Math. Proc. Camb. Phil. Soc. (2015), **159**, 239–252 © *Cambridge Philosophical Society* 2015
doi:10.1017/S030500411500033X
First published online 8 June 2015

Number fields without n-ary universal quadratic forms

BY VALENTIN BLOMER† AND VÍTĚZSLAV KALA‡
Mathematisches Institut, Bunsenstr. 3-5*, D*-37073 *Göttingen, Germany.*
e-mail: blomer@uni-math.gwdg.de; vita.kala@gmail.com

(*Received* 25 *March* 2015*; revised* 23 *April* 2015)

Abstract

Given any positive integer M, we show that there are infinitely many real quadratic fields that do not admit universal quadratic forms with even cross coefficients in M variables.

1. *Introduction*

A famous theorem of Lagrange states that every positive integer is a sum of four squares, one can rephrase this by saying that the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is universal, where here and in the following we call a positive form universal if it represents all positive integers.

It is a classical fact that there exist no integral, positive, ternary, universal quadratic forms (see e.g. [**Ro**]), since every such form misses a whole residue class (such as $x_1^2 + x_2^2 + x_3^2$ misses all integers $\equiv 7 \pmod 8$). Therefore the smallest number of variables, for which positive universal quadratic forms exist, is four. In fact, universal forms over $\mathbb{Z}$ can be characterised very easily: if they represent $1, 2, \dots, 15$, then they are universal. This is the 15-theorem of Conway and Schneeberger with its beautiful proof by Bhargava [**Bh**]. Here and for the rest of the paper we restrict ourselves to *classical* quadratic forms, i.e. homogeneous quadratic polynomials with integral coefficients whose off-diagonal coefficients are even.

Universal quadratic forms have also been investigated over number fields. Chan, Kim and Raghavan [**CKR**] determined all totally positive universal ternary quadratic forms over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$ (there are 4, 2 and 5, respectively, up to equivalence) and showed in addition that no other real quadratic number field admits totally positive universal ternary quadratic forms. (A form is called totally positive if it is positive and the form with conjugate coefficients is also positive.) The proof uses, among other things, a theorem of Siegel [**Si**] which states that in no totally real field other than $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$, every totally positive integer is a sum of *any* number of squares. This is a first indication that more complicated fields might admit fewer universal quadratic forms. Kim [**Ki1**] showed that for squarefree $D \geqslant 38446$, the field $\mathbb{Q}(\sqrt{D})$ admits no diagonal septenary universal form.

The aim of this paper is a proof that there exist infinitely many fields that do not admit universal forms of *arbitrary* length, diagonal or not.

† Supported by the Volkswagen Foundation and a Starting Grant of the European Research Council.
‡ Supported by a Starting Grant of the European Research Council.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

THEOREM 1. *Given any positive integer M, there exist infinitely many real quadratic fields that do not admit classical universal quadratic forms in M variables.*

Our proof constructs a very sparse sequence of such fields, about $e^{-cM}\sqrt{X}$ discriminants $D \leqslant X$ for some constant $c > 1$, but it seems likely that such fields occur very frequently. Roughly speaking, if $K = \mathbb{Q}(\sqrt{D})$ has small class number, it contains many integers of small norm and we will see that this often forces a universal form to have many variables. On the other hand, Kim [**Ki2**] showed that there are infinitely many real quadratic fields that admit universal quadratic forms in 8 variables; these fields are all of the form $\mathbb{Q}(\sqrt{n^2+1})$ and have in particular very large class number.

This indicates already the difficulty of the proof of Theorem 1: although we expect that real quadratic fields often have small class number, it is one of the old unsolved problems in number theory to make any substantial progress in this direction. Our proof needs to work around the difficulty that we know very little about real quadratic fields with small class number. In the final section we make some explicit calculations for the field $K = \mathbb{Q}(\sqrt{73})$, which has class number 1.

2. *Generalities*

Throughout the paper we will use the following notation. Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ squarefree. If $D \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = (1+\sqrt{D})/2$. In the former case we let $\delta := 2\sqrt{D}$, in the latter $\delta := \sqrt{D}$. We write $a \succ b$ to mean that $a - b$ is totally positive, and we denote by $\mathcal{O}_K^+$ the set of totally positive integers. For $a \in K$ we denote its conjugate by a'. The norm of a is denoted by $Na = aa'$.

In order to avoid repetition, by a *form* we mean a totally positive quadratic form with coefficients in $\mathcal{O}_K$ whose off-diagonal coefficients are even (i.e. divisible by 2). The restriction to classical forms is quite typical in questions of universality (see e.g. [**Bh**, **CKR**]); they are convenient to work with since they can be represented in the form as $x^\top Ax$ where A is a symmetric matrix with integral coefficients.

We start with some simple lemmas.

LEMMA 1. *Let $a, b \in K$ be totally positive. Then $\sqrt{N(a+b)} \geqslant \sqrt{N(a)} + \sqrt{N(b)}$.*

Proof. We have

$$N(a+b) = N(a)+N(b)+ab'+a'b \geqslant N(a)+N(b)+2\sqrt{aa'bb'} = \left(\sqrt{N(a)}+\sqrt{N(b)}\right)^2.$$

LEMMA 2. *Let $a \in \mathcal{O}_K^+$ be such that $a \notin \mathbb{Z}$ and $a > a'$. Then $a > \delta$.*

Proof. Let $a = x + y\sqrt{D}$ and assume first that $x, y \in \mathbb{Z}$. Since $a \notin \mathbb{Z}$, we have $y \neq 0$. Since $a > a'$ is totally positive, it follows that $x > 0$ and $y > 0$. Since $a' > 0$, we have $x > y\sqrt{D} \geqslant \sqrt{D}$. Thus $a = x + y\sqrt{D} > 2\sqrt{D} = \delta$.

If x, y can be half-integers, we show the result in the same way.

LEMMA 3. *Let $\alpha \in \mathcal{O}_K^+$. If $N\alpha \leqslant \delta$ and $n \nmid \alpha$ for all $2 \leqslant n \in \mathbb{Z}$, then α is not a sum of two totally positive integers.*

Proof. Assume that $\alpha = a + b$ with a, b totally positive. If $ab' \notin \mathbb{Z}$, then without loss of generality assume that $ab' > a'b$. It follows from Lemma 2 that $ab' > \delta$. This is a

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

contradiction, since then $N(\alpha) = N(a)+N(b)+ab'+a'b > ab' > \delta$. Hence $ab' = a'b \in \mathbb{N}$, so that $q := ab'/N(a) \in \mathbb{Q}$, say $q = u/v$ with coprime $u, v \in \mathbb{N}$. Since $a, b \in \mathcal{O}_K$ and $b = uv/a$, we have that $v \mid a$. Then $a = vc$ and $b = uc$ for some $c \in \mathcal{O}_K$ and $\alpha = (u+v)c$, a contradiction.

We can now make more precise the final remarks from the introduction: if K has sufficiently many elements of small norm satisfying some conditions, then it does not admit universal forms with few variables.

PROPOSITION 4. *Assume that there exist* $1 = a_1, a_2, \ldots, a_M \in \mathcal{O}_K^+$ *such that for all* $1 \leqslant i \neq j \leqslant M$ *we have that* :

(i) $Na_i \leqslant \delta$;
(ii) $n \not\succ a_i$ *for* $2 \leqslant n \in \mathbb{Z}$;
(iii) a_i *and* a_j *are not in the same square class, i.e. there exists no* $x \in \mathcal{O}_K$ *such that* $a_i = a_j x^2$; *and*
(iv) *if* $a_i a_j \succ c^2$ *for* $c \in \mathcal{O}_K$, *then* $c = 0$.

Then there are no universal classical totally positive $(M-1)$*-ary quadratic forms over* $\mathcal{O}_K$.

Conditions (i), (ii) *and* (iv) *are implied by*:

(v) $Na_i \leqslant \delta^{1/2}$ *and* $n \not\succ a_i a_j$ *for* $2 \leqslant n \in \mathbb{Z}$.

Proof. That (i) and (ii) are implied by (v) is trivial, and that (iv) is implied by (v) follows from Lemma 3 applied to $a_i a_j$.

The proof of the proposition uses the language of lattices and is inspired by the escalation technique of Bhargava [**Bh**]. Let $L_i = \langle a_1, \ldots, a_i \rangle$ be the lattice associated to the diagonal form $\sum_{j \leqslant i} a_j x_j^2$. Let L be a lattice representing $a_1, \ldots, a_M$. In particular it must have a vector of length $a_1 = 1$. Since a_2 is not a square, L_1 does not represent a_2, so L must contain

$$\begin{pmatrix} a_1 & c \\ c & a_2 \end{pmatrix},$$

for some $c \in \mathcal{O}_K$. Since L is totally positive, we have $a_1 a_2 - c^2 \succ 0$, so that $c = 0$, and so L contains L_2. Having shown by induction that L must contain L_{i-1}, we proceed similarly: each of the a_i satisfies the assumptions of Lemma 3, so it is not a sum of totally positive elements. Hence if L_{i-1} represents it, we must have $a_i = a_j x_j^2$ for some $j \leqslant i-1$ which is not possible by assumption. Thus L_{i-1} does not represent a_i, so we need a linearly independent vector of length a_i. Hence L contains

$$\begin{pmatrix} L_{i-1} & c \\ c & a_i \end{pmatrix},$$

for some $c \in \mathcal{O}_K^{i-1}$. Considering 2-by-2 subdeterminants, we see as above that each entry of c must be 0. It follows that L contains L_i. In particular, we conclude that there cannot be a universal lattice of dimension $M-1$.

As mentioned in the introduction, for any given M, fields with the properties of Proposition 4 should exist in abundance, yet their existence is not easy to prove.

PROPOSITION 5. *Assume the Riemann hypothesis for* $L(s, \chi_D)$, *and that* $K = \mathbb{Q}(\sqrt{D})$ *has narrow class number one. Then for each* $\varepsilon > 0$ *there exists a constant* $C(\varepsilon)$ *such that a totally positive universal quadratic form needs at least* $C(\varepsilon) D^{1/4-\varepsilon}$ *variables.*

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Proof. Let I_n be the set of ideals of norm n, and let r be the arithmetic function defined by

$$r(n) = |I_n| = \sum_{d|n} \chi_D(d).$$

Clearly $r(n)$ is bounded by the divisor function which itself is bounded by $c(\varepsilon)n^\varepsilon$ for every $\varepsilon > 0$. If n is squarefree and $\mathfrak{a} = \prod_j \mathfrak{p}_j \in I_n$ with distinct prime ideals $\mathfrak{p}_j$, then every ideal in I_n is of the form $\prod_j \tilde{\mathfrak{p}}_j$ where $\tilde{\mathfrak{p}}_j \in \{\mathfrak{p}_j, \mathfrak{p}_j'\}$. For each pair $\{\mathfrak{p}, \mathfrak{p}'\}$ fix one of the two prime ideals, and for each squarefree n for which $I_n \neq \varnothing$ fix a totally positive generator $\alpha(n)$ of the unique element of I_n that is the product of our selected prime ideals. Then the set of all $\alpha(n)$ with $n \leqslant \delta^{1/2}$ satisfies assumptions (iii) and (v) of Proposition 4. If μ denotes the Möbius function, then their cardinality is

$$\sum_{\substack{n \leqslant \delta^{1/2} \\ r(n) \neq 0}} \mu^2(n) \geqslant c(\varepsilon) D^{-\varepsilon} \sum_{n \leqslant \delta^{1/2}} \mu^2(n) r(n) \geqslant c(\varepsilon) D^{-\varepsilon} \sum_{n \leqslant \delta^{1/2}} \mu^2(n) r(n) \Big(1 - \frac{n}{\delta^{1/2}}\Big).$$

By Mellin inversion, the sum on the right-hand side equals

$$\int_{2-i\infty}^{2+\infty} \sum_n \frac{r(n)\mu^2(n)}{n^s} \frac{\delta^{s/2}}{s(s+1)} \frac{ds}{2\pi i} = \int_{2-i\infty}^{2+\infty} \zeta(s) L(s, \chi_D) H(s) \frac{\delta^{s/2}}{s(s+1)} \frac{ds}{2\pi i},$$

where the Euler product

$$H(s) = \prod_{\chi_D(p)=1} \left(1 - \frac{3}{p^{2s}} + \frac{2}{p^{3s}}\right) \prod_{\chi_D(p) \neq 1} \left(1 - \frac{1}{p^{2s}}\right)$$

is absolutely convergent and uniformly bounded from above and below in $\Re s \geqslant 1/2 + \varepsilon$. We evaluate the integral by shifting the contour to line $\Re s = 2/3$, say, and picking up the residue of the pole at $s = 1$. The Riemann hypothesis implies the Lindelöf hypothesis [**IK**, p. 116], so that $L(2/3 + it, \chi_D) \ll_\varepsilon ((1 + |t|)D)^\varepsilon$. Hence

$$\int_{2-i\infty}^{2+i\infty} \zeta(s) L(s, \chi_D) H(s) \frac{\delta^{s/2}}{s(s+1)} \frac{ds}{2\pi i} = \frac{1}{2} L(1, \chi_D) H(1) \delta^{1/2} + O(\delta^{1/3} D^\varepsilon) \gg \frac{D^{1/4}}{\log\log D},$$

since the Riemann hypothesis also implies $L(1, \chi_D) \gg 1/\log\log D$ [**Li**]. This completes the proof.

Remark. Replacing ideals $\mathfrak{a} \in I_n$ by $\mathfrak{a}^h$ if the class number of K is $h \geqslant 1$, the same proof shows that a totally positive universal quadratic form needs in general at least $C(\varepsilon) D^{1/(4h)-\varepsilon}$ variables.

3. *Squarefree values of quadratic and linear polynomials*

The aim of this section is a proof of the following essentially classical result.

LEMMA 6. *Let $f(x) = ax^2 + bx + c$ be an integral quadratic polynomial with discriminant $\Delta = b^2 - 4ac \neq 0$. For $j = 1, \dots, m$ let $g_j(x) = k_j x + r_j$ be linear integral polynomials. Assume that each of $f, g_1, \dots, g_m$ takes at least one squarefree value. Then for a positive proportion of natural numbers n, the values $f(n), g_1(n), \dots, g_m(n)$ are simultaneously squarefree. More precisely, the asymptotic formula*

$$\mathcal{S} := \sum_{n \leqslant X} \mu^2(f(n)) \prod_{j=1}^m \mu^2(g_j(n)) = CX + O\left(X^{1 - \frac{2}{3(m+1)} + \varepsilon}\right)$$

holds for a constant $C > 0$. Here C and the O-constant depend on f and the g_j.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Remark. By replacing $f(x)$ with $f(4x)$, we can also guarantee $f(n) \equiv c \pmod 4$.

Proof. We have

$$\mathcal{S} = \sum_{n \leqslant X} \mu^2(f(n)) \prod_{j=1}^{m} \sum_{d_j^2 | g_j(n)} \mu(d_j).$$

Let $Y \geqslant 2$ be a parameter to be chosen later. We would like to approximate $\mathcal{S}$ by

$$\mathcal{S}_0 := \sum_{n \leqslant X} \mu^2(f(n)) \prod_{j=1}^{m} \sum_{\substack{d_j^2 | g_j(n) \\ d_j \leqslant Y}} \mu(d_j).$$

To estimate the error, let $1 \leqslant \mu \leqslant m$ and define

$$\mathcal{S}_\mu := \sum_{n \leqslant X} \mu^2(f(n)) \prod_{j=1}^{\mu-1} \sum_{\substack{d_j^2 | g_j(n) \\ d_j \leqslant Y}} \mu(d_j) \sum_{\substack{d_\mu^2 | g_\mu(n) \\ d_\mu > Y}} \mu(d_\mu) \prod_{j=\mu+1}^{m} \sum_{d_j^2 | g_j(n)} \mu(d_j).$$

Then

$$\begin{aligned} |\mathcal{S}_\mu| &\leqslant \sum_{n \leqslant X} \prod_{j=1}^{\mu-1} \sum_{\substack{d_j^2 | g_j(n) \\ d_j \leqslant Y}} \mu^2(d_j) \sum_{\substack{d_\mu^2 | g_\mu(n) \\ d_\mu > Y}} \mu^2(d_\mu) \leqslant \sum_{\substack{d_1, \dots, d_{\mu-1} \leqslant Y \\ Y < d_\mu \leqslant \sqrt{|k_\mu| X + |r_\mu|}}} \mu^2(d_1) \cdots \mu^2(d_\mu) \sum_{\substack{n \leqslant X \\ d_j^2 | g_j(n)}} 1 \\ &\leqslant \sum_{\substack{d_1, \dots, d_{\mu-1} \leqslant Y \\ Y < d_\mu \leqslant \sqrt{|k_\mu| X + |r_\mu|}}} \left(\frac{\mu^2(d_1) \cdots \mu^2(d_\mu)}{[d_1^2, \dots, d_\mu^2]} X + O(1) \right) \\ &\leqslant X \sum_{d_1, \dots, d_{\mu-1}} \sum_{d_\mu > Y} \frac{\mu^2(d_1) \cdots \mu^2(d_\mu)}{[d_1^2, \dots, d_\mu^2]} + O\left(Y^{\mu-1} X^{1/2} \right). \end{aligned}$$

To estimate the multiple sum, we apply Rankin's trick and choose $0 < s < 1$. Then the sum is bounded by

$$\frac{1}{Y^s} \sum_{d_1, \dots, d_\mu} \frac{\mu^2(d_1) \cdots \mu^2(d_\mu) d_\mu^s}{[d_1^2, \dots, d_\mu^2]} \leqslant \frac{1}{Y^s} \prod_p \left(1 + \frac{2^\mu p^s}{p^2} \right) \ll Y^{-s}. \tag{3·1}$$

With $s = 1 - \varepsilon$ we conclude $\mathcal{S}_\mu \ll X Y^{\varepsilon - 1} + Y^{\mu - 1} X^{1/2}$, and hence

$$\mathcal{S} = \mathcal{S}_0 + \sum_{\mu=1}^{m} \mathcal{S}_\mu = \mathcal{S}_0 + O\left(X Y^{\varepsilon - 1} + Y^{m-1} X^{1/2} \right).$$

We proceed to manipulate $\mathcal{S}_0$. Let $Z > Y$ be another parameter. We have

$$\mathcal{S}_0 = \sum_{d_1, \dots, d_m \leqslant D} \mu(d_1) \cdots \mu(d_m) \sum_{d_0} \mu(d_0) \sum_{\substack{n \leqslant X \\ d_0^2 | f(n) \\ d_j^2 | g_j(n)}} 1 = \mathcal{S}^{(1)} + \mathcal{S}^{(2)},$$

say, where $\mathcal{S}^{(1)}$ is the contribution of $d_0 \leqslant Z$ and $\mathcal{S}^{(2)}$ is the contribution $d_0 > Z$. We first

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

bound $\mathcal{S}^{(2)}$. We write

$$d_0^2 k = f(n) = \frac{(2an+b)^2 - \Delta}{4a}.$$

For given $a, k, \Delta \neq 0$, the equation $4akd_0^2 - (2an+b)^2 = -\Delta \neq 0$ is of Pellian type and has at most $O(\log X)$ solutions (d_0, n) with $n \leqslant X$ (with an absolute implied constant). We obtain

$$|\mathcal{S}^{(2)}| \leqslant Y^m \sum_{n \leqslant X} \sum_{\substack{d_0^2 k = f(n) \\ d_0 > Z}} 1 \ll Y^m \sum_{k \leqslant (|a|X^2 + |b|X + |c|)/Z^2} \log X \ll Y^m X^{2+\varepsilon} Z^{-2}.$$

In order to evaluate $\mathcal{S}^{(1)}$, we write $\mathbf{d} = (d_0, d_1, \dots, d_m)$ for squarefree $d_0, \dots, d_m$ and define

$$\rho(\mathbf{d}) := \left| \left\{ n \pmod{[d_0^2, \dots, d_m^2]} \mid f(n) \equiv 0 \pmod{d_0^2},\ g_j(n) \equiv 0 \pmod{d_j^2} \right\} \right|.$$

For notational simplicity we also write $\mu(\mathbf{d}) = \mu(d_0) \cdots \mu(d_m)$. By the Chinese remainder theorem, ρ is multiplicative in each variable and $\rho(p, d_1, \dots, d_m) \leqslant 2$ for all primes $p \nmid \Delta$, hence $\rho(\mathbf{d}) \ll \tau(d_0)$, where τ is the divisor function. Moreover,

$$\rho(\mathbf{d}) < [d_0^2, \dots, d_m^2] \tag{3·2}$$

for all $\mathbf{d} \neq (1, \dots, 1)$, for otherwise at least one of $f, g_1, \dots, g_m$ would have a fixed square divisor. Now

$$\begin{aligned} \mathcal{S}^{(1)} &= \sum_{d_1, \dots, d_m \leqslant Y} \sum_{d_0 \leqslant Z} \mu(\mathbf{d}) \left(\frac{\rho(\mathbf{d})}{[d_0^2, \dots, d_m^2]} X + O(\rho(\mathbf{d})) \right) \\ &= \sum_{d_1, \dots, d_m \leqslant Y} \sum_{d_0 \leqslant Z} \frac{\mu(\mathbf{d})\rho(\mathbf{d})}{[d_0^2, \dots, d_m^2]} X + O\left(Y^m Z \log Z\right). \end{aligned}$$

The same argument as in (3·1) implies that we may complete the multiple sum at the cost of an error $O(XY^{\varepsilon-1})$, and the resulting Euler product is absolutely convergent with value $C \neq 0$ by (3·2). Combining everything, we have shown

$$\mathcal{S} = CX + O\left(Y^m Z \log Z + Y^m X^{2+\varepsilon} Z^{-2} + XY^{\varepsilon-1} + Y^{m-1} X^{1/2}\right),$$

and the lemma follows upon choosing $Z = X^{2/3}$, $Y = X^{\frac{2}{3(m+1)}}$.

4. *Continued fractions and elements of small norm*

First we collect some useful results on continued fractions. Let $\gamma = [a_0, a_1, \dots]$ be an infinite continued fraction of a real number $\gamma > 0$, let and $p_i/q_i = [a_0, \dots, a_i]$ be its ith approximation ($a_i, p_i, q_i \in \mathbb{N}$). Then it is easy to see and well-known that $p_{i+1} = a_{i+1}p_i + p_{i-1}$ and $q_{i+1} = a_{i+1}q_i + q_{i-1}$ and

$$\left| \frac{p_i}{q_i} - \gamma \right| < \left| \frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}} \right| = \frac{1}{q_i q_{i+1}} < \frac{1}{a_{i+1} q_i^2}.$$

Assume now that $\gamma = \sqrt{D}$ (with squarefree D) and let

$$\alpha_i = p_i + q_i\sqrt{D}, \quad N_i = N(\alpha_i) = p_i^2 - Dq_i^2.$$

Then $|p_i - q_i\sqrt{D}| < 1/(a_{i+1}q_i) \leqslant 1/q_i$ and so

$$|N_i| = (p_i + q_i\sqrt{D})|p_i - q_i\sqrt{D}| < \left(2q_i\sqrt{D} + \frac{1}{q_i}\right) \frac{1}{a_{i+1}q_i} = \frac{2\sqrt{D}}{a_{i+1}} + \frac{1}{a_{i+1}q_i^2}. \tag{4·1}$$

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Since $(p_i, q_i) = 1$, we see that α_i is not divisible by a rational integer $\geqslant 2$.

Remark. We see that if a_{i+1} is not too small compared to $\sqrt{D}$, then N_i has a small norm. There are several explicit examples of such continued fractions. For instance, take $b, n, k \in \mathbb{N}$ and let

$$D = D(b, n, k) = (b(1 + 2bn)^k + n)^2 + 2(1 + 2bn)^k.$$

Then for each $j < k$, we have that $b_j = 2b(1 + 2bn)^{k-j}$ appears as a coefficient in the continued fraction for $\sqrt{D}$ (see [**Ma**, Section 3]). We have $\lfloor \sqrt{D} \rfloor = b(1 + 2bn)^k + n$, and so

$$\frac{2\sqrt{D}}{b_j} < \frac{b(1 + 2bn)^k + n + 1}{b(1 + 2bn)^{k-j}} < (1 + 2bn)^j + 1 < D^{\frac{j}{2k}} + 1.$$

Although this produces many elements of small norm, it is not so easy to choose b, n, k so that D is (almost) squarefree, and it is also not trivial to verify the other conditions of Proposition 4. Therefore we proceed slightly differently in the following.

Let us now consider periodic continued fractions of the form

$$\gamma = [k; \overline{u, \ldots, u, 2k}] \tag{4·2}$$

with ℓ elements u in the period. Friesen [**Fr**] gave, for general periodic, symmetric continued fractions, certain necessary and sufficient parity conditions that ensure that there are infinitely many k such that $\gamma = \sqrt{D}$ with squarefree D. We shall need more explicit information than this (in particular on the convergents p_i/q_i, see Proposition 10 below), so let's compute the special case (4·2) in complete detail. Let

$$\rho_\pm := \frac{1}{2}(u \pm \sqrt{u^2 + 4}), \quad c_\pm := \frac{\pm 1 \pm (k + \sqrt{D})\rho_\pm}{\sqrt{4 + u^2}}, \quad c'_\pm := \frac{\pm 1 \pm (k - \sqrt{D})\rho_\pm}{\sqrt{4 + u^2}}. \tag{4·3}$$

Since $q_{-1} = 0, q_0 = 1, q_1 = u$, we have

$$q_i = \frac{\rho_+^{i+1} - \rho_-^{i+1}}{\rho_+ - \rho_-}$$

for $i \leqslant \ell$, so that q_i is a function of u. Then we can evaluate p_i by $p_i = kq_i + q_{i-1}$ for $i \leqslant \ell$.

Clearly,

$$\rho_+ > u, \quad \rho_+\rho_- = -1, \quad -\frac{1}{u} < \rho_- < 0, \quad c_+ > c_-.$$

We start with the following essentially well-known lemma.

LEMMA 7. *Let γ be as in* (4·2) *and keep the notation developed so far.*
(a) *For $0 \leqslant j < i \leqslant \ell$ we have*

$$q_i q_{j-1} - q_{i-1} q_j = (-1)^{j+1} q_{i-j-1} \quad \textit{and} \quad q_i q_{i-2} - q_{i-1}^2 = (-1)^i.$$

(b) *For $0 \leqslant i \leqslant \ell$, the sequences p_i, q_i, α_i and α'_i are linear combinations of ρ_+^i and ρ_-^i, and we have explicitly*

$$\alpha_i = c_+\rho_+^i + c_-\rho_-^i \quad \textit{and} \quad \alpha'_i = c'_+\rho_+^i + c'_-\rho_-^i.$$

(c) *For $0 \leqslant i \leqslant \ell$ and u even, we have $q_i \equiv 0 \pmod 2$ when $i \equiv 1 \pmod 2$.*

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Proof.
(a) We have

$$q_iq_{j-1} - q_{i-1}q_j = (uq_{i-1} + q_{i-2})q_{j-1} - q_{i-1}(uq_{j-1} + q_{j-2})$$
$$= (-1)(q_{i-1}q_{j-2} - q_{i-2}q_{j-1}) = \cdots = (-1)^j(q_{i-j}q_{-1} - q_{i-j-1}q_0) = (-1)^{j+1}q_{i-j-1},$$

because $q_0 = 1$ and $q_{-1} = 0$. We obtain the second identity by taking $j = i - 1$.
(b) This follows in a well-known fashion from the recurrence $\alpha_{i+1} = u\alpha_i + \alpha_{i-1}$ for $i \leqslant \ell - 1$.
(c) This follows directly from the recurrence relation.

The following lemma contains some technical estimates for the quantities defined in (4·3) for future reference.

LEMMA 8.
(a) *If $k \geqslant u$, then $c_- > 0$.*
(b) *If $u \geqslant 2$, then $\rho_-^2 < |c'_-| < 1$.*
(c) *If $u \geqslant 2$, then $|c'_+| < 2\rho_+^{-\ell} = 2|\rho_-|^\ell$.*
(d) *If $n \leqslant (\ell - 4)/2$ and $u \geqslant 2$, then $|c'_+\rho_+^n| < |c'_-\rho_-^n|/2$.*

Proof.
(a) We observe that $k + \sqrt{D} > 2k \geqslant 2u > \rho_+$, so that $-1 - (k + \sqrt{D})\rho_- > 0$.
(b) We have $[(\sqrt{D} - k)^{-1}] = u$, so that $0 > k - \sqrt{D} > -u^{-1}$. This implies

$$c'_-\sqrt{4 + u^2} = -1 - (k - \sqrt{D})\rho_- < -1,$$

so that in particular $c'_- < 0$ and

$$|c'_-| > \frac{1}{\sqrt{4 + u^2}} > \frac{1}{2u} \geqslant \frac{1}{u^2} > \rho_-^2.$$

For the other inequality we have

$$|c'_-|\sqrt{4 + u^2} = 1 + (k - \sqrt{D})\rho_- < 1 - \frac{2}{u}\rho_- < 1 + \frac{2}{u^2} < \sqrt{4 + u^2}.$$

(c) From (b) we have $|c'_-\rho_-^\ell| < 1$. Since $|\alpha'_\ell| < 1$, we must have $|c'_+\rho_+^\ell| < 2$.

(d) Since $\rho_+ > u \geqslant 2$, we conclude from part (c) that

$$|c'_+\rho_+^n| < 2\rho_+^{n-\ell} < \frac{1}{2}\rho_+^{n-\ell+2}.$$

On the other hand, from part (b) we obtain

$$|c'_-\rho_-^n| > |\rho_-^{n+2}| = \rho_+^{-2-n}.$$

Combining the last two displays proves the claim for $n < (\ell - 4)/2$.

PROPOSITION 9. *Let γ be as in* (4·2). *Then $\gamma = \sqrt{D}$ for some $D \in \mathbb{N}$ if and only if $q_\ell \mid kp_\ell + p_{\ell-1}$. When u and q_ℓ have the same parity, this condition is satisfied when $2k = q_\ell t + u$ for $t \in \mathbb{N}$ if u is even, and $t \in \mathbb{N}$ odd if u is odd. In this case,*

$$D = D(t) = k^2 + tq_{\ell-1} + 1 = t^2\frac{q_\ell^2}{4} + t\frac{uq_\ell + 2q_{\ell-1}}{2} + \frac{u^2}{4} + 1. \tag{4·4}$$

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Moreover, if $\alpha_i = p_i + q_i\sqrt{D}$ *for* $i \leqslant \ell$, *then*

$$N_i = N(\alpha_i) = (-1)^{i+1}(tq_iq_{\ell-i-1} + 1) \tag{4·5}$$

is a linear polynomial in t.

Proof. It is a well-known property of continued fractions that

$$\frac{(k+\gamma)p_\ell + p_{\ell-1}}{(k+\gamma)q_\ell + q_{\ell-1}} = \gamma.$$

Using $p_\ell = kq_\ell + q_{\ell-1}$ it then simplifies to $\gamma^2 q_\ell = kp_\ell + p_{\ell-1}$. We see that $\gamma = \sqrt{D}$ if and only if $q_\ell \mid kp_\ell + p_{\ell-1} = k^2q_\ell + 2kq_{\ell-1} + q_{\ell-2}$; in other words,

$$q_\ell = uq_{\ell-1} + q_{\ell-2} \mid 2kq_{\ell-1} + q_{\ell-2}.$$

We obtain that we can take $2k = q_\ell t + u$, and (4·4) follows.

Since $p_i = kq_i + q_{i-1}$, we get

$$\begin{aligned} N_i = p_i^2 - Dq_i^2 &= (kq_i + q_{i-1})^2 - (k^2 + tq_{\ell-1} + 1)q_i^2 \\ &= k^2q_i^2 + 2kq_iq_{i-1} + q_{i-1}^2 - k^2q_i^2 - tq_{\ell-1}q_i^2 - q_i^2 \\ &= (q_\ell t + u)q_iq_{i-1} + q_{i-1}^2 - tq_{\ell-1}q_i^2 - q_i^2 \\ &= q_it(q_\ell q_{i-1} - q_{\ell-1}q_i) + q_{i-1}(q_{i-1} + uq_i) - q_i^2 \\ &= q_it(-1)^{i+1}q_{\ell-i-1} + q_{i-1}q_{i+1} - q_i^2 = (-1)^{i+1}(tq_iq_{\ell-i-1} + 1), \end{aligned}$$

where in the last two equalities we have used the two identities from Lemma 7a) and the recurrence $q_{i+1} = uq_i + q_{i-1}$ for $i \leqslant \ell - 1$. When $i = \ell$, then $q_{\ell+1}$ is not given by this recurrence, but we still have $q_{\ell-1}(q_{\ell-1} + uq_\ell) - q_\ell^2 = (-1)^{\ell+1}$.

We are now ready to state and prove the first key ingredient for the proof of Theorem 1.

PROPOSITION 10. *For every* $u \in \mathbb{N}$ *with* $u \equiv 2 \pmod 4$ *and* $u^2/4 + 1$ *squarefree and every odd* $\ell \in \mathbb{N}$, *there exist infinitely many squarefree* $D \equiv 2 \pmod 4$ *with* $\sqrt{D} = [k; \overline{u, \ldots, u, 2k}]$ *with* ℓ *elements* u *in the period, such that for odd* $1 \leqslant i \leqslant (\ell-1)/2$ *we have*:

(1) $N(\alpha_i)$ *is squarefree and not* ± 1;

(2) $n \nmid \alpha_i$ *for* $2 \leqslant n \in \mathbb{N}$;

(3) $N(\alpha_i) < 2\frac{\sqrt{D}}{u} + \frac{1}{u}\frac{\sqrt{D}}{u}$ *and* $\alpha_i \succ 0$.

Moreover, these numbers $N(\alpha_i)$ *are pairwise distinct.*

Proof. Since u is even and ℓ is odd, it follows from Lemma 7(c) that q_ℓ is even, so that Proposition 9 is applicable. Recall from (4·5) that

$$N_i = N_i(t) = k_it + 1, \quad k_i = q_iq_{\ell-i-1} \tag{4·6}$$

for i odd. In particular, α_i is not a unit for $i \leqslant \ell - 1$, which is the second part of condition (1). It follows from the recurrence relation similarly as in Lemma 7(b) that

$$k_i = \alpha^2\rho_+^{\ell-1} + \beta^2\rho_-^{\ell-1} + \alpha\beta\left((-1)^{\ell-i-1}\rho_+^{2i+1-\ell} + (-1)^i\rho_+^{\ell-2i-1}\right),$$

for certain real numbers α, β. The last parenthesis of the previous display is strictly decreasing in absolute value for $i \leqslant (\ell-1)/2$, so that $k_i \neq k_j$ for $1 \leqslant i < j \leqslant (\ell-1)/2$ and $i \equiv j \equiv 1 \pmod 2$. In particular, $N_i \neq N_j$.

Conditions (2) and (3) are automatic; notice that (4·6) implies $\alpha_i \succ 0$ if i is odd. The first part of condition (1) follows directly from Lemma 6 applied to the quadratic polynomial in

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

(4·4) and the linear polynomials in (4·6). Notice that the constant terms of $D(t)$ and $N_i(t)$ are squarefree, so all considered polynomials take squarefree values.

The α_i constructed in the previous proposition satisfy properties (i) – (iii) from Proposition 4, but a comparison of (4·4) and (4·5) shows that $N\alpha_i \asymp \sqrt{D}$, so they fail to satisfy condition (v) from Proposition 4. Hence we must find another way to ensure (iv), and the rest of this section is devoted to this task.

From now on we assume that $\sqrt{D} = [k; \overline{u, \dots, u, 2k}]$ for a squarefree $D \equiv 2, 3 \pmod 4$ with $k > u \geqslant 5$. For $i \leqslant \ell - 1$ we know that $\alpha_i = p_i + q_i\sqrt{D}$ is totally positive if and only if i is odd, and we know from (4·1) that

$$|N_i| = |N(\alpha_i)| < \frac{2\sqrt{D}}{u} + \frac{1}{uq_i^2} < \frac{1}{2}\sqrt{D}.$$

LEMMA 11. *Take odd $i < j \leqslant (\ell - 4)/2$. There is no $h \geqslant 0$ such that $\alpha_i\alpha_j \succ \alpha_h^2$.*

Proof. Assume that $\alpha_i\alpha_j \succ \alpha_h^2$. First note that the sequence α_n is strictly increasing, and so $h < 2j + 1$. Hence the explicit formulae from Lemma 7(b) hold for α_i, α_j and α_h. From Lemma 8a) we have that $c_+ > c_- > 0$. Now, for $h \geqslant 1$ we have

$$\begin{aligned} c_+^2\rho_+^{2h-\frac{1}{2}} &< c_+^2(\rho_+^{2h} - 2) < c_+^2\rho_+^{2h} + 2c_+c_-(-1)^h < \alpha_h^2 \\ &< \alpha_i\alpha_j = (c_+\rho_+^i + c_-\rho_-^i)(c_+\rho_+^j + c_-\rho_-^j) < c_+^2\rho_+^{i+j} \end{aligned}$$

(in the last inequality we have used that ρ_- is negative and i, j are odd). Hence $2h - \frac{1}{2} < i + j$ and so $2h \leqslant i + j$. With slightly more precise estimates we can even exclude the case $2h = i + j$. In this case, the inequality $\alpha_i\alpha_j > \alpha_h^2$ is after some simplification equivalent to

$$c_-c_+(\rho_+^i\rho_-^j + \rho_-^i\rho_+^j) > 2c_-c_+(-1)^h.$$

Since c_- and c_+ are positive and i, j are odd, the left-hand side is negative, so that h must be odd, and we obtain $2 > \rho_+^{i-j} + \rho_+^{j-i}$ which is a contradiction. We conclude that $2h < i + j$.

On the other hand, since i, $j \leqslant (\ell - 4)/2$ we have from Lemma 8(d) that

$$\alpha_i'\alpha_j' < (|c_+'\rho_+^i| + |c_-'\rho_-^i|)(|c_+'\rho_+^j| + |c_-'\rho_-^j|) < \left(\frac{3}{2}\right)^2 |c_-'^2||\rho_-|^{i+j}.$$

If $2h \leqslant i + j \leqslant \ell - 4$, then from Lemma 8(b) and (c) we have

$$\begin{aligned} (\alpha_h')^2 &= (c_-'\rho_-^h)^2 + 2c_-'c_+'\rho_+^h\rho_-^h + (c_+'\rho_+^h)^2 > (c_-'\rho_-^h)^2 - 2|c_-'c_+'| \\ &> (c_-'\rho_-^h)^2 - 4|c_-'\rho_-^\ell| > (c_-'\rho_-^h)^2(1 - 4|\rho_-|^{\ell-2-2h}) > (c_-'\rho_-^h)^2(1-4u^{-2}) = \frac{21}{25}(c_-'\rho_-^h)^2. \end{aligned}$$

Now our assumption $\alpha_i'\alpha_j' \geqslant (\alpha_h')^2$ implies $|\rho_-|^{i+j} > |\rho_-|^{2h}/3 > |\rho_-|^{2h+1}$, so that $i + j < 2h + 1$, and hence $i + j \leqslant 2h$. This contradicts our previous conclusion $2h < i + j$, so that the original assumption $\alpha_i\alpha_j \succ \alpha_h^2$ was wrong.

