Bull. Aust. Math. Soc. **103** (2021), 390–404
doi:10.1017/S000497272000101X

PRIME-UNIVERSAL DIAGONAL QUADRATIC FORMS

JANGWON JU, DAEJUN KIM✉, KYOUNGMIN KIM, MINGYU KIM and BYEONG-KWEON OH

(Received 3 July 2020; accepted 17 July 2020; first published online 5 October 2020)

Abstract

A (positive definite and integral) quadratic form is said to be *prime-universal* if it represents all primes. Recently, Doyle and Williams ['Prime-universal quadratic forms $ax^2 + by^2 + cz^2$ and $ax^2 + by^2 + cz^2 + dw^2$', *Bull. Aust. Math. Soc.* **101** (2020), 1–12] classified all prime-universal diagonal ternary quadratic forms and all prime-universal diagonal quaternary quadratic forms under two conjectures. We classify all prime-universal diagonal quadratic forms regardless of rank, and prove the so-called 67-theorem for a diagonal quadratic form to be prime-universal.

2020 *Mathematics subject classification*: primary 11E12; secondary 11E20.

Keywords and phrases: diagonal quadratic forms, prime-universal.

1. Introduction

A positive definite integral quadratic form

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} f_{ij} x_i x_j \quad (f_{ij} = f_{ji} \in \mathbb{Z})$$

is said to be *prime-universal* if for any prime p, the Diophantine equation

$$f(x_1, x_2, \ldots, x_n) = p$$

has an integer solution $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$. Any quadratic form that represents all positive integers, which we call a *universal* quadratic form, is also prime-universal. By the 15-theorem of Conway and Schneeberger [1], any quadratic form that represents all integers less than or equal to 15 is universal and also prime-universal. On the other hand, there are many prime-universal quadratic forms that are not universal.

The first author was supported by a National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2019R1F1A1064037), the third author was supported by an NRF grant funded by MSIT (NRF-2020R1I1A1A01055225), the fourth author was supported by the NRF (NRF-2019R1A6A3A01096245) and the fifth author was supported by the NRF grant funded by MSIT (NRF-2020R1A5A1016126).

© 2020 Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

Recently, Doyle and Williams [2] classified all prime-universal diagonal ternary quadratic forms which are not universal. They also determined all possible prime-universal diagonal quaternary quadratic forms, except for the 27 forms listed in (2.1). They proved the prime-universality of those 27 forms assuming the following two conjectures, which they proposed in [2]:

(1) The quadratic form $2x_1^2 + 3x_2^2 + 4x_3^2$ represents all odd integers $n > 647$.
(2) The quadratic form $2x_1^2 + 3x_2^2 + 5x_3^2$ represents all odd integers $p \neq 43$.

In this article, we classify all prime-universal diagonal quadratic forms without any assumption, and we prove the following 67-theorem.

THEOREM 1.1. *Let f be a diagonal quadratic form, and let*

$$\mathcal{S} = \{2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 23,\ 41,\ 43,\ 67\}.$$

If f represents all primes in $\mathcal{S}$, then it is prime-universal. Moreover, the set $\mathcal{S}$ is minimal in the sense that any proper subset of $\mathcal{S}$ does not guarantee the prime-universality.

We do not use the two conjectures of Doyle and Williams in proving our results; these conjectures remain open.

Let $f = \sum f_{ij}x_ix_j$ be a (positive definite integral) quadratic form. The symmetric matrix corresponding to f is $M_f = (f_{ij})$. If f is diagonal, its matrix is diagonal and we simply write

$$f = \langle f_{11}, f_{22}, \ldots, f_{nn}\rangle.$$

For a positive integer a, we say that a is represented by f, denoted by $a \to f$, if the Diophantine equation $f(x_1, \ldots, x_n) = a$ has an integer solution $(x_1, \ldots, x_n) \in \mathbb{Z}^n$. For a prime p, if there is a solution $(x_1, \ldots, x_n) \in \mathbb{Z}_p$, the ring of p-adic integers, we say that a is represented by f over $\mathbb{Z}_p$. If a is represented by f over $\mathbb{Z}_p$ for all primes p, we say that a is *locally* represented by f. The set of all integers that are represented by f will be denoted by $Q(f)$. The genus of f, denoted by $\mathrm{gen}(f)$, is the set of quadratic forms that are isometric to f over $\mathbb{Z}_p$ for any prime p. An integer a is locally represented by f if and only if there is a quadratic form $g \in \mathrm{gen}(f)$ that represents a. The set of integers locally represented by f will be denoted by $Q(\mathrm{gen}(f))$.

Any unexplained notation and terminology can be found in [4] or [7].

2. Prime-universal diagonal quaternary quadratic forms

In this section, we classify all prime-universal diagonal quaternary quadratic forms. In [2], the authors classified all prime-universal diagonal quaternary quadratic forms except for the following 27 forms:

$$\begin{aligned} &\langle 2,3,4,5\rangle, \quad \langle 2,3,4,11\rangle, \quad \langle 2,3,5,5\rangle, \quad \langle 2,3,5,11\rangle, \\ &\langle 2,3,5,13\rangle, \quad \langle 2,3,5,14\rangle, \quad \langle 2,3,5,16\rangle, \quad \langle 2,3,5,17\rangle, \\ &\langle 2,3,5,h\rangle \quad \text{for} \quad h = 20,\ldots,27,29,\ldots,33,35,36,38,40,41,43. \end{aligned} \tag{2.1}$$

Hence, it suffices to prove the prime-universality of these 27 diagonal forms.

