Bull. Aust. Math. Soc. **110** (2024), 77–89
doi:10.1017/S0004972723000953

THE LIFTING PROBLEM FOR UNIVERSAL QUADRATIC FORMS OVER SIMPLEST CUBIC FIELDS

DANIEL GIL-MUÑOZ and MAGDALÉNA TINKOVÁ✉

(Received 21 July 2023; accepted 13 August 2023; first published online 6 October 2023)

Abstract

The lifting problem for universal quadratic forms over a totally real number field K consists of determining the existence or otherwise of a quadratic form with integer coefficients (or $\mathbb{Z}$-form) that is universal over K. We prove the nonexistence of universal $\mathbb{Z}$-forms over simplest cubic fields for which the integer parameter is big enough. The monogenic case is already known. We prove the nonexistence in the nonmonogenic case by using the existence of a totally positive nonunit algebraic integer in K with minimal (codifferent) trace equal to one.

2020 *Mathematics subject classification*: primary 11R16; secondary 11E12, 11R04, 11R80.

Keywords and phrases: universal quadratic form, totally real number field, additively indecomposable integer.

1. Introduction

A quadratic form with integer coefficients is said to be universal if it represents all positive integers. These objects appear in classical problems and results in arithmetic, such as the Lagrange four-square theorem: the quadratic form $x^2 + y^2 + z^2 + w^2$ is universal because every positive integer can be written as the sum of four squares. As in this case, we will restrict our work to positive definite quadratic forms.

More generally, if K is a totally real number field, a quadratic form with coefficients in its ring of algebraic integers O_K is universal (over K) if it represents all totally positive elements in O_K. In this definition, an element in O_K is totally positive if it is mapped by any embedding of K to a positive real number. The subset of all totally positive elements in O_K will be denoted by O_K^+. As in the case of integers, we will restrict our work to totally positive definite quadratic forms (those that represent totally positive elements only).

The first author was supported by Czech Science Foundation GAČR, grant 21-00420M, and by Charles University Research Centre program UNCE/SCI/022. The second author was supported by Czech Science Foundation GAČR, grant 22-11563O.

© The Author(s), 2023. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

Given a totally real number field K, there is some universal quadratic form with coefficients in O_K [4]. The lifting problem of universal quadratic forms for a number field K consists of determining whether there is some quadratic form with integer coefficients (or $\mathbb{Z}$-form) that is universal over K. Sums of squares are particular instances of $\mathbb{Z}$-forms. Maaß [10] found that the sum of three squares is universal over $\mathbb{Q}(\sqrt{5})$ and Siegel [13] proved that this case, together with the universality of the sum of four squares over $\mathbb{Q}$, are the only two cases of universality of a sum of squares. More generally, Kala and Yatsyna [6] proved the nonexistence of universal $\mathbb{Z}$-forms not only in the other quadratic fields, but also in further families with small degrees.

We define the codifferent ideal of O_K by

$$O_K^\vee = \{\delta \in K \mid \mathrm{Tr}(\delta\alpha) \in \mathbb{Z} \text{ for every } \alpha \in O_K\}.$$

We write $O_K^{\vee,+}$ for the subset of totally positive elements in $O_K^\vee$.

THEOREM 1.1 [6, Theorem 1.2]. *Let K be a number field with degree $1, 2, 3, 4, 5$ or 7 that has principal codifferent ideal and such that there is some universal $\mathbb{Z}$-form over K. Then $K = \mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, where $\zeta_7 = e^{2\pi i/7}$.*

We explore the lifting problem for the family of simplest cubic fields introduced by Shanks [12]. These are the fields of the form $K = \mathbb{Q}(\rho)$, where ρ is a root of the polynomial

$$f(x) = x^3 - ax^2 - (a+3)x - 1 \quad \text{for every } a \in \mathbb{Z}_{\geq -1}.$$

Among their nice arithmetic properties, they possess units of all signatures. Every totally real number field over which we can find universal $\mathbb{Z}$-forms must have this property [6, Corollary 4.5].

A nonmonogenic simplest cubic field $K = \mathbb{Q}(\rho)$ admits an integral basis of the form

$$\left\{1, \frac{j+\rho}{n_1}, \frac{k+l\rho+\rho^2}{n_2}\right\},$$

where $n_1, n_2 \in \mathbb{Z}_{>0}$ are such that $n_1 n_2 = [O_K : \mathbb{Z}[\rho]]$, $0 \leq j \leq n_1 - 1$ and $1 \leq k, l \leq n_2 - 1$ (see, for example, [1]). Our main result is the following theorem.

THEOREM 1.2. *Let $K = \mathbb{Q}(\rho)$ be a simplest cubic field. If $j = 0$ or $a \geq n_1 + n_2 - j$, there are no universal $\mathbb{Z}$-forms over K. In particular, if n_1 and n_2 are fixed, this holds for all simplest cubic fields except possibly finitely many.*

Kala and Yatsyna [6, Lemma 4.6] proved that, in fields with universal $\mathbb{Z}$-forms, every element $\alpha \in O_K^+$ such that $\mathrm{Tr}(\delta\alpha) \leq \mathrm{Tr}(\delta\beta)$ for all $\beta \in O_K^+$ is necessarily a unit in O_K. Thus, if a totally real number field K contains some nonunit $\alpha \in O_K^+$ such that $\mathrm{Tr}(\delta\alpha) = 1$ for some $\delta \in O_K^{\vee,+}$, then there are no universal $\mathbb{Z}$-forms over K. When α satisfies this condition, we say that α has minimal (codifferent) trace one. In order to prove Theorem 1.2, we find such an element in K.

