JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Noam D. ELKIES, Daniel M. KANE et Scott Duke KOMINERS

Minimal $\mathcal{S}$-universality criteria may vary in size

Tome 25, n° 3 (2013), p. 557-563.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_3_557_0>

Journal de Théorie des Nombres
de Bordeaux **25** (2013), 557–563

Minimal $\mathcal{S}$-universality criteria may vary in size

par Noam D. ELKIES, Daniel M. KANE et Scott Duke KOMINERS

Résumé. Nous donnons des exemples simples d'ensembles $\mathcal{S}$ de formes quadratiques qui ont des critères d'universalité minimaux de plusieurs cardinalités. Nous donnons ainsi une réponse négative à une question de Kim, Kim et Oh [KKO05].

Abstract. In this note, we give simple examples of sets $\mathcal{S}$ of quadratic forms that have minimal $\mathcal{S}$-universality criteria of multiple cardinalities. This answers a question of Kim, Kim, and Oh [KKO05] in the negative.

1. Introduction

A quadratic form Q *represents* another quadratic form L if there exists a $\mathbb{Z}$-linear, bilinear form-preserving injection $L \to Q$. In this note, we consider only positive-definite quadratic forms, and assume unless stated otherwise that every form is classically integral (equivalently: has a Gram matrix with integer entries). For a set $\mathcal{S}$ of such forms, a quadratic form is called *(classically) $\mathcal{S}$-universal* if it represents all quadratic forms in $\mathcal{S}$.

Denote by $\mathbb{N}$ the set $\{1, 2, 3, \ldots\}$ of natural numbers. In 1993, Conway and Schneeberger (see [Bha00, Con00]) proved the "Fifteen Theorem": $\{ax^2 : a \in \mathbb{N}\}$-universal forms can be exactly characterized as the set of forms which represent all of the forms in the finite set

$$\{x^2, 2x^2, 3x^2, 5x^2, 6x^2, 7x^2, 10x^2, 14x^2, 15x^2\}.$$

This set is thus said to be a "criterion set" for $\{ax^2 : a \in \mathbb{N}\}$. In general, for a set $\mathcal{S}$ of quadratic forms of bounded rank, a form Q is $\mathcal{S}$-universal if it represents every form in $\mathcal{S}$; an *$\mathcal{S}$-criterion set* is a subset $\mathcal{S}_* \subset \mathcal{S}$ such that every $\mathcal{S}_*$-universal form is $\mathcal{S}$-universal. Following the Fifteen Theorem, Kim, Kim, and Oh [KKO05] proved that, surprisingly, finite $\mathcal{S}$-universality criteria exist in general.

Theorem 1.1 (Kim, Kim, and Oh [KKO05])**.** *Let $\mathcal{S}$ be any set of quadratic forms of bounded rank. Then, there exists a finite $\mathcal{S}$-criterion set.*

Manuscrit reçu le 11 juin 2012.
Mots clefs. universality criteria, quadratic forms.
Classification math. 11E20, 11E25.

Kim, Kim, and Oh [KKO05] observed that there may be multiple $\mathcal{S}$-criterion sets $\mathcal{S}_* \subset \mathcal{S}$ which are *minimal* in the sense that for each $L \in \mathcal{S}_*$ there exists a Q that is $(\mathcal{S}_* \setminus \{L\})$-universal but not $\mathcal{S}$-universal.[1]

Given this observation, they asked the following question:

Question (Kim, Kim, and Oh [KKO05]; Kim [Kim04])**.** Is it the case that for all sets $\mathcal{S}$ of quadratic forms (of bounded rank), all minimal $\mathcal{S}$-criterion sets have the same cardinality? Formally, is

$$|\mathcal{S}_*| = |\mathcal{S}'_*|$$

for all minimal $\mathcal{S}$-criterion sets $\mathcal{S}_*$ and $\mathcal{S}'_*$?

In this brief note, we give simple examples that answer this question in the negative. In each case we choose some quadratic form A, and let $\mathcal{S}$ be the set of quadratic forms represented by A, so that $\mathcal{S}_* = \{A\}$ is a minimal $\mathcal{S}$-criterion set. We then exhibit one or more $\mathcal{S}'_* \subset \mathcal{S}$ that are finite but of cardinality 2 or higher, and prove that $\mathcal{S}'_*$ is also a minimal $\mathcal{S}$-criterion set.

We first give an example where A is diagonal of rank 3 and $\mathcal{S}'_*$ consists of one diagonal form of rank 2 and one of rank 3. We then give even simpler examples of higher rank where each $L \in \mathcal{S}'_*$ has rank smaller than that of A, often with $A = \oplus_{L \in \mathcal{S}'_*} L$.

It will at times be convenient to switch from the terminology of quadratic forms to the equivalent notions for lattices; we shall do this henceforth without further comment. For example we identify the form $\langle 1 \rangle$ with the lattice $\mathbb{Z}$.

2. An example of rank 3

Let $A := \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 2 \rangle$; that is, let A be the orthogonal direct sum of two copies of the form $\langle 1 \rangle$ and one copy of the form $\langle 2 \rangle$. Let $B := \langle 1 \rangle \oplus \langle 1 \rangle$ and $C := \langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle$. Let $\mathcal{S}$ be the set of quadratic forms represented by A.

Theorem 2.1. *Both $\{A\}$ and $\{B, C\}$ are minimal $\mathcal{S}$-criterion sets.*

Theorem 2.1 provides an example of two minimal $\mathcal{S}$-criterion sets of different cardinalities.

Proof of Theorem 2.1. Clearly, $\{A\}$ is a minimal $\mathcal{S}$-criterion set. Moreover, it is clear that while $B, C \in \mathcal{S}$, neither $\{B\}$ nor $\{C\}$ is an $\mathcal{S}$-criterion set since neither B nor C can embed A. It therefore only remains to show that $\{B, C\}$ is an $\mathcal{S}$-criterion set. To show this, it suffices to prove that any quadratic form Q that represents both B and C also represents A.

---

[1] Kim, Kim, and Oh [KKO05] gave a simple example of a set of quadratic forms $\mathcal{S}$ with multiple minimal $\mathcal{S}$-criterion sets: $\mathcal{S} = \left\{ \langle 2^i \rangle \oplus \langle 2^j \rangle \oplus \langle 2^k \rangle : 0 \le i, j, k \in \mathbb{Z} \right\}$, which has $\mathcal{S}$-criterion sets $\left\{ \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle, \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 2 \rangle \right\}$ and $\left\{ \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle, \langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle \right\}$.

First, we note that any vector v of norm 2 in an integer-matrix quadratic form Q that is not a sum of two orthogonal Q-vectors of norm 1 must be orthogonal to all Q-vectors of norm 1. Indeed, if $v, w \in Q$, $(v,v) = 2$, $(w,w) = 1$, and $(v,w) \neq 0$, then we may assume that $(v,w) = 1$ (by Cauchy-Schwarz, (v,w) is either 1 or -1, and in the latter case we may replace w by $-w$). Then $v = w + (v-w)$, where w and $v-w$ are orthogonal vectors of norm 1.

Suppose for sake of contradiction that Q is a quadratic form that represents B and C but not A. Since Q represents B but not A, there is no norm-2 vector of Q orthogonal to all norm-1 vectors of Q. Since Q represents C, it must contain three orthogonal norm-2 vectors, u, v, and w. By the above observation, we may write u as a sum of norm-1 vectors, say $u = x + y$ for some orthogonal norm-1 vectors $x, y \in Q$.

Now, each of v and w is orthogonal to u but not orthogonal to both x and y (since otherwise we could embed A as the span of $\{x, y, v\}$ or $\{x, y, w\}$). We claim that this implies that both v and w are of the form $\pm(x-y)$: Since v is not orthogonal to both x and y, we may assume without loss of generality that v is not orthogonal to x. Perhaps replacing v with $-v$, we may assume that $(v,x) = 1$. We then have $v = x + z$ for some unit vector z orthogonal to x. We have

$$0 = (u,v) = (x+y, x+z) = (x,x) + (x,z) + (y,x) + (y,z) = 1 + (y,z),$$

hence $(y,z) = -1$. Since both y and z are unit vectors, this implies that $z = -y$, hence $v = x - y$. An analogous argument shows that w is of the form $\pm(x-y)$.