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

In [3], [5] and [6], we developed a method to determine whether or not integers in an arithmetic progression are represented by a particular ternary quadratic form. Let d be a positive integer and let a be a nonnegative integer ($a \le d$). We define

$$S_{d,a} = \{dn + a \mid n \in \mathbb{N} \cup \{0\}\}.$$

For two quadratic forms f and g, we define

$$R(g, d, a) = \{v \in (\mathbb{Z}/d\mathbb{Z})^3 \mid vM_g v^t \equiv a \pmod{d}\}$$

and

$$R(f, g, d) = \{T \in M_3(\mathbb{Z}) \mid T^t M_f T = d^2 M_g\}.$$

A coset (or a vector in the coset) $v \in R(g, d, a)$ is said to be *good* with respect to f, g, d and a if there is a $T \in R(f, g, d)$ such that $d^{-1} \cdot vT^t \in \mathbb{Z}^3$. The set of all good vectors in $R(g, d, a)$ is denoted by $R_f(g, d, a)$. If $R(g, d, a) = R_f(g, d, a)$, we write

$$g \prec_{d,a} f.$$

If $g \prec_{d,a} f$, then by [5, Lemma 2.2],

$$S_{d,a} \cap Q(g) \subset Q(f). \tag{2.2}$$

In particular, if $g \prec_{d,a} f$ for any $g \in \mathrm{gen}(f)$, then $Q(\mathrm{gen}(f)) \cap S_{d,a} \subset Q(f)$.

A MAPLE-based computer program for computing these sets is available from the authors upon request.

THEOREM 2.1. *Both quaternary quadratic forms $f = \langle 2, 3, 4, 5\rangle$ and $\langle 2, 3, 4, 11\rangle$ are prime-universal.*

PROOF. As the proofs are quite similar, we only give the proof for $f = \langle 2, 3, 4, 5\rangle$.

The class number of $g = \langle 2, 3, 4\rangle$ is 2 and its genus mate is $\langle 1, 2, 12\rangle$. If an even integer is represented by $\langle 1, 2, 12\rangle$, then it is also represented by $\langle 4, 2, 12\rangle$, which is a subform of g. Therefore, $Q(\mathrm{gen}(g)) \cap 2\mathbb{Z} \subset Q(g)$, and so g represents all nonnegative even integers except those integers of the form $2^{2s+1}(8t + 5)$ for some nonnegative integers s and t. Since one may check directly that $p \to f$ for any prime p such that $p \le 113$, we assume that $p \ge 127$. Then, one may easily check that

$$p - 5 \cdot d^2 \to g,$$

where

$$d = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8,\ p \equiv 7 \pmod{16} \text{ or } p \equiv 21 \pmod{64}, \\ 5 & \text{if } p \equiv 13, 45 \pmod{64}, \\ 3 & \text{otherwise.} \end{cases}$$

This completes the proof. □

THEOREM 2.2. *For an integer α that is not divisible by 7 with $5 \le \alpha \le 43$, the quaternary quadratic form $f = \langle 2, 3, 5, \alpha\rangle$ listed in (2.1) is prime-universal.*

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

PROOF. The class number of $g = \langle 2, 3, 5\rangle$ is 2 and its genus mate is $g_1 = \langle 1, 1, 30\rangle$. One may easily check that

$$g_1 \prec_{7,0} g, \quad g_1 \prec_{7,3} g, \quad g_1 \prec_{7,5} g \quad \text{and} \quad g_1 \prec_{7,6} g.$$

Therefore, for any $a \in \{0, 3, 5, 6\}$, $Q(\mathrm{gen}(g)) \cap S_{7,a} \subset Q(g)$. Consequently, g represents all nonnegative integers that are not divisible by 3 and are congruent to $0, 3, 5$ or 6 modulo 7. Since one may check directly that $p \to f$ for any prime p such that $p \le 36\alpha$, we assume that $p > 36\alpha$. If p is congruent to $3, 5$ or 6 modulo 7, then p is represented by g. Assume that p is congruent to $1, 2$ or 4 modulo 7. Then, one may easily check that

$$p - \alpha \cdot 3^2 \cdot d^2 \to g,$$

where

$$d = \begin{cases} 1 & \text{if } p - 2\alpha \equiv 0, 3, 5 \text{ or } 6 \pmod 7, \\ 2 & \text{otherwise.} \end{cases}$$

This completes the proof. □

THEOREM 2.3. *The quaternary quadratic form $f = \langle 2, 3, 5, 14\rangle$ is prime-universal.*

PROOF. The class number of $g = \langle 2, 3, 14\rangle$ is two and its genus mate is

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & 4 \\ 0 & 4 & 10 \end{pmatrix}.$$

One may easily check that

$$g_1 \prec_{8,3} g, \quad g_1 \prec_{32,12} g \quad \text{and} \quad g_1 \prec_{32,16} g.$$

Thus, if we put

$$A = S_{8,3} \cup S_{32,12} \cup S_{32,16},$$

then $Q(\mathrm{gen}(g)) \cap A \subset Q(g)$. Consequently, g represents all integers in A except for those of the form $3^{2s+1}(3t + 2)$ for some nonnegative integers s and t. One may check directly that $p \to g$ for any prime $p < 2207$. Thus, we assume that p is a prime greater than or equal to 2207. If we define

$$d = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 8, \\ 1 & \text{if } p \equiv 25 \text{ or } 29 \pmod{32}, \\ 2 & \text{if } p \equiv 7 \pmod 8, \\ 3 & \text{if } p \equiv 1 \text{ or } 5 \pmod{32}, \\ 5 & \text{if } p \equiv 17 \text{ or } 21 \pmod{32}, \\ 7 & \text{if } p \equiv 9 \text{ or } 13 \pmod{32}, \end{cases}$$

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

then one may easily check that

$$n = p - 5 \cdot 3^2 \cdot d^2 \in A \quad \text{and} \quad n \not\equiv 0 \pmod 3.$$