The elements with minimal trace one are particular instances of what we call indecomposable elements: those elements of O_K^+ that cannot be written as sums of

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

other elements of O_K^+. Kala and the second author [5] proved that all indecomposables of a totally real number field K, up to multiplication by totally positive units, lie in a disjoint union of simplicial cones in the Minkowski space of K. If K is a totally real cubic field, then this reduces to two specific parallelepipeds which contain all elements with minimal trace one. Furthermore, they identified all the indecomposables when $O_K = \mathbb{Z}[\rho]$. In this case, the codifferent ideal $O_K^\vee$ is principal; therefore, Theorem 1.1 gives the nonexistence of universal $\mathbb{Z}$-forms over K.

In [2], the authors considered the simplest cubic fields $K = \mathbb{Q}(\rho)$ for which $[O_K : \mathbb{Z}[\rho]] = p$ is a prime number p. The only possibilities are $p = 3$ or $p \equiv 1 \pmod 6$. In the first of these cases, they found all the indecomposables and the elements with minimal trace one among them. Otherwise, the structure of indecomposables is much trickier.

After submitting this paper, we learned of the recent result [8, Theorem 1.3] that if K is a totally real cubic number field and $K \neq \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, then there are no universal $\mathbb{Z}$-forms over K. Our Theorem 1.2 is a particular case of this result.

2. Preliminaries

Let K be a totally real number field with degree d and let $\sigma_1, \dots, \sigma_d$ be the embeddings of K in an algebraic closure. By the symbols $\mathrm{Tr}(\alpha)$ and $N(\alpha)$, we mean the algebraic trace and norm of $\alpha \in K$ over K. An element $\alpha \in K$ is totally positive if $\sigma_i(\alpha) > 0$ for $1 \leq i \leq d$. Let O_K be the ring of integers of K. The subset of totally positive elements of O_K will be denoted by O_K^+. An element $\alpha \in O_K^+$ is indecomposable if $\alpha \neq \beta + \gamma$ for any $\beta, \gamma \in O_K^+$.

A quadratic form over a number field K is a homogeneous polynomial of degree two with coefficients in its ring of integers O_K, that is, a polynomial of the form

$$Q(x_1, \dots, x_n) = \sum_{r,s=1}^{n} a_{rs} x_r x_s \quad \text{for every } a_{rs} \in O_K.$$

If $a_{rs} \in \mathbb{Z}$ for $1 \leq r, s \leq n$, we say that Q is a $\mathbb{Z}$-form. From now on, it is assumed that all quadratic forms Q are totally positive definite, that is, $Q(x_1, \dots, x_n)$ is totally positive as an element of O_K for every $(x_1, \dots, x_n) \in O_K^n$ with $(x_1, \dots, x_n) \neq (0, \dots, 0)$. Such a form is universal if it represents all elements in O_K^+.

A simplest cubic field is a number field of the form $K = \mathbb{Q}(\rho)$, where ρ is a root of the polynomial

$$f(x) = x^3 - ax^2 - (a+3)x - 1 \quad \text{for every } a \in \mathbb{Z}_{\geq -1}.$$

The other roots of f are

$$\rho' = -1 - \frac{1}{\rho} = a + 2 + a\rho - \rho^2, \quad \rho'' = -\frac{1}{1+\rho} = -2 - (a+1)\rho + \rho^2.$$

We see immediately that K is a cyclic cubic extension of $\mathbb{Q}$ (and, therefore, a totally real number field). Using the above relations and Vieta's formulas, it is easy to compute the

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

coefficients of the minimal polynomial for every $\alpha \in \mathbb{Q}(\rho)$. If this minimal polynomial is of the form $x^3 - Ax^2 + Bx - C$ for some $A, B, C > 0$, Descartes' rule of signs implies that α is totally positive. If $a \geq 7$, we can assume without loss of generality that

$$a+1 < \rho < a+1+\frac{2}{a}, \quad -1-\frac{1}{a+1} < \rho' < -1-\frac{1}{a+2}, \quad -\frac{1}{a+2} < \rho'' < -\frac{1}{a+3}.$$

The first and third estimates come from [9]; the second can be easily verified.

Let us denote $\Delta := a^2+3a+9$ and write $\delta := [O_K : \mathbb{Z}[\rho]]$ for the index of ρ in K. With this notation, $\operatorname{disc}(f) = \Delta^2$. Recall that $\operatorname{disc}(f) = \delta^2 \operatorname{disc}(K)$, where we write $\operatorname{disc}(K)$ for the discriminant of K. The conductor-discriminant formula is $\operatorname{disc}(K) = \mathfrak{c}^2$, where $\mathfrak{c}$ is the conductor of K. Hence, the index of ρ may be expressed as

$$\delta = \frac{\Delta}{\mathfrak{c}}.$$

PROPOSITION 2.1 [7, Corollary 1.6]. *The following statements are equivalent.*

(1) *The field K is monogenic.*
(2) *$a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $\Delta/\mathfrak{c}$ is a cube.*
(3) *$a \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ or $a \not\equiv 3, 21 \pmod{27}$ and $v_p(\Delta) \not\equiv 2 \pmod 3$ for all $p \neq 3$.*

In statement (3), $v_p(x)$ stands for the p-adic valuation of the integer number x: the greatest power of p that is a divisor of x.

