involve

Sums of squares in quaternion rings

Anna Cooke, Spencer Hamblen and Sam Whitfield

Sums of squares in quaternion rings

Anna Cooke, Spencer Hamblen and Sam Whitfield

(Communicated by Michael E. Zieve)

Lagrange's four squares theorem states that any positive integer can be expressed as the sum of four integer squares. We investigate the analogous question for quaternion rings, focusing on squares of elements of quaternion rings with integer coefficients. We determine the minimum necessary number of squares for infinitely many quaternion rings, and give global upper and lower bounds.

1. Introduction and definitions

Waring's problem.

Theorem 1.1 (Waring's problem/Hilbert–Waring theorem). *For every integer $k \geq 2$ there exists a positive integer $g(k)$ such that every positive integer is the sum of at most $g(k)$ k-th powers of integers.*

Generalizations of Waring's problem have been studied in a variety of settings (for example, number fields [Siegel 1921] and polynomial rings over finite fields [Car 1973]). Additionally, calculation of the exact values of $g(k)$ for all $k \geq 2$ was completed only relatively recently. For an excellent and thorough exposition of the research on Waring's problem and its generalizations, see Vaughan and Wooley [2002]. We will examine a generalization of Waring's problem to quaternion rings.

Definition 1.2. Let $Q_{a,b}$ denote the quaternion ring

$$\{\alpha_0 + \alpha_1 \boldsymbol{i} + \alpha_2 \boldsymbol{j} + \alpha_3 \boldsymbol{k} \mid \alpha_n, a, b \in \mathbb{Z}, \boldsymbol{i}^2 = -a, \boldsymbol{j}^2 = -b, \boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}\}.$$

Let $Q_{a,b}^n$ denote the additive group generated by all n-th powers in $Q_{a,b}$.

Note here that $\boldsymbol{k}^2 = -ab$, and if $a = b = 1$, we have what are called the *Lipschitz quaternions*. We then have the following analogue of Waring's Problem.

Conjecture 1.3. For every integer $k \geq 2$ and all positive integers a, b there exists a positive integer $g_{a,b}(k)$ such that every element of $Q_{a,b}^k$ can be written as the sum of at most $g_{a,b}(k)$ k-th powers of elements of $Q_{a,b}$.

Main results. We will examine sums of squares in quaternion rings, that is, when $k = 2$. We are therefore looking to generalize Lagrange's four squares theorem, the inspiration for Waring's initial conjecture.

Theorem 1.4 (Lagrange's four squares theorem). *Any positive integer can be written as the sum of four integer squares.*

We prove the following general result giving the upper and lower bounds for $g_{a,b}(2)$ for any positive integers a and b.

Theorem 1.5. *For all positive integers a, b, we have*

$$3 \leq g_{a,b}(2) \leq 5.$$

Additionally, each possible value of $g_{a,b}(2)$ (i.e., 3, 4, and 5) occurs infinitely often.

We prove the general upper and lower bounds in Section 2; more specific results, including the proof of the latter half of Theorem 1.5, are given in Section 3. Note that for any positive integers a and b, the quaternion rings $Q_{a,b}$ and $Q_{b,a}$ are naturally isomorphic; we therefore generally assume $a \leq b$.

2. Squares of quaternions — upper and lower bounds

In this section we prove the upper and lower bounds of Theorem 1.5. We will use the following classical result on sums of squares extensively; for this result and a more general look at sums of squares of integers, see [Grosswald 1985].

Theorem 2.1 (Legendre's three squares theorem). *A positive integer N can be written as the sum of three integer squares if and only if N is not of the form $4^m(8\ell + 7)$ with ℓ, m nonnegative integers.*

To study $g_{a,b}(2)$, we first need to establish the general form of squares of quaternions, and to characterize elements of $Q_{a,b}^2$.

Let $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in Q_{a,b}$. We call α_0 the *real* part of α and $\alpha_1 i + \alpha_2 j + \alpha_3 k$ the *pure* part of α, with $\alpha_1, \alpha_2, \alpha_3$ the *pure coefficients*. Then note that

$$\alpha^2 = \alpha_0^2 - a\alpha_1^2 - b\alpha_2^2 - ab\alpha_3^2 + 2\alpha_0\alpha_1 i + 2\alpha_0\alpha_2 j + 2\alpha_0\alpha_3 k. \quad (1)$$

We therefore have that all the pure coefficients of squares of quaternions, and therefore the pure coefficients of all elements of $Q_{a,b}^2$, are even. Additionally, any set of even pure coefficients can be achieved (for example, set $\alpha_0 = 1$ in (1)), as can any negative real coefficient (since we are assuming $a, b \geq 1$). We therefore have

$$Q_{a,b}^2 = \{\alpha_0 + 2\alpha_1 i + 2\alpha_2 j + 2\alpha_3 k \mid \alpha_n \in \mathbb{Z}\}. \quad (2)$$

In 1946, Niven computed $g_{1,1}(2)$ and studied extensions of Waring's problem in other various settings, including complex numbers.

Theorem 2.2 [Niven 1946]. *Every element in $Q_{1,1}^2$ can be written as the sum of at most three squares in $Q_{1,1}$. Additionally, $6 + 2i$ is not expressible as the sum of two squares in $Q_{1,1}$, so $g_{1,1}(2) = 3$.*

We extend this result to $Q_{a,b}$ for all positive integers a, b. The proofs for the lower bounds are similar to Niven's work (i.e., finding examples); the proofs for the upper bounds take more work.