Thus, $n \to g$, which completes the proof. □

THEOREM 2.4. *The quaternary quadratic form $f = \langle 2, 3, 5, 21\rangle$ is prime-universal.*

PROOF. One may check directly that f represents all primes less than 88211. Thus, we assume that p is a prime greater than or equal to 88211. The class number of $g = \langle 3, 5, 21\rangle$ is three and its genus mates are

$$g_1 = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 6 & 3 \\ 0 & 3 & 12 \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 8 & 0 \\ 0 & 0 & 21 \end{pmatrix}.$$

One may easily show that any positive integer m which is congruent to 2 modulo 3 and relatively prime to 35 is represented by the genus of g. If we define

$$d = \begin{cases} 2 & \text{if } p \equiv 1 \pmod{12}, \\ 6 & \text{if } p \equiv 5 \pmod{12}, \\ 1 & \text{if } p \equiv 7 \pmod{12}, \\ 3 & \text{if } p \equiv 11 \pmod{12}, \end{cases}$$

and

$$n = p - 2 \cdot 35^2 \cdot d^2,$$

then one may easily check that n is a positive integer congruent to 5 modulo 12 and is relatively prime to 35. Thus,

$$n \equiv 1 \pmod 4 \quad \text{and} \quad n \to \mathrm{gen}(g).$$

Hence, the integer n is represented by a quadratic form in the genus of g. Suppose that $n \to g_1$. Then there is a vector $(x, y, z) \in \mathbb{Z}^3$ such that

$$n = 5x^2 + 6y^2 + 12z^2 + 6yz.$$

Since $n \equiv 1 \pmod 4$, either $y \equiv 0 \pmod 2$ or $yz \equiv 1 \pmod 2$. If $y = 2y'$ for some $y' \in \mathbb{Z}$, then

$$n = 5x^2 + 24y'^2 + 12z^2 + 12y'z = 3(y' + 2z)^2 + 5x^2 + 21y'^2,$$

which means that $n \to g$. If $yz \equiv 1 \pmod 2$, then we may write $y = z - 2y'$. Then,

$$\begin{aligned} n &= 5x^2 + 6(z - 2y')^2 + 12z^2 + 6(z - 2y')z \\ &= 5x^2 + 24y'^2 + 24z^2 - 36y'z \\ &= 3(y' + z)^2 + 5y^2 + 21(y' - z)^2 \end{aligned}$$

and thus $n \to g$. Similarly, one may show that the supposition $n \to g_2$ also implies that $n \to g$. This completes the proof. □

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

THEOREM 2.5. *The quaternary quadratic form* $f = \langle 2, 3, 5, 35\rangle$ *is prime-universal.*

PROOF. One may check directly that f represents all primes less than 596243. Thus, we assume that p is a prime greater than or equal to 596243. Note that the class number of g is three and its genus mates are

$$g_1 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 10 & 5 \\ 0 & 5 & 20 \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 8 & 0 \\ 0 & 0 & 35 \end{pmatrix}.$$

One may easily show that any positive integer m which is congruent to 2 or 3 modulo 5 and is relatively prime to 21 is represented by the genus of g. If we define

$$d = \begin{cases} 13 & \text{if } p \equiv 1 \pmod{20}, \\ 10 & \text{if } p \equiv 3 \text{ or } 7 \pmod{20}, \\ 1 & \text{if } p \equiv 9 \pmod{20}, \\ 2 & \text{if } p \equiv 11 \pmod{20}, \\ 5 & \text{if } p \equiv 13 \text{ or } 17 \pmod{20}, \\ 26 & \text{if } p \equiv 19 \pmod{20} \end{cases}$$

and $n = p - 2 \cdot 21^2 \cdot d^2$, then one may easily check that $n \equiv 3 \pmod 4$, $n \to \text{gen}(g)$. For each $i = 1, 2$, one may easily show that any positive integer m represented by g_i which is congruent to 3 modulo 4 is also represented by g as in the proof of Theorem 2.4. Therefore, $n \to g$, which implies that $p \to f$. □

3. Higher-dimensional prime-universal diagonal quadratic forms

Let $a_1, \ldots, a_n \in \mathbb{N}$ be such that $a_1 \le a_2 \le \cdots \le a_n$, and let $f = \langle a_1, \ldots, a_n\rangle$. For $1 \le i \le n$, we define the diagonal subform $\hat{f}_i$ of f of rank $i - 1$ by

$$\hat{f}_i = \langle a_1, \ldots, \hat{a}_i, \ldots, a_n\rangle,$$

where the 'hat' symbol over a_i indicates that this integer is deleted from the sequence $a_1, \ldots, a_n$.

A prime-universal diagonal quadratic form f is called *proper* if any diagonal subform $\hat{f}_i$ is not prime-universal. To find all prime-universal diagonal quadratic forms, it suffices to find all proper ones. In this section, we classify all proper prime-universal diagonal quadratic forms with rank greater than 4.

If a diagonal quadratic form f fails to represent a prime, we call the smallest prime not represented by f its *prime truant*.

