$. Thus, $\alpha_1 + \beta_1$ is a cubic algebraic integer

TABLE 3. Numerical roots of irreducible polynomials $x^3 + px - q$ with $|p| \le 4$, $q \in \{-1, 0, 1\}$, and positive discriminant

Polynomial	*Roots*
$x^3 - 4x + 1$	−2.11491 0.25410 1.86081
$x^3 - 4x - 1$	−1.86081 −0.25410 2.11491
$x^3 - 3x + 1$	−1.87939 0.34730 1.53209
$x^3 - 3x - 1$	−1.53209 −0.34730 1.87939

We have

$$-5 < (\alpha_1 + \beta_1)(\alpha_2 + \beta_2) + (\alpha_2 + \beta_2)(\alpha_3 + \beta_3) + (\alpha_3 + \beta_3)(\alpha_1 + \beta_1) < 5.$$

Therefore, the minimal polynomial of $\alpha_1 + \beta_1$, denoted by $x_3 + px - q$, satisfies $|p| \le 4$ and $q \in \{-1, 0, 1\}$. Table 3 shows numerical roots of $x^3 + px - q$ which is irreducible and whose discriminant is positive. From the above argument, all the roots of the minimal polynomial of $\alpha_1 + \beta_1$ are greater than -1, but every polynomial in Table 3 has a root less than -1. So again we arrive at a contradiction.

The proof for the case $b = 0$ with $c = -n^2 (n \in \mathbb{Z}, n \ge 2)$ can be obtained by a similar argument.

We now consider the case $b = 0$ with $-n^2 - n - 1 < c < -n^2 (n \in \mathbb{Z}, n \ge 2)$. We can see that f satisfies $f(0) > 0$, $f(1) < 0$, $f(-n-1) < 0$, $f(-n) > 0$, $f(n - 1/2) < 0$, and $f(n + 1/2) > 0$. Thus, f has three real roots, each of which is contained in one of the three intervals $(0, 1)$, $(-n-1, -n)$, and $(n - 1/2, n + 1/2)$. We now show that $I_{0,c}^{3,tr}$ contains only one quadratic element and that all other elements are cubic. In order to clarify the dependence of f on d, we denote $x^3 + cx + d$ by $f_d(x)$ below. Letting $i = -c - n^2$, we find $i \in \{1,2, \dots, n\}$ and $ni \in \{1, 2, \dots, -c-2\}$. Since $x^3 + cx + ni = (x - n)(x^2 + nx - i)$, the root of fd with $d = ni$ in the interval $(0, 1)$ is a quadratic algebraic integer, whose minimal polynomial is given by $x^2 + nx - i$. Let $\gamma(d)$ be the root of f_d in the interval $(n - 1/2, n + 1/2)$. We see easily that $\gamma(d)$ satisfies $\gamma(1) > \gamma(2) > \cdots > \gamma(-c-2)$. Since n is only one integer in the interval $(n - 1/2, n + 1/2)$, f_d is reducible if and only if $d = ni$. Thus, the above quadratic element is the only quadratic element in $I_{0,c}^{3,tr}$, and all the other elements are cubic algebraic integers.

We denote, for now, the root of f_d in the interval $(0, 1)$ by $\alpha(d)$ $(d \in \{1,2,\dots,-c-2\})$. As noted above, $\alpha(ni)$ is the only quadratic element in $I_{0,c}^{3,tr}$, and thus $\mathbb{Q}(\alpha(d)) \neq \mathbb{Q}(\alpha(ni))$ holds for all $d \neq ni$. Hence it suffices to show that $\mathbb{Q}(\alpha(d)) \neq \mathbb{Q}(\alpha(d'))$ holds for all $d, d' \in$

$\{1,2,\dots,-c-2\}\setminus\{ni\}$ with $d \neq d'$. We put $\alpha = \alpha(d)$ and $\beta = \alpha(d')$ and assume that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, as before. We let $\alpha_i (i \in \{1,2,3\})$ (resp. $\beta_i (i \in \{1,2,3\})$) be the conjugates of α (resp. β) and let $\alpha_1 = \alpha$, $\beta_1 = \beta$, and $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\beta_i)(i \in \{1,2,3\})$. Note that α_i and β_i with $i > 1$ are in either $(n-1/2, n+1/2)$ or $(-n-1,-n)$. We assume that α_2 is in $(n-1/2, n+1/2)$ (β_2 can be in $(n-1/2, n+1/2)$ or $(-n-1,-n)$).

