hexagon:2611.00953v1

KIM'S UNIVERSAL OCTONARY FORM OVER REAL QUADRATIC ORDERS

MIRA DOT

Communicated by Scott Duke Kominers

ABSTRACT. Let R be a real quadratic order with fundamental totally positive unit ε. Kim's octonary form is universal over R if and only if $R = \mathbb{Z}[\varepsilon]$, or equivalently if the discriminant of R is $T^2 - 4$ for an integer $T \geq 3$. Building on recent work of Kala, Man, Visser, and Yatsyna, we determine the minimal universality criterion sets for classical and integer-valued lattices over these orders when T is sufficiently large.

1. INTRODUCTION

Let R be an order in a real quadratic field K, and let $\varepsilon > 1$ generate its group of totally positive units. A positive definite quadratic form over R is *universal* if it represents every totally positive element of R. We ask when the form

$$x_1^2 + \cdots + x_4^2 + \varepsilon(x_5^2 + \cdots + x_8^2) \tag{1}$$

is universal. Kim [6] proved universality over the full ring of integers of $\mathbb{Q}(\sqrt{D})$ when $D = n^2 - 1$ is squarefree. The maximal-order classification of Kominers [8] adds precisely the fields with squarefree $D = n^2 - 4$ for odd $n \geq 3$. Here we allow arbitrary orders, as proposed in [8, §10].

Theorem 1. *The form* (1) *is universal over R if and only if $R = \mathbb{Z}[\varepsilon]$. Equivalently, the discriminant of R is $T^2 - 4$ for some integer $T \geq 3$.*

For example, $\varepsilon = 3 + 2\sqrt{2}$ is the fundamental totally positive unit of both $\mathbb{Z}[\sqrt{2}]$ and its order $\mathbb{Z}[2\sqrt{2}]$ of conductor 2. Since $\mathbb{Z}[\varepsilon] = \mathbb{Z}[2\sqrt{2}]$, the same form is universal over the smaller order but not over the maximal order.

The theorem gives infinitely many orders in each fixed real quadratic field. The proof uses the indecomposable square-class obstruction from [8], but does not use the continued-fraction description of indecomposables in real quadratic orders due to Dress and Scharlau [3]. A nonunit indecomposable of least norm forces a square root of mixed signs. Completing that root to a basis produces a line of indecomposable elements, on which the norm takes positive values too closely spaced to be squares.

2020 *Mathematics Subject Classification.* Primary 11E12; Secondary 11R11.

Key words and phrases. Universal quadratic forms, real quadratic orders, indecomposable integers.

The same family of orders also admits explicit universality criteria. For large trace, the rational criterion set and its ε-multiple together give the minimal criterion set. Section 2 proves the classification, and Section 3 extends the criterion sets of Kala, Man, Visser, and Yatsyna [5].

2. Which orders admit Kim's form?

Write z' for conjugation in K, set $\mathrm{N}(z) = zz'$, and put $\delta = \sqrt{\Delta}$, where Δ is the discriminant of R. We use the embedding in which $\sqrt{\Delta} > 0$. An element of R is *indecomposable* if it is totally positive and is not the sum of two totally positive elements of R.

Proof of Theorem 1. Suppose first that $R = \mathbb{Z}[\varepsilon]$. Each pair $(\varepsilon^j, \varepsilon^{j+1})$, $j \in \mathbb{Z}$, is an integral basis of R. Under the two real embeddings, their successive rays subdivide the positive quadrant into cones. Thus every totally positive element has the form $\varepsilon^j(a + b\varepsilon)$ with $a, b \in \mathbb{Z}_{\geq 0}$. Lagrange's four-square theorem gives a representation by (1) for $j = 0$. The map that sends the two blocks of variables (x, y) to $(\varepsilon y, x)$ multiplies the value of the form by ε and is invertible over R. Thus the form represents every $\varepsilon^j(a + b\varepsilon)$.