According to the results in [2], there are no prime-universal diagonal binary quadratic forms, and there are five proper prime-universal diagonal ternary quadratic forms, namely,

$$\langle 1, 1, 2\rangle, \quad \langle 1, 1, 3\rangle, \quad \langle 1, 2, 3\rangle, \quad \langle 1, 2, 4\rangle \quad \text{and} \quad \langle 1, 2, 5\rangle.$$

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

TABLE 1. Proper prime-universal forms $\langle a_1, a_2, \ldots, a_k \rangle$ $(5 \le k \le 6)$.

a_1	a_2	a_3	a_4	a_5	a_6	Conditions on a_k $(5 \le k \le 6)$
2	2	2	2	3		
2	2	2	3	a_5		$a_5 = 8, 11, 17$
2	2	3	8	17		
2	2	3	11	17		
2	2	3	16	17		
2	2	3	17	a_5		$17 \le a_5 \le 41, a_5 \ne 26, 32, 35, 40$
2	3	3	3	4		
2	3	3	4	a_5		$a_5 = 4, 6, 10, 13$
2	3	4	4	a_5		$4 \le a_5 \le 17, a_5 \ne 5, 8, 9, 11, 16$
2	3	4	6	a_5		$6 \le a_5 \le 23, a_5 \ne 8, 9, 11, 22$
2	3	4	7	a_5		$7 \le a_5 \le 17, a_5 \ne 8, 9, 11, 16$
2	3	4	10	a_5		$10 \le a_5 \le 23, a_5 \ne 11, 22$
2	3	4	12	13		
2	3	4	13	a_5		$13 \le a_5 \le 23, a_5 \ne 13, 22$
2	3	5	7	a_5		$a_5 = 7, 19, 28, 34$
2	3	5	19	19		
2	3	6	6	7		
2	3	6	7	a_5		$7 \le a_5 \le 23, a_5 \ne 8, 19, 20, 22$
2	3	6	7	19	20	
2	3	6	7	20	a_6	$20 \le a_6 \le 67, a_6 \ne 21, 23, 63, 66$
2	3	7	7	a_5		$7 \le a_5 \le 13, a_5 \ne 7, 8, 9, 10, 12$
2	3	7	7	7	10	
2	3	7	9	a_5		$9 \le a_5 \le 13, a_5 \ne 9, 12$
2	3	7	10	a_5		$10 \le a_5 \le 23, a_5 \ne 17, 19, 22$
2	3	7	11	a_5		$11 \le a_5 \le 17, a_5 \ne 11, 13, 16$
2	3	7	12	13		
2	3	7	13	a_5		$13 \le a_5 \le 17, a_5 \ne 13, 16$

All prime-universal diagonal quaternary quadratic forms from the previous section with minimum greater than 1 are listed in Table 1 of [2]. Therefore, it suffices to classify all proper prime-universal diagonal quadratic forms with rank greater than or equal to 5. These are listed in Table 1.

THEOREM 3.1. *Every diagonal quadratic form in Table 1 is proper prime-universal.*

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

We will prove Theorem 3.1 at the end of this section. Assuming Theorem 3.1, we first prove the following theorem, which guarantees that Table 1 is the complete list of proper prime-universal diagonal quadratic forms of rank greater than or equal to 5.

THEOREM 3.2. *Let f be a proper prime-universal diagonal quadratic form with rank greater than or equal to 5. Then f is isometric to one of the quadratic forms listed in Table 1.*

PROOF. Let $f = \langle a_1, a_2, \ldots, a_n \rangle$ be a proper prime-universal diagonal quadratic form, where the a_is are integers such that $1 \le a_1 \le \cdots \le a_n$. For the sake of convenience, we define $f_i = \langle a_1, \ldots, a_i \rangle$ for $1 \le i \le n$. Since we are assuming that f is proper, f_4 should not be prime-universal. Following the argument used in the proof of Theorem 1.3 of [2], one may easily obtain all candidates of f_4. After removing those forms that are already prime-universal among all possible candidates, f_4 is isometric to one of the following:

Case 1	$\langle 2, 2, 2, a_4 \rangle$	where $a_4 = 2, 3,$
Case 2	$\langle 2, 2, 3, a_4 \rangle$	where $a_4 = 8, 11, 16, 17,$
Case 3	$\langle 2, 3, 3, a_4 \rangle$	where $a_4 = 3, 4, 6,$
Case 4	$\langle 2, 3, 4, a_4 \rangle$	where $a_4 = 4, 6, 7, 10, 12, 13,$
Case 5	$\langle 2, 3, 5, a_4 \rangle$	where $a_4 = 7, 19, 28, 34, 37, 39, 42,$
Case 6	$\langle 2, 3, 6, a_4 \rangle$	where $a_4 = 6, 7,$
Case 7	$\langle 2, 3, 7, a_4 \rangle$	where $a_4 = 7, 9, 10, 11, 12, 13.$

Note that any diagonal form $\langle a_1, a_2, a_3, a_4 \rangle$ listed above is not prime-universal. Although what we have to check is different case by case, we repeat the following process, starting from $i = 5$.

Let p be the prime truant of $f_{i-1} = \langle a_1, \ldots, a_{i-1} \rangle$. Since f is prime-universal, it should represent p. Hence, $a_{i-1} \le a_i \le p$. For each integer a with $a_{i-1} \le a \le p$, it is easy to check that one of the following possibilities must occur.

(I) The form $g_i = g_{i,a} := \langle a_1, \ldots, a_{i-1}, a \rangle$ is prime-universal, and either

  (I-1) g_i is proper, or
  (I-2) g_i is not proper.

(II) The form g_i is not prime-universal, and either

  (II-1) g_i fails to represent another prime p' greater than p, or
  (II-2) g_i still fails to represent the prime p.

Since any prime-universal form contains a proper prime-universal form as its subform, one may use Table 1 above and Table 1 of [2] to check the prime-universality of g_i as well as its properness.

If (I-1) happens, one may easily check that g_i is listed in Table 1; hence, the theorem is proved. If (I-2) happens, one may easily find a proper subform of g_i which is listed in Table 1.