It is possible to determine explicitly the value of the conductor $\mathfrak{c}$ from the factorisation of Δ. We write $\Delta = bc^3$ with $b, c > 0$ integers and b cube-free. From [7, Remark 1.5],

$$\mathfrak{c} = \begin{cases} \prod_{p \mid b} p & \text{if } 3 \nmid a \text{ or } a \equiv 12 \pmod{27}, \\ 3^2 \prod_{p \mid b, p \neq 3} p & \text{otherwise.} \end{cases}$$

3. Bases of nonmonogenic simplest cubic fields

Let $K = \mathbb{Q}(\rho)$ be a nonmonogenic simplest cubic field. An integral basis of K can be taken of the form

$$B_{n_1,n_2}(j,k,l) = \left\{1, \frac{j+\rho}{n_1}, \frac{k+l\rho+\rho^2}{n_2}\right\} = \{g_1, g_2, g_3\}, \tag{3.1}$$

for $n_1, n_2 \in \mathbb{Z}_{>0}$, $n_1 n_2 = \delta$, $0 \leq j \leq n_1 - 1$ and $1 \leq k, l \leq n_2 - 1$. Hashimoto and Aoki [3, Proposition 1] derived another form for an integral basis of simplest cubic fields.

In this section, we determine the possible values for δ and, for each of these, how to determine the explicit form of an integral basis as in (3.1). We already know the answer when δ is a prime number p. If $p \neq 3$, then, from the form of $\mathfrak{c}$ and $\Delta = p\mathfrak{c}$, it follows that $p^2 \mid \Delta$. This is true only for $p \equiv 1 \pmod 6$ (see [2, Proposition 3.15]).

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

PROPOSITION 3.1 [2, Theorem 1.1]. *Let $K = \mathbb{Q}(\rho)$ be a simplest cubic field and assume that $\delta = [O_K : \mathbb{Z}[\rho]]$ is a prime number. Then, exactly one of these statements holds.*

(1) *$\delta = 3$ and K has integral basis $B_{1,3}(0, 1, 1)$.*
(2) *$\delta = p$, $p > 3$ prime with $p \equiv 1 \pmod 6$ and K has integral basis $B_{1,p}(0, k, l)$ for some k, l with $1 \le k, l \le p - 1$.*

Next, we move on to the general case. We need the following lemmas.

LEMMA 3.2. *Let p^s be the largest power of a prime p dividing δ.*

(1) *If $p = 3$ and $s = 3$, then $(2 + \rho)/3$ is an algebraic integer in K.*
(2) *If $p \neq 3$, then, for $s_1 \le \lfloor s/3 \rfloor$, there exists j with $0 \le j \le p^{s_1} - 1$ such that $(j + \rho)/p^{s_1}$ is an algebraic integer in K.*

PROOF. If $p = 3$ and $s = 3$, then, necessarily, $v_3(\Delta) = 3$ and $a \equiv 12 \pmod{27}$ (see [7, Proposition 3.2]). It can be easily checked that $(2 + \rho)/3$ is a root of

$$x^3 - \left(\frac{a}{3} + 2\right)x^2 + \left(\frac{a}{3} + 1\right)x - \frac{2a + 3}{27}.$$

Thus, it is clearly an algebraic integer for these cases of a.

We will proceed with $p \neq 3$. Assume that $\lfloor s/3 \rfloor \ge 1$ since, otherwise, our claim is trivial. The trace of $(j + \rho)/p^{s_1}$ is equal to $(a + 3j)/p^{s_1}$, which is a rational integer if $j \equiv -3^{-1}a \pmod{p^{s_1}}$. For these cases of p, the inverse of 3 modulo p^{s_1} exists and we denote it by 3^{-1}. The next coefficient of the minimal polynomial of $(j + \rho)/p^{s_1}$ is

$$\frac{-a - 3 + 2aj + 3j^2}{p^{2s_1}}.$$

Let $j = -3^{-1}a + Up^{s_1}$ for some $U \in \mathbb{Z}$. Then $-a - 3 + 2aj + 3j^2 = -3^{-1}\Delta + 3Up^{2s_1}$. This is clearly 0 modulo p^{2s_1} since $v_p(\Delta) \in \{s, s + 1\}$ and $s_1 \le \lfloor s/3 \rfloor$. Thus, this coefficient is a rational integer. Finally, the norm of $(j + \rho)/p^{s_1}$ is

$$\frac{1 - (a + 3)j + aj^2 + j^3}{p^{3s_1}}.$$

For $j = -3^{-1}a + Up^{s_1}$, we obtain

$$1 - (a + 3)j + aj^2 + j^3 = 3^{-3}(2a + 3)\Delta - 3^{-1}\Delta Up^{s_1} + U^3p^{3s_1} \equiv 0 \pmod{p^{3s_1}},$$

since $p^{3s_1} \mid \Delta$. Therefore, for $j \equiv -3^{-1}a \pmod{p^{s_1}}$, we get an algebraic integer. □

LEMMA 3.3. *Let p^s be the largest power of a prime p dividing δ.*

(1) *If $p = 3$ and $s = 3$, then $(1 + 7\rho + \rho^2)/9$, $(4 + 4\rho + \rho^2)/9$ and $(7 + \rho + \rho^2)/9$ are algebraic integers in K.*
(2) *If $p \neq 3$, then, for $s_2 \le s - \lfloor s/3 \rfloor$, there exist k, l with $1 \le k, l \le p^{s_2} - 1$ such that $(k + l\rho + \rho^2)/p^{s_2}$ is an algebraic integer in K.*

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

PROOF. If $p = 3$ and $s = 3$, we already know that $a \equiv 12 \pmod{27}$. The element $(1 + 7\rho + \rho^2)/9$ is a root of

$$x^3 - \frac{a^2 + 9a + 9}{9}x^2 - \frac{4(a+6)^2}{3^4}x + \frac{5a^2 + 15a - 171}{3^6}.$$

The coefficient $(a^2 + 9a + 9)/9$ is obviously a rational integer. The same is true for $(4(a + 6)^2)/3^4$ since $a + 6 \equiv 18 \pmod{27}$. Let $a = 12 + 27\overline{a}$ for some $\overline{a} \in \mathbb{Z}$. Then

$$5a^2 + 15a - 171 = 3^6(5\overline{a}^2 + 5\overline{a} + 1).$$

Therefore, the norm is also a rational integer. The proof for the remaining two elements is similar.