Lemma 2.3. *Suppose a and b are positive integers.*

(1) *If $a \equiv 1$ or $2 \bmod 4$, then $2 + 2i$ is not expressible as the sum of two squares in $Q_{a,b}$.*

(2) *If $a \equiv 0$ or $3 \bmod 4$, then $4 + 2i$ is not expressible as the sum of two squares in $Q_{a,b}$.*

Proof. Let $x = x_0 + x_1 i + x_2 j + x_3 k$, and $y = y_0 + y_1 i + y_2 j + y_3 k$, with $x_m, y_n \in \mathbb{Z}$ for $m, n \in \{0, 1, 2, 3\}$. Then if $x^2 + y^2 = \alpha$ with $\alpha = \alpha_0 + 2\alpha_1 i + 2\alpha_2 j + 2\alpha_3 k \in Q_{a,b}^2$, we have

$$\alpha_0 = x_0^2 + y_0^2 - a(x_1^2 + y_1^2) - b(x_2^2 + y_2^2) - ab(x_3^2 + y_3^2), \tag{3}$$

$$\alpha_1 = x_0 x_1 + y_0 y_1, \tag{4}$$

$$\alpha_2 = x_0 x_2 + y_0 y_2, \tag{5}$$

$$\alpha_3 = x_0 x_3 + y_0 y_3. \tag{6}$$

Case 1 ($a \equiv 1, 2 \bmod 4$): Suppose $a \equiv 1, 2 \bmod 4$, and let $\alpha = 2 + 2i$, so $\alpha_0 = 2$, $\alpha_1 = 1$, and $\alpha_2 = \alpha_3 = 0$. Since $\alpha_1 = 1$, (4) and Bézout's identity then imply that x_0 and y_0 must be relatively prime, since they have a linear combination equal to 1. Then, by (5), we must have $x_0 \mid y_2$ and $y_0 \mid x_2$. However, since $b \geq 1$, if $x_2, y_2 \neq 0$, (3) then implies $\alpha_0 \leq 0$. As $\alpha_0 = 2$, we must have $x_2 = y_2 = 0$. A similar argument using (6) implies $x_3 = y_3 = 0$.

By (4), since $\alpha_1 = 1$, we have that exactly one of the products $x_0 x_1$ and $y_0 y_1$ must be odd; we therefore assume y_0 and y_1 are odd. The following table shows that (3) has no solutions mod 4 if $a \equiv 1, 2 \bmod 4$:

x_0	x_1	equation (3) mod 4
even	odd	$\alpha_0 = 2 \equiv 1 - 2a$
even	even	$\alpha_0 = 2 \equiv 1 - a$
odd	even	$\alpha_0 = 2 \equiv 2 - a$

Therefore $2 + 2i$ cannot be written as the sum of two squares in $Q_{a,b}$.

Case 2 ($a \equiv 0, 3 \bmod 4$): Suppose $a \equiv 0, 3 \bmod 4$. Then let $\alpha = 4 + 2i$. By the same argument as above, we get three possibilities for (3) mod 4, none of which have solutions. Therefore $4 + 2i$ cannot be written as the sum of two squares in $Q_{a,b}$. $\square$

As both $2+2i$ and $4+2i$ are in $Q^2_{a,b}$, this gives us the lower bound in Theorem 1.5. We then turn to the upper bound; we establish an algorithm for expressing every element as a sum of squares.

Lemma 2.4. *Every element in $Q^2_{a,b}$ can be written as a sum of at most five squares in $Q_{a,b}$.*

Proof. Let $\alpha = \alpha_0 + 2\alpha_1 i + 2\alpha_2 j + 2\alpha_3 k \in Q^2_{a,b}$; we want to show that we can represent α as a sum of squares of no more than five quaternions.

Let $v = 1 + Ui + \alpha_2 j + \alpha_3 k$ for some $U \in \mathbb{Z}$, and note that

$$\alpha - v^2 = \alpha_0 - 1 + aU^2 + b\alpha_2^2 + ab\alpha_3^2 + 2(\alpha_1 - U)i.$$

If we also let $A = \alpha_0 - 1 + a\alpha_1^2 + b\alpha_2^2 + ab\alpha_3^2$, we have

$$\alpha - v^2 = A + a(U^2 - \alpha_1^2) + 2(\alpha_1 - U)i. \tag{7}$$

We then have three cases:

(1) $A \geq 0$,

(2) $A < 0$ and A cannot be written as $4^m(8\ell + 7)$ for any nonnegative integer m and $\ell \in \mathbb{Z}$, and

(3) $A < 0$ and $A = 4^m(8\ell + 7)$ for some nonnegative integer m and $\ell \in \mathbb{Z}$.

Case 1 ($A \geq 0$): If $A \geq 0$, then by Theorem 1.4, there exists $w, x, y, z \in \mathbb{Z}$ such that $A = w^2 + x^2 + y^2 + z^2$. Letting $U = \alpha_1$, (7) becomes

$$\alpha - v^2 = A = w^2 + x^2 + y^2 + z^2,$$

so we can represent α as the sum of five squares.