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

If (II) happens, we increase i by 1 and repeat the process. In particular, if (II-2) happens, then one might come across the following situation: any diagonal quadratic form $\langle a_1, \dots, a_{i-1}, a, \dots, a\rangle$ fails to represent p, no matter how many times the integer a is repeated. Even if it happens, the equation

$$a_1x_1^2 + \cdots + a_{i-1}x_{i-1}^2 + a_ix_i^2 + \cdots + a_nx_n^2 = p$$

has an integer solution, as f represents the prime p. Therefore, there is an integer b with $a < b \le p$ such that $\langle a_1, \dots, a_i, a, b\rangle$ represents p. Now, we repeat the process from the diagonal quadratic form

$$\langle a_1, \dots, a_i, \overbrace{a, \dots, a}^{s\text{-times}}, b\rangle$$

for each $s \ge 1$. For *Case 1* to *Case 7* given above, one may check that this process terminates in a finite number of steps. Since the proofs of all cases are quite similar, we only give the proofs of *Case 2* and *Case 6*.

Case 2: $f_4 = \langle 2, 2, 3, a_4\rangle$ with $a_4 = 8, 11, 16, 17$.

First, we consider the case where $f_4 = \langle 2, 2, 3, 8\rangle$. Since the prime truant of f_4 is 17, $8 \le a_5 \le 17$. For $a = 9, 10, 12, 13, 14, 15$, the form $\langle 2, 2, 3, a\rangle$ is already prime-universal; hence, f is not proper if $a_i = a$ for some $i \ge 5$. Therefore, we may assume that

$$a_i \in \{8, 11, 16, 17\} \quad \text{or} \quad a_i \ge 18$$

for any $i \ge 5$. If $a_i \ne 17$ for any $i \ge 5$, then the diagonal quadratic form $\langle 2, 2, 3, 8, a_5 \dots, a_n\rangle$ does not represent 17. Therefore, $a_i = 17$ for some i. Since $\langle 2, 2, 3, 8, 17\rangle$ is prime-universal, the only proper prime-universal diagonal quadratic form f with $f_4 = \langle 2, 2, 3, 8\rangle$ is $\langle 2, 2, 3, 8, 17\rangle$. One may similarly prove the case where $a_4 = 11, 16$.

Next, we consider the case where $f_4 = \langle 2, 2, 3, 17\rangle$. Note that the prime truant of $\langle 2, 2, 3, 17\rangle$ is 41; hence, $17 \le a_5 \le 41$. Since $\langle 2, 2, 3, 17\rangle$ does not represent $1, 6, 9, 15, 41$, f represents 41 if and only if

$$a_i \in \mathcal{A} = \{17 \le a \le 41 : a \ne 26, 32, 35, 40\}$$

for some $i \ge 5$. Furthermore, one may easily check using Table 1 that any quadratic form $\langle 2, 2, 3, 17, a_5\rangle$ with $a_5 \in \mathcal{A}$ is proper prime-universal.

Case 6: $f_4 = \langle 2, 3, 6, a_4\rangle$ with $a_4 = 6, 7$.

First, we consider the case where $f_4 = \langle 2, 3, 6, 6\rangle$. Note that the prime truant of f_4 is 7, and f can represent 7 if and only if $a_i = 7$ for some $i \ge 5$. Also, note that $\langle 2, 3, 6, 6, 7\rangle$ is prime-universal, whereas $\langle 2, 3, 6, 7\rangle$ does not represent 23.

Next, we consider the case where $f_4 = \langle 2, 3, 6, 7\rangle$. Since the prime truant of f_4 is 23, $7 \le a_5 \le 23$. Note that every form $\langle 2, 3, 6, 7, a_5\rangle$ with $7 \le a_5 \le 23$ and $a_5 \ne 19, 20, 22$ is proper prime-universal. On the other hand, the prime truants of $\langle 2, 3, 6, 7, 19\rangle$, $\langle 2, 3, 6, 7, 20\rangle$ and $\langle 2, 3, 6, 7, 22\rangle$ are 23, 67 and 23, respectively.

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

Now, assume that $a_5 = 19$. If $a_i \in \{21, 23\}$ for some $i \geq 6$, then f is prime-universal but not proper. Since $\langle 2, 3, 6, 7, 19\rangle$ does not represent integers $1, 4$ or 23, f can represent 23 if and only if $a_i = 20$ for some $i \geq 6$. Note that $\langle 2, 3, 6, 7, 19, 20\rangle$ is proper prime-universal. Therefore, the only proper prime-universal diagonal quadratic form f with $f_5 = \langle 2, 3, 6, 7, 19\rangle$ is $\langle 2, 3, 6, 7, 19, 20\rangle$.

Next, assume that $a_5 = 20$. Since the prime truant of $\langle 2, 3, 6, 7, 20\rangle$ is 67, $20 \leq a_6 \leq 67$. Note that $\langle 2, 3, 6, 7, 20, a_6\rangle$ with $20 \leq a_6 \leq 67$ and $a_6 \neq 63, 66$ is proper prime-universal, and $f = \langle 2, 3, 6, 7, 20, \{63 \text{ or } 66\}, a_7, \cdots\rangle$ can represent 67 if and only if $a_i = 64, 65, 67$ or $a_i = 67$, respectively, for some $i \geq 7$. However, since $\langle 2, 3, 6, 7, 20, a\rangle$ with $a = 64, 65$ or 67 is already prime-universal, any prime-universal form $\langle 2, 3, 6, 7, 20, \{63 \text{ or } 66\}, a_7, \cdots\rangle$ is not proper.