Now, let $p \neq 3$. Here, we can closely follow [2, Proposition 3.8]. The expression for the trace of $(k + l\rho + \rho^2)/p^{s_2}$ leads to the condition

$$k = -3^{-1}(al + a^2 + 2a + 6) + Up^{s_2}$$

for some $U \in \mathbb{Z}$. For this k, the numerator of the second coefficient of the minimal polynomial is

$$-3^{-1}(a^2 + a + 1 + (2a + 1)l + l^2)\Delta + 3U^2p^{2s_2}.$$

Therefore, we must have $p^{2s_2 - v_p(\Delta)} \mid a^2 + a + 1 + (2a + 1)l + l^2$. As in [2, Proposition 3.8], the numerator of the norm of $(k + l\rho + \rho^2)/p^{s_2}$ can be expressed as

$$27^{-1}g(l) - 3^{-1}\Delta U(a^2 + a + 1 + (2a + 1)l + l^2)p^{s_2} + U^3p^{3s_2},$$

where

$$\begin{aligned} g(l) = {} & \Delta((2a^2 - 3)\Delta + 8(2a + 3) \\ & + ((6a - 3)\Delta - 12a + 36)l + (6\Delta - 6a - 36)l^2 + (2a + 3)l^3). \end{aligned}$$

Clearly, we still need $p^{2s_2 - v_p(\Delta)} \mid a^2 + a + 1 + (2a + 1)l + l^2$ and, moreover, $p^{3s_2} | g(l)$. The latter is true if

$$l \equiv -(2a + 3)^{-1}(2a^2 + 4a + 6) \pmod{p^{3s_2 - v_p(\Delta)}}.$$

It remains to check the first part. If $l = -(2a + 3)^{-1}(2a^2 + 4a + 6) + Vp^{3s_2 - v_p(\Delta)}$ for some $V \in \mathbb{Z}$, then

$$a^2 + a + 1 + (2a + 1)l + l^2 = 3(2a + 3)^{-2}\Delta - 9(2a + 3)^{-1}Vp^{3s_2 - v_p(\Delta)} + V^2p^{6s_2 - 2v_p(\Delta)}.$$

This expression is divisible by $p^{2s_2 - v_p(\Delta)}$ if $p^{2s_2 - v_p(\Delta)} \mid \Delta$, which is valid for $s_2 \leq s - \lfloor s/3 \rfloor$. This completes the proof. □

We can use the above lemmas to find an explicit basis as in (3.1) for any simplest cubic field K. If $\delta = p_1^{s_1} \cdots p_m^{s_m}$ for primes p_i, then we can take $n_1 = p_1^{s_{1,1}} \cdots p_m^{s_{1,m}}$ and $n_2 = p_1^{s_{2,1}} \cdots p_m^{s_{2,m}}$, where $s_{1,i} = \lfloor s_i/3 \rfloor$ and $s_{2,i} = s_i - \lfloor s_i/3 \rfloor$. To prove that n_1 and n_2 can be chosen this way, it is enough to check that there exist j, k, l with $0 \leq j \leq n_1 - 1$ and $1 \leq k, l \leq n_2 - 1$ such that g_2 and g_3 are algebraic integers. For example, for g_2, there exists j_i with $0 \leq j_i \leq p_i^{s_{1,i}} - 1$ such that $(j_i + \rho)/p^{s_{1,i}}$ is an algebraic integer for

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

each i, by Lemma 3.2. We will proceed by induction on i. Assume that $(j_{i+1}+\rho)/p^{s_{1,i+1}}$ and $(J_i+\rho)/p^{s_{1,1}}\cdots p^{s_{1,i}}$ are algebraic integers, where $1 \le J_i \le p^{s_{1,1}}\cdots p^{s_{1,i}} - 1$. Since $p^{s_{1,i+1}}$ and $p^{s_{1,1}}\cdots p^{s_{1,i}}$ are coprime, by Bezout's identity, there exist $u, v \in \mathbb{Z}$ such that $up^{s_{1,i+1}} + vp^{s_{1,1}}\cdots p^{s_{1,i}} = 1$. Then

$$v\frac{j_{i+1}+\rho}{p^{s_{1,i+1}}} + u\frac{J_i+\rho}{p^{s_{1,1}}\cdots p^{s_{1,i}}} = \frac{vj_{i+1}p^{s_{1,1}}\cdots p^{s_{1,i}} + uJ_ip^{s_{1,i+1}} + \rho}{p^{s_{1,1}}\cdots p^{s_{1,i+1}}}.$$

Since the summands are algebraic integers, the element on the right-hand side is also an algebraic integer. Moreover, we can take J_{i+1} as $vj_{i+1}p^{s_{1,1}}\cdots p^{s_{1,i}} + uJ_ip^{s_{1,i+1}}$ modulo $p^{s_{1,1}}\cdots p^{s_{1,i+1}}$. We can use similar arguments for g_3.

4. Lifting problem for universal quadratic forms

In this section, we prove the nonexistence of $\mathbb{Z}$-forms over a simplest cubic field $K = \mathbb{Q}(\rho)$. As highlighted in the introduction, we will exhibit a nonunit $\alpha \in O_K^+$ with minimal trace one and apply [6, Lemma 4.6]. The elements with minimal trace one are, in particular, indecomposables of K.