Case 2 ($A < 0$ and $A \neq 4^m(8\ell + 7)$): Here we again let $U = \alpha_1$, so $\alpha - v^2 = A$. Then let e_1 be the greatest exponent of 4 such that 4^{e_1} divides A, and let e_2 be the least exponent of 4 such that $4^{2e_2} + A \geq 0$. We then let $e = \max\{e_1 + 1, e_2\}$, and let $w = 4^e i$.

We then have $\alpha - v^2 - w^2 = A + a4^{2e} \geq 0$. Additionally, since $2e \geq 2e_1 + 2$, if A cannot be written in the form $4^m(8\ell + 7)$, then neither can $A + 4^{2e}$. Therefore by Theorem 2.1, there exist $x, y, z \in \mathbb{Z}$ such that $A + 4^{2e} = x^2 + y^2 + z^2$. So

$$\alpha - v^2 - w^2 = A + 4^{2e} = x^2 + y^2 + z^2,$$

so we can represent α as the sum of five squares.

Case 3 ($A < 0$ and $A = 4^m(8\ell + 7)$): We first treat the case when $m > 0$. Here we let

$$w = 2^{m-1} + \left(\frac{\alpha_1 - U}{2^{m-1}}\right)i$$

and choose $U = \alpha_1 + 2^{m-1}U_1$, where U_1 satisfies the following three conditions:

(a) $4^{m+1} \mid U_1$,

(b) $U_1 > -(2^m \alpha_1)/(4^{m-1}+1)$, and

(c) $U_1 > (A - 4^{m-1})/a$.

Note that it is always possible to meet these conditions; for example,

$$U_1 = 4^{m+1}|A| \cdot \max\{1, |\alpha_1|\}$$

satisfies all three. We then have

$$\alpha - v^2 - w^2 = (A + a(U^2 - \alpha_1^2) + 2(\alpha_1 - U)i)$$
$$- \left(4^{m-1} + 2(\alpha_1 - U)i - a\left(\frac{\alpha_1 - U}{2^{m-1}}\right)^2\right)$$
$$= A + a(\alpha_1^2 + 2^m \alpha_1 U_1 + 4^{m-1}U_1^2 - \alpha_1^2) - 4^{m-1} + aU_1^2$$
$$= A - 4^{m-1} + aU_1(2^m \alpha_1 + (4^{m-1}+1)U_1).$$

Note that condition (b) on U_1 ensures the quantity in parentheses must be positive, and condition (c) ensures that $\alpha - v^2 - w^2$ is positive. Letting $A = 4^m(8\ell + 7)$ and since 4^{m+1} divides U_1, the remainder of the equation equals $4^{m+1}\ell_1$ for some $\ell_1 \in \mathbb{Z}$, we have

$$\alpha - v^2 - w^2 = 4^m(8\ell + 7) - 4^{m-1} + 4^{m+1}\ell_1$$
$$= 4^{m-1}(4(8\ell + 7) - 1 + 16\ell_1)$$
$$= 4^{m-1}(8(4\ell + 3 + 2\ell_1) + 3).$$

Since this is not of the form excluded by Legendre's Three Squares Theorem, there exist $x, y, z \in \mathbb{Z}$ such that $\alpha - v^2 - w^2 = x^2 + y^2 + z^2$, so we can represent α as the sum of five squares.

Lastly, we treat the case when $A = 8\ell + 7$ for some negative integer ℓ. Here we let $U = \alpha_1 + U_1$ and $w = 1 + U_1 i$, choosing U_1 such that $8 \mid U_1$ and $U_1 > \max\{|A|, |\alpha_1|\}$. Then

$$\alpha - v^2 - w^2 = (A + a(U^2 - \alpha_1^2) + 2(\alpha_1 - U)i) - (1 - U_1 i)^2$$
$$= A + a(2\alpha_1 U_1 + U_1^2) - 1 + aU_1^2$$
$$= 8\ell + 6 + 8\ell_1,$$

where we have $\ell_1 + \ell \geq 0$ by the conditions on U_1. Since this is a positive number that is 6 mod 8, it is expressible as the sum of three integer squares by Legendre's three squares theorem. So we can represent α as the sum of five squares here and in all cases. □

Lemmas 2.3 and 2.4 combined give the bounds for $g_{a,b}(2)$ in Theorem 1.5.

3. Values of $g_{a,b}(2)$

In this section, we establish exact values for $g_{a,b}(2)$ for several infinite families of quaternion rings, and for each of the possible values of $g_{a,b}(2)$. We note that the methods for showing each are different: for example, to show $g_{a,b}(2) = 3$, all we need is an algorithm to express every element in $Q_{a,b}^2$ as a sum of three squares, and to show $g_{a,b}(2) = 5$, all we need is to find an element that cannot be expressed as the sum of four squares.

Quaternion rings with $g_{a,b}(2) = 3$. We examine $Q_{1,b}$, where $b \in \mathbb{N}$. We can view $Q_{1,b}$ as an extension of the Gaussian integers $\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} \mid x, y \in \mathbb{Z}\}$ by adjoining j and k. The following lemma then provides a shortcut for representing elements of $Q_{1,b}$ as sums of squares.

Lemma 3.1 [Niven 1940, Theorem 2]. *The equation $\alpha_0 + 2\alpha_1 i = x^2 + y^2$ is solvable in $\mathbb{Z}[\sqrt{-1}]$ if $\frac{1}{2}\alpha_0$ and α_1 are not both odd integers.*

Note that this lemma also implies that $g_{\mathbb{Z}[\sqrt{-1}]}(2) = 3$.