TABLE 4. Numerical roots of irreducible polynomials x^3+px-q with $p \in \{-6,-5,\dots,3,4\}$, $q \in \{-1,0,1,2,3,4\}$, and positive discriminant

Polynomial	*Roots*
x^3-6x+1	−2.52892 0.16745 2.36147
x^3-6x-1	−2.36147 −0.16745 2.52892
x^3-6x-2	−2.26180 −0.33988 2.60168
x^3-6x-3	−2.14510 −0.52398 2.66908
x^3-5x+1	−2.33006 0.20164 2.12842
x^3-5x-1	−2.12842 −0.20164 2.33006
x^3-5x-3	−1.83424 −0.65662 2.49086
x^3-4x+1	−2.11491 0.25410 1.86081
x^3-4x+1	−1.86081 −0.25410 2.11491
x^3-4x-2	−1.67513 −0.53919 2.21432
x^3-3x+1	−1.87939 0.34730 1.53209
x^3-3x-1	−1.53209 −0.34730 1.87939

First assume that $\beta_2 \in (-n-1,-n)$. Since $|\alpha_1-\beta_1| < 1, |\alpha_2-\beta_2| < 1$, and $|\alpha_3-\beta_3| < 1$, we have $|(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3)| < 1$. Since $(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3) \in \mathbb{Z}$, we see that $(\alpha_1-\beta_1)(\alpha_2-\beta_2)(\alpha_3-\beta_3) = 0$. This contradicts $\alpha \neq \beta$.

Now assume that $\beta_2 \in (-n-1,-n)$. Then, we have $0 < \alpha_1+\beta_1 < 2, -3/2 < \alpha_2+\beta_2 < 1/2$, and $-3/2 < \alpha_3+\beta_3 < 1/2$, which give $-3/2 < (\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3) < 9/2$. Since $(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3) \in \mathbb{Z}$, we see that $(\alpha_1+\beta_1)(\alpha_2+\beta_2)(\alpha_3+\beta_3) \in \{-1,0,1,2,3,4\}$. We now show that $\alpha_1+\beta_1 \notin \mathbb{Q}$ (i.e., $\alpha_1+\beta_1 \notin \mathbb{Z}$). Assuming $r := \alpha_1+\beta_1 \in \mathbb{Q}$, we have $3r = (\alpha_1+\beta_1)+(\alpha_2+\beta_2)+(\alpha_3+\beta_3) = 0$, which contradicts $r \neq 0$. Thus, $\alpha_1+\beta_1$ is a cubic algebraic integer. We have

$$-\frac{27}{4} < (\alpha_1+\beta_1)(\alpha_2+\beta_2)+(\alpha_2+\beta_2)(\alpha_3+\beta_3)+(\alpha_3+\beta_3)(\alpha_1+\beta_1) < \frac{17}{4}.$$

Therefore, the minimal polynomial of $\alpha_1+\beta_1$, denoted by x^3+px-q, satisfies $p \in \{-6,-5,\dots,3,4\}$ and $q \in \{-1,0,1,2,3,4\}$. Table 4 shows numerical roots of x^3+px-q which is irreducible and whose discriminant is positive. From the above argument, all the roots of the minimal polynomial of $\alpha_1+\beta_1$ are greater than $-3/2$, but every polynomial in Table 4 has a root less than $-3/2$. So again we arrive at a contradiction

The proof for the case $b = 0$ with $-n^2 < c < -n^2 - n - 1 (n \in \mathbb{Z}, n \leq -3)$ can be obtained by a similar argument.

Thus we have completed the proof for the case $b = 0$.

The proof for the case $b = -1$ is obtained from an argument analogous to that used in the case $b = 0$.

By (14) together with discussions succeeding (8) and preceding (13), proofs for the cases $b = -2$ and $b = -3$ follow from the cases $b = -1$ and $b = 0$, respectively.