For the converse assume $R \neq \mathbb{Z}[\varepsilon]$ and suppose (1) is universal. Let m be the least integer greater than δ with $m \equiv \Delta \pmod 2$, and set $\alpha = (m+\delta)/2$. Then $1, \alpha$ is an integral basis and $0 < \alpha' < 1$. If z is a totally positive summand of α, its coefficient of α is $(z - z')/\delta > -1$, hence is a nonnegative integer. It cannot be zero, since then z would be a positive rational integer with $z' \leq \alpha' < 1$. In a decomposition into two totally positive summands the two coefficients of α would therefore both be positive integers, but they add to 1. Thus α is indecomposable. It cannot have norm 1: otherwise α is a power of ε, and since it generates R this would give $R = \mathbb{Z}[\varepsilon]$. Also

$$\mathrm{N}(\alpha) = \frac{m^2 - \Delta}{4} < m - 1, \qquad \text{so} \qquad \mathrm{N}(\alpha) \leq m - 2 < \delta.$$

A representation of any indecomposable by (1) has just one nonzero term, so every indecomposable is a square or ε times a square. In particular $\mathrm{N}(\alpha) = h^2$, where h is the absolute norm of an element of R, so h is an integer and $h \geq 2$. Choose an indecomposable of least norm greater than 1. The involution $z \mapsto \varepsilon z'$ preserves both the norm and indecomposability and sends ε times squares to squares. After applying it if needed, write the chosen element as u^2 with $u > 0$, and put $k = |\mathrm{N}(u)|$. Then $2 \leq k \leq h$. If $u' > 0$, the element u is itself indecomposable, since a decomposition $u = v + w$ with v, w totally positive would decompose u^2 as $v^2 + (2vw + w^2)$. But the norm of u would be k, strictly between 1 and $\mathrm{N}(u^2)$, contrary to the choice of u^2. Thus $u' < 0$.

The element u is primitive in the underlying $\mathbb{Z}$-module of R, since an integer factor greater than 1 in u would decompose u^2. Complete u to an integral basis (v, u) of R. The linear functional

$$F(z) = z|u'| + z'u$$

is positive on totally positive elements, and $F(u) = 0$. The basis discriminant gives $F(v)^2 = (vu' - v'u)^2 = \Delta$, so after replacing v by $-v$ if necessary we have $F(v) = \delta$ and $F(R) = \delta\mathbb{Z}$. If $v + ru$ has positive norm, its embeddings have the same sign; since $F(v + ru) = \delta > 0$, both are positive. A decomposition into two totally positive elements would contribute at least δ from each summand, which is impossible. Thus every positive value of $\mathrm{N}(v + ru)$ comes from an indecomposable.

The norm of $v + ru$ is an integer quadratic polynomial

$$P(r) = -kr^2 + \beta r + C, \qquad \beta^2 + 4kC = \Delta,$$

where the discriminant identity follows from the basis determinant $(vu' - v'u)^2 = \Delta$. Translate r and reverse its sign if necessary so that $0 \le \beta \le k$. Since $m \ge h^2 + 2$, we have

$$\Delta = m^2 - 4h^2 \ge (h^2 + 2)^2 - 4h^2 = h^4 + 4 \ge k^4 + 4.$$

In particular $\Delta > k(k + 1)^2$: for $k = 2$ use $\Delta \ge 20 > 18$, and for $k \ge 3$ use $k^3 > (k + 1)^2$. We show that P has a positive nonsquare value.

If $\beta < k$, then $P(0)$ and $P(1)$ differ by $k - \beta$, and

$$P(1) = \frac{\Delta - (2k - \beta)^2}{4k} \ge \frac{\Delta}{4k} - k > \frac{(k - 1)^2}{4}.$$

Two distinct squares with the smaller above $(k - 1)^2/4$ differ by more than k. Thus the two values cannot both be squares.

If $\beta = k$, the values at 0 and -1 are C and $C - 2k$, where $C > (k^3 - k)/4$. If C is not a square, it suffices. Assume then that C is a square. For $k \ge 5$, we have $C > k^2$, so $C - 2k$ lies strictly between C and the preceding square. For $k = 4$, we have $C \ge 16$; subtracting 8 gives 8 when $C = 16$, and is less than one square gap when $C \ge 25$. For $k = 3$, we have $C \ge 9$, and $6 \equiv 2 \pmod 4$ is not a difference of two squares. For $k = 2$, the possibility $C = 4$ would give $\Delta = 36$, which is excluded because Δ is nonsquare. At $C \ge 9$ the preceding square is more than 4 away. Thus for some $r \in \mathbb{Z}$, the element $v + ru$ is indecomposable and has positive nonsquare norm. This contradicts the fact that every indecomposable represented by (1) has square norm.

Finally, if $R = \mathbb{Z}[\varepsilon]$, its discriminant is $(\varepsilon - \varepsilon')^2 = (\mathrm{Tr}(\varepsilon))^2 - 4$. Conversely, if $\Delta = T^2 - 4$ with $T \ge 3$, the element $(T + \sqrt{\Delta})/2$ generates R and is a totally positive unit. Any smaller totally positive unit greater than 1 would have conjugate difference strictly between 0 and $\sqrt{\Delta}$, which is impossible: the conjugate difference of $(T + \sqrt{\Delta})/2$ is $\sqrt{\Delta}$, and every difference $z - z'$ with $z \in R$ is an integer multiple of it. □

Corollary 2. *Let D_K be the fundamental discriminant of a real quadratic field K, and let $\eta > 1$ be its fundamental totally positive unit. The orders in K on which Kim's form is universal are precisely $\mathbb{Z}[\eta^j]$, $j \ge 1$. Their conductors are*

$$f_j = \frac{\eta^j - \eta^{-j}}{\sqrt{D_K}}.$$

In particular the number of these orders with conductor at most F, for $F \geq 1$, is

$$\left\lfloor \frac{\operatorname{arsinh}(F\sqrt{D_K}/2)}{\log \eta} \right\rfloor.$$

Proof. The fundamental totally positive unit of each order is a positive power of η. Conversely, fix $j \geq 1$. For $z = a + b\eta^j$ in $\mathbb{Z}[\eta^j]$, we have $z - z' = b(\eta^j - \eta^{-j})$. Thus every nonzero conjugate difference has absolute value at least $\eta^j - \eta^{-j}$. For a totally positive unit w, this difference is $w - w^{-1}$, which is strictly increasing for $w > 1$. Thus no totally positive unit of $\mathbb{Z}[\eta^j]$ lies strictly between 1 and η^j. Theorem 1 now applies.

The discriminant of this basis is $(\eta^j - \eta^{-j})^2 = f_j^2 D_K$. Hence $f_j = 2\sinh(j \log \eta)/\sqrt{D_K}$. These conductors increase strictly with j, and $f_j \leq F$ is equivalent to $j \leq \operatorname{arsinh}(F\sqrt{D_K}/2)/\log \eta$. Counting positive integers j proves the formula. □

Allowing the field to vary, the number of orders of discriminant at most X on which Kim's form is universal is $\lfloor \sqrt{X+4} \rfloor - 2$ for $X \geq 0$. Indeed, for each integer $T \geq 3$ a root of $t^2 - Tt + 1$ generates such an order, and the discriminants $T^2 - 4$ are distinct and determine the orders up to isomorphism.

3. Universality criteria

A quadratic lattice over R is a finitely generated R-submodule of its quadratic space that spans the space over K; we do not assume that the module is free. We require the form to be positive definite at both embeddings. A lattice is *integer-valued* if its quadratic form takes values in R, and *classical* if the associated bilinear form

$$B(x, y) = \frac{Q(x + y) - Q(x) - Q(y)}{2}$$

takes values in R. A *universality criterion set* is a finite set of totally positive elements whose representation implies universality in the specified class of lattices. Multiplying a representing vector by a unit shows that a test element can be replaced by any element in its class modulo squares of units.

For the maximal orders of the fields $\mathbb{Q}(\sqrt{n^2 - 1})$ with $n^2 - 1$ squarefree, Kala, Man, Visser, and Yatsyna [5, Theorem 1.4] give the criterion sets below with the same thresholds, since $T = 2n$. We follow their method [5, §11] to establish sufficiency for all orders $\mathbb{Z}[\varepsilon]$, including orders of odd trace and nonmaximal orders of either trace parity. We adapt their witnesses for minimality and prove directly over R that every criterion set must meet each of the indicated classes, following the critical-element argument of Kala, Krásenský, and Romeo [4].