Theorem 3.2. *For all $b \in \mathbb{N}$, every element in $Q_{1,b}^2$ can be written as the sum of at most three squares in $Q_{1,b}$. Therefore $g_{1,b}(2) = 3$ for all $b \in \mathbb{N}$.*

Proof. Let $\alpha = \alpha_0 + 2\alpha_1 i + 2\alpha_2 j + 2\alpha_3 k \in Q_{1,b}^2$; we wish to find $x, y, z \in Q_{1,b}$ such that $\alpha = x^2 + y^2 + z^2$. Since $\mathbb{Z}[\sqrt{-1}] \subset Q_{1,b}$, Lemma 3.1 implies that it is sufficient to find $z \in Q_{1,b}$ such that $\alpha - z^2 \in \mathbb{Z}[\sqrt{-1}]$ and satisfies the hypotheses of Lemma 3.1.

Therefore, let $z = 1 + Ui + \alpha_2 j + \alpha_3 k$, where $U = 0$ if α_1 is even and $U = 1$ if α_1 is odd. We then examine $\alpha - z^2$:

$$\alpha - z^2 = \alpha_0 + 2\alpha_1 i + 2\alpha_2 j + 2\alpha_3 k - 1 + U^2 + b\alpha_2^2 + b\alpha_3^2 - 2Ui - 2\alpha_2 j - 2\alpha_3 k$$
$$= \alpha_0 - 1 + U^2 + b\alpha_2^2 + b\alpha_3^2 + 2(\alpha_1 - U)i.$$

Note that if α_1 is even, then $U = 0$, so $\alpha_1 - U$ is even; conversely, if α_1 is odd, then $U = 1$, so $\alpha_1 - U$ is again even. We can therefore apply Lemma 3.1 to find $x, y \in \mathbb{Z}[\sqrt{-1}] \subset Q_{1,b}$ such that $\alpha - z^2 = x^2 + y^2$. $\qquad\square$

We note that the proof relies on the fact that squares in the Gaussian integers can be easily characterized. This is not generally true of imaginary quadratic fields (see [Eljoseph 1954; Niven 1940, Theorem 3]).

Quaternion rings with $g_{a,b}(2) = 4$. We combine a standard lower bound proof and a constructive upper bound proof to find a family of quaternion rings with $g_{a,b}(2) = 4$.

Lemma 3.3. *There exist elements in $Q_{4m,4n+3}^2$ that are not the sum of three squares.*

Proof. Suppose that there exist x, y, $z \in Q_{4m,4n+3}$ such that $x^2 + y^2 + z^2 = 9 + 2\boldsymbol{j}$. Letting

$$x = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k},$$
$$y = y_0 + y_1\boldsymbol{i} + y_2\boldsymbol{j} + y_3\boldsymbol{k},$$
$$z = z_0 + z_1\boldsymbol{i} + z_2\boldsymbol{j} + z_3\boldsymbol{k},$$

the resulting equations for the real and $\boldsymbol{j}$ coefficients of $9 + 2\boldsymbol{j}$ are, respectively,

$$x_0^2 + y_0^2 + z_0^2 - 4m(x_1^2 + y_1^2 + z_1^2) - (4n+3)(x_2^2 + y_2^2 + z_2^2)$$
$$- (4m)(4n+3)(x_3^2 + y_3^2 + z_3^2) = 9, \tag{8}$$
$$x_0 x_2 + y_0 y_2 + z_0 z_2 = 1. \tag{9}$$

Examining (8) mod 4, we have

$$x_0^2 + y_0^2 + z_0^2 + x_2^2 + y_2^2 + z_2^2 \equiv 1 \bmod 4. \tag{10}$$

Recall then that for all integers ℓ, we have $\ell^2 \equiv 0 \bmod 4$ (if ℓ is even) or $\ell^2 \equiv 1 \bmod 4$ (if ℓ is odd). From this we have two possibilities that satisfy (10): we must have either 1 or 5 of x_0, y_0, z_0, x_2, y_2, z_2 odd in order for the left side of (10) to sum to 1 mod 4.

If only one of the terms is odd, then the left side of (9) will be even since the lone odd term must be multiplied by an even term, and therefore cannot equal 1. Likewise, if there are five odd terms, the left side of (9) will be the sum of two odd terms and one even term, which cannot sum to 1.

Since (8) and (9) cannot simultaneously be satisfied, $9 + 2\boldsymbol{j}$ cannot be expressed as the sum of three squares in $Q_{4m,4n+3}^2$. □

When a is a sum of two integer squares. When a is a sum of integer squares, we can construct an algorithm to express elements of $Q_{a,b}^2$ as the sum of four squares. This gives us a general result when combined with the lower bound results of Lemma 3.3.

Lemma 3.4. *Every element of $Q_{a,b}^2$ is the sum of at most four squares in $Q_{a,b}$ in the following two cases*:

- $a = n_1^2 + n_2^2$ with $\gcd(n_1, n_2) = 1$; *or*
- $a = n_1^2 + n_2^2$ with $\gcd(n_1, n_2) = 2$ *and* $n_1 \equiv 0 \bmod 4$, *and* $b \not\equiv 0 \bmod 4$.