Finally, assume that $a_5 = 22$. Since $f_5 = \langle 2, 3, 6, 7, 22\rangle$ does not represent 23, $a_i = 23$ for some $i \geq 6$. Note that $\langle 2, 3, 6, 7, 23\rangle$ is proper prime-universal. □

THEOREM 3.3. *The quadratic form $f = \langle 2, 2, 2, 3\rangle$ represents all primes except 17. Hence, the quadratic forms $\langle 2, 2, 2, 2, 3\rangle$ and $\langle 2, 2, 2, 3, a_5\rangle$ with $3 \leq a_5 \leq 17$ and $a_5 \neq 16$ are prime-universal.*

PROOF. Note that the class number of $g = \langle 2, 2, 2\rangle$ is 1. Therefore, $Q(\text{gen}(g)) = Q(g)$, and consequently g represents all nonnegative even integers except those of the form $4^s(16t + 14)$ for some nonnegative integers s and t.

Since one may directly check that $p \to f$ for any prime p such that $p \leq 73$ except 17, we assume that $p \geq 79$. Then, one may easily check that

$$p - 3 \cdot d^2 \to g,$$

where

$$d = \begin{cases} 5 & \text{if } p \equiv 27 \pmod{32}, \\ 3 & \text{if } p \equiv 1, 3, 17 \pmod{12}, \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, $p \to f$. Now, the proof of the last assertion is straightforward. □

THEOREM 3.4. *The quadratic form $f = \langle 2, 2, 3, 17\rangle$ represents all primes but not 41. Hence, the quadratic forms $\langle 2, 2, 3, a_4, 17\rangle$ with $a_4 = 8, 11, 16$ and $\langle 2, 2, 3, 17, a_5\rangle$ with $17 \leq a_5 \leq 41$ and $a_5 \neq 26, 32, 35, 40$ are prime-universal.*

PROOF. The class number of $g = \langle 2, 2, 3\rangle$ is 1. Therefore, $Q(\text{gen}(g)) = Q(g)$, and consequently g represents all nonnegative integers except those of the forms $8t + 1$ and $9^s(9t + 6)$ for some nonnegative integers s and t.

Since one may check directly that $p \to f$ for any prime p such that $p \leq 607$ except 41, we assume that $p \geq 613$. Then, one may easily check that

$$p - 17 \cdot 6^2 \to g.$$

Therefore, $p \to f$. Now, the proof of the last assertion is straightforward. □

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

THEOREM 3.5. *The quadratic form* $f = \langle 2, 3, 3, 4\rangle$ *represents all primes except* 13. *Hence, the quadratic forms* $\langle 2, 3, 3, 3, 4\rangle$ *and* $\langle 2, 3, 3, 4, a_5\rangle$ *with* $4 \le a_5 \le 13$ *and* $a_5 \ne 12$ *are prime-universal.*

PROOF. The class number of $g = \langle 2, 3, 3\rangle$ is 1. Therefore, $Q(\mathrm{gen}(g)) = Q(g)$, and so g represents all nonnegative integers except for those of the form $9^s(3t + 1)$ for some nonnegative integers s and t. Since one may check directly that $p \to f$ for any prime p such that $p \le 13$ except 13, we assume that $p \ge 17$. One may easily check that

$$p - 4 \cdot d^2 \to g,$$

where

$$d = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 9, \\ 2 & \text{if } p \equiv 4 \pmod 9. \end{cases}$$

Therefore, $p \to f$. Now, the proof of the last assertion is straightforward. □

THEOREM 3.6. *For the following quadratic forms:*

$\langle 2, 3, 4, 4\rangle$, $\langle 2, 3, 4, 7\rangle$	*represent all primes except* 17,
$\langle 2, 3, 4, 6\rangle$, $\langle 2, 3, 4, 10\rangle$, $\langle 2, 3, 4, 13\rangle$	*represent all primes except* 23,
$\langle 2, 3, 4, 12\rangle$	*represents all primes except* 13.

Hence, all quadratic forms of the form $\langle 2, 3, 4, a_4, a_5\rangle$ *listed in Table 1 are prime-universal.*

PROOF. Let f be one of the six quaternary forms given above. Let

$$\alpha = \begin{cases} 7 & \text{if } f = \langle 2, 3, 4, 7\rangle, \\ 13 & \text{if } f = \langle 2, 3, 4, 13\rangle, \\ 3 & \text{otherwise,} \end{cases}$$

and let g be the ternary subform such that $f = g \perp \langle \alpha\rangle$. Note that g represents all even integers except those of the form

$$\begin{cases} 4^s(16t + 10) & \text{if } g = \langle 2, 3, 4\rangle \text{ or } \langle 2, 4, 12\rangle, \\ 4^s(16t + 14) & \text{if } g = \langle 2, 4, 4\rangle, \\ 4^s(32t + 20) & \text{if } g = \langle 2, 4, 6\rangle, \\ 25^s(50t + \{20 \text{ or } 30\}) & \text{if } g = \langle 2, 4, 10\rangle. \end{cases}$$

For the proof of the case where $g = \langle 2, 3, 4\rangle$, see the proof of Theorem 2.1; for all the other cases, note that the class number of g is 1.

Since one may check directly that $p \to f$ for any prime p such that $p \le 317$ except the one prime given above, we assume that $p \ge 331$. One may easily check that

$$p - \alpha \cdot d^2 \to g,$$

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

where

$$d = \begin{cases} 5 & \text{if } \ell = \langle 2, 4, 10\rangle, \\ 1, 3, \text{ or } 5 & \text{otherwise, defined according to the residue of } p \text{ modulo } 32. \end{cases}$$

Therefore, $p \to f$. Now, the proof of the last assertion is straightforward. □

THEOREM 3.7. *The quadratic form* $f = \langle 2, 3, 6, 7\rangle$ *represents all primes except* 23, 47 *and* 67. *Hence, the quadratic forms*

$$\langle 2, 3, 6, 6, 7\rangle, \quad \langle 2, 3, 6, 7, a_5\rangle \quad \text{and} \quad \langle 2, 3, 6, 7, a_5, a_6\rangle$$

listed in Table 1 are prime-universal. Moreover,

$$\begin{array}{ll} \langle 2, 3, 6, 7, 19\rangle, \quad \langle 2, 3, 6, 7, 22\rangle & \textit{represent all primes except } 23, \\ \langle 2, 3, 6, 7, 20\rangle & \textit{represents all primes except } 67. \end{array}$$

PROOF. The class number of $g = \langle 2, 3, 6\rangle$ is 1. Thus, $Q(\text{gen}(g)) = Q(g)$ and g represents all nonnegative integers except those of the forms $4^s(8t + 7)$ and $9^s(3t + 1)$ for some nonnegative integers s and t.