PROPOSITION 12. *Take odd $i < j \leqslant (\ell - 4)/2$. Assume that there is $\mu \in \mathcal{O}_K$ such that $\alpha_i\alpha_j \succ \mu^2$. Then $\mu = 0$.*

Proof. If $\mu \in \mathbb{Z}$, then $1 > \alpha_i'\alpha_j' > \mu^2$, which is possible only for $\mu = 0$. From now on assume that $\mu \notin \mathbb{Z}$. We will show that this implies $\mu = \alpha_h$ which is a contradiction by the previous lemma.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Let $\alpha_i\alpha_j = \mu^2 + \nu$ with $\nu \succ 0$. Since also $\mu^2 \succ 0$, we have $D/4 > N(\alpha_i\alpha_j) > N(\mu)^2$, and so $|N(\mu)| < \sqrt{D}/2$. Let $\mu = x + y\sqrt{D} \notin \mathbb{Z}$. Clearly x and y must have the same sign (otherwise $\alpha_i'\alpha_j' > (\mu')^2$ cannot be satisfied), and without loss of generality assume that $x, y > 0$. We distinguish two cases.

Case 1. $\mu' < 0$. Then $y^2D - x^2 = |N(\mu)| < \sqrt{D}/2$, and so $y^2D - \sqrt{D}/2 - x^2 < 0$, hence $\sqrt{D}$ lies between the roots of $2y^2T^2 - T - 2x^2$. Thus

$$\sqrt{D} < \frac{1 + \sqrt{1 + 16x^2y^2}}{4y^2} < \frac{1}{4y^2} + \frac{\sqrt{1 + 8xy + 16x^2y^2}}{4y^2} = \frac{x}{y} + \frac{1}{2y^2}.$$

By assumption $x/y < \sqrt{D}$, and so we see that $|x/y - \sqrt{D}| < 1/2y^2$, but as is well known [**HW**, Theorem 184], this implies that $\mu = \alpha_h$ for some h.

Case 2. $\mu' > 0$. Then $x^2 - y^2D = |N(\mu)| < \sqrt{D}/2$, and so $2y^2D + \sqrt{D} - 2x^2 > 0$. Since $\sqrt{D} > 0$, we must have that $\sqrt{D}$ is greater than the positive root of the polynomial, i.e.,

$$\sqrt{D} > \frac{-1 + \sqrt{1 + 16x^2y^2}}{4y^2} > \frac{-1}{4y^2} + \frac{\sqrt{1 - 8xy + 16x^2y^2}}{4y^2} = \frac{x}{y} - \frac{1}{2y^2}.$$

Since $\sqrt{D} < x/y$, we again obtain $|x/y - \sqrt{D}| < 1/2y^2$, and so $\mu = \alpha_h$ for some h.

The proof of Theorem 1 is now a direct consequence of Propositions 4, 10 and 12.

5. *An example*

We conclude the paper with an explicit example for the field $\mathbb{Q}(\sqrt{73})$. We will see that in such specific situation one can get a little further than the general results of the previous sections. We suppress some of the fairly straightforward computations.

Since $73 \equiv 1 \pmod 4$, the ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = (1 + \sqrt{73})/2 \approx 4.772$. We know from Lemma 3 that if $\alpha \in \mathcal{O}_K^+$ has norm $\leqslant 8 < \sqrt{73}$ and is not divisible by any $n \in \mathbb{Z}$, $n > 1$, then α is not the sum of two totally positive integers. We shall use the following elements of $\mathcal{O}_K$:

(i) $\varepsilon = 943 + 250\omega \approx 2136$ is the fundamental unit, $N(\varepsilon) = -1$;
(ii) $\rho = 4 + \omega \approx 8.772$ and $\rho' = 5 - \omega \approx 0.228$ are totally positive elements of norm 2;
(iii) $\sigma = 83 + 22\omega \approx 187.984$ and $\sigma' = 105 - 22\omega \approx 0.016$ are totally positive elements of norm 3.

We shall often use the following variant of Lemma 3:

LEMMA 13. *Let* $\gamma \in \{\rho, \rho', \sigma, \sigma', \rho\sigma, \rho\sigma', \rho'\sigma, \rho'\sigma', \rho^2\sigma, \rho'^2\sigma', \rho\sigma'^2, \rho'\sigma^2, 2\rho, 2\rho', 2\sigma, 2\sigma', 2\rho\sigma, 2\rho'\sigma', 3\rho, 3\rho'\}$, $\alpha \in \mathcal{O}_K$ *and* $\beta \in \mathcal{O}_K^+$. *If* $\gamma = \alpha^2 + \beta$, *then* $\alpha = 0$.

Proof. If $\gamma \in \{\rho, \rho', \sigma, \sigma', \rho\sigma, \rho\sigma', \rho'\sigma, \rho'\sigma'\}$, then the claim follows from Lemma 3, as all these elements have norm $\leqslant 6 < \sqrt{73}$.

Assume that $\alpha \neq 0$. Without loss of generality we can assume that $\alpha > 0$. By Lemma 1 we know that $\sqrt{N(\gamma)} \geqslant |N(\alpha)| + \sqrt{N(\beta)}$. Since γ has norm at most 24, it follows that $|N(\alpha)| \leqslant \sqrt{24} - 1 \approx 3.9$. Hence $N(\alpha) = \pm 1, \pm 2, \pm 3$.

We have $\alpha^2 < \gamma \leqslant \rho^2\sigma \approx 14465$, and so $\alpha < 121$. Similarly $\alpha'^2 < 121$. Since ε is fairly big, we can check that the only possibilities are $\alpha = 1, \rho, \rho', \varepsilon\sigma', \varepsilon'\sigma$. One then just checks that in each of these cases, $\gamma - \alpha^2$ is not totally positive.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

Note that three cases which do not satisfy Lemma 13 are $2\rho'\sigma \succ \rho^2$, $\rho\sigma^2 \succ (\varepsilon\rho')^2$ and $\rho^2\sigma' \succ 1^2$.

Let us now start constructing a universal quadratic form L: L has to represent 1, and so $L = L_1 \oplus L_1'$ for $L_1 = \langle 1 \rangle$.

Since ρ is not a square, L_1 does not represent ρ. Let

$$L_2 = \begin{pmatrix} 1 & a \\ a & \rho \end{pmatrix}.$$

We have $1 \cdot \rho \succ a^2$, and so $a = 0$ by Lemma 13. Hence we obtain that $L = L_2 \oplus L_2'$ with $L_2 = \langle 1, \rho \rangle$.

Similarly L_2 does not represent σ. Let

$$L_3 = \begin{pmatrix} 1 & 0 & a \\ 0 & \rho & b \\ a & b & \sigma \end{pmatrix}$$

be an escalation of L_2. Then $\sigma \succ a^2$ and $\rho\sigma \succ b^2$, and so by Lemma 13 we see that $a = b = 0$ and $L_3 = \langle 1, \rho, \sigma \rangle$.

Now L_3 does not represent ρ'. Again we can show that all the off-diagonal elements after the escalation by ρ' are zero, except for the one in the same row as ρ, so that

$$L_4 = \langle 1, \sigma \rangle \oplus \begin{pmatrix} \rho & a \\ a & \rho' \end{pmatrix},$$

where $2 = \rho\rho' \succ a^2$. Thus $a = 0, \pm 1$. However, in the case $a = -1$, the form is equivalent to the form with $a = 1$. Hence it suffices to consider $a = 0, 1$.