Note that we allow $n_1 = 0$ only if $n_2 = 1$ or 2; in the latter case we get $a = 4$, which will be useful in light of Lemma 3.3.

Proof. Let $\alpha = \alpha_0 + 2\alpha_1\boldsymbol{i} + 2\alpha_2\boldsymbol{j} + 2\alpha_3\boldsymbol{k}$. If we let $z = 1 + \alpha_1\boldsymbol{i} + \alpha_2\boldsymbol{j} + \alpha_3\boldsymbol{k} \in Q_{a,b}$, then $\alpha - z^2 \in \mathbb{Z}$. We claim that every integer can be represented as the sum of three squares in $Q_{a,b}$; we could then represent α as the sum of four squares.

Let $x = n_1\ell + r$, $y = n_2\ell + s$, and $w = \ell i + \delta j$ for some $\ell, r, s, \delta \in \mathbb{Z}$. We then have

$$x^2 + y^2 + w^2 = (n_1\ell + r)^2 + (n_2\ell + s)^2 + (\ell i + \delta j)^2$$
$$= 2(rn_1 + sn_2)\ell + r^2 + s^2 - b\delta^2. \tag{11}$$

Our method will be to choose r and s to determine a "modulus" $(rn_1 + sn_2)$ and residue class $(r^2 + s^2 - b\delta^2)$. Since ℓ is independent of r and s, we will therefore be able to represent every integer in that residue class (we will only use δ in one particularly troublesome case).

Recall that by Bézout's identity there exist $r_0, s_0 \in \mathbb{Z}$ such that $r_0n_1 + s_0n_2 = \gcd(n_1, n_2) \in \{1, 2\}$; these will inform our choices of r and s. We then have three cases (relabeling if necessary) which we address separately:

(a) n_1 odd, n_2 even, and $\gcd(n_1, n_2) = 1$;

(b) n_1, n_2 odd, and $\gcd(n_1, n_2) = 1$; and

(c) $\frac{1}{2}n_1$ even, $\frac{1}{2}n_2$ odd, and $\gcd(n_1, n_2) = 2$.

Case (a): Our modulus here will be 2. Note that if $r = r_0$, $s = s_0$, and $\delta = 0$, we have from (11)

$$x^2 + y^2 + w^2 = 2\ell + r_0^2 + s_0^2.$$

Next, if $r = r_0 - n_2$, $s = s_0 + n_1$, and $\delta = 0$, (11) yields

$$x^2 + y^2 + w^2 = 2\ell + (r_0 - n_2)^2 + (s_0 + n_1)^2.$$

Recalling that n_1 is assumed to be odd and n_2 is assumed to be even, we necessarily have that $r_0^2 + s_0^2$ and $(r_0 - n_2)^2 + (s_0 + n_1)^2$ cover all residue classes mod 2 with the two equations above. With a proper choice of ℓ, we can therefore directly find $x, y, w \in Q_{a,b}$ such that $\alpha - z^2 = x^2 + y^2 + w^2$, and so we can write α as a sum of four squares in $Q_{a,b}$.

Case (b): Our modulus here will be 4. Since n_1 and n_2 are here both odd, we may assume without loss of generality that r_0 is odd and s_0 is even.

We then use three choices of r and s to represent all possible residue classes mod 4; we let $\delta = 0$ for all subcases. First, let $r = r_0$ and $s = s_0$. Equation (11) is then

$$x^2 + y^2 + w^2 = 2\ell + r_0^2 + s_0^2,$$

which represents all odd integers, since r_0 is odd and s_0 is even.

If we then let $r = 2r_0$ and $s = 2s_0$, (11) then yields

$$x^2 + y^2 + w^2 = 4\ell + 4(r_0^2 + s_0^2).$$

This allows us to represent all multiples of 4.

If, instead, we let $r = 2r_0 - n_2$ and $s = 2s_0 + n_1$, (11) then yields

$$x^2 + y^2 + w^2 = 4\ell + (2r_0 - n_2)^2 + (2s_0 + n_1)^2.$$

As $2r_0 - n_2$ and $2s_0 + n_1$ are necessarily both odd, this allows us to represent all integers that are 2 mod 4. Combined with the above two choices, this covers all residue classes mod 4, and so, similarly to Case (a), we are done.

Case (c): Our modulus here will be 8. We will need four choices of r and s, along with letting $\delta = 1$ if $\alpha - z^2 \equiv 3$ mod 4. Note that we are assuming $n_2 \equiv 2$ mod 4, so we know that $\frac{1}{2}n_2$ is odd. Additionally, we may assume that s_0 is odd and r_0 is even.

First, let $r = r_0$ and $s = s_0$. Equation (11) is then

$$x^2 + y^2 + w^2 = 4\ell + r_0^2 + s_0^2. \tag{12}$$

If we let $r = r_0 - \frac{1}{2}n_2$ and $s = s_0 + \frac{1}{2}n_1$, (11) yields

$$x^2 + y^2 + w^2 = 4\ell + (r_0 - \tfrac{1}{2}n_2)^2 + (s_0 + \tfrac{1}{2}n_1)^2. \tag{13}$$

Since s_0 and $\frac{1}{2}n_2$ are both odd, while r_0 and $\frac{1}{2}n_1$ are even, (12) represents all integers that are 1 mod 4, while (13) represents all integers that are 2 mod 4.

