Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 94 (2019)
Heft: 2

Artikel: A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real number field
Autor: Yatsyna, Pavlo
DOI: https://doi.org/10.5169/seals-846781

Comment. Math. Helv. 94 (2019), 221–239
DOI 10.4171/CMH/459

Commentarii Mathematici Helvetici

A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real number field

Pavlo Yatsyna

Abstract. We show that if K is a monogenic, primitive, totally real number field, that contains units of every signature, then there exists a lower bound for the rank of integer universal quadratic forms defined over K. In particular, we extend the work of Blomer and Kala, to show that there exist infinitely many totally real cubic number fields that do not have a universal quadratic form of a given rank defined over them. For the real quadratic number fields with a unit of negative norm, we show that the minimal rank of a universal quadratic form goes to infinity as the discriminant of the number field grows. These results follow from the study of interlacing polynomials. Specifically, we show that there are only finitely many irreducible monic polynomials related to primitive number fields of a given degree, that have a bounded number of interlacing polynomials.

Mathematics Subject Classification (2010). 11E12, 11H06, 11R80.

Keywords. Universal quadratic forms, totally real number fields, ideal lattices, interlacing polynomials.

1. Introduction

Theorem 290 [5] tells us when a given positive definite quadratic form over rational integers represents all natural numbers. Relatively little is known about universal quadratic forms with coefficients in the ring of integers R of a totally real number field K. Götzky [14], Maass [22] and Siegel [27] showed that if all of the totally positive integers in K can be represented as the sum of squares, then $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{5})$. Chan, Kim, and Raghavan [7] proved that one finds universal ternary quadratic forms only over $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$. On another hand, B. M. Kim [20] gave an explicit construction of an octonary diagonal universal quadratic form for infinitely many real quadratic number fields. Blomer and Kala in [6] (and Kala in [18]) proved that for a given m there are infinitely many real quadratic number fields that do not admit universal quadratic forms with m coefficients. This result was extended to multiquadratic fields by Kala and Svoboda in [19]. For a totally real number field K of an odd degree, it was shown in [10], by Earnest and Khosravani, that there are at most finitely many inequivalent quaternary

universal quadratic forms over K. Kitaoka suggested [21] that there may only exist finitely many totally real number fields over which there exists a universal ternary quadratic form.

In this paper, we investigate universal quadratic forms defined over the ring of integers R of a totally real number field K by studying interlacing polynomials. Specifically, we establish a correspondence between elements of the codifferent of R over K and interlacing polynomials. For primitive extensions we prove the following result:

Theorem 1.1. *Let $d, r \in \mathbb{N}$. Up to $\mathbb{Z}$-equivalence, there are only finitely many irreducible monic polynomials $f \in \mathbb{Z}[x]$ of degree d such that $\mathbb{Q}[x]/(f)$ is a primitive field and f is interlaced by at most r monic integer polynomials.*

We show that there exists an infinite family of non-interlacing polynomials:

Theorem 1.2. *Let $d \in \mathbb{N}$ such that d is square-free, d is not a prime number or twice a prime number, $d > 20$ and $d \neq 30$. Then the minimal polynomial of $\zeta_d + \zeta_d^{-1}$ is non-interlacing.*

But, such polynomials do not exist for the first few degrees:

Theorem 1.3. *There does not exist a non-interlacing irreducible integer polynomial of degree 2, 3, 4, 5, or 7.*

Let us say that a totally real number field satisfies Condition (A) if it is monogenic and has units of every signature. In the spirit of the work of Blomer and Kala, for primitive number fields we show:

Theorem 1.4. *Let $d, r \in \mathbb{N}$. There are only finitely many totally real primitive number fields of degree d that satisfy Condition (A) and have an integer universal quadratic form of rank r defined over them.*

As an application of the theorem above, we have:

Theorem 1.5. *For any given $r \in \mathbb{Z}$, there exist infinitely many totally real quadratic and cubic number fields that do not have a universal quadratic form of rank r defined over them.*

We also show that the minimal rank of a universal quadratic form over quadratic fields grows at the order of the fourth root of the discriminant (Corollary 5.5). This was previously shown in [6, Prop. 5] conditionally on the Riemann hypothesis.

The basic idea of this paper stems from the observation that if the codifferent of R is a principal ideal generated by a totally positive number, i.e. $R^\vee = \gamma R$, then a universal quadratic form Q over R can be scaled to represent all the totally positive elements in the codifferent. Furthermore, $\mathrm{tr}_{K/\mathbb{Q}}(\gamma Q)$ becomes a quadratic form over $\mathbb{Z}$, where all the minimal vectors of $\mathrm{tr}_{K/\mathbb{Q}}(\gamma Q)$ relate to the totally positive numbers of the minimal trace in the codifferent represented by γQ. On the other hand, totally positive elements of trace one correspond to lattice points in certain convex sets, and in particular, to interlacing polynomials. By showing that the number of

interlacing polynomials grows to infinity for a given degree, we are able to show that the rank of universal quadratic forms over R has to grow also, else we would have quadratic forms with the number of minimal vectors surpassing the kissing number, which is impossible.

In the first section, after the preliminaries, we focus on the interlacing polynomials and show the correspondence between lattice points in certain convex sets and totally positive elements of trace one in the codifferent of R. Theorem 1.1 appears in this section. In the following section, we tackle Theorems 1.2 and 1.3 and look at some of the examples of non-interlacing polynomials. Finally, the last section consists of results relating to universal quadratic forms. Appropriately, it contains proofs of Theorem 1.4 and Theorem 1.5.

Acknowledgements. I would like to thank James McKee for his valuable comments on the first manuscript, and the anonymous referee for careful revisions and many helpful suggestions. This research was supported through the programme "Oberwolfach Leibniz Fellows" by the Mathematisches Forschungsinstitut Oberwolfach in 2017.

2. Preliminaries

Throughout the paper, K is a totally real number field with the ring of integers R. A number field is *monogenic* if its ring of integers has integer power basis, i.e. $R = \mathbb{Z}[\alpha]$. We say that K is *primitive* if there is no proper subfield of K other than $\mathbb{Q}$. We let $\sigma_1, \ldots, \sigma_d$ to be the distinct embedding of K into $\mathbb{R}$. For $\alpha \in K$, we write $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha)$ and $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha)$. For an ideal I in R, $\mathrm{N}(I)$ is the absolute norm of I. We assume that all the polynomials are integer, monic, separable, and have only real roots unless stated otherwise. Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial such that $K \cong \mathbb{Q}[x]/(f)$. Let $\alpha \in \mathbb{R}$ be a root of f, then $\mathbb{Z}[\alpha]$ is an *order* in K. We denote the *dual* of it by $\mathbb{Z}[\alpha]^\vee = \{\beta \in K \mid \mathrm{tr}_{K/\mathbb{Q}}(\beta\mathbb{Z}[\alpha]) \subset \mathbb{Z}\}$. For the ring of integers R of K, its dual is the *codifferent* ideal, $R^\vee$. An element $\alpha \in K$ is *totally positive*, and denoted by $\alpha \gg 0$, if $\sigma_i(\alpha) > 0$ for all the embedding of K in $\mathbb{R}$. For the set of all the totally positive numbers and integers, we write K_+ and R_+, respectively. We denote by $\mathrm{Disc}(f)$ the discriminant of a polynomial f, and by $\mathrm{Disc}(K)$ the discriminant of a number field K. Let $g \in \mathbb{R}[x]$, we write $\mathrm{Res}(f, g)$ for the resultant of f and g.