For each integer m in $\{0, -1, -2, -3\}$, we define the set $S_m^{3,tr}$ by

$$S_m^{3,tr} := \bigcup_{n \leq -m-3} I_{m,n}^{3,tr}.$$

We denote by Quad(S) the set of all quadratic elements of a given set S. From the above theorem and the discussion at the beginning of the proof of Theorem 3, we obtain:

Corollary 15. *The followings hold:*

(i) The set of all quadratic algebraic integers in $S_0^{3,tr}$ (resp. $S_{-1}^{3,tr}$, $S_{-2}^{3,tr}$, and $S_{-3}^{3,tr}$) is expressed as

$$\mathrm{Quad}\left(S_0^{3,tr}\right) = \bigcup_{n \in \mathbb{Z} \setminus \{-2,-1,0,1\}} I_n^{2,r} = \left(S^{2,r} \setminus \left\{\tfrac{-1+\sqrt{5}}{2}\right\}\right) \cup (-S^{2,r} + 1),$$
$$\mathrm{Quad}\left(S_{-1}^{3,tr}\right) = \mathrm{Quad}\left(S_{-2}^{3,tr}\right) = \bigcup_{n \in \mathbb{Z} \setminus \{-2,-1,0\}} I_n^{2,r} = S^{2,r} \cup (-S^{2,r} + 1),$$
$$\mathrm{Quad}\left(S_{-3}^{3,tr}\right) = \bigcup_{n \in \mathbb{Z} \setminus \{-3,-2,-1,0\}} I_n^{2,r} = S^{2,r} \cup \left((-S^{2,r} + 1) \setminus \left\{\tfrac{3-\sqrt{5}}{2}\right\}\right),$$

where $S^{2,r}$ is given by (7) in Section 2.

(ii) In particular, $S_m^{3,tr}$ with $m \in \{0, -1, -2, -3\}$ includes a primitive element of any real quadratic field.

To rephrase Corollary 15 (ii), $S_m^{3,tr}$ with $m \in \{0, -1, -2, -3\}$ are full generative with respect to real quadratic fields. Moreover, analogously to Theorem 12, we show that $S_m^{3,tr}$ with $m = 0$ and -3 (i.e., $S_0^{3,tr}$ and $S_{-3}^{3,tr}$) are full generative with respect to totally real cubic fields:

Theorem 16. *The set $S_0^{3,tr}$ includes a primitive element of any totally real cubic field. The same is true of $S_{-3}^{3,tr}$.*

Proof. By (14), it suffices to prove the statement for $S_0^{3,tr}$. Let K be a totally real cubic field. Let O_K be the ring of algebraic integers of K. We denote by $\sigma\_\{i\}, i = 1, 2, 3$, the three embeddings of K into $\mathbb{C}$, where we may assume that σ_1 is the identity map on K. Let ϕ be the embedding of K into $\mathbb{R}^3$ defined by $\phi(\alpha) := (\sigma_1(\alpha), \sigma_2(\alpha), \sigma_3(\alpha))$ for $\alpha \in K$. For positive real numbers λ_1, λ_2, and λ_3, we define the set $D(\lambda_1, \lambda_2, \lambda_3) \subset \mathbb{R}^3$ by

$$D(\lambda_1, \lambda_2, \lambda_3) := \{(x_1, x_2, x_3) \in \mathbb{R}^3 \,|\, |x_1| \leq \lambda_1, |x_2|, |x_3| \leq \lambda_2, |x_2 + x_3| \leq \lambda_3\}.$$

This set is convex and symmetric with respect to the origin. If $\sigma_2(\alpha) + \sigma_3(\alpha) = 0$ holds for $\alpha \in K$, then $\alpha = 0$ since the trace of α is zero. Therefore, there exists $0 < \epsilon < 1/2$ such that

$$D(1/4, 3 + \epsilon, \epsilon) \cap \phi(O_K) = \{\phi(0)\}.$$

We choose $\lambda > 0$ sufficiently large so that there exists $\beta \in O_K$ such that $\beta \neq 0$ and $\phi(\beta) \in D(1/4, \lambda, \epsilon)$ by Minkowski's theorem. Due to the symmetry of $D(1/4, \lambda, \epsilon)$, we can assume that $\beta > 0$. Note that β is not a rational number (i.e., $\beta \neq \mathbb{Z}$) since $0 < \epsilon < 1/2$. We denote the minimal polynomial of β by $X^3 + bX^2 + cX + d$. We put β_{1}$: = \beta$, $\beta_2 \coloneqq \sigma_2(\beta)$, and $\beta_3 \coloneqq \sigma_3(\beta)$. Then,

$$|\beta_1 + \beta_2 + \beta_3| \leq |\beta_1| + |\beta_2 + \beta_3| < \frac{1}{4} + \frac{1}{2} < 1.$$

Since $\beta_1 + \beta_2 + \beta_3 \in \mathbb{Z}$, we see that $\beta_1 + \beta_2 + \beta_3 = 0$, which implies $b = 0$. Since $(\beta_1, \beta_2, \beta_3) \in D(1/4, \lambda, \epsilon) \setminus D(1/4, 3 + \epsilon, \epsilon)$, we have $|\beta_2 + \beta_3| \leq \epsilon$, and at least one of $|\beta_2| > 3 + \epsilon$ or $|\beta_3| > 3 + \epsilon$ holds. This gives $|\beta_2| > 3$ and $|\beta_3| > 3$. Combined with $|\beta_2 + \beta_3| < 1/2$, this yields $\beta_2\beta_3 < -9$. Then, we have

$$c = \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 = \beta_1(\beta_2 + \beta_3) + \beta_2\beta_3 < \frac{1}{8} - 9 < -8,$$

and

$$1 + c + d = 1 + \beta_1(\beta_2 + \beta_3) + \beta_2\beta_3(1 - \beta_1) < 1 + \frac{1}{8} - 9 \cdot \frac{3}{4} < 0.$$

Since $\beta_1 > 0$ and $\beta_2\beta_3 < -9$, we see that $d > 0$. Therefore, we have $\beta \in S_0^{3,tr}$.

Similarly to $S_{-1}^{3,ntr}$ and $S_{-2}^{3,ntr}$ discussed in the previous section, we note that $S_{-1}^{3,tr}$ and $S_{-2}^{3,tr}$ are not full generative with respect to totally real cubic fields, in contrast with $S_0^{3,tr}$ and $S_{-3}^{3,tr}$. For example, consider a totally real cubic field $K = \mathbb{Q}(\alpha)$, where α is one of the roots of $X^3 - 3X + 1$. The $\{1, \alpha, \alpha^2\}$ forms an integral basis of K, and the traces of these elements are given by 3, 0, and 6, respectively. Since any algebraic integer in K has a multiple of three as its trace, it does not belong to $S_{-1}^{3,tr}$ and $S_{-2}^{3,tr}$.

Acknowledgement. We thank Shigeki Akiyama and Zeev Rudnick for their helpful comments. We are also grateful to the anonymous referee for useful suggestions. This research was supported by JSPS KAKENHI Grant Numbers JP15K00342, JP16KK0005, and JP22K12197.

REFERENCES

[1] SAITO, A.—YAMAGUCHI, A.: Pseudorandom number generation using chaotic true orbits of the Bernoulli map, Chaos 26 (2016), 063122.

[2] SAITO, A.—YAMAGUCHI, A.: Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers, Chaos 28 (2018), 103122.

[3] DELONE, B. N.—FADDEEV, D. K.: The Theory of Irrationalities of the Third Degree. American Mathematical Society, Providence, R.I., 1964.

[4] HAMBLETON, S. A.—WILLIAMS, H. C.: Cubic Fields with Geometry. Springer, 2018.

[5] SILVERMAN, J. H.: The Arithmetic of Dynamical Systems. Springer, New York, 2007.

[6] SHANKS, D.: The simplest cubic fields, Math. Comp. 28 (1974), 1137—1152.

[7] MORTON, P.: Characterizing cyclic cubic extensions by automorphism polynomials, J. Number Theory 49 (1994), 183–208.

[8] HOSHI, A.: On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields, J. Number Theory 131 (2011), 2135–2150.

[9] HOSHI, A.: On the simplest sextic fields and related Thue equations, Funct. Approx. Comment. Math. 47 (2012), 35–49.

[10] HOSHI, A.: Complete solutions to a family of Thue equations of degree 12, J. Théor. Nombres Bordeaux 29 (2017), 549—568.

[11] NIEDERREITER, H.: Random Number Generation and Quasi-Monte Carlo Methods. SIAM, 1992.

[12] HARDY, G. H.—WRIGHT, E. M.: An Introduction to the Theory of Numbers, 5th ed. Oxford University Press, 1979.

Received November 15, 2023
Accepted August 18, 2025

Asaki Saito
Department of Complex and Intelligent Systems
Future University Hakodate. 16-2 Kamedanakano-cho. Hakodate, Hokkaido 041-8655. JAPAN
E-mail: saito@fun.ac.jp

Jun-ichi Tamura
Institute for Mathematics and Computer Science
Tsuda College. 2-1-1 Tsuda-machi. Kodaira, Tokyo 187-8577. JAPAN
E-mail: jtamura@tsuda.ac.jp

Shin-ichi Yasutomi
Faculty of Science. Toho University. 2-2-1 Miyama
Funabashi, Chiba 274-8510. JAPAN
E-mail: shinichi.yasutomi@sci.toho-u.ac.jp