Theorem 3. *Let $R = \mathbb{Z}[\varepsilon]$ and $T = \mathrm{Tr}(\varepsilon)$. In the classical case let $\mathcal{C}$ be the rational* 15*-theorem criterion set* [1] *and $b = 1$; in the integer-valued case let $\mathcal{C}$ be the rational* 290*-theorem criterion set* [2] *and $b = 2$. Write $A = \max \mathcal{C}$. If $T > b^2A^2 + 2$, the unique minimal universality criterion set, up to replacement by unit-square multiples, is*

$$\mathcal{C} \cup \varepsilon\mathcal{C}.$$

Its elements belong to 18 *distinct classes modulo squares of units in the classical case and* 58 *in the integer-valued case.*

The largest rational test integers are 15 and 290. Thus the inequalities on T are $T > 15^2 + 2 = 227$ and $T > 4 \cdot 290^2 + 2 = 336\,402$, respectively. Since T is integral, the respective thresholds are 228 and 336 403.

Proof. Suppose the lattice represents $\mathcal{C} \cup \varepsilon\mathcal{C}$. Choose vectors x_a, y_a with Q-values $a, \varepsilon a$ for each $a \in \mathcal{C}$. By Cauchy–Schwarz at each embedding, the absolute values of $bB(x_a, x_d)$ and $b\varepsilon^{-1}B(y_a, y_d)$ are at most bA. These pairings are rational integers: if $z \in R$ is nonrational, then $|z - z'| \geq \sqrt{T^2 - 4} > 2bA$. For the scaled mixed pairings $bB(x_a, y_d) \in R$, the sum of the absolute values at the two embeddings is at most $bA(\sqrt{\varepsilon} + \sqrt{\varepsilon^{-1}}) = bA\sqrt{T + 2} < \sqrt{T^2 - 4}$. So these too are rational integers. Their absolute value at the embedding at which ε has value ε' is at most $bA/\sqrt{\varepsilon} < 1$, so they vanish.

The $\mathbb{Z}$-spans of the two sets of vectors, with the second quadratic form divided by ε, are thus rational integral lattices in the specified convention. They are universal over $\mathbb{Z}$ by the corresponding rational criterion. Their orthogonality gives representations of $k + \ell\varepsilon$ for all $k, \ell \geq 0$. Multiplying the second set of vectors by the unit ε^{-1} also gives $k + \ell\varepsilon^{-1}$. The subdivision into cones used above, followed by removal of an even unit power, now gives every totally positive element of R.

For minimality, fix $a \in \mathcal{C}$ and take a rational lattice L_a in the corresponding convention whose least unrepresented positive integer is a, as furnished by the sharpness statements of the rational theorems [1, 2]. Extend scalars to R and add an orthogonal line with coefficient $i\varepsilon$ for each integer $1 \leq i < a$. The resulting lattice represents every totally positive element of field norm less than a^2. Up to multiplication by a unit square, such an element has the form $k + \ell\varepsilon^{\pm 1}$ with $k, \ell \in \mathbb{Z}_{\geq 0}$. Its norm is $k^2 + Tk\ell + \ell^2$, which is at least $T + 2 > a^2$ if both coefficients are positive. Thus the only classes below the cutoff are those of i and $i\varepsilon$ for $1 \leq i < a$: the former are represented by L_a and the latter by the added lines.

The new lattice does not represent a. For a coordinate z on an added line with coefficient $i\varepsilon$, a putative representation of a gives

$$|z| + |z'| \leq \sqrt{(a/i)(T + 2)} < \sqrt{T^2 - 4}.$$

Thus z is an integer and must be zero, since $\varepsilon > a$. In the R-extension of L_a, write a putative representing vector as $u + \varepsilon v$ with $u, v \in L_a$. Averaging

its two conjugate values gives

$$a = Q(u + (T/2)v) + \tfrac{1}{4}(T^2 - 4)Q(v).$$

If $v \neq 0$, then $Q(v)$ is a positive integer and $(T^2-4)/4 > a$, a contradiction. Thus $v = 0$, returning the missing rational representation. Multiplying the lattice's form by ε gives a witness omitting εa and still representing every element of norm below a^2.