Next, let $r = 2r_0$ and $2s = s_0$. Equation (11) is then

$$x^2 + y^2 + w^2 = 8\ell + 4(r_0^2 + s_0^2).$$

As r_0 is even and s_0 is odd, this represents all integers that are 4 mod 8.

If we let $r = 2r_0 - n_2$ and $s = 2s_0 + n_1$, (11) yields

$$x^2 + y^2 + w^2 = 8\ell + (2r_0 - n_2)^2 + (2s_0 + n_1)^2.$$

Since $2r_0 \equiv n_1 \equiv 0$ mod 4 and $2s_0 \equiv n_2 \equiv 2$ mod 4, this represents all integers that are 0 mod 8, and we therefore have all integers that are 0 mod 4.

We still need to represent integers that are 3 mod 4; this is where δ comes in. If we let $\delta = 1$, (11) becomes

$$x^2 + y^2 + w^2 = 2(rn_1 + sn_2)\ell + r^2 + s^2 - b.$$

If $b \not\equiv 0$ mod 4 and $\alpha - z^2 \equiv 3$ mod 4, this allows us to represent $\alpha - z^2 + b$ via one of the choices of r and s above. Therefore we can always represent α as the sum of four squares in $Q_{a,b}$ in Case (c). $\qquad\square$

If $a = n_1^2 + n_2^2$ with $\gcd(n_1, n_2) = 2$, then necessarily $a \equiv 0$ mod 4; we can then combine Lemmas 3.3 and 3.4 to get the following theorem.

Theorem 3.5. *Suppose* $a = n_1^2 + n_2^2$, *where* $n_1, n_2 \in \mathbb{N}$ *are such that* $\gcd(n_1, n_2) = 2$, *and* $m \in \mathbb{N}$. *Then* $g_{a,4m+3} = 4$.

Specifically, if $n_1 = 0$ and $n_2 = 2$, we get that $g_{4,4m+3} = 4$ for all $m \in \mathbb{N}$.

Quaternion rings with $g_{a,b}(2) = 5$. In this section, we find $a, b \in \mathbb{N}$ such that there exists elements of $Q_{a,b}$ that require five squares, which by Lemma 2.4 gives us that $g_{a,b}(2) = 5$.

Theorem 3.6. *For all* $m, n \in \mathbb{N}$, *there are elements of* $Q_{4m,4n}^2$ *that are not the sum of four squares in* $Q_{4m,4n}$. *Therefore* $g_{4m,4n}(2) = 5$ *for all* $m, n \in \mathbb{N}$.

Proof. Suppose that there exist $w, x, y, z \in Q_{4m,4n}$ such that $w^2 + x^2 + y^2 + z^2 = 8 + 2k$. Letting

$$w = w_0 + w_1 i + w_2 j + w_3 k,$$
$$x = x_0 + x_1 i + x_2 j + x_3 k,$$
$$y = y_0 + y_1 i + y_2 j + y_3 k,$$
$$z = z_0 + z_1 i + z_2 j + z_3 k,$$

the resulting equations for the real, i, j, and k coefficients are, respectively,

$$w_0^2 + x_0^2 + y_0^2 + z_0^2 - 4m(w_1^2 + x_1^2 + y_1^2 + z_1^2)$$
$$- 4n(w_2^2 + x_2^2 + y_2^2 + z_2^2) - 16mn(w_3^2 + x_3^2 + y_3^2 + z_3^2) = 8, \tag{14}$$
$$w_0 w_1 + x_0 x_1 + y_0 y_1 + z_0 z_1 = 0, \tag{15}$$
$$w_0 w_2 + x_0 x_2 + y_0 y_1 + z_0 z_1 = 0, \tag{16}$$
$$w_0 w_3 + x_0 x_3 + y_0 y_3 + z_0 z_3 = 1. \tag{17}$$

We start by examining (17) mod 2, and note that at least one of w_0, x_0, y_0, z_0 must be odd, as otherwise the sum of the terms would be even. Since at least one of these terms must be odd, we assume without loss of generality that $w_0 \equiv 1 \mod 2$. With that in mind, (14) mod 8 is

$$1 + x_0^2 + y_0^2 + z_0^2 - 4m(w_1^2 + x_1^2 + y_1^2 + z_1^2) - 4n(w_2^2 + x_2^2 + y_2^2 + z_2^2) \equiv 0 \mod 8. \tag{18}$$

Recall then that for all odd ℓ, we have $\ell^2 \equiv 1 \mod 8$, and for all even ℓ, $\ell^2 \equiv 0$ or 4 mod 8. Since the left side of (18) is 1 added to three squares followed by multiples of 4; in order for it to sum to 0 mod 8, the values of x_0^2, y_0^2, z_0^2 must all be 1 mod 8. So $w_0^2, x_0^2, y_0^2, z_0^2$ are odd.

Then $w_0^2 + x_0^2 + y_0^2 + z_0^2 \equiv 4 \mod 8$, so an odd number of $w_1^2, x_1^2, y_1^2, z_1^2$ or $w_2^2, x_2^2, y_2^2, z_2^2$ must be odd to contribute an additional 4 mod 8. But this forces an odd number of odd terms on the left side of either (15) or (16), which contradicts their even sums.