We now summarise the method of [5] to locate indecomposables of K. We write $B = B_{n_1,n_2}(j,k,l) = \{g_1, g_2, g_3\}$ for the integral basis of K, as above, and embed $K \hookrightarrow \mathbb{R}^3$ by means of this integral basis: that is,

$$\begin{array}{ccc} K & \longrightarrow & \mathbb{R}^3, \\ \sum_{i=1}^3 x_i g_i & \mapsto & (x_1, x_2, x_3). \end{array}$$

The parallelepiped with nodes $\ell_1, \ell_2, \ell_3 \in \mathbb{Z}^3$ will be the set

$$\mathcal{D}(\ell_1, \ell_2, \ell_3) = [0,1]\ell_1 + [0,1]\ell_2 + [0,1]\ell_3.$$

PROPOSITION 4.1 [5, Section 4, pages 11–12]. *Let K be a totally real cubic field and let $(\varepsilon_1, \varepsilon_2)$ be a proper pair of totally positive units of K (see* [14, page 2]*). The indecomposables of K lie, up to multiplication by totally positive units in K, in either of the parallelepipeds $\mathcal{D}(1, \varepsilon_1, \varepsilon_2), \mathcal{D}(1, \varepsilon_1, \varepsilon_1\varepsilon_2^{-1})$.*

REMARK 4.2. The idea behind Proposition 4.1 is that the two parallelepipeds are contained in the fundamental domain for the action of the totally positive units of K on $\mathbb{R}^{3,+}$ by multiplication (after the embedding $K \hookrightarrow \mathbb{R}^3$).

In the case of a simplest cubic field K, $(\rho^2, 1 + 2\rho + \rho^2)$ is a proper pair of totally positive units; therefore, we are left with the parallelepipeds

$$\mathcal{D}(1, \rho^2, 1 + 2\rho + \rho^2), \quad \mathcal{D}(1, \rho^2, \rho^2\rho'^2).$$

It can be checked that $\rho^2\rho'^2 = -1 - a - (a^2 + 3a + 3)\rho + (a+2)\rho^2$.

An element $\alpha \in O_K^+$ has minimal trace one if there is $\delta \in O_K^{\vee,+}$ such that $\mathrm{Tr}(\delta\alpha) = 1$. By [11, Proposition 4.14], the elements $\varphi_1, \varphi_2, \varphi_3 \in O_K$, the coordinates of which with

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

respect to B are the columns of the inverse of the matrix $(\mathrm{Tr}(g_r g_s))_{r,s=1}^3$, form a $\mathbb{Z}$-basis of $O_K^\vee$ such that

$$\mathrm{Tr}\Big(\Big(\sum_{r=1}^{3} a_r g_r\Big)\Big(\sum_{s=1}^{3} b_s \varphi_s\Big)\Big) = \sum_{r=1}^{3} a_r b_r$$

for every $a_r, b_s \in \mathbb{Z}$. In our case,

$$\begin{aligned}
\varphi_1 = \frac{1}{\Delta}\big((a^2+5a+11-(2a^2+8a+4)j+2(a^2+a+1)j^2+2(a+4)k-2(2a+1)jk\\
+2k^2-2(a+4)jl+2(2a+1)j^2l-4jkl+2j^2l^2)g_1\\
+(a^2+4a+2-2(a^2+a+1)j+(2a+1)k+(a+4)l-2(2a+1)jl+2kl\\
-2jl^2)n_1g_2-(a+4-(2a+1)j+2k-2jl)n_2g_3\big),\\
\varphi_2 = \frac{1}{\Delta}\big((a^2+4a+2-2(a^2+a+1)j+(2a+1)k+(a+4)l-2(2a+1)jl+2kl\\
-2jl^2)n_1g_1+(2a^2+2a+2+2l+4al+2l^2)n_1^2g_2-(2a+2l+1)n_1n_2g_3\big),\\
\varphi_3 = \frac{1}{\Delta}(-(a+4-j-2aj+2k-2jl)n_2g_1-(2a+2l+1)n_1n_2g_2+2n_2^2g_3).
\end{aligned}$$

4.1. The case $j = 0$. We will start with the case when $j = 0$. This implies that $n_1 = 1$. Indeed, since ρ/n_1 is an algebraic integer, it is a root of some monic polynomial $g \in \mathbb{Z}[x]$. Now, ρ is a root of the polynomial $h(x) = n_1^3 g(x/n_1)$, and since this is monic, $h(x) = f(x)$ is the minimal polynomial of ρ. But then $n_1^3 \mid f(0) = -1$, so $n_1 = 1$.

On the other hand, under this condition, we must have $n_2^2 \mid \Delta$, which is the consequence of the following arguments. Let $p \mid n_2$ be a prime. If $p^s \mid \Delta$ for some $s \geq 3$, then either $j \neq 0$, or $p = 3$, $27 \mid \Delta$ but $9 \nmid n_2$ (see Lemmas 3.2 and 3.3). Therefore, for $p \neq 3$, $s = 1, 2$. If $s = 1$, then $p \nmid \delta$, and thus, $p \nmid n_2$. Thus, $s = 2$ and, by the formula for the conductor, $p^2 \nmid \delta$. In summary, we must have $n_2^2 \mid \Delta$.

In the following proof, we use a simple consequence of this fact. If $n_2^2 \mid \Delta$, then, clearly, for $a > 5$,

$$n_2^2 \leq \Delta = a^2 + 3a + 9 < a^2 + 4a + 4 = (a+2)^2,$$

which gives $n_2 \leq a + 1$. For $a \leq 5$ (or $a \leq 7$, needed later), we obtain only monogenic simplest cubic fields, which are covered by the result of Kala and Yatsyna [6].

PROPOSITION 4.3. *Let K be a nonmonogenic simplest cubic field with $a > 5$ and $j = 0$. Then $-g_2 + g_3$ is a nonunit indecomposable integer in O_K with minimal trace one.*

PROOF. First, we show that $-g_2 + g_3$ is totally positive. It will be enough to check that it lies in the parallelepiped $\mathcal{D}(1, \rho^2, \rho^2\rho''^2)$. It is easily verified that $-g_2 + g_3$ equals

$$\frac{ka^2 + (3k - l + n_2)(a+1)}{n_2(a^2+3a+3)} + \frac{a^2+3a+3+(l-n_2)(a+2)}{n_2(a^2+3a+3)}\rho^2 + \frac{n_2 - l}{n_2(a^2+3a+3)}\rho^2\rho''^2.$$

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

The first and the third terms are clearly positive since $n_2 > l$. The numerator of the coefficient of ρ^2 is

$$\geq a^2 + 3a + 3 - n_2(a+2) \geq a^2 + 3a + 3 - (a+1)(a+2) = 1 > 0.$$

Here, we use the facts that $l \geq 0$ and $n_2 \leq a+1$, which we derived above. Next, we show that all of these coefficients are bounded above by 1. For the first one, the inequality

$$ka^2 + (3k - l + n_2)(a+1) < n_2(a^2 + 3a + 3)$$

is equivalent to

$$(n_2 - k)a^2 + (2n_2 + l - 3k)(a+1) > 0.$$

Now, the inequalities $1 \leq k, l \leq n_2 - 1$ give $l - 3k \geq 1 - 3(n_2 - 1) = 4 - 3n_2$, so

$$(n_2 - k)a^2 + (2n_2 + l - 3k)(a+1) \geq a^2 - (n_2 - 4)(a+1).$$

Since $n_2 \leq a+1$ for $a > 5$,

$$a^2 - (n_2 - 4)(a+1) \geq a^2 - (a-3)(a+1) = a^2 - (a^2 - 2a - 3) = 2a + 3 > 0.$$

Therefore, the original inequality is true. For the second coefficient,

$$a^2 + (l + 3 - n_2)a + 2l - 2n_2 + 3 < n_2(a^2 + 3a + 3)$$

if and only if

$$(n_2 - 1)a^2 + (4n_2 - l - 3)a + 5n_2 - 2l - 3 > 0,$$

which holds trivially. Finally, for the third coefficient, clearly, $n_2 - l < n_2(a^2 + 3a + 3)$.

Therefore, $-g_2 + g_3$ is totally positive. Since it lies in the interior of the parallelepiped $\mathcal{D}(1, \rho^2, \rho^2\rho''^2)$ and this is contained in the fundamental domain for the action of totally positive units on elements of K, it follows that $-g_2 + g_3$ is not a unit.

Now, the statement will be established as soon as we prove that the element of the codifferent $\varphi_1 + \varphi_3$ is totally positive. Indeed, in that case, we have $\varphi_1 + \varphi_3 \in O_K^{\vee,+}$ and

$$\mathrm{Tr}((\varphi_1 + \varphi_3)(-g_2 + g_3)) = 1.$$

We prove that $\varphi_1 + \varphi_3$ is totally positive. We use the coefficients of the minimal polynomial of $(a^2 + 3a + 9)(\varphi_1 + \varphi_3)$ and prove that they are all positive. Now,

$$\begin{aligned}(a^2 + 3a + 9)(\varphi_1 + \varphi_3) = {} & (a^2 + 5a + 11 + 2k^2 + 2ak + 8k - n_2(a + 2k + 4))g_1 \\ & + (a^2 + 4a + 2 + k(2a + 2l + 1) + l(a+4) \\ & - n_2(2a + 2l + 1))g_2 + (2n_2^2 - n_2(a + 2k + 4))g_3.\end{aligned}$$

Thus,

$$\mathrm{Tr}((a^2 + 3a + 9)(\varphi_1 + \varphi_3)) = a^2 + 3a + 9 > 0.$$

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

The second coefficient of the minimal polynomial is

$$(a^2+3a+9)(-1-4k-k^2+4n_2+2kn_2-n_2^2+(n_2-k-1)a)$$
$$=(a^2+3a+9)g(a,n_2,k),$$

where $g(a,n_2,k)$ is a linear polynomial in a with a positive leading coefficient if $k\neq n_2-1$. If $k=n_2-1$, then we obtain $g(a,n_2,n_2-1)=2>0$. If $k\neq n_2-1$, then $g(a,n_2,k)$ is positive if

$$a>\frac{n_2^2-2kn_2-4n_2+k^2+4k+1}{n_2-k-1}=n_2-k-1+\frac{2(k-n_2)}{n_2-k-1}.$$

This is clearly true if $a\geq n_2-k-1$, that is, if $a+1\geq n_2-k$, which is valid for $n_2\leq a+1$ and $k\geq 0$.

We will proceed with the norm, $N((a^2+3a+9)(\varphi_1+\varphi_3))$, which is equal to

$$(a^2+3a+9)(-1+3k^2+k^3-6kn_2-3k^2n_2+3n_2^2+3kn_2^2-n_2^3$$
$$+(n_2^2-2kn_2-n_2+k^2+k)a)=(a^2+3a+9)h(a,n_2,k).$$

Again, $h(a,n_2,k)$ is a linear polynomial in a, and we now study its leading coefficient. The roots of $n_2^2-2kn_2-n_2+k^2+k$ as a polynomial in k are n_2-1 and n_2. Thus, this coefficient is positive if $k\neq n_2-1$. If $k=n_2-1$, then we obtain $h(a,n_2,n_2-1)=1>0$. If $k\neq n_2-1$, then $h(a,n_2,k)$ is positive if a is greater than

$$\frac{1-3k^2-k^3+6kn_2+3k^2n_2-3n_2^2-3kn_2^2+n_2^3}{n_2^2-2kn_2-n_2+k^2+k}=n_2-k-2+\frac{2(k-n_2)+1}{n_2^2-2kn_2-n_2+k^2+k},$$

which is true because $n_2\leq a+1$.

Therefore, $\varphi_1+\varphi_3$ is totally positive and gives trace one for $-g_2+g_3$. □

4.2. The case $j\neq 0$. Now, let us discuss the element $g_2=(j+\rho)/n_1$ with $j\neq 0$. Recall that its norm is

$$\frac{1-(a+3)j+aj^2+j^3}{n_1^3}.$$

For $j=1$, we obtain $-1/n_1^3$, which is not a rational integer for $n_1\geq 3$. Therefore, $j\geq 2$, and g_2 is totally positive since the smallest negative conjugate of ρ satisfies $-2<\rho'<-1$. In the following, we prove that g_2 has minimal trace one.

We can easily verify that $(j+\rho)/n_1$ is not a unit:

$$\frac{j+\rho}{n_1}\rho^2\rho''^2=\frac{1}{n_1}(a+2-j(a+1)$$
$$+(a^2+4a+5-j(a^2+3a+3))\rho-(a+3-j(a+2))\rho^2)$$

and also

$$=\frac{1}{n_1(a^2+3a+3)}+\frac{a+1}{n_1(a^2+3a+3)}\rho^2+\frac{j(a^2+3a+3)-(a^2+4a+5)}{n_1(a^2+3a+3)}\rho^2\rho''^2.$$

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

We see that all of the coefficients are positive and less than one for $2 \le j \le n_1 - 1$. Therefore, $((j+\rho)/n_1)\rho^2\rho''^2$ lies inside $\mathcal{D}(1, \rho^2, \rho^2\rho''^2)$ and cannot be a unit.

PROPOSITION 4.4. *Let K be a simplest cubic field with $a \ge 7$ and $j \ne 0$. If $a \ge n_1 + n_2 - j$, then there exists $W \in \mathbb{N}$ such that the element $\varphi_1 + \varphi_2 + W\varphi_3$ is totally positive.*

PROOF. First, it is not difficult to check that the elements of the basis of the codifferent can be rewritten as $\varphi_1 = (k - (a+l)j)\psi_1 - j\psi_2 + \psi_3$, $\varphi_2 = (a+l)n_1\psi_1 + n_1\psi_2$ and $\varphi_3 = -n_2\psi_1$, where

$$\psi_1 = \frac{1}{\Delta}(a + 4 + (2a+1)\rho - 2\rho^2),$$
$$\psi_2 = \frac{1}{\Delta}(2 + (a+2)\rho - \rho^2),$$
$$\psi_3 = \frac{1}{\Delta}(a^2 + 5a + 11 + (a^2 + 4a + 2)\rho - (a+4)\rho^2).$$

The advantage of the elements ψ_i is that they depend only on a. Thus, it is not difficult to find good estimates on their conjugates, which we do in the following steps.

The element ψ_1 is a root of the polynomial

$$x^3 - \frac{1}{\Delta}x - \frac{1}{\Delta^2}.$$

This polynomial has roots satisfying

$$-\frac{1}{a^2+3a+7} < \psi_1 < -\frac{1}{a^2+3a+8}, \quad -\frac{1}{a+2} < \psi_1' < -\frac{1}{a+3}, \quad \frac{1}{a+2} < \psi_1'' < \frac{1}{a+1}.$$

This can be verified by checking the values of the polynomial in the above intervals and by considering estimates on conjugates of ρ. Similarly, ψ_2 is a root of

$$x^3 - \frac{1}{\Delta}x + \frac{1}{\Delta^2},$$

and we have

$$\frac{1}{a+3} < \psi_2 < \frac{1}{a+2}, \quad -\frac{1}{a+1} < \psi_2' < -\frac{1}{a+2}, \quad \frac{1}{a^2+3a+8} < \psi_2'' < \frac{1}{a^2+3a+7}.$$

Finally, the element ψ_3 is a root of

$$x^3 - x^2 - \frac{a+1}{\Delta}x + \frac{1}{\Delta^2},$$

which gives

$$\frac{1}{\Delta(a+1)+a+3} < \psi_3 < \frac{1}{\Delta(a+1)+a+2}, \quad -\frac{1}{a+3} < \psi_3' < -\frac{1}{a+4},$$
$$1 + \frac{1}{a+4} < \psi_3'' < 1 + \frac{1}{a+3}.$$

The element $\delta_W = \varphi_1 + \varphi_2 + W\varphi_3$ can be rewritten as

$$\varphi_1 + \varphi_2 + W\varphi_3 = (M - n_2 W)\psi_1 + (n_1 - j)\psi_2 + \psi_3,$$

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

where $M := (a+l)(n_1-j)+k$. Clearly, the coefficient n_1-j is positive, and the same is true for M. Since $\psi_1', \psi_2', \psi_3' < 0$, the necessary condition to get $\delta_W' > 0$ is that $n_2 W > M$. If this is the case, then, obviously, $\delta_W > 0$ since $\psi_1 < 0$ and $\psi_2, \psi_3 > 0$. Thus, it remains to discuss δ_W' and δ_W''.

Using the above estimates, we conclude that

$$\delta_W' > \frac{n_2 W - M}{a+3} - \frac{n_1-j}{a+1} - \frac{1}{a+3}.$$

The expression on the right-hand side is positive if

$$n_2 W > M + n_1 - j + 1 + \frac{2}{a+1}(n_1-j).$$

Note that this also implies that $n_2 W > M$. On the other hand,

$$\delta_W'' > \frac{M - n_2 W}{a+1} + \frac{n_1-j}{a^2+3a+8} + 1 + \frac{1}{a+4}.$$

Again, the right-hand side is positive if

$$n_2 W < M + a + 1 + \frac{a+1}{a+4} + \frac{(a+1)(n_1-j)}{a^2+3a+8}.$$

The difference between the upper and lower bound is

$$a - n_1 + j + \frac{a+1}{a+4} + \frac{(a+1)(n_1-j)}{a^2+3a+8} - \frac{2}{a+1}(n_1-j).$$

Moreover, $(a+2)^2 > a^2+3a+9 \geq n_1 n_2 \geq n_1^3$, so $n_1 < (a+2)^{2/3}$ and

$$\frac{a+1}{a+4} + \frac{(a+1)(n_1-j)}{a^2+3a+8} - \frac{2(n_1-j)}{a+1} > \frac{a+1}{a+4} + \frac{a+1}{a^2+3a+8} - \frac{2(a+2)^{2/3}}{a+1} > 0$$

for $a \geq 13$, which we have checked by computer. For $-1 \leq a \leq 12$, the corresponding simplest cubic fields are monogenic. Now, the hypothesis gives $a - n_1 + j \geq n_2$, so the difference above is clearly bounded below by n_2. Therefore, we obtain the existence of a suitable W. □

COROLLARY 4.5. *Let K be a simplest cubic field with $a \geq n_1 + n_2 - j$ and $j \neq 0$. Then $(j+\rho)/n_1$ is a nonunit indecomposable integer with minimal trace one.*

PROOF. As we have deduced, $(j+\rho)/n_1$ is a nonunit totally positive algebraic integer. Together with the totally positive element of codifferent $\varphi_1 + \varphi_2 + W\varphi_3$ from Proposition 4.4, it gives the minimal trace one, as required. □

Therefore, if n_1 and n_2 are fixed and $j \neq 0$, there are at most finitely many simplest cubic fields for which $(j+\rho)/n_1$ does not necessarily have minimal trace one. However, simplest cubic fields with $a < n_1 + n_2 - j$ exist, and there could be infinitely many of them. For example, $a = 101471$, 182451 and 18128865, which are exceptional cases in the paper of Kashio and Sekigawa [7, page 7], do not satisfy this condition.

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press

References

[1] S. Alaca, 'p-integral bases of a cubic field', *Proc. Amer. Math. Soc.* **126** (1998), 1949–1953.
[2] D. Gil-Muñoz and M. Tinková, 'Additive structure of non-monogenic simplest cubic fields', Preprint, 2022, arXiv:2212.00364.
[3] Y. Hashimoto and M. Aoki, 'Normal integral bases and Gaussian periods in the simplest cubic fields', *Ann. Math. Qué.*, to appear. Published online (19 July 2022).
[4] J. S. Hsia, Y. Kitaoka and M. Kneser, 'Representations of positive definite quadratic forms', *J. reine angew. Math.* **301** (1978), 132–141.
[5] V. Kala and M. Tinková, 'Universal quadratic forms, small norms and traces in families of number fields', *Int. Math. Res. Not. IMRN* **2023** (2023), 7541–7577.
[6] V. Kala and P. Yatsyna, 'Lifting problem for universal quadratic forms', *Adv. Math.* **377** (2021), Article no. 107497.
[7] T. Kashio and R. Sekigawa, 'The characterization of cyclic cubic fields with power integral bases', *Kodai Math. J.* **44** (2021), 290–306.
[8] D. Kim and S. H. Lee, 'Lifting problem for universal quadratic forms over totally real cubic number fields', Preprint, 2023, arXiv:2307.07118.
[9] F. Lemmermeyer and A. Pethö, 'Simplest cubic fields', *Manuscripta Math.* **88** (1995), 53–58.
[10] H. Maaß, 'Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten', *Abh. Math. Sem. Univ. Hamburg* **14** (1941), 185–191.
[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers* (Polish Scientific Publishers, Warszawa, 1974).
[12] D. Shanks, 'The simplest cubic fields', *Math. Comput.* **28** (1974), 1137–1152.
[13] C. L. Siegel, 'Sums of m-th powers of algebraic integers', *Ann. of Math. (2)* **46** (1945), 313–339.
[14] E. Thomas and A. T. Vasquez, 'On the resolution of cusp singularities and the Shintani decomposition in totally real cubic number fields', *Math. Ann.* **247** (1980), 1–20.

DANIEL GIL-MUÑOZ, Department of Algebra,
Faculty of Mathematics and Physics, Charles University,
Sokolovská 83, 186 00 Praha 8, Czech Republic
e-mail: daniel.gil-munoz@mff.cuni.cz

MAGDALÉNA TINKOVÁ, Faculty of Information Technology,
Czech Technical University in Prague, Thákurova 9,
160 00 Praha 6, Czech Republic
and
Institute of Analysis and Number Theory, TU Graz,
Kopernikusgasse 24/II, 8010 Graz, Austria
e-mail: tinkova.magdalena@gmail.com

https://doi.org/10.1017/S0004972723000953 Published online by Cambridge University Press