Since one may directly check that $p \to f$ for any prime p such that $p \le 251$ except 23, 47 and 67, we assume that $p \ge 257$. Then, one may easily check that

$$p - 7 \cdot d^2 \to g,$$

where

$$d = \begin{cases} 0 & \text{if } p \equiv 5, 11, 17 \pmod{24}, \\ 2 & \text{if } p \equiv 1, 7, 13 \pmod{24}, \\ 4 & \text{if } p \equiv 19 \pmod{24}, \\ 6 & \text{if } p \equiv 23 \pmod{24}. \end{cases}$$

Therefore, $p \to f$. Now, the proof of the last assertion is straightforward. □

THEOREM 3.8. *The quadratic form* $\langle 2, 3, 5, 19\rangle$ *represents all primes except* 43. *Hence, the quadratic form* $\langle 2, 3, 5, 19, 19\rangle$ *is prime-universal. Moreover, the quadratic forms* $\langle 2, 3, 5, 7, a_5\rangle$, $\langle 2, 3, 7, a_4, a_5\rangle$ *and* $\langle 2, 3, 7, 7, 7, 10\rangle$ *listed in Table 1 are prime-universal.*

PROOF. Since 19 is not divisible by 7, the quadratic form $\langle 2, 3, 5, 19\rangle$ represents every prime $p \ge 36 \times 19 = 684$ (see the proof of Theorem 2.2). One may easily check that $\langle 2, 3, 5, 19\rangle$ represents all primes less than 684 except 43. Also, since $\langle 2, 3, 5, 19, 19\rangle$ represents 43, it is prime-universal.

Now, we prove the 'moreover' part of the theorem. Let $f = \langle 2, 3, 7, \alpha, \beta\rangle$ be one of the quadratic forms that we should prove to be prime-universal. (For the quadratic form $\langle 2, 3, 5, 7, a_5\rangle$, we let $\alpha = 5$ and $\beta = a_5$. We defer the senary quadratic form $\langle 2, 3, 7, 7, 7, 10\rangle$ for a moment.) Since one may easily check that $p \to f$ for any prime p such that $p \le 13121$, we assume that $p \ge 13127$. Note that the class number of

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

$g = \langle 2, 3, 7\rangle$ is 3 and all isometric classes in the genus are

$$g = \langle 2, 3, 7\rangle, \quad g_1 = \langle 1, 3, 14\rangle \quad \text{and} \quad g_2 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 9 \end{pmatrix}.$$

Now, one may easily check that

$$g_1 \prec_{3,0} g \quad \text{and} \quad g_2 \prec_{3,0} g.$$

Therefore, $Q(\text{gen}(g)) \cap 3\mathbb{Z} \subset Q(g)$, and consequently g represents all nonnegative odd integers that are multiples of 3. In the case where neither α nor β is divisible by 3, one may easily check that

$$p - \alpha \cdot d^2 - \beta \cdot e^2 \to g$$

for some integers $d, e \in \{0, 1, 2\}$. Therefore, $p \to f = \langle 2, 3, 7, \alpha, \beta\rangle$ in this case, and we may also have $p \to \langle 2, 3, 7, 7, 7, 10\rangle$.

Now, the remaining quadratic forms f under consideration are

$$\begin{array}{llll} \langle 2, 3, 7, 9, \beta\rangle & \text{with } \beta = 11, 13, & \langle 2, 3, 7, 10, \beta\rangle & \text{with } \beta = 12, 15, 18, 21, \\ \langle 2, 3, 7, 11, \beta\rangle & \text{with } \beta = 12, 15, & \langle 2, 3, 7, 12, 13\rangle, & \langle 2, 3, 7, 13, 15\rangle. \end{array}$$

One may check by a MAPLE-based computer program that

$$g_1 \prec_{30,r} g \quad \text{and} \quad g_2 \prec_{30,r} g$$

for any integer r in $A_{30} = \{0, 2, 3, 6, 8, 9, 10, 12, 15, 18, 20, 21, 22, 24, 27, 28\}$. Therefore, for any $a \in A_{30}$, $Q(\text{gen}(g)) \cap S_{30,a} \subset Q(g)$, and consequently g represents all nonnegative integers in the set

$$M_{30} = \{m \mid m \not\equiv 0, 6, 22, 24 \pmod{32},\ m \equiv a \pmod{30} \text{ for some } a \in A_{30}\}.$$

Using this, for $\gamma = 9, 11, 13, 21$, one may check that

$$p - \gamma \cdot d^2 \to g$$

for some $0 \le d \le 25$, defined according to the residue of p modulo $32 \cdot 15$. Therefore, $p \to \langle 2, 3, 7, \gamma\rangle$. This proves the prime-universality of f except for those forms with $\alpha = 10$ and $\beta = 12, 15, 18$, namely,

$$\langle 2, 3, 7, 10, 12\rangle, \quad \langle 2, 3, 7, 10, 15\rangle \quad \text{and} \quad \langle 2, 3, 7, 10, 18\rangle.$$

To prove these cases, one may check by a MAPLE-based computer program that

$$g_1 \prec_{42,r} g \quad \text{and} \quad g_2 \prec_{42,r} g$$

for any r in $A_{42} = \{0, 3, 6, 7, 9, 12, 14, 15, 18, 21, 24, 27, 28, 30, 33, 35, 36, 39\}$. Therefore, for any $a \in A_{42}$, $Q(\text{gen}(g)) \cap S_{42,a} \subset Q(g)$, and consequently g represents all nonnegative integers in the set

$$M_{42} = \{m \mid m \not\equiv 0, 6, 22, 24 \pmod{32},\ m \equiv a \pmod{42} \text{ for some } a \in A_{42}\}.$$

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

TABLE 2. Diagonal forms representing all primes but one.

f	Exception of f
$\langle 1,3,4\rangle$	2
$\langle 1,1,6\rangle$	3
$\langle 1,2,6,10\rangle$	5
$\langle 1,1,1,9\rangle$	7
$\langle 2,3,3,4\rangle$, $\langle 2,3,4,12\rangle$	13
$\langle 2,2,2,3\rangle$, $\langle 2,3,4,4\rangle$, $\langle 2,3,4,7\rangle$, $\langle 2,3,7,11\rangle$, $\langle 2,3,7,13\rangle$	17
$\langle 2,3,4,6\rangle$, $\langle 2,3,4,10\rangle$, $\langle 2,3,4,13\rangle$, $\langle 2,3,6,7,19\rangle$, $\langle 2,3,6,7,22\rangle$	23
$\langle 2,2,3,17\rangle$	41
$\langle 2,3,5,19\rangle$	43
$\langle 2,3,6,7,20\rangle$	67

Using this, for $\alpha = 10$ and $\beta = 12, 15, 18$, one may check that

$$n = p - \alpha \cdot d^2 - \beta \cdot e^2 \to g$$

for some integers $d \in \{0,1,2\}$ and $0 \le e \le 6$, defined according to the residue of p modulo $32 \cdot 21$. Therefore, $n \to f$ in this case. This completes the proof. □

REMARK 3.9. From the proof of Theorem 3.8, one may verify that

$\langle 2,3,7,9\rangle$	represents all primes except 13 and 97,
$\langle 2,3,7,11\rangle$	represents all primes except 17,
$\langle 2,3,7,13\rangle$	represents all primes except 17,
$\langle 2,3,10,21\rangle$	represents all primes except 13, 17, 43 and 47.

Now, we are ready to prove Theorems 3.1 and 1.1.

PROOF OF THEOREM 3.1. The properness can be checked through a straightforward calculation. The prime-universality of each diagonal quadratic form in Table 1 follows from Theorems 3.3–3.8. □

PROOF OF THEOREM 1.1. Note that if we repeat the proof of Theorem 3.2 under the assumption that f represents all primes in $\mathcal{S}$, we arrive at the same conclusion. Also, note that for each prime $p \in \mathcal{S}$, some quadratic forms representing all primes except p are given in Table 2. The representability of primes for each of the first four quadratic forms $\langle 1,3,4\rangle$, $\langle 1,1,6\rangle$, $\langle 1,2,6,10\rangle$ and $\langle 1,1,1,9\rangle$ in Table 2 can be proved as usual, since the class number of each of the forms $\langle 1,3,4\rangle$, $\langle 1,1,6\rangle$, $\langle 1,2,6\rangle$ and $\langle 1,1,1\rangle$

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press

is 1. Representability of primes for each of the other quadratic forms is proved in Theorems 3.3–3.8 and Remark 3.9. Therefore, the set S is minimal. □

REMARK 3.10. As pointed out in [2], Bhargava asserted that if any quadratic form, which is not necessarily diagonal, represents

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 67,\ 73,$$

then it is prime-universal. However, no proof of this has appeared in the literature to the authors' knowledge.

References

[1] M. Bhargava, 'On the Conway–Schneeberger fifteen theorem', *Contemp. Math.* **272** (2000), 27–38.
[2] G. Doyle and K. S. Williams, 'Prime-universal quadratic forms $ax^2 + by^2 + cz^2$and $ax^2 + by^2 + cz^2 + dw^2$', *Bull. Aust. Math. Soc.* **101** (2020), 1–12.
[3] J. Ju, B.-K. Oh and B. Seo, 'Ternary universal sums of generalized polygonal numbers', *Int. J. Number Theory* **15** (2019), 655–675.
[4] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Tracts in Mathematics, 106 (Cambridge University Press, Cambridge, 1993).
[5] B.-K. Oh, 'Regular positive ternary quadratic forms', *Acta Arith.* **147** (2011), 233–243.
[6] B.-K. Oh, 'Ternary universal sums of generalized pentagonal numbers', *J. Korean Math. Soc.* **48** (2011), 837–847.
[7] O. T. O'Meara, *Introduction to Quadratic Forms* (Springer Verlag, New York, 1963).

JANGWON JU, Department of Mathematics,
University of Ulsan, Ulsan, 44610, Republic of Korea
e-mail: jangwonju@ulsan.ac.kr

DAEJUN KIM, Research Institute of Mathematics,
Seoul National University, Seoul 08826, Korea
e-mail: goodkdj@snu.ac.kr

KYOUNGMIN KIM, Department of Mathematics,
Sungkyunkwan University, Suwon 16419, Korea
e-mail: kiny30@skku.edu

MINGYU KIM, Department of Mathematics,
Sungkyunkwan University, Suwon 16419, Korea
e-mail: kmg2562@skku.edu

BYEONG-KWEON OH, Department of Mathematical Sciences
and Research Institute of Mathematics, Seoul National University,
Seoul 08826, Korea
e-mail: bkoh@snu.ac.kr

https://doi.org/10.1017/S000497272000101X Published online by Cambridge University Press