Since the equations required for $8 + 2k$ to be a sum of four squares in $Q_{4m,4n}$ cannot hold, $8 + 2k$ cannot be expressed as a sum of four squares in $Q_{4m,4n}$. □

4. Other individual cases

We were able to find $g_{a,b}(2)$ in several other cases for specific values of a and b. We include these here for completeness but also to demonstrate the methods used, which vary significantly from those used in Section 3.

Theorem 4.1. $$g_{2,2}(2) = g_{2,3}(2) = 3.$$

These proofs rely of the theory of quadratic forms — specifically, representations of integers via ternary diagonal quadratic forms. A ternary diagonal quadratic form is a function $f(x, y, z) = rx^2 + sy^2 + tz^2$; for our purposes, we have $r, s, t \in \mathbb{N}$. We say a ternary diagonal quadratic form *represents* $n \in \mathbb{N}$ if there exists an integer solution to $f(x, y, z) = n$. Lastly, we say that a ternary diagonal quadratic form is *regular* if the only positive integers it does not represent coincide with certain arithmetic progressions. The most common example of this is Legendre's three squares theorem: every positive integer not of the form $4^m(8\ell+7)$ can be represented in the form $x^2 + y^2 + z^2$ with $x, y, z \in \mathbb{Z}$. For more information on representation of integers via quadratic forms, see [Jones and Pall 1939] or (more recently) [Hanke 2004].

Noting that
$$(x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k})^2 = -(ax^2 + by^2 + abz^2),$$

for our theorem, we will examine the expressions $2x^2 + 2y^2 + 4z^2$ and $2x^2 + 3y^2 + 6z^2$. Dickson has a complete list of regular diagonal ternary quadratic forms, from whence we get the following lemma.

Lemma 4.2 [Dickson 1939, Table 5]. (1) *Let* $f_{2,2}(x, y, z) = 2x^2 + 2y^2 + 4z^2$. *Then* $f_{2,2}$ *represents all even integers not of the form* $2 \cdot 4^n(16\ell + 14)$.

(2) *Let* $f_{2,3}(x, y, z) = 2x^2 + 3y^2 + 6z^2$. *Then* $f_{2,3}$ *represents all positive integers not of the form* $4^n(8\ell + 7)$ *or* $3m + 1$.

Proof of Theorem 4.1. Let $\alpha = \alpha_0 + 2\alpha_1\boldsymbol{i} + 2\alpha_2\boldsymbol{j} + 2\alpha_3\boldsymbol{k} \in Q_{a,b}^2$. Then, letting $x = 1 + \alpha_1\boldsymbol{i} + \alpha_2\boldsymbol{j} + \alpha_3\boldsymbol{k}$, we have

$$\alpha - x^2 = \alpha_0 - 1 + a\alpha_1^2 + b\alpha_2^2 + ab\alpha_3^2 := A \in \mathbb{Z}. \tag{19}$$

It then suffices to find elements $y, z \in Q_{a,b}$ with $y = y_0 \in \mathbb{Z}$ and $z = z_1\boldsymbol{i} + z_2\boldsymbol{j} + z_3\boldsymbol{k}$ such that

$$A = y^2 + z^2 = y_0^2 - az_1^2 - bz_2^2 - abz_3^2, \tag{20}$$

as we would then have $\alpha = x^2 + y^2 + z^2$.

Case 1 ($a = b = 2$): In light of Lemma 4.2 and the regularity of the associated quadratic form, we know that if we can represent the residue class of A mod 32, then we can find y_0, z_0, z_1, z_2 that satisfy (20).

We let $S_{a,b;m}$ be the set of residue classes mod m that are completely represented by

$$f_{a,b}(z_0, z_1, z_2) = az_0^2 + bz_1^2 + abz_2^2.$$

For example, $2 \in S_{2,2;32}$ since $f_{2,2}(1, 0, 0) = 2$, $2 \not\equiv 2 \cdot 4^n(16\ell + 14)$ mod 32 for any n, $\ell \in \mathbb{N}$, and by Lemma 4.2 $f_{2,2}$ represents all even integers not of the form $2 \cdot 4^n(16\ell + 14)$. But $16 \notin S_{2,2;32}$ since $16 \equiv 2 \cdot 4^1(16\ell + 14)$ mod 32.

When $a = b = 2$ and $m = 32$, we have

$$S_{2,2;32} = \{2, 4, 6, 8, 10, 12, 14, 18, 20, 22, 24, 26, 30\};$$

our goal then is to show that for any $A \in \mathbb{Z}$, we can find $y_0 \in \mathbb{Z}$ and $s \in S_{2,2;32}$ such that $A \equiv y_0^2 - s$ mod 32. By Lemma 4.2, there would then exist $z = z_1 \boldsymbol{i} + z_2 \boldsymbol{j} + z_3 \boldsymbol{k} \in Q_{2,2}$ such that $-s \equiv z^2$ mod 32 and $A = y_0^2 + z^2$.

We can then break this search for y_0 and s into cases:

- if $A \not\equiv 0, 1, 4, 5, 16,$ or 17 mod 32, then A is congruent to either $-s$ or $1 - s$ for some $s \in S_{2,2;32}$;

- if $A \equiv 0, 16$ mod 32, then $A \equiv 4 - s$ mod 32 for $s = 4, 20 \in S_{2,2;32}$;

- if $A \equiv 1, 5, 17$ mod 32, then $A \equiv 9 - s$ mod 32 for $s = 8, 4, 24 \in S_{2,2;32}$; and

- if $A \equiv 4$ mod 32, then $A \equiv 16 - s$ mod 32 for $s = 12 \in S_{2,2;32}$.