Finally, if both v and w are of the form $\pm(x-y)$, then $(v,w) \in \{2, -2\}$, contradicting the fact that v and w are orthogonal. $\square$

3. Examples of higher rank

We begin with a simple example of rank 9. We give two proofs of the correctness of this example, each of which suggests a different generalization.

Proposition 3.1. *Let $A = E_8 \oplus \mathbb{Z}$, and let $\mathcal{S}$ be the set of quadratic forms represented by A. Then both $\{A\}$ and $\{E_8, \mathbb{Z}\}$ are minimal $\mathcal{S}$-criterion sets.*

Proof. As in the proof of Theorem 2.1, we need only prove that any quadratic form Q that represents both E_8 and $\mathbb{Z}$ also represents $E_8 \oplus \mathbb{Z}$.

First argument. Fix a copy of E_8 in Q. Choose any copy of $\mathbb{Z}$ in Q, that is, any vector $v \in Q$ with $(v,v) = 1$. Let $\pi : Q \to E_8 \otimes \mathbb{Q}$ be orthogonal projection. Then, $(\pi(v), w) = (v, w) \in \mathbb{Z}$ for all $w \in E_8$, so $\pi(v) \in E_8^*$. But E_8 is self-dual, and has minimal norm 2. Since $(\pi(v), \pi(v)) \leq (v,v)$, it follows that $\pi(v) = 0$, that is, v is orthogonal to E_8. Hence Q contains $E_8 \oplus \mathbb{Z}$ as claimed.

Second argument. Since E_8 and $\mathbb{Z}$ are unimodular, they are direct summands of Q (again because $\pi(v) \in E_8$ for all $v \in Q$, and likewise for the projection to $\mathbb{Z} \otimes \mathbb{Q}$). But E_8 and $\mathbb{Z}$ are indecomposable, and any positive-definite lattice is uniquely the direct sum of indecomposable summands. Hence $Q = \oplus_k Q_k$ for some indecomposable $Q_k \subset Q$, which include E_8 and $\mathbb{Z}$, so again we conclude that Q represents $E_8 \oplus \mathbb{Z}$. ☐

The first argument for Proposition 3.1 generalizes as follows.

Proposition 3.2. *Let $A = L \oplus L'$, where L' is generated by vectors v_i of norms (v_i, v_i) less than the minimal norm of nonzero vectors in the dual lattice*[2] *L^*. Let $\mathcal{S}$ be the set of quadratic forms represented by A. Then, both $\{A\}$ and $\{L, L'\}$ are minimal $\mathcal{S}$-criterion sets.*

Proof. As before, it is enough to show that if Q represents both L and L' then it represents $L \oplus L'$. Let π be the orthogonal projection to $L \otimes \mathbb{Q}$. Then $\pi(v_i) \in L^*$ for each i, whence $\pi(v_i) = 0$ because

$$(\pi(v_i), \pi(v_i)) \leq (v_i, v_i) < \min_{\substack{v \in L^* \\ v \neq 0}} (v, v).$$

Thus, the copy of L' generated by the v_i is orthogonal to L. This gives the desired representation of $L \oplus L'$ by Q. ☐

Examples. We may take $L' = \mathbb{Z}^n$ for any $n \in \mathbb{N}$, and $L \in \{E_6, E_7, E_8\}$; choosing $L = E_6$ and $n = 1$ gives an example of rank 7, the smallest we have found with this technique. We may also take L to be the Leech lattice; then L' can be any lattice generated by its vectors of norms 1, 2, and 3. There are even examples with neither L nor L' unimodular — indeed, such examples may have arbitrarily large discriminants. For instance, let Λ_{23} be the laminated lattice of rank 23 (the intersection of the Leech lattice with the orthogonal complement of one of its minimal vectors); this is a lattice of discriminant 4 and minimal dual norm 3. So we can take $L = \Lambda_{23}^n$ for arbitrary $n \in \mathbb{N}$, and choose any root lattice for L'.