Definition 2.1. Let $f = \prod_{i=1}^{d}(x - \alpha_i)$, $g = \prod_{i=1}^{d-1}(x - \beta_i) \in \mathbb{Z}[x]$, where $d \geq 2$. Then g *interlaces* f, or f is *interlaced* (by g), if

$$\alpha_1 < \beta_1 < \alpha_2 < \cdots < \alpha_{d-1} < \beta_{d-1} < \alpha_d.$$

Let us denote by

$$\mathrm{Span}(\alpha) = \max_{i,j} |\alpha_i - \alpha_j|$$

the *span* of a totally real algebraic number α, where $\alpha = \alpha_1, \ldots, \alpha_d$ are all of the conjugates of α. Note that $\mathrm{Span}(m) = 0$ if and only if $m \in \mathbb{Q}$. And $\mathrm{Span}(\alpha) = \mathrm{Span}(\alpha + k)$ for all $k \in \mathbb{Z}$. We say that $f, g \in \mathbb{Z}[x]$ are $\mathbb{Z}$-*equivalent* if $f(x) = g(x + n)$ for $n \in \mathbb{Z}$.

We say that a quadratic form $Q(v_1, \ldots, v_r) = \sum_{1 \le i \le j \le r} a_{ij} v_i v_j$ is *integral* (or over R) if $a_{ij} \in R$ for all i, j. Furthermore, those integral quadratic forms that have $a_{ij} \in 2R$ whenever $i \neq j$ are called *classical*. If $Q(v) \gg 0$ for all $v \in R^r$, $v \neq 0$, then Q is said to be *totally positive definite*. An R-lattice (L, B_Q) is a pair, where L is a free R-module of finite rank, with a non-degenerate symmetric bilinear form $B_Q \colon L \times L \to R$ and the associated quadratic form $Q(v) = B_Q(v, v)$ for $v \in L$. Thus, an R-lattice naturally corresponds to a classical quadratic form over R. An R-lattice (L, B_Q) is positive definite if and only if Q is positive definite. Of special importance to us will be *ideal lattices*, i.e. those lattices that can be represented in the form $(I, \mathrm{tr}_{K/\mathbb{Q}}(\gamma x y))$, where I is a fractional ideal in K and $\gamma \in K$ (see [3,4]).

We say that a quadratic form Q over R *represents* α if there exits $v \in R^r$ such that $Q(v) = \alpha$. A totally positive definite quadratic form is *universal* over R if it represents all elements in R_+. As a convention, we always assume that the universal quadratic form is totally positive definite. We say that a lattice is universal if the corresponding quadratic form is universal. For a positive definite $\mathbb{Z}$-lattice L, we write

$$\min(L, B_Q) = \min\left\{Q(v) \mid v \in L\right\}$$

for the minimum of L, and

$$\mathcal{M}(L, B_Q) = \left\{v \in L \mid Q(v) = \min(L, B_Q)\right\}$$

for the set of the minimal vectors of L (we may write $\mathcal{M}(L)$ if the bilinear form is clear from the context). Let us write

$$\tau_d = \max_{(L, B_Q)} |\mathcal{M}(L, B_Q)|$$

for the *kissing number* for lattices in dimension d, where L ranges through all the positive definite $\mathbb{Z}$-lattices of rank d. We shall write

$$\mathcal{M}(K) = \left\{\alpha \in R_+^\vee \mid \mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \min_{\gamma \in R_+^\vee} \mathrm{tr}_{K/\mathbb{Q}}(\gamma)\right\}.$$

For lattices L_1 and L_2 we write $L = L_1 \perp L_2$, if $L = L_1 \oplus L_2$ and $B_Q(l_1, l_2) = 0$ for all $l_1 \in L_1$, $l_2 \in L_2$. For $\alpha \in K$, we define a symmetric bilinear form scaled by α

$$B_Q^\alpha(v, v) = \alpha B_Q(v, v)$$

and a quadratic form scaled by α

$$Q^{\alpha}(v) = \alpha Q(v).$$

The following identity clearly holds $B_Q^{\alpha} = B_{Q^{\alpha}}$.

Let $\mathrm{Mat}(d, K)$ denote the set of all square $d \times d$ matrices, and $\mathrm{diag}(a_1, \ldots, a_d)$ is a $d \times d$ diagonal matrix with elements a_i on the diagonal. For a matrix $A \in \mathrm{Mat}(d, K)$, A^t and $\det(A)$ denotes its transpose and determinant, respectively. For a given set S, we write $|S|$ for the cardinality of S.

Definition 2.2. Let (L, B_Q) be an $\mathbb{Z}$-lattice in $\mathbb{R}^d$, and let $C \subset \mathbb{R}^d$ be a convex set. Then the *width* of C is

$$w(C, L) = \min\Big\{ \max_{w \in C} B_Q(v, w) - \min_{w \in C} B_Q(v, w) \mid v \in L \setminus \{0\}\Big\},$$

where B_Q is defined on $L \times L$, extended to $L \times \mathbb{R}^d$.

Finally, $\mathrm{conv}\{b_1, \ldots, b_k\}$ denotes the *convex hull* of elements $b_1, \ldots, b_k \in \mathbb{R}^d$.

3. Interlacing polynomials

Our definition of interlacing (see Definition 2.1) requires that both polynomials are integer, and throughout the paper, the term interlaced will refer to integer polynomials unless stated otherwise. However, interlacing is defined analogously for real polynomials, and for interlacing with real polynomials we have:

Proposition 3.1 ([16]). *The set of all the polynomials $g \in \mathbb{R}[x]$ that interlace $f = \prod_{i=1}^{d}(x - \alpha_i)$ forms a convex set with vertices $\prod_{j \neq i}^{d}(x - \alpha_j)$ for $i = 1, \ldots, d$.*

We can associate any monic polynomial g of degree $d-1$ with a vector in $\mathbb{R}^d$ as follows:

$$\begin{aligned} \big\{g \in \mathbb{R}[x] \mid \deg(g) = d - 1\big\} &\longrightarrow \mathbb{R}^d \\ x^{d-1} + \sum_{i=1}^{d-1} a_i x^{d-1-i} &\mapsto (1, a_1, \ldots, a_{d-1})^t. \end{aligned} \tag{1}$$

Thus finding interlacing polynomials of f is equivalent to finding integer points in the convex set

$$\mathcal{K}(f) = \mathrm{conv}\big\{\big(1, b_1^{(i)}, \ldots, b_{d-1}^{(i)}\big)^t \mid i = 1, \ldots, d\big\},$$

where $\prod_{j \neq i}^{d}(x - \alpha_j) = x^{d-1} + \sum_{j=1}^{d-1} b_j^{(i)} x^{d-1-j}$.