Next L_4 does not represent σ': if it did, we would need to have $a = 1$ and $\rho x^2 + 2xy + \rho' y^2 = \sigma'$, which implies $(\rho x + y)^2 + y^2 = \rho\sigma'$, a contradiction with Lemma 13. Let L_5 be the corresponding escalation. We can again show that some off-diagonal elements are zero; we are left with

$$L_5 = \langle 1 \rangle \oplus \begin{pmatrix} \rho & a \\ a & \rho' \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix},$$

where $b = 0, 1$.

The only way how L_5 could represent 2 is if $a = 1$ and $\rho x^2 + 2xy + \rho' y^2 \in \{1, 2\}$, or if $b = 1$ and $\sigma x^2 + 2xy + \sigma' y^2 \in \{1, 2\}$. These two cases imply $(\rho x + y)^2 + y^2 \in \{\rho, 2\rho\}$ and $(\sigma x + y)^2 + 2y^2 \in \{\sigma, 2\sigma\}$, respectively. But all of these conditions contradict Lemma 13.

The escalation of L_5 by 2 is

$$L_6^0 = \begin{pmatrix} \rho & a \\ a & \rho' \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix} \oplus \begin{pmatrix} 1 & c \\ c & 2 \end{pmatrix}.$$

We have $c^2 \prec 2$, and so $c = 0, 1$. If $c = 1$, the last matrix is equivalent to the diagonal form

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence we conclude that L_6^0 is equivalent to the form

$$L_6 = \langle 1, m \rangle \oplus \begin{pmatrix} \rho & a \\ a & \rho' \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix},$$

where $m = 1, 2$.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

In the same manner as before we verify that $\rho'\sigma$ is not represented by L_6. The corresponding escalation is

$$L_7 = \langle 1\rangle \oplus \begin{pmatrix} \rho & a & 0 & 0 \\ a & \rho' & c & 0 \\ 0 & c & \rho'\sigma & d \\ 0 & 0 & d & m \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix},$$

where $c = 0, 1$; $d = 0$ if $m = 1$ and $d = 0, \rho$ if $m = 2$.

Finally let us show that L_7 does not represent $\rho\sigma$. For this we distinguish two cases according to the value of c:

$c = 0$: Then

$$L_7 = \langle 1\rangle \oplus \begin{pmatrix} \rho & a \\ a & \rho' \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix} \oplus \begin{pmatrix} \rho'\sigma & d \\ d & m \end{pmatrix}.$$

As before, if $\rho\sigma$ were represented by this form, at least one of the equations $x^2+(x+\rho' y)^2 = \rho\rho'\sigma = 2\sigma$, $2x^2 + (x + \sigma' y)^2 = \rho\sigma\sigma' = 3\rho$, and $\rho x^2 + (\rho x + 2y)^2 = 2\rho\sigma$ (note here that $2\rho'\sigma - \rho^2 = \rho$) would have a solution, but this is not possible by Lemma 13.

$c = 1$: Let us first show that in this case, $a = d = 0$. Assume that $a = 1$. But then

$$\begin{pmatrix} \rho & 1 & 0 \\ 1 & \rho' & 1 \\ 0 & 1 & \rho'\sigma \end{pmatrix}$$

has determinant $\rho'\sigma - \rho$, which is not totally positive, a contradiction.

Assume now that $d = \rho$, which is possible only when $m = 2$. Then

$$\begin{pmatrix} \rho' & 1 & 0 \\ 1 & \rho'\sigma & \rho \\ 0 & \rho & 2 \end{pmatrix}$$

has determinant $2\rho'^2\sigma - 2\rho - 2 = 0$, so it is again not totally positive.

Hence we see that in the case $c = 1$,

$$L_7 = \langle 1, m, \rho\rangle \oplus \begin{pmatrix} \rho' & 1 \\ 1 & \rho'\sigma \end{pmatrix} \oplus \begin{pmatrix} \sigma & b \\ b & \sigma' \end{pmatrix}.$$

As before we verify that this form does not represent $\rho\sigma$.

We could probably continue a little longer by escalating L_7 by $\rho\sigma$, but the situation is becoming messy, so let's stop here by concluding that we have shown:

PROPOSITION 14. *A (classical) universal totally positive quadratic forms over* $\mathbb{Z}[(1 + \sqrt{73})/2]$ *must have at least* 8 *variables.*

Since the elements $1, 2, \rho, \rho', \sigma, \sigma', \rho\sigma, \rho\sigma', \rho'\sigma, \rho'\sigma'$ cover 10 different square classes and (with the exception of $2 = 1 + 1$) are not sums of totally positive elements, we can also conclude that a universal *diagonal* form over $\mathbb{Z}[(1 + \sqrt{73})/2]$ must have at least 10 variables.

Acknowledgements. We would very much like to thank the referee, not only for a careful reading of the manuscript, but also for very concrete and useful suggestions how to streamline the presentation and the argument.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press

REFERENCES

[**Bh**] M. BHARGAVA. On the Conway–Schneeberger fifteen theorem. *Contemp. Math.* **272** (1999), 27–37.

[**CKR**] W. K. CHAN, M.-H. KIM and S. RAGHAVAN. Ternary universal integral quadratic forms. *Japan. J. Math.* **22** (1996), 263–273.

[**Fr**] C. FRIESEN. On continued fractions of given period. *Proc. Amer. Math. Soc.* **103** (1988), 8–14.

[**HW**] G. H. HARDY and E. M. WRIGHT. *An Introduction to the Theory of Numbers*, 5th edition (The Clarendon Press, Oxford University Press, New York, 1979).

[**IK**] H. IWANIEC and E. KOWALSKI. *Analytic Number Theory*. AMS Colloquium Publications **53** (Providence, RI, 2004).

[**Ki1**] B. M. KIM. Finiteness of real quadratic fields which admit positive integral diagonal septenary universal forms. *Manuscr. Math.* **99** (1999), 181–184.

[**Ki2**] B. M. KIM. Universal octonary diagonal forms over some real quadratic fields. *Comment. Math. Helv.* **75** (2000), 410–414.

[**Li**] J. E. LITTLEWOOD. On the class-number of the corpus $P(\sqrt{-k})$. *Proc. Lond. Math. Soc.* **27** (1928), 358–372.

[**Ma**] D. MADDEN. Constructing families of long continued fractions. *Pacific J. Math.* **198** (2001), 123–147.

[**Ro**] A. E. ROSS. On representation of integers by quadratic forms. *Proc. Nat. Acad. Sci.* **18** (1932), 600–608.

[**Si**] C. L. SIEGEL. Sums of mth powers of algebraic integers. *Ann. Math.* **46** (1945), 313–339.

https://doi.org/10.1017/S030500411500033X Published online by Cambridge University Press