The second argument for Proposition 3.1 generalizes in a different direction. We use the following notations. For a collection Π of sets, let $U(\Pi)$ be their union $\cup_{\mathcal{P} \in \Pi} \mathcal{P}$; and for a finite set $\mathcal{P}$ of lattices, let $\mathsf{P}(\mathcal{P})$ be the direct sum $\oplus_{L \in \mathcal{P}} L$. Say that two lattices L, L' are *coprime* if they have no indecomposable summands in common.

Proposition 3.3. *Let $A = \mathsf{P}(\mathcal{P})$, where $\mathcal{P}$ is a finite set of pairwise coprime, unimodular lattices; and let Π be a family of subsets of $\mathcal{P}$ such that $U(\Pi) = \mathcal{P}$. Then $\mathcal{S}'_* := \{\mathsf{P}(\mathcal{R}) : \mathcal{R} \in \Pi\}$ is an $\mathcal{S}$-criterion set for the set $\mathcal{S}$*

---

[2] This dual lattice is the only lattice we consider that might fail to be classically integral.

of quadratic forms represented by A. Moreover, $\mathcal{S}'_*$ is a minimal $\mathcal{S}$-criterion set if and only if $U(\Pi \setminus \{\mathcal{R}\})$ is smaller than $\mathcal{P}$ for each $\mathcal{R} \in \Pi$.

Proof. We repeatedly apply the observation that if $\mathcal{P}$ is a set of pairwise coprime lattices, each of which is a direct summand of a lattice Q, then $\mathsf{P}(\mathcal{P})$ is also a direct summand of Q. Since any unimodular sublattice of an integer-matrix lattice is a direct summand, it follows that Q represents $\mathsf{P}(\mathcal{R})$ for each $\mathcal{R} \in \Pi \iff Q$ represents each lattice in $U(\Pi) = \mathcal{P} \iff Q$ represents $\mathsf{P}(\mathcal{P}) = A$. That is, $\mathcal{S}'_*$ is a criterion set for A. Moreover, replacing Π by any subset $\Pi' = \Pi \setminus \{\mathcal{R}\}$ shows that $\{\mathsf{P}(\mathcal{R}) : \mathcal{R} \in \Pi'\}$ is a criterion set for $\mathsf{P}(U(\Pi'))$. Thus $\mathcal{S}'_*$ is minimal if and only if $U(\Pi \setminus \{\mathcal{R}\}) \subsetneq \mathcal{P}$ for each $\mathcal{R} \in \Pi$. ☐

Examples. We may take for Π any partition of $\mathcal{P}$, and then $A = \mathsf{P}(\mathcal{S}'_*) = \oplus_{L \in \mathcal{S}'_*} L$. Proposition 3.1 is the special case $\mathcal{P} = \{E_8, \mathbb{Z}\}$, $\Pi = \{\{E_8\}, \{\mathbb{Z}\}\}$. (The similar case $\mathcal{P} = \{E_8, \mathbb{Z}^8\}$, $\Pi = \{\{E_8\}, \{\mathbb{Z}^8\}\}$ was in effect used already by Oh [Oh00, Theorem 3.1] and the third author [Kom08a] in the study of 8-universality criteria.) Since $|\mathcal{P}|$ can be any natural number n, Proposition 3.3 produces for each n a lattice A for which $\mathcal{S}$ has minimal criterion sets of (at least) n distinct cardinalities.