Lemma 3.2. *Let $A = A_{\mathcal{K}(f)} \in \mathrm{Mat}(d, \mathbb{R})$, such that its columns are the vertices of $\mathcal{K}(f)$. Then*

$$A_{ij}^{-1} = \frac{\alpha_i^{n-j}}{f'(\alpha_i)}.$$

Proof. By a direct computation it follows that

$$\begin{aligned}\delta_{ij} &= \frac{1}{f'(\alpha_i)} \prod_{\substack{k=1 \\ k\neq j}}^{d} (\alpha_i - \alpha_k) \\ &= \frac{1}{f'(\alpha_i)} \sum_{k=1}^{d} \alpha_i^{d-k} \sum_{\substack{1\leq m_1<\cdots<m_{k-1}\leq d \\ m_i\neq j}} (-1)^{k-1} \alpha_{m_1} \ldots \alpha_{m_{k-1}} \\ &= \sum_{k=1}^{d} \frac{\alpha_i^{d-k}}{f'(\alpha_i)} A_{kj} \\ &= (A^{-1}A)_{ij}.\end{aligned}$$

□

For $\mathcal{K}(f) \subset \mathbb{R}^d$ we define the set

$$\Lambda_{\mathcal{K}(f)} = \left\{\lambda \in \mathbb{R}_+^d \mid A_{\mathcal{K}(f)}\lambda \in \mathbb{Z}^d,\ \sum_{i=1}^{d} \lambda_i = 1\right\}.$$

Clearly, $\mathcal{K}(f) \cap \mathbb{Z}^d \neq \emptyset$ if and only if $\Lambda_{\mathcal{K}(f)} \neq \emptyset$. And for any polynomial, $\mathcal{K}(f)$ being compact implies that $|\mathcal{K}(f) \cap \mathbb{Z}^d|$ is a finite set.

Proposition 3.3. *Let $f \in \mathbb{Z}[x]$ and $\lambda \in \Lambda_{\mathcal{K}(f)}$, and let $g \in \mathbb{Z}[x]$ be the polynomial that interlaces f corresponding to λ. Then*

$$\left|\prod_{i=1}^{d} \lambda_i\right| = \left|\frac{\mathrm{Res}(f,g)}{\mathrm{Disc}(f)}\right|.$$

Proof. Let $A = A_{\mathcal{K}(f)}$ be the matrix as defined in the lemma above, and let $\lambda \in \Lambda_{\mathcal{K}(f)}$. Now,

$$A\lambda = b = (1, b_1, \ldots, b_{d-1})^t \in \mathbb{Z}^d,$$

and

$$\begin{aligned}g &= x^{d-1} + \sum_{i=1}^{d-2} b_i x^{d-1-i} \\ &= \sum_{i=1}^{d} \lambda_i \prod_{j\neq i} (x - \alpha_j)\end{aligned}$$

interlaces f. As $\lambda = A^{-1}b$, by applying Lemma 3.2 it follows that

$$\begin{aligned}\lambda_i &= \sum_{j=1}^{d} A_{ij}^{-1} b_j \\ &= \frac{1}{f'(\alpha_i)} \sum_{j=1}^{d} \alpha_i^{d-j} b_j \\ &= \frac{g(\alpha_i)}{f'(\alpha_i)}. \end{aligned} \tag{2}$$

Therefore,

$$\prod_{i=1}^{d} \lambda_i = \prod_{i=1}^{d} \frac{g(\alpha_i)}{f'(\alpha_i)}$$

and

$$\left| \prod_{i=1}^{d} \lambda_i \right| = \left| \frac{\operatorname{Res}(g, f)}{\operatorname{Disc}(f)} \right|,$$

as was required to show. □

Definition 3.4. Let

$$\begin{aligned}\psi_d \colon \mathbb{R} &\longrightarrow \mathbb{R}^d \\ r &\mapsto (r^{d-1}, \ldots, r, 1)^t\end{aligned}$$

define a curve in dimension d. For n real numbers $r_1 > r_2 > \cdots > r_n$ we define the *cyclic polytope* $\mathcal{C}(r_1, \ldots, r_n)$ to be the convex hull of those points on the curve ψ_d corresponding to the r_i, i.e.

$$\mathcal{C}(r_1, \ldots, r_n) = \operatorname{conv}\{\psi_d(r_i) \mid i = 1, \ldots, n\}.$$

Let $f = \prod_{i=1}^{d}(x - \alpha_i)$, we write $\mathcal{C}(f) = \mathcal{C}(\alpha_1, \ldots, \alpha_d) \subset \mathbb{R}^d$ for a cyclic polytope of the roots of f in dimension d. The associated matrix is $A_{\mathcal{C}(f)}$, where $(A_{\mathcal{C}(f)})_{ij} = \alpha_j^{d-i}$. It is known that $\det(A_{\mathcal{C}(f)}) = \prod_{1 \le i < j \le d}(\alpha_i - \alpha_j)$ [25, p. 11]. Furthermore, from the proof of Proposition 3.3, we deduce that

$$A_{\mathcal{K}(f)}^{-1} = D A_{\mathcal{C}(f)}^{t}, \tag{3}$$

where $D = \operatorname{diag}(f'(\alpha_1)^{-1}, \ldots, f'(\alpha_d)^{-1})$. For an irreducible polynomial f we have

$$A_{\mathcal{C}(f)} A_{\mathcal{C}(f)}^{t} = \left(\operatorname{tr}_{K/\mathbb{Q}}\left(\alpha^{2d-i-j}\right)\right) \in \operatorname{Mat}(d, \mathbb{Z}).$$

In particular, for any $\beta \in R^{\vee}$, let $B = \operatorname{diag}(\sigma_1(\beta), \ldots, \sigma_d(\beta))$. Then

$$A_{\mathcal{C}(f)} B A_{\mathcal{C}(f)}^{t} = \left(\operatorname{tr}_{K/\mathbb{Q}}\left(\beta\alpha^{2d-i-j}\right)\right) \in \operatorname{Mat}(d, \mathbb{Z}). \tag{4}$$

Proposition 3.5. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial, and let $\alpha \in \mathbb{R}$ be a root of f. Then there exists a one-to-one correspondence between the interlacing polynomials of f and elements in $\{\gamma \in \mathbb{Z}[\alpha]^\vee \mid \gamma \gg 0,\ \mathrm{tr}_{K/\mathbb{Q}}(\gamma) = 1\}$.*

Proof. Let us consider an injective homomorphism

$$\begin{aligned} j : \mathbb{Z}[\alpha]^\vee &\longrightarrow \mathbb{R}^d \\ \gamma &\mapsto (\sigma_1(\gamma), \dots, \sigma_d(\gamma))^t. \end{aligned}$$

Given that $\mathbb{Z}[\alpha]^\vee = \frac{1}{f'(\alpha)}\mathbb{Z}[\alpha]$ [25, Prop. 2.2], we have (by Lemma 3.2) a one-to-one map defined by $A^{-1}_{\mathcal{K}(f)}$:

$$J : \mathbb{Z}^d \longrightarrow j\left(\mathbb{Z}[\alpha]^\vee\right). \tag{5}$$

By Proposition 3.1, a polynomial $g \in \mathbb{Z}[x]$ interlaces f if and only if there exists $\lambda_1, \dots, \lambda_d \in \mathbb{R}_+$ such that $\sum \lambda_i = 1$, and $g = \sum_{i=1}^d \lambda_i \prod_{j\neq i}^d (x - \alpha_j)$. The map (1) associates such a polynomial g with the vector $b \in \mathbb{Z}^d$ such that $A_{\mathcal{K}(f)}\lambda = b$. Therefore $J(b) \in j(\mathbb{Z}[\alpha]^\vee)$ corresponds to a totally positive element of trace one in $\mathbb{Z}[\alpha]^\vee$, as was required to show. □

Let us notice that if we remove the trace requirement, then we would need to allow for non-monic polynomials that interlace f. Thus counting elements of trace t is equivalent to counting integral points in $t\mathcal{K}(f)$.

Before we move in to counting the interlacing polynomials, let us list some of the properties of sets $\mathcal{C}(f)$ and $\mathcal{K}(f)$.

Corollary 3.6. *Let $f \in \mathbb{Z}[x]$ be a separable polynomial of degree d such that all its roots are real. Then $|\Lambda_{\mathcal{C}(f)}| = |\mathcal{C}(f) \cap \mathbb{Z}^d|$.*

Proof. We have $r \in \mathbb{Z}^d \cap \mathcal{C}(f)$ if and only if there exists $\lambda \in \Lambda_{\mathcal{C}(f)}$ such that $A_{\mathcal{C}(f)}\lambda = r$. Therefore it suffices to show that there cannot exist $\mu \in \Lambda_{\mathcal{C}(f)}$ such that $\mu \neq \lambda$ and $A_{\mathcal{C}(f)}\mu = r$. Given that f is a separable polynomial implies that $A_{\mathcal{C}(f)}$ is an invertible matrix, the corollary follows. □

Proposition 3.7. *For a separable $f \in \mathbb{Z}[x]$ we have $\Lambda_{\mathcal{K}(f)} = \Lambda_{\mathcal{C}(f)}$.*

Proof. Let $\lambda \in \Lambda_{\mathcal{K}(f)}$. Using identity (3) we have from $A_{\mathcal{K}(f)}\lambda = b$ that

$$\begin{aligned} \lambda &= DA^t_{\mathcal{C}(f)}b \\ A_{\mathcal{C}(f)}\lambda &= A_{\mathcal{C}(f)}DA^t_{\mathcal{C}(f)}b, \end{aligned}$$

where both b and $A_{\mathcal{C}(f)}DA^t_{\mathcal{C}(f)}$ are integral (see (4)), thus $\lambda \in \Lambda_{\mathcal{C}(f)}$. The reverse inclusion is analogous. □

Corollary 3.8. *Let $f \in \mathbb{Z}[x]$ be a separable monic polynomial such that all its roots are real. Then $|\mathcal{C}(f) \cap \mathbb{Z}^d| = |\mathcal{K}(f) \cap \mathbb{Z}^d|$.*

Example 3.9. Let $f = x^2 - D$, where $D \in \mathbb{N}$. Then

$$\begin{aligned}\mathcal{K}(f) &= \left\{(1, \lambda\sqrt{D} - (1-\lambda)\sqrt{D})^t \mid \lambda \in [0,1]\right\} \\ &= \left\{(1, (2\lambda - 1)\sqrt{D})^t \mid \lambda \in [0,1]\right\} \\ &= \left\{(1, \lambda'\sqrt{D})^t \mid \lambda' \in [-1,1]\right\}.\end{aligned}$$

Therefore all the integer points in $\mathcal{K}(f)$ correspond to integers in the interval $[-\sqrt{D}, \sqrt{D}]$, and from equation (2), the elements of $\Lambda_{\mathcal{C}(f)}$ correspond to

$$\left(\frac{-\sqrt{D} + r}{-2\sqrt{D}}, \frac{\sqrt{D} + r}{2\sqrt{D}}\right)^t$$

for $r \in [-\sqrt{D}, \sqrt{D}] \cap \mathbb{Z}$. In particular,

$$|\mathcal{K}(f) \cap \mathbb{Z}^2| = 2\lfloor\sqrt{D}\rfloor + 1 \approx \sqrt{\mathrm{Disc}(f)}. \tag{6}$$

A similar result holds for quadratic polynomials of the form $x^2 - x - D$.

Corollary 3.10. *The number of interlacing polynomials of an irreducible quadratic polynomial goes to infinity with the discriminant of the polynomial.*

We would like to replicate the above result for polynomials of higher degrees. More generally, we wish to determine the conditions under which a given polynomial is interlaced, and count the interlacing polynomials. We cannot apply Minkowski's First Theorem [25], as the associated convex set to a polynomial is not symmetric and generally, it does not contain the origin. We shall use the following variant of the Flatness Theorem:

Theorem 3.11 ([1, Remark 2.7]). *Let S be a simplex in $\mathbb{R}^d$. Then*

$$w(S, \mathbb{Z}^d) \leq cd\left(1 + \log(d) + |S \cap \mathbb{Z}^d|^{1/d}\right),$$

where c is a universal constant.

Observe that $\mathcal{C}(f)$ (and $\mathcal{K}(f)$) can be projected onto a simplex S in $\mathbb{R}^{d-1}$. In particular, if $\mathcal{C}(f) = \mathrm{conv}(b_1, \ldots, b_d)$, then $S = \mathrm{conv}(b_1', \ldots, b_d')$, where $(b_i')_j = (b_i)_j$ for $1 \leq j \leq d-1$. Therefore, without loss of generality, we can consider $\mathcal{C}(f)$ (and $\mathcal{K}(f)$) as a simplex.

Proposition 3.12. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial such that totally real algebraic integer α is a root of f. Then*

$$w(\mathcal{C}(f), \mathbb{Z}^d) = \min\left\{\mathrm{Span}(\gamma) \mid \gamma \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}\right\}.$$

Proof. Let $(\mathbb{Z}^d, \langle\,,\rangle)$ denote the integer lattice of rank d, where $\langle\,,\rangle$ is the usual inner product, i.e. $\langle v, w\rangle = \sum_{i=1}^d v_i w_i$ for $v, w \in \mathbb{R}^d$. Let A be the associated

matrix of $\mathcal{C}(f)$. Thus every element $\gamma \in \mathcal{C}(f)$ may be written as $\gamma = A\lambda$, where $\lambda \in \Lambda = \{\theta \in \mathbb{R}^d_+ \mid \sum_{i=1}^d \theta_i = 1\}$. Let $v \in \mathbb{Z}^d$, then

$$\max_{w \in \mathcal{C}(f)} \langle v, w \rangle = \max_{\lambda \in \Lambda} v^t A\lambda.$$

As $v^t A = \left(\sum_{i=1}^d v_i \alpha_1^{d-i}, \ldots, \sum_{i=1}^d v_i \alpha_d^{d-i}\right)$, it follows that

$$\max_{w \in \mathcal{C}(f)} \langle v, w \rangle = \max_j \sum_{i=1}^d v_i \alpha_j^{d-i}.$$

Similarly we have that

$$\min_{w \in \mathcal{C}(f)} \langle v, w \rangle = \min_j \sum_{i=1}^d v_i \alpha_j^{d-i}.$$

For $v \in \mathbb{Z}^d$ let $g \in \mathbb{Z}[x]$ such that $g = \sum_{i=1}^d v_i x^{d-i}$. Therefore

$$\max_{w \in \mathcal{C}(f)} \langle v, w \rangle - \min_{w \in \mathcal{C}(f)} \langle v, w \rangle = \mathrm{Span}(\gamma),$$

where $\gamma = g(\alpha) \in \mathbb{Z}[\alpha]$. By the definition of the width the proposition follows. □

For a totally real algebraic integer $\beta \in \mathbb{R}$ there can exist infinitely many (up to equivalence) totally real algebraic integers α of a bounded degree such that $\beta \in \mathbb{Z}[\alpha]$. For example, consider the family of polynomials

$$\left\{x^4 - 2ax^2 + a^2 - 2 \in \mathbb{Z}[x] \mid a \geq 2\right\}.$$

The roots of these polynomials are $\pm\sqrt{a \pm \sqrt{2}}$. Thus for each of the corresponding simplices, the width is bounded above by $2\sqrt{2}$. More generally, it suffices to consider number fields of bounded degree that contain $\mathbb{Q}[\beta]$ as a subfield.

Theorem 1.1. *Let $d, r \in \mathbb{N}$. Up to $\mathbb{Z}$-equivalence, there are only finitely many irreducible monic polynomials $f \in \mathbb{Z}[x]$ of degree d such that $\mathbb{Q}[x]/(f)$ is a primitive field and f is interlaced by at most r monic integer polynomials.*

Proof. First, we claim that, up to $\mathbb{Z}$-equivalence, there are only finitely many $g \in \mathbb{Z}[x]$ of degree d of bounded span. Without loss of generality, we assume that all roots of g are positive, and at least one of the roots is less than one. Given that $|\{\sum_{i=0}^d a_i x^i \mid |a_j| < M\}|$ is a finite set, our claim follows.

Let $f \in \mathbb{Z}[x]$ such that $K = \mathbb{Q}[x]/(f)$ is a primitive field, and $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$. If $\beta \in \{\gamma \in \mathbb{Z}[\alpha] \mid \mathrm{span}(\gamma) = \min_{\delta \in \mathbb{Z}[\alpha]} \mathrm{span}(\delta)\}$, then there are only finitely many algebraic integers $\gamma \in K$ (up to $\mathbb{Z}$-equivalence) such that $\beta \in \mathbb{Z}[\gamma]$ [11, Corollary 6.2.2]. From Proposition 3.12, it follows that up to $\mathbb{Z}$-equivalence, there are only finitely many such f with bounded width, and in the light of Theorem 3.11, follows the theorem. □

4. Non-interlacing polynomials

Here we demonstrate that there exist irreducible polynomials that are non-interlacing, but, not for degrees 2, 3, 4, 5, and 7. The following proposition was proved by Dobrowolski for minimal polynomials of integer symmetric matrices. We shall reprove it, using the results from the previous section:

Proposition 4.1 ([8, Lemma 1]). *Let $f \in \mathbb{Z}[x]$ be a monic and irreducible polynomial of degree d. If f is interlaced then $|\mathrm{Disc}(f)| \geq d^d$.*

Proof. Let $f = \prod_{i=1}^{d}(x-\alpha_i) \in \mathbb{Z}[x]$ be interlaced by g. Then there exists $\lambda \in \Lambda_{\mathcal{C}(f)}$ such that $g = \sum_{i=1}^{d} \lambda_i \prod_{j\neq i}(x-\alpha_j) \in \mathbb{Z}[x]$. By Proposition 3.3 it follows that

$$\left|\frac{\mathrm{Res}(f,g)}{\mathrm{Disc}(f)}\right| = \left|\prod_{i=1}^{d}\lambda_i\right| \leq \left|\frac{1}{d}\sum_{i=1}^{d}\lambda_i\right|^d,$$

and so

$$\left|d^d \mathrm{Res}(f,g)\right| \leq \left|\mathrm{Disc}(f)\right|.$$

As $f, g \in \mathbb{Z}[x]$ are monic polynomials, we conclude that $\mathrm{Res}(f,g) \in \mathbb{Z}\setminus\{0\}$, and the proposition follows. □

There exist polynomials that satisfy the hypothesis of the theorem above, but have the discriminant smaller than d^d [29]. The smallest such example known has degree 2880. We shall show that the smallest degree for which there exists an irreducible non-interlacing polynomial is 6. We begin by characterising an infinite family of non-interlacing polynomials. For this we need to use the following result:

Lemma 4.2. *Let $M = \mathbb{Q}[\zeta_d]$ such that d is square-free, d is not a prime number or twice a prime number, $d > 20$ and $d \neq 30$. Let S be the ring of integers in M. Let K be the maximal totally real subfield of M, i.e. $K = \mathbb{Q}[\zeta_d + \zeta_d^{-1}]$, with its ring of integers R. Then the minimum of any ideal R-lattice is at least 2.*

Proof. Let I be an ideal in R, and let $\gamma \in K$ such that $(I, \mathrm{tr}_{K/\mathbb{Q}}(\gamma xy))$ is an ideal lattice. Let $m = \min(I, \mathrm{tr}_{K/\mathbb{Q}}(\gamma xy))$ and $z \in \mathcal{M}(I, \mathrm{tr}_{K/\mathbb{Q}}(\gamma xy))$. We extend this lattice to S, let

$$I^e = \Big\{\sum a_i b_i \mid a_i \in I,\ b_i \in S\Big\},$$

and $\mathrm{tr}_{M/K}(\mathrm{tr}_{K/\mathbb{Q}}(\gamma xy)) = \mathrm{tr}_{M/\mathbb{Q}}(\gamma x\overline{y})$. Clearly $(I^e, \mathrm{tr}_{M/\mathbb{Q}}(\gamma x\overline{y}))$ is an ideal S-lattice. Given that $z \in I^e$, we have that the minimum of $\mathrm{tr}_{M/\mathbb{Q}}(\gamma x\overline{y})$ is smaller

than $\mathrm{tr}_{M/\mathbb{Q}}(\gamma z^2)$. Thus

$$\begin{aligned}\mathrm{tr}_{M/\mathbb{Q}}(\gamma z^2) &= \mathrm{tr}_{M/K}(m)\\ &= 2m\\ &\geq 4,\end{aligned}$$

the last inequality follows from [2, Lemma 1.4 and Corollary 2.2], thus $m \geq 2$. □

From the lemma above and Proposition 3.5 follows:

Theorem 1.2. *Let $d \in \mathbb{N}$ such that d is square-free, d is not a prime number or twice a prime number, $d > 20$ and $d \neq 30$. Then the minimal polynomial of $\zeta_d + \zeta_d^{-1}$ is non-interlacing.*

An example of such polynomial of smallest degree is the minimal polynomial of $\zeta_{21} + \zeta_{21}^{-1}$,

$$x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1. \tag{7}$$

It is known that for primes p larger than 5, the minimal polynomial of $\zeta_p + \zeta_p^{-1}$ is always interlaced ([13]). A classification of interlacing minimal polynomials of $\zeta_d + \zeta_d^{-1}$ in relation to integer symmetric matrices can be found in [24].

Let us define $\sigma_r(I) = \sum_{J|I} \mathrm{N}(J)^r$, where I is an ideal of R. Furthermore, let

$$s_l^K(m) = \sum_{\substack{\gamma \in R_+^\vee \\ \mathrm{tr}_{K/\mathbb{Q}}(\gamma)=l}} \sigma_{m-1}\big((\gamma)(R^\vee)^{-1}\big),$$

where $(R^\vee)^{-1}$ is the *different* ideal.

Theorem 4.3 ([28, 31]). *Let K be a totally real algebraic number field of degree $d > 1$ and let ζ_K be its Dedekind zeta function. Let $h = 2dm$, where $m \in \mathbb{N}$. Then*

$$\zeta_K(1-2m) = 2^d \sum_{l=1}^{r} b_l(h) s_l^K(2m) \in \mathbb{Q} \setminus \{0\}.$$

The numbers $r \geq 1, b_1(h), \ldots, b_r(h)$ are rational and they only depend on h, where

$$r = \begin{cases} \left\lfloor \dfrac{h}{12} \right\rfloor, & \text{if } h \equiv 2 \pmod{12},\\ \left\lfloor \dfrac{h}{12} \right\rfloor + 1, & \text{if } h \not\equiv 2 \pmod{12}. \end{cases}$$

Theorem 1.3. *There does not exist a non-interlacing irreducible integer polynomial of degree 2, 3, 4, 5, or 7.*

Proof. Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 2, 3, 4, 5, or 7, such that $K \cong \mathbb{Q}[x]/(f)$ with the ring of integers R, and $\alpha \in \mathbb{R}$ be a root of f. Given that $\mathbb{Z}[\alpha] \subseteq R$ implies that $R^\vee \subseteq \mathbb{Z}[\alpha]^\vee$. From the theorem above it follows that for $d = 2, 3, 4, 5$, or 7, we have

$$\zeta_K(-1) = 2^d b_1(h) \sum_{\substack{\gamma \in R_+^\vee \\ \mathrm{tr}_{K/\mathbb{Q}}(\gamma)=1}} \sigma_1\big((\gamma)(R^\vee)^{-1}\big).$$

As $\zeta_K(-1) \neq 0$, therefore there exists at least one $\gamma \in R_+^\vee \subseteq \mathbb{Z}[x]^\vee$ such that $\mathrm{tr}_{K/\mathbb{Q}}(\gamma) = 1$. By Proposition 3.5 follows the proof. □

The requirement for irreducibility is necessary. For example, $(x-1)(x-2)$ is non-interlacing.

Theorem 4.4 ([12]). *Let K be a totally real algebraic number field of degree d and let R be its ring of integers. For $1 \leq d \leq 7$, if K satisfies Condition (A), then there always exists an element $\alpha \in R_+^\vee$ such that $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = 1$.*

Proof. Let f be the minimal polynomial of α such that $R = \mathbb{Z}[\alpha]$. From Theorem 1.3 it follows that for $d = 2, 3, 4, 5$, and 7, polynomial f is interlacing. This leaves us to prove the theorem for sextic number fields. Given that there exist units of every signature in K, implies that the codifferent is narrowly equivalent to a square of an ideal in K [15, Theorem 176], i.e. there exists a fractional ideal I in K, such that $\gamma I^2 = R^\vee$, where $\gamma \in K$ and $\gamma \gg 0$. Therefore, $(I, \mathrm{tr}_{K/\mathbb{Q}}(\gamma xy))$ is a positive definite unimodular $\mathbb{Z}$-lattice. From the classification of unimodular quadratic forms [26, 106:13] it follows that there exists an element of trace one in $R_+^\vee$. □

The number field $\mathbb{Q}(\zeta_{21} + \zeta_{21}^{-1})$ is monogenic (see [30, Prop. 2.16]), and given that the polynomial (7) is non-interlacing, this implies that there cannot exist units of every signature in $\mathbb{Z}[\zeta_{21} + \zeta_{21}^{-1}]$.

5. Universal quadratic forms

For a quadratic form Q of rank r over R, in what follows, we shall write L for R^r. We begin by proving the following useful proposition:

Proposition 5.1. *Let K be a totally real algebraic number field satisfying Condition (A), and let R be its ring of integers. Let Q be a universal quadratic form over R. Then there exists $\delta \in K_+$ and a positive definite $\mathbb{Z}$-lattice $(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta))$ such that*

$$\big|\mathcal{M}\big(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta)\big)\big| \geq 2\big|\mathcal{M}(K)\big|. \tag{8}$$

Proof. Given that K satisfies Condition (A), implies that there exists $\delta \in K_+$ such that $R^\vee = \delta R$. Therefore, Q^δ represents all the elements in $R_+^\vee$. Let us consider a $\mathbb{Z}$-lattice $(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta))$ (replacing δ by 2δ if necessary). We note that $\min(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta))$ is equal to $\min_{\gamma \in R_+^\vee} \mathrm{tr}_{K/\mathbb{Q}}(\gamma)$ (or twice as much). Thus

$$\left|\mathcal{M}\left(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta)\right)\right| \geq 2\left|\mathcal{M}(K)\right|,$$

where a factor of two on the right follows from the fact that $Q(\pm v) = \alpha$ for all $\alpha \in R_+$. □

Example 5.2. Let Q be a quadratic form

$$x^2 + 2y^2 + 2yz + (2+\epsilon)z^2$$

over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, where $\epsilon = \frac{1+\sqrt{5}}{2}$. From Theorem 1.1 in [7] we know that Q is a universal quadratic form. Given that ϵ is a unit of negative norm implies that $\mathbb{Q}(\sqrt{5})$ satisfies Condition (A), and thus fulfils the hypothesis of the above proposition. The minimal polynomial of $\frac{1+\sqrt{5}}{2}$ is $f = x^2 - x - 1$. It is interlaced only by two polynomials, x and $x - 1$. By Proposition 3.5, it follows that $|\mathcal{M}(L, \mathrm{tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(B_Q^\delta))| \geq 4$ (note that this bound will hold for all the lattices over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, invariant of Q). On the other hand, let

$$\delta = \frac{\epsilon}{f'(\epsilon)} = \frac{\epsilon + 2}{5},$$

and by computing the minimal vectors of the $\mathbb{Z}$-lattice we conclude that (8) is an equality in this case. However, we can have a strict inequality also. Let us consider an another universal quadratic form Q' over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$:

$$x^2 + y^2 + z^2.$$

In this case $|\mathcal{M}(L, \mathrm{tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}(B_{Q'}^\delta))| = 12$.