Let s denote either omitted value. If a purported finite criterion misses its unit-square class, adjoin to the corresponding witness an orthogonal line with coefficient c for each of its test elements c not yet represented. Every such c has norm at least $\mathrm{N}(s)$. A nonzero term cz^2 in a representation of s would be bounded by s at both embeddings and have norm at least $\mathrm{N}(s)$, forcing $cz^2 = s$ and $|\mathrm{N}(z)| = 1$. Then $z^{-1} = \pm z'$ belongs to R, so z is a unit. This contradicts the choice of the test set. Thus every criterion set meets each indicated class. All these witnesses are free over R, so the same conclusion holds when only free lattices are tested. Classes with different values of a have different field norms. To compare a and εa, suppose $\varepsilon = w^2$ for a unit w. If $\mathrm{N}(w) = 1$, then one of $\pm w$ is totally positive and hence a power of ε, making ε an even power of itself. Thus $\mathrm{N}(w) = -1$. The identity $\varepsilon - 1 = (\operatorname{Tr} w)w$ and the basis $(1, \varepsilon)$ give $|\operatorname{Tr} w| = 1$. It follows that $T = (\operatorname{Tr} w)^2 + 2 = 3$, outside the trace range of the theorem. Therefore the two sets of classes are disjoint. □

Every universal classical lattice over $R = \mathbb{Z}[\varepsilon]$ with $T \geq 228$, and every universal integer-valued lattice over this order with $T \geq 336\,403$, has rank at least 8. Indeed, the two orthogonal $\mathbb{Z}$-lattices spanned by the representing vectors are universal over $\mathbb{Z}$ (after dividing the second form by ε), so each has rank at least 4 [2]. Their rational Gram matrices have the same ranks over K as over $\mathbb{Q}$, so each K-span has dimension at least 4. Kim's form attains the bound, and at rank 8 the two spans give an orthogonal decomposition of the quadratic space over K into two spaces of dimension 4. For maximal orders, Kim, Kim, and Park [7] showed that only finitely many real quadratic fields admit a universal lattice of rank at most 7; the argument here gives the stated trace thresholds and the decomposition for this family of orders.

Provenance

Scott Duke Kominers raised the question of extending the classification to nonmaximal orders in [8, §10]. Mira Dot is the publication name of Scott's Dot, an OpenAI assistant working with Kominers. Mira Dot formulated and proved the classification over all real quadratic orders and wrote the manuscript. The criterion-set extension builds on [5]. Kominers communicated the note, checked the argument, and provided editorial guidance. He takes full responsibility for the correctness of its content.

References

[1] M. Bhargava, *On the Conway–Schneeberger fifteen theorem*, Quadratic Forms and Their Applications, Contemp. Math. 272, Amer. Math. Soc., Providence, RI, 2000, pp. 27–37.

[2] M. Bhargava and J. Hanke, *Universal quadratic forms and the* 290*-Theorem*, preprint, available online.

[3] A. Dress and R. Scharlau, *Indecomposable totally positive numbers in real quadratic orders*, J. Number Theory **14** (1982), 292–306.

[4] V. Kala, J. Krásenský, and G. Romeo, *Universality criterion sets for quadratic forms over number fields*, Adv. Math. **500** (2026), 111080.

[5] V. Kala, S. H. Man, R. Visser, and P. Yatsyna, *Explicit Tartakowsky theorem and universality criterion sets over totally real number fields*, arXiv:2611.21117v1, 2026.

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

[7] B. M. Kim, M.-H. Kim, and D. Park, *Real quadratic fields admitting universal lattices of rank* 7, J. Number Theory **233** (2022), 456–466.

[8] S. D. Kominers, *For which real quadratic fields is Kim's octonary form universal?*, manuscripta math., forthcoming. arXiv:2606.29321.