4. Remarks

The examples presented here show that minimal $\mathcal{S}$-criterion sets may vary in size. Further examples can be obtained by mixing the techniques of Theorem 2.1 and Propositions 3.2 and 3.3; for instance,

$$\{\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 2\rangle \oplus E_8 \oplus \Lambda_{23}\} \text{ and } \{\langle 1\rangle \oplus \langle 1\rangle, \langle 2\rangle \oplus \langle 2\rangle \oplus \langle 2\rangle \oplus E_8, \Lambda_{23}\}$$

are both minimal criterion sets for the set of lattices represented by $\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 2\rangle \oplus E_8 \oplus \Lambda_{23}$. However, it is unclear (and appears difficult to characterize in general) for which $\mathcal{S}$ this phenomenon occurs.

For the sets $\mathcal{S}_n$ of rank-n quadratic forms, criterion sets are known only in the cases $n = 1, 2, 8$ (see [Bha00, Con00], [KKO99], and [Oh00], respectively). Few criterion sets beyond those for $\mathcal{S}_n$ ($n = 1, 2, 8$) have been explicitly computed.

Meanwhile, in the cases $n = 1, 2, 8$, the minimal $\mathcal{S}_n$-criterion sets are known to be *unique* (see [Kim04], [Kom08b], and [Kom08a]), in which case the answer to the question we examine is (trivially) affirmative. But there is not yet a general characterization of the $\mathcal{S}$ that have unique minimal $\mathcal{S}$-criterion sets (see [Kim04]). It seems likely that such a result would be essential in making progress towards a general answer to the question of Kim, Kim, and Oh [KKO05] that we studied here.

Acknowledgements

While working on this paper, Elkies was supported in part by NSF grants DMS-0501029 and DMS-1100511, Kane and Kominers were supported in part by NSF Graduate Research Fellowships, and Kominers was also supported in part by an AMS–Simons Travel Grant.

References

[Bha00] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*. Quadratic forms and their applications: Proceedings of the Conference on Quadratic Forms and Their Applications, July 5–9, 1999, University College Dublin, Contemporary Mathematics, vol. **272**, American Mathematical Society, 2000, pp. 27–37.

[Con00] J. H. Conway, *Universal quadratic forms and the fifteen theorem*. Quadratic forms and their applications: Proceedings of the Conference on Quadratic Forms and Their Applications, July 5–9, 1999, University College Dublin, Contemporary Mathematics, vol. **272**, American Mathematical Society, 2000, pp. 23–26.

[Kim04] M.-H. Kim, *Recent developments on universal forms*. Algebraic and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, vol. **344**, American Mathematical Society, 2004, pp. 215–228.

[KKO99] B. M. Kim, M.-H. Kim, and B.-K. Oh, 2-*universal positive definite integral quinary quadratic forms*. Integral quadratic forms and lattices: Proceedings of the International Conference on Integral Quadratic Forms and Lattices, June 15–19, 1998, Seoul National University, Korea, Contemporary Mathematics, vol. **249**, American Mathematical Society, 1999, pp. 51–62.

[KKO05] ——, *A finiteness theorem for representability of quadratic forms by forms*. Journal fur die Reine und Angewandte Mathematik **581** (2005), 23–30.

[Kom08a] S. D. Kominers, *The* 8-*universality criterion is unique*. Preprint, `arXiv:0807.2099`, 2008.

[Kom08b] ——, *Uniqueness of the* 2-*universality criterion*. Note di Matematica **28** (2008), no. 2, 203–206.

[Oh00] B.-K. Oh, *Universal* $\mathbb{Z}$-*lattices of minimal rank*. Proceedings of the American Mathematical Society **128** (2000), 683–689.

Noam D. Elkies
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138
E-mail: `elkies@math.harvard.edu`

Daniel M. Kane
Department of Mathematics
Stanford University
Building 380, Sloan Hall
Stanford, California 94305
E-mail: `dankane@math.stanford.edu`
E-mail: `aladkeenin@gmail.com`

Scott Duke Kominers
Society of Fellows
Dpt of Economics
Program for Evolutionary Dynamics
Center for Research on Computation and Society
Harvard University
One Brattle Square, Suite 6
Cambridge, MA 02138-3758
E-mail: `kominers@fas.harvard.edu`
E-mail: `skominers@gmail.com`