Corollary 5.3. *Let K be a totally real algebraic number field of degree d satisfying Condition (A), and let R be its ring of integers. Let r be the rank of a universal quadratic form over R. Then*

$$r \geq \frac{\log\left(2|\mathcal{M}(K)|\right)}{0.401d\left(1 + o(1)\right)\log(2)}.$$

Proof. As in Proposition 5.1, a given quadratic form of rank r over the ring of integers of K can be lifted to a rational integer lattice of rank dr. From the bound on the kissing number $\tau_{dr} \leq 2^{0.401dr(1+o(1))}$ [17] and inequality (8) follows the corollary. □

This bound can be improved to

$$r \geq \frac{2|\mathcal{M}(K)|}{\tau_d}$$

for universal diagonal forms. As a special case, we have the following theorem:

Theorem 5.4. *Let K be a totally real algebraic number field of degree d satisfying Condition (A), and let R be its ring of integers. If there exists an element $\alpha \in R_+^\vee$ such that $\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = 1$, then the rank of a universal quadratic form Q over R is larger than*

$$\begin{cases} \dfrac{|\mathcal{M}(K)|}{d} & \text{if } Q \text{ is a classical quadratic form,} \\ \dfrac{1+\sqrt{1+4|\mathcal{M}(K)|}}{2d} & \text{if } d > 5, \\ \dfrac{|\mathcal{M}(K)|}{15d} & \text{otherwise.} \end{cases}$$

Proof. Observe that for a classical quadratic form if $\min_{v\in L}(L, B_Q) = 1$, then $L \cong < 1 > \perp L'$. Therefore, if L is a $\mathbb{Z}$-lattice, then the rank of L is larger or equal to $|\mathcal{M}(L)|/2$. Consider a $\mathbb{Z}$-lattice $(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^\delta))$ as in Proposition 5.1, where Q is a classical quadratic form of rank r, and thus the rank of L over $\mathbb{Z}$ is dr. By Proposition 5.1 we have

$$\begin{aligned} \frac{|\mathcal{M}(L)|}{2} &\geq |\mathcal{M}(K)| \\ dr &\geq |\mathcal{M}(K)| \\ r &\geq \frac{1}{d}|\mathcal{M}(K)|. \end{aligned}$$

On the other hand, if Q is an integral quadratic form, then $2Q$ is a classical quadratic form. The minimum of $\mathbb{Z}$-lattice $(L, \mathrm{tr}_{K/\mathbb{Q}}(B_Q^{2\delta}))$ is 2. Let M be a lattice generated by the minimum vectors of L. It follows that M is a direct sum of root lattices (see Theorem 4.10.6 in [23]) and $|\mathcal{M}(M)| = |\mathcal{M}(L)|$. Considering root lattices A_n, D_n and E_8, we observe that $|\mathcal{M}(A_n)| \leq |\mathcal{M}(D_n)|$ for $n \geq 5$ (see Table 4.10.13 in [23]). Given that $|\mathcal{M}(D_n)| = 2n(n-1)$ and $|\mathcal{M}(E_8)| = 240$, if $dr > 16$, we can bound the number of minimal vectors in L by $2dr(dr-1)$. For the case when $dr \leq 16$, we can bound the number of minimal vectors by $30dr$. Given that there cannot exist a positive definite binary universal quadratic form, we assume that $r \geq 3$. The rest of the proof follows as for the classical quadratic form. □

Corollary 5.5. *The minimal rank of a universal quadratic form over quadratic fields that contains a unit of negative norm grows at the order of the fourth root of the discriminant.*

Proof. This follows from the theorem above and equation (6). □

The above result appeared previously as Proposition 5 in [6], however, here it is independent of the Riemann hypothesis. In the light of Theorem 1.1 we have:

Theorem 1.4. *Let $d, r \in \mathbb{N}$. There are only finitely many totally real primitive number fields of degree d that satisfy Condition (A) and have an integer universal quadratic form of rank r defined over them.*

Proof. Let f be the minimal polynomial of α such that $R = \mathbb{Z}[\alpha]$. From the proof of Theorem 1.1, we know that there are only finitely many fields for which there are at most r interlacing polynomials. Therefore, the number of interlacing polynomials grows, and from Proposition 3.5, we deduce that the right side of inequality (8) grows also. Given that the maximal number of the minimal vectors is bounded by the kissing number, follows that the rank of a universal quadratic form over such number fields should grow also, as was required to show. □

Quadratic number fields are always monogenic, thus the main difficulty in satisfying Condition (A) is to show that there exists a unit of negative norm. For number fields of higher degrees, along with proving that the field has units of every signature, we will have to prove that the field is monogenic. In general, it is unclear how to meet those two conditions. But, for a given field of low degree, it can be readily checked. Let us consider an example:

Example 5.6. Let $f = x^5-2x^4-9x^3+4x^2+15x+3$. It is an irreducible polynomial with only real roots. Let K be the number field generated by the root of f, let R be its ring of integers. We note that $\mathrm{Disc}(f) = 3 \times 61 \times 241 \times 547$, therefore K is monogenic, in particular, $R = \mathbb{Z}[\alpha]$, where α is a root of f. Furthermore, the narrow class number of R is 1, thus we have units of every signature, and therefore, K satisfies Condition (A). We computed that f has 218 interlacing polynomials, thus if there exists a classical universal quadratic form over K, then it has to be at least of rank 44.

Dummit and Kisilevsky, in [9], studied a parametric family of cubic polynomials

$$f_k = x^3 + x^2 - (3k^2 + k + 2)x - (2k^3 + 2k^2 + 2k + 1),$$

related to the cubic subfield of $\mathbb{Q}(\zeta_d)$. They proved that for infinitely many k, a root of f_k forms a power integer basis of the ring of integers.

Theorem 1.5. *For any given $r \in \mathbb{Z}$, there exist infinitely many totally real quadratic and cubic number fields that do not have a universal quadratic form of rank r defined over them.*

Proof. This clearly holds for real quadratic number fields, as it a classical result about Pell equations that there are infinitely many real quadratic number fields that have a unit of negative norm.

For cubic number fields, let $\alpha \in \mathbb{R}$ be a root of f_k, let $K \cong \mathbb{Q}[x]/(f_k)$ be a number field with the roots of integers R. As for infinitely many k, the ring K is monogenic [9, Theorem 3], it suffices to show that a proportion of them has units of every signature. This will give us Condition (A), and the proof of this theorem will follow from Theorem 1.4.

Both $\alpha + k$ and $\alpha + k + 1$ are units in R, as $f_k(-k) = -1$ and $f_k(-k-1) = 1$. We claim that $\alpha + k, \alpha + k + 1$ and -1 generate units of every signature. This follows from the fact that the $\mathrm{N}_{K/\mathbb{Q}}(\alpha + k) = 1$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha + k + 1) = -1$, thus $\alpha + k$ is not totally positive. Letting $\epsilon_1 = \alpha + k$ and $\epsilon_2 = \alpha + k + 1$, then $\{\pm 1, \pm\epsilon_1, \pm\epsilon_2, \pm\epsilon_1\epsilon_2\}$ contains a unit of every possible signature, as was claimed. □

References

[1] W. Banaszczyk, A. E. Litvak, A. Pajor, and S. J. Szarek, The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces, *Math. Oper. Res.*, **24** (1999), no. 3, 728–750. Zbl 0965.52009 MR 1854250

[2] E. Bayer-Fluckiger, Definite unimodular lattices having an automorphism of given characteristic polynomial, *Comment. Math. Helv.*, **59** (1984), no. 4, 509–538. Zbl 0558.10029 MR 780074

[3] E. Bayer-Fluckiger, Lattices and number fields, in *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, 69–84, Contemp. Math., 241, Amer. Math. Soc., Providence, RI, 1999. Zbl 0951.11016 MR 1718137

[4] E. Bayer-Fluckiger, Ideal lattices, in *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, 168–184, Cambridge Univ. Press, Cambridge, 2002. Zbl 1043.11057 MR 1975451

[5] M. Bhargava and J. Hanke, Universal quadratic forms and the 290-theorem, to appear in *Invent. Math.*

[6] V. Blomer and V. Kala, Number fields without n-ary universal quadratic forms, *Math. Proc. Cambridge Philos. Soc.*, **159** (2015), no. 2, 239–252. Zbl 1371.11084 MR 3395370

[7] W. Chan, M. H. Kim, and S. Raghavan, Ternary universal integral quadratic forms over real quadratic fields, *Japan. J. Math. (N.S.)*, **22** (1996), no. 2, 263–273. Zbl 0868.11020 MR 1432376

[8] E. Dobrowolski, A note on integer symmetric matrices and Mahler's measure, *Canad. Math. Bull.*, **51** (2008), no. 1, 57–59. Zbl 1132.11312 MR 2384738

[9] D. S. Dummit and H. Kisilevsky, Indices in cyclic cubic fields, in *Number theory and algebra*, 29–42, Academic Press, New York, 1977. Zbl 0377.12003 MR 460272

[10] A. G. Earnest and A. Khosravani, Universal positive quaternary quadratic lattices over totally real number fields, *Mathematika*, **44** (1997), no. 2, 342–347. Zbl 0895.11017 MR 1600557

[11] J.-H. Evertse and K. Győry, *Discriminant equations in Diophantine number theory*, New Mathematical Monographs, 32, Cambridge University Press, Cambridge, 2017. Zbl 1361.11002 MR 3586280

[12] D. K. Faddeev, On the characteristic equations of rational symmetric matrices, *Doklady Akad. Nauk SSSR (N. S.)*, **58** (1947), 753–754. Zbl 0029.20104 MR 22860

[13] D. K. Faddeev, Representations of algebraic numbers by matrices. Modules and representations, *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, **46** (1974), 89–91, 141. Zbl 0405.12012 MR 366865

[14] F. Götzky, Über eine zahlentheoretische Anwendung von Modulfunktionen zweier Veränderlicher, *Math. Ann.*, **100** (1928), no. 1, 411–437. Zbl 54.0407.01 MR 1512493

[15] E. Hecke, *Lectures on the theory of algebraic numbers*. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen, Graduate Texts in Mathematics, 77, Springer-Verlag, New York-Berlin, 1981. Springer-Verlag, New York, 1981. Zbl 0504.12001 MR 638719

[16] C. R. Johnson, Interlacing polynomials, *Proc. Amer. Math. Soc.*, **100** (1987), no. 3, 401–404. Zbl 0622.15018 MR 891133

[17] G. A. Kabatjanskiĭand V. I. Levenšteĭn, Bounds for packings on the sphere and in space, *Problemy Peredači Informacii*, **14** (1978), no. 1, 3–25. MR 514023

[18] V. Kala, Universal quadratic forms and elements of small norm in real quadratic fields, *Bull. Aust. Math. Soc.*, **94** (2016), no. 1, 7–14. Zbl 1345.11025 MR 3539315

[19] V. Kala and J. Svoboda, Universal quadratic forms over multiquadratic fields, *Ramanujan J.*, **48** (2019), no. 1, 151–157. MR 3902500

[20] B. M. Kim, Universal octonary diagonal forms over some real quadratic fields, *Comment. Math. Helv.*, **75** (2000), no. 3, 410–414. Zbl 1120.11301 MR 1793795

[21] M. H. Kim, Recent developments on universal forms, in *Algebraic and arithmetic theory of quadratic forms*, 215–228, Contemp. Math., 344, Amer. Math. Soc., Providence, RI, 2004. Zbl 1143.11309 MR 2058677

[22] 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), no. 1, 185–191. Zbl 0025.01602 MR 5505

[23] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 327, Springer-Verlag, Berlin, 2003. Zbl 1017.11031 MR 1957723

[24] J. McKee, Small-span characteristic polynomials of integer symmetric matrices, in *Algorithmic number theory*, 270–284, Lecture Notes in Comput. Sci., 6197, Springer, Berlin, 2010. Zbl 1260.11017 MR 2721426

[25] J. Neukirch, *Algebraic number theory*. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322, Springer-Verlag, Berlin, 1999. Zbl 0956.11021 MR 1697859

[26] O. T. O'Meara, *Introduction to quadratic forms*. Second corrected printing, Die Grundlehren der mathematischen Wissenschaften, Band 117, Springer-Verlag, New York-Heidelberg, 1971. Zbl 0207.05304 MR 347768

[27] C. L. Siegel, Sums of mth powers of algebraic integers, *Ann. of Math. (2)*, **46** (1945), 313–339. Zbl 0063.07010 MR 12630

[28] C. L. Siegel, Berechnung von Zetafunktionen an ganzzahligen Stellen, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, (1969), 87–102. Zbl 0186.08804 MR 252349

[29] D. Simon, Construction de polynômes de petits discriminants, *C. R. Acad. Sci. Paris Sér. I Math.*, **329** (1999), no. 6, 465–468. Zbl 0970.11007 MR 1715142

[30] L. C. Washington, *Introduction to cyclotomic fields*. Second edition, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997. Zbl 0966.11047 MR 1421575

[31] D. Zagier, On the values at negative integers of the zeta-function of a real quadratic field, *Enseignement Math. (2)*, **22** (1976), no. 1-2, 55–95. Zbl 0334.12021 MR 406957

Received March 20, 2017

P. Yatsyna, Department of Mathematics, Royal Holloway,
Egham, Surrey TW20 0EX, UK

E-mail: pavlo.yatsyna.2012@live.rhul.ac.uk