Therefore we can represent A as a sum of two squares from $Q_{2,2}$, and so we can always express α as a sum of three squares from $Q_{2,2}$.

Case 2 ($a = 2$, $b = 3$): We again use the set $S_{a,b;m}$, letting $m = 24$; this yields

$$S_{2,3;24} = \{2, 3, 5, 6, 9, 11, 14, 17, 18, 21\}.$$

Similarly to Case 1, we search for $y_0 \in \mathbb{Z}$ and $s \in S_{2,3;24}$ such that $A \equiv y_0^2 - s$ mod 24:

- if $A \not\equiv 0, 1, 2, 5, 9, 12,$ or 17 mod 24, then A is congruent to either $-s$ or $1 - s$ for some $s \in S_{2,3;24}$;

- if $A \equiv 1, 2, 17$ mod 24, then $A \equiv 4 - s$ mod 24 for $s = 3, 2, 11 \in S_{2,3;24}$;

- if $A \equiv 0, 12$ mod 24, then $A \equiv 9 - s$ mod 24 for $s = 9, 21 \in S_{2,3;24}$;

- if $A \equiv 5$ mod 24, then $A \equiv 16 - s$ mod 24 for $s = 11 \in S_{2,3;24}$; and

- if $A \equiv 9$ mod 24, then $A \equiv 36 - s$ mod 24 for $s = 3 \in S_{2,3;24}$.

Therefore as above we can always express α as a sum of three squares from $Q_{2,3}$. Given the lower bound for $g_{a,b}(2)$ in Lemma 2.3, we therefore have $g_{a,b}(2) = 3$ in both cases. $\qquad\square$

The proof of Theorem 4.1 relies entirely on the regularity of the associated ternary quadratic forms given in Lemma 4.2. There are, unfortunately, only finitely many regular diagonal ternary quadratic forms ([Dickson 1939, Table 5] is a complete list), so this exact method has limited general use. Nonetheless, there does seem to be a close relationship between these quaternion rings and ternary quadratic forms, and one might be able to relax the regularity condition slightly and be able to represent "enough" integers to use a similar method as in Theorem 4.1.

5. Open questions

There are many questions left to explore here. It seems like it should be possible to find $g_{a,b}(2)$ for all a and b positive; at the very least, we'd like to know the proportion of such quaternion rings that have each of the possible values of $g_{a,b}(2)$. We have also been using as our analog of the integers the Lipschitz quaternions; the Hurwitz Quaternions would be an equally good choice, especially since we would get unique factorization. Lastly, we have been focusing on the cases when i^2 and j^2 are negative; one could easily investigate the cases when one or both are positive.

References

[Car 1973] M. Car, "Le problème de Waring pour l'anneau des polynômes sur un corps fini", pp. 13 in *Séminaire de théorie des nombres* (Talence, France), Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence, France, 1973. MR Zbl

[Dickson 1939] L. Dickson, *Modern elementary theory of numbers*, University of Chicago Press, 1939. Zbl

[Eljoseph 1954] N. Eljoseph, "On the representation of a number as a sum of squares", *Riveon Lematematika* **7** (1954), 38–43. MR

[Grosswald 1985] E. Grosswald, *Representations of integers as sums of squares*, Springer, New York, 1985. MR Zbl

[Hanke 2004] J. Hanke, "Some recent results about (ternary) quadratic forms", pp. 147–164 in *Number theory*, edited by H. Kisilevsky and E. Z. Goren, CRM Proc. Lecture Notes **36**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Jones and Pall 1939] B. W. Jones and G. Pall, "Regular and semi-regular positive ternary quadratic forms", *Acta Math.* **70**:1 (1939), 165–191. MR Zbl

[Niven 1940] I. Niven, "Integers of quadratic fields as sums of squares", *Trans. Amer. Math. Soc.* **48** (1940), 405–417. MR Zbl

[Niven 1946] I. Niven, "A note on the number theory of quaternions", *Duke Math. J.* **13** (1946), 397–400. MR Zbl

[Siegel 1921] C. Siegel, "Darstellung total positiver Zahlen durch Quadrate", *Math. Z.* **11**:3 (1921), 246–275. MR

[Vaughan and Wooley 2002] R. C. Vaughan and T. D. Wooley, "Waring's problem: a survey", pp. 301–340 in *Number theory for the millennium, III* (Urbana, IL, 2000), edited by M. A. Bennett et al., A K Peters, Natick, MA, 2002. MR Zbl

anc003@mcdaniel.edu   *McDaniel College, 2 College Hill, Westminster, MD 21157,*
                             United States

shamblen@mcdaniel.edu   *McDaniel College, 2 College Hill, Westminster, MD 21157,*
                             United States

slw001@mcdaniel.edu   *McDaniel College, 2 College Hill, Westminster, MD 21157,*
                             United States

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR

Kenneth S. Berenhaut   Wake Forest University, USA

BOARD OF EDITORS

PRODUCTION

Silvio Levy, Scientific Editor

Cover: Alex Scorpan

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve