WARING'S PROBLEM FOR INTEGRAL QUATERNIONS

PAUL POLLACK

Abstract. A (Lipschitz) *integral quaternion* is a Hamiltonian quaternion of the form $a+bi+cj+dk$ with all of $a,b,c,d \in \mathbb{Z}$. In 1946, Niven showed that the integral quaternions expressible as a sum of squares of integral quaternions are precisely those for which $2 \mid b,c,d$; moreover, all of these are expressible as sums of three squares. Now let m be an integer with $m > 2$, and suppose $2^r \parallel m$. We show that if $r = 0$ (i.e., m is odd), then all integral quaternions are sums of mth powers, while if $r > 0$, then the integral quaternions that are sums of mth powers are precisely those for which $2^r \mid b,c,d$ and $2^{r+1} \mid b+c+d$. Moreover, all of these are expressible as a sum of $g(m)$ mth powers, where $g(m)$ is a positive integer depending only on m.

1. Introduction

In 1770, Edward Waring asserted in his *Meditationes Arithmeticæ* [25, p. 336] that "Every [positive] integer is a square, or the sum of two, three, or four squares. Every integer is a cube, or the sum of two, three, ..., nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth." It has become traditional to interpret the phrase "and so forth" as a statement of the following conjecture.

Waring's problem. *Let $m \in \mathbb{Z}_{>0}$. There is a $g \in \mathbb{Z}_{>0}$ with the property that every nonnegative integer is a sum of g mth powers of nonnegative integers.*

The first solution to Waring's problem — meaning a proof of the existence of g for all m — was given by Hilbert in 1909 [7]. Hilbert's argument had a strong algebraic flavor and depended on the existence of certain remarkable polynomial identities. Around 1920, Hardy and Littlewood realized that Waring's problem could be attacked analytically by the circle method, and this approach led to significantly better understanding of admissible values of g. With $g(m)$ denoting smallest admissible value of g for a given m, it is now known that

$$g(m) = 2^m + \lfloor (3/2)^m \rfloor - 2$$

except when the fractional part of $(3/2)^m$ is extraordinarily close to 1. This exceptional case probably never occurs; Mahler proved that it happens only finitely often, while Kubina and Wunderlich have shown that it never happens for $m \le 471\,600\,000$. (Contained here are the results that $g(2) = 4, g(3) = 9$, and $g(4) = 19$, in agreement with Waring's conjectures.) For a precise definition of "extraordinary close to 1" as well as further references, see the surveys [3, 23].

Several authors have considered generalizations of Waring's problem of the following kind. Let R be a (not necessarily commutative) semiring. For each pair of positive integers m and s, let

$$R_m[s] = \left\{ \sum_{i=1}^{s} \alpha_i^m : \alpha_i \in R \right\}.$$

2010 *Mathematics Subject Classification.* 11P05 (primary), 11R52 (secondary).

Note that $R_m[s] \subset R_m[s+1]$, since $0 \in R$. We let

$$R_m[\infty] = \bigcup_{s \geq 0} R_m[s].$$

We say that *Waring's conjecture holds for the pair* R, m if $R_m[g] = R_m[\infty]$ for some positive integer g. Thus, Hilbert's 1909 theorem is the assertion that Waring's conjecture holds for $R = \mathbb{Z}_{\geq 0}$ and every $m \in \mathbb{Z}_{>0}$.

Let us list some more recent examples of "Waring problems" from the literature. To begin with, let $m = 2$. The minimal g with $R_2[g] = R$ — when it exists! — is known as the *Pythagoras number* of R. When R is a field of rational functions, the study of these Pythagoras numbers is closely linked with Hilbert's 17th problem; here important contributions were made by Artin, Cassels, Colliot-Thélène, Ellison, Jannsen, Landau, Pfister, Pourchet, and others. (For an introduction to this material see, e.g., the expository monograph of Rajwade [13].) Next, suppose that $R = k[X]$, with k a finite field. In this situation, Paley [12] proved in 1933 that Waring's conjecture holds for every m. More recently, Vaserstein has obtained remarkably far-reaching results for algebras over fields [19, 22] (containing, in particular, Paley's theorem). For $k[X]$, see also [9], and for general commutative rings, see [8] and [20]. Results of Siegel [15, 16] imply that Waring's conjecture holds for every m when R is the ring of integers in an arbitrary number field or the semiring of totally nonnegative integers. For matrix rings, see [6, 10, 18, 14]; to quote just one result, it is shown in [14] that if $n \geq m \geq 2$, then every element of $R = \mathrm{M}_n(\mathbb{Z})$ is a sum of seven mth powers in R.

In this paper, we consider the case of $R = \mathbb{L}$, the ring of (Lipschitz) integral quaternions, those Hamiltonian quaternions of the form $a + bi + cj + dk$ with all of $a, b, c, d \in \mathbb{Z}$. Our main result is the following.

Theorem 1.1. *Let $m \in \mathbb{Z}_{>0}$.*

(i) *Waring's conjecture is true for $\mathbb{L}, m$.*

(ii) *Suppose $2^r \mid m$ but $2^{r+1} \nmid m$. If $r = 0$, then $\mathbb{L}_m[\infty] = \mathbb{L}$. If $r = 1$ and $m = 2$, then $\mathbb{L}_m[\infty] = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}, 2 \mid b, c, d\}$. In all other cases,*

$$\mathbb{L}_m[\infty] = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}, 2^r \mid b, c, d, \text{ and } 2^{r+1} \mid b + c + d\}.$$

Our proof of Theorem 1.1 is similar in overall structure to the proof of Paley cited above; there are also several parallels with the works of Stemmler [17], Cohn [1], and Vaserstein (again see above).

The case $m = 2$ of Theorem 1.1 was treated by Niven [11]; in fact, Niven proves that every $a + bi + cj + dk \in \mathbb{L}$ with b, c, d even is a sum of three squares and that $6 + 2i$ is not a sum of two squares. (See the recent paper [2] for analogous results in other rational quaternion algebras.) Thus, if we define

$$g_R(m) = \inf\{m \in \mathbb{Z}_{>0} : R_m[g] = R_m[\infty]\},$$

then $g_{\mathbb{L}}(2) = 3$. Our proof of Theorem 1.1, while sufficient to show that $g_{\mathbb{L}}(m) < \infty$ for each m, yields only a very crude upper bound. In §5, we describe how to modify the argument to prove that $g_{\mathbb{L}}(m) = O(m \log m)$ for all $m \geq 2$.

2. A warm-up: the easier Waring problem

Our argument hinges on the following 1933 result of V. Veselý [24].

Proposition 2.1. *Fix $m \in \mathbb{Z}_{>0}$. There is a $v \in \mathbb{Z}_{>0}$ such that every integer n can be written as a sum or difference of v mth powers. More precisely, we can always write*

$$n = \sum_{\ell=1}^{v} \pm x_\ell^m$$

for some integers $x_1, \dots, x_v$ and some choice of signs.

For completeness, and for ease of reference in §6, we include Wright's short proof of Proposition 2.1 [26].

Proof. We let $\Delta\colon \mathbb{R}[X] \to \mathbb{R}[X]$ denote the forward-difference operator defined by $\Delta F(X) = F(X+1) - F(X)$. It is easy to check that if F has degree n with leading coefficient a_n, then ΔF has degree $n-1$ and leading coefficient na_n. Applying this observation $m-1$ times, we find that

$$\Delta^{(m-1)}(X^m) = m!X + C_m$$

for some integer C_m. (In fact, $C_m = \frac{1}{2}(m-1)m!$, but this will not be needed.) On the other hand, directly from the definition of Δ, we find that $\Delta^{(j)}X^m$, for each j, is the sum/difference of 2^j terms of the form $X^m, (X+1)^m, \dots, (X+j)^m$. For instance, $\Delta^{(2)}(X^m)$ has the 4-term expansion

$$(X+2)^m - (X+1)^m - (X+1)^m + X^m.$$

In particular, $\Delta^{(m-1)}(X^m)$ is the sum/difference of 2^{m-1} terms of the form X^m, $(X+1)^m$, $\dots$, $(X+m-1)^m$.

Replacing X by an element of $\mathbb{Z}$, we deduce from the results of the last paragraph that all integers congruent to C_m modulo $m!$ are the sum or difference of 2^{m-1} mth powers. If n is any integer, the least absolute remainder R of $n - C_m$ modulo $m!$ satisfies $|R| \le \frac{m!}{2}$. Since $n - R \equiv C_m$ modulo $m!$, we can write $n - R$ as a sum or difference of 2^{m-1} mth powers. Since $|R| \le \frac{m!}{2}$, we can write R as a sum or difference of $\frac{m!}{2}$ terms of the form 0^k and 1^k. Concatenating the representations of $n - R$ and R gives us a representation of n as a sum or difference of $2^{m-1} + \frac{m!}{2}$ mth powers. □

Let $v(m)$ be the smallest positive integer for which the conclusion of Proposition 2.1 holds. From the above proof,

$$v(m) \le 2^{m-1} + \frac{m!}{2}.$$

In [26], Wright termed the problem of determining the value of $v(m)$ the "easier Waring problem", on the basis of the ease with which Proposition 2.1 is proved in comparison to Hilbert's theorem. While it is indeed easy to prove that $v(2) = 3$, we still do not know the precise value of $v(m)$ for any $m > 2$. Considerations such as these led Wright himself to eventually repudiate the name "easier Waring problem" as "absurd" [27].

3. A local-global principle for representations as sums of powers, and the proof of Theorem 1.1(i)

Henceforth, $m \ge 2$ is fixed, and r is the nonnegative integer for which $2^r \mid m$ and $2^{r+1} \nmid m$. In this section, we begin in earnest our study of representations of elements of $\mathbb{L}$ as sums of mth powers.

We let $\sqrt{-2}$ denote a fixed complex square root of -2, and we define integers U and V by the equation

$$(1+\sqrt{-2})^m = U + V\sqrt{-2}. \tag{1}$$

Lemma 3.1. *We have $2^r \mid V$ and $2^{r+1} \nmid V$. In particular, $V \neq 0$.*

Proof. Noting that $(1+\sqrt{-2})^2 \equiv 1 \pmod 2$ in the ring $\mathbb{Z}[\sqrt{-2}]$, and that $m' := m/2^r$ is odd, we see that $(1+\sqrt{-2})^{m'} \equiv 1+\sqrt{-2} \pmod 2$. Thus, if we write $(1+\sqrt{-2})^{m'} = U_0 + V_0\sqrt{-2}$, then U_0 and V_0 are odd. For $\ell \geq 1$, define U_ℓ, V_ℓ by the equation $U_\ell + V_\ell\sqrt{-2} = (U_0 + V_0\sqrt{-2})^{2^\ell}$. A straightforward induction shows that for each $\ell \geq 0$, the integer V_ℓ is divisible by 2^ℓ but not $2^{\ell+1}$. Since $V = V_r$, the lemma follows. □

Lemma 3.2. *Every element of $\mathbb{L}$ congruent to an integer modulo $2V$ can be written as a sum of w mth powers in $\mathbb{L}$, where $w \in \mathbb{Z}_{>0}$ depends only on m.*

Proof. Starting from the observation that $(i+j)^2 = -2$, it is easy to see that there is an embedding $\mathbb{Z}[\sqrt{-2}] \hookrightarrow \mathbb{L}$ determined by sending $\sqrt{-2}$ to $i+j$. Hence,

$$(1 \pm (i+j))^m = U \pm V(i+j), \tag{2}$$

where U and V are the integers defined in (1) and the signs on both sides agree. Similarly,

$$(1 \pm (i+k))^m = U \pm V(i+k), \tag{3}$$

and

$$(1 \pm (j+k))^m = U \pm V(j+k). \tag{4}$$

Let b be an arbitrary integer. With v as in Proposition 2.1, we can write $b = \sum_{\ell=1}^{v} \pm x_\ell^m$. Hence, the nonreal component (pure part) of

$$\sum_{\ell=1}^{v} (x_\ell(1 \pm (i+j)))^m + \sum_{\ell=1}^{v} (x_\ell(1 \pm (i+k)))^m + \sum_{\ell=1}^{v} (x_\ell(1 \mp (j+k)))^m$$

is exactly $2bVi$. Similarly, for any integers c, d, one can find elements of $\mathbb{L}_m[3v]$ with nonreal components $2cVj$ and $2dVk$. Thus, there is an element of $\mathbb{L}_m[9v]$ with pure part $2V(bi+cj+dk)$.

Next, we fix integers A, B with $A > 0$ for which $\mathrm{Re}((A+Bi)^m) < 0$. It is easy to see that this is always possible. For instance, if $m = 2$, we may choose any pair of positive integers A and B with $A < B$. If $m > 2$, the real part of $(A+Bi)^m$ will certainly be negative if $\frac{\pi}{2m} < \mathrm{Arg}(A+Bi) < \frac{\pi}{m}$. For a given $A > 0$, this condition is satisfied when $A\tan\frac{\pi}{2m} < B < A\tan\frac{\pi}{m}$. For large enough A, the interval $(A\tan\frac{\pi}{2m}, A\tan\frac{\pi}{m})$ has length at least 1, and so we can certainly find an integer B contained therein.

Let $a_1 = \mathrm{Re}((A+Bi)^m)$ and notice that

$$(A+Bi)^m + (A-Bi)^m = 2a_1. \tag{5}$$

For any $x \in \mathbb{Z}$, Proposition 2.1 allows us to write $x = \sum_{\ell=1}^{v} \pm x_\ell^m$. Then

$$2a_1 x = \sum_{\ell=1}^{v} \pm 2a_1 x_\ell^m.$$

For those ℓ where the plus sign holds, $+2a_1x_\ell^m = ((A+Bi)x_\ell)^m + ((A-Bi)x_\ell)^m$, so $2a_1x_\ell^m$ is a sum of 2 mth powers in $\mathbb{L}$. On the other hand, $-2a_1x_\ell^m = 2|a_1|x_\ell^m = x_\ell^m + \cdots + x_\ell^m$ is a sum of $2|a_1|$ mth powers. It follows that every integer multiple of $2a_1$ belongs to $\mathbb{L}_m[2|a_1|v]$.

With this preparation out of the way, we can quickly complete the proof of the lemma. Let α be any element of $\mathbb{L}$ congruent to an integer modulo $2V$. Then $\alpha = a + 2V(bi + cj + dk)$ for some $a, b, c, d \in \mathbb{Z}$. Select $\beta \in \mathbb{L}_m[9v]$ with pure part $2V(bi + cj + dk)$, so that $\alpha - \beta = a_0$ for some $a_0 \in \mathbb{Z}$. Let M be the largest multiple of $2a_1$ not exceeding a_0, so that $a_0 = M + R$ where $0 \le R < 2|a_1|$. Then

$$\alpha = \beta + M + R \in \mathbb{L}_m[9v] + \mathbb{L}_m[2|a_1|v] + \mathbb{L}_m[2|a_1| - 1].$$

So we may take $w = 9v + 2|a_1|v + 2|a_1| - 1$. □

The next proposition is a local-global principle for sums of mth powers in $\mathbb{L}$.

Proposition 3.3. *An $\alpha \in \mathbb{L}$ is a sum of mth powers if and only if it is congruent to a sum of mth powers modulo $2V$.*

Proof. The "only if" direction is trivial. Now suppose that $\alpha \equiv \alpha_1^m + \cdots + \alpha_s^m \pmod{2V}$. By Lemma 3.2, $\beta := \alpha - \sum_{\ell=1}^s \alpha_\ell^m$ is a sum of mth powers. But then $\alpha = \sum_{\ell=1}^s \alpha_\ell^m + \beta$ is also a sum of mth powers. □

Proof of Theorem 1.1(i). We must show that any $\alpha \in \mathbb{L}$ that is a sum of mth powers is a sum of g mth powers, for some finite g depending only on m. Since α is a sum of mth powers in $\mathbb{L}$, it is certainly a sum of mth powers in the quotient $\mathbb{L}/(2V)$, say

$$\alpha \equiv \alpha_1^m + \cdots + \alpha_s^m \pmod{2V}. \tag{6}$$

Choose a representation of this kind where s is minimal. If $s > (2V)^4 = \#\mathbb{L}/(2V)$, then the sequence of partial sums $\alpha_1^m, \alpha_1^m + \alpha_2^m, \ldots, \alpha_1^m + \cdots + \alpha_s^m$ contains a repetition modulo $2V$, say $\sum_{\ell=1}^t \alpha_\ell^s \equiv \sum_{\ell=1}^{t'} \alpha_\ell^s \pmod{2V}$, where $1 \le t < t' \le s$. Hence, $\sum_{\ell=t+1}^{t'} \alpha_\ell^s \equiv 0 \pmod{2V}$. But then the representation of α in (6) can be shortened by deleting the $t' - t$ summands $\alpha_{t+1}^s, \ldots, \alpha_{t'}^s$, contradicting the minimality of s. Thus, $s \le (2V)^4$. By Lemma 3.2, $\alpha - \sum_{\ell=1}^s \alpha_\ell^m$ is a sum of $w = w(m)$ mth powers, and so α is a sum of $s + w$ mth powers. So we may take $g = (2V)^4 + w$. □

4. Proof of Theorem 1.1(ii)

According to Proposition 3.3, an $\alpha \in \mathbb{L}$ belongs to $\mathbb{L}_m[\infty]$ if and only if $\alpha \bmod 2V \in (\mathbb{L}/(2V))_m[\infty]$. In this section, we determine when this local condition is satisfied.

Write the prime factorization of $2V$ in the form

$$2V = \pm \prod_{p \mid 2V} p^{e_p}.$$

The Chinese remainder theorem implies that

$$\mathbb{L}/(2V) \cong \bigoplus_{p \mid 2V} \mathbb{L}/(p^{e_p}); \tag{7}$$

consequently, $\alpha \in \mathbb{L}$ is a sum of mth powers modulo $2V$ if and only if α is a sum of mth powers modulo p^{e_p} for all $p \mid 2V$. The next lemma, which is contained in [5, Proposition 4], will imply that the odd primes $p \mid 2V$ impose no restriction.

Lemma 4.1. *Let p be an odd prime, and let e be a positive integer. Then $\mathbb{L}/(p^e)$ is isomorphic to $\mathrm{M}_2(\mathbb{Z}/p^e\mathbb{Z})$.*

Proof (sketch). One shows that there are integers a and b with $a^2 + b^2 \equiv -1 \pmod{p^e}$. Then one checks that the homomorphism $\varphi\colon \mathbb{L}/(p^e) \to \mathrm{M}_2(\mathbb{Z}/p^e\mathbb{Z})$ determined by mapping $i \bmod p^e$ to $\left(\begin{smallmatrix} \bar{0} & -\bar{1} \\ \bar{1} & \bar{0} \end{smallmatrix}\right)$ and $j \bmod p^e$ to $\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{b} & -\bar{a} \end{smallmatrix}\right)$ is in fact an isomorphism. □

Lemma 4.2. *For each odd prime $p \mid 2V$, every element of $\mathbb{L}/(p^{e_p})$ is a sum of mth powers.*

Proof. In view of Lemma 4.1, it suffices to prove that every element $\left(\begin{smallmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}/p^{e_p}\mathbb{Z})$ is a sum of mth powers. Clearly, we may assume that $a \geq 0$ and $d \geq 2$. Then

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = a \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}^m + \begin{pmatrix} \bar{0} & \bar{b} \\ \bar{0} & \bar{1} \end{pmatrix}^m + \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{c} & \bar{1} \end{pmatrix}^m + (d-2) \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}^m$$
$$\in (\mathrm{M}_2(\mathbb{Z}/p^{e_p}\mathbb{Z}))_m[a+d] \subset (\mathrm{M}_2(\mathbb{Z}/p^{e_p}\mathbb{Z}))_m[\infty].$$

(Cf. the proof of Theorem 3 in [21].) □

Recall that r is defined by the conditions that $2^r \mid m$ but $2^{r+1} \nmid m$. By Lemma 3.1, 2 appears in the prime factorization of $2V$ with exponent $e_2 = r+1$. So by Proposition 3.3, the decomposition (7), and Lemma 4.2, α is a sum of mth powers precisely when it is a sum of mth powers modulo 2^{r+1}. Therefore, the next lemma completes the proof of Theorem 1.1(ii).

Lemma 4.3. *The following conditions are necessary and sufficient for $\alpha = a + bi + cj + dk \in \mathbb{L}$ to be congruent, modulo 2^{r+1}, to a sum of mth powers in $\mathbb{L}$.*

(i) when $r = 0$: $\alpha \in \mathbb{L}$. (*That is, all $\alpha \in \mathbb{L}$ are congruent to sums of mth powers.*)

(ii) $r = 1$ and $m = 2$: $2 \mid b, c, d$.

(iii) $r = 1$ and $m > 2$, or $r > 1$: $2^r \mid b, c, d$ *and* $2^{r+1} \mid b + c + d$.

Proof. We first prove necessity in every case and then turn to sufficiency.

For (i), necessity is trivial. Turning to (ii), note that for any $A + Bi + Cj + Dk \in \mathbb{L}$,

$$\begin{aligned} (A + Bi + Cj + Dk)^2 &= A^2 + 2A(Bi + Cj + Dk) + (Bi + Cj + Dk)^2 \\ &= A^2 - B^2 - C^2 - D^2 + 2A(Bi + Cj + Dk). \end{aligned} \tag{8}$$

So every square (mth power) in $\mathbb{L}$ has even components for i, j, k, which implies the same for every sum of squares in $\mathbb{L}$.

Finally we treat (iii). To start with, suppose $r = 1$, so that $m = 2m'$ with m' odd and greater than 1. For an arbitrary integral quaternion $A + Bi + Cj + Dk \in \mathbb{L}$,

$$\begin{aligned} &(A + Bi + Cj + Dk)^m = (A^2 - B^2 - C^2 - D^2 + 2A(Bi + Cj + Dk))^{m'} \\ &\equiv (A^2 - B^2 - C^2 - D^2)^{m'} + 2Am'(A^2 - B^2 - C^2 - D^2)^{m'-1}(Bi + Cj + Dk) \pmod 4. \end{aligned}$$

It is clear from this last expression that the i, j, k components of $(A + Bi + Cj + Dk)^m$ are even. Moreover, the sum of these components is congruent, modulo 4, to twice

$$Am'(A^2 - B^2 - C^2 - D^2)^{m'-1}(B + C + D).$$

Notice that modulo 2,

$$\begin{aligned} Am'(A^2 - B^2 - C^2 - D^2)^{m'-1}(B + C + D) &\equiv A(A^2 - B^2 - C^2 - D^2)(B + C + D) \\ &\equiv A(A + B + C + D)(B + C + D) \equiv 0; \end{aligned}$$

in the last step, we used that a product of three integers such that one factor is the sum of the other two is always even. Thus, the sum of the i, j, k components of $(A + Bi + Cj + Dk)^m$ is a multiple of 4. The property having i, j, k components individually divisible by 2 and with sum divisible by 4 is preserved under addition, which finishes the proof of necessity for this half of case (iii).

Finally, suppose that $r \geq 2$. For any $A + Bi + Cj + Dk \in \mathbb{L}$,

$$(A + Bi + Cj + Dk)^4 =$$
$$(A^2 - B^2 - C^2 - D^2)^2 - 4A^2(B^2 + C^2 + D^2) + 4A(A^2 - B^2 - C^2 - D^2)(Bi + Cj + Dk).$$

Clearly, the i, j, k components on the right-hand side are all divisible by 4, and an argument essentially identical to one we have just seen shows that their sum is a multiple of 8. When an integral quaternion has its i, j, k components divisible by 2^t and their sum divisible by 2^{t+1}, for a certain t, it follows from (8) that its square has i, j, k components divisible by 2^{t+1} with a sum divisible by 2^{t+2}. By induction, we deduce that every 2^rth power of an element of $\mathbb{L}$ has each of its i, j, k components divisible by 2^r and their sum divisible by 2^{r+1}. Since sums of mth powers are sums of 2^rth powers, necessity in the remaining half of case (iii) follows.

We turn now to sufficiency. In case (i), m is odd, and sufficiency is easy. Indeed, every element of $\mathbb{L}$ is congruent, modulo 2, to a sum of terms from the list $1^m = 1, i^m = \pm i, j^m = \pm j, k^m = \pm k$. Case (ii) is also easy; every quaternion with even i, j, k components is congruent, modulo 4, to a sum of terms from the list $1^2 = 1$, $(1+i)^2 = 2i$, $(1 + j)^2 = 2j$, and $(1 + k)^2 = 2k$.

Wrapping up, suppose that we are in case (iii). For each $\alpha = a + bi + cj + dk \in \mathbb{L}$, let

$$\psi(\alpha) = (\bar{b}, \bar{c}, \bar{d}) \in (\mathbb{Z}/2^{r+1}\mathbb{Z})^3.$$

Let H_0 be the 2-torsion subgroup of $(\mathbb{Z}/2^{r+1}\mathbb{Z})^3$, and let H be the subgroup of H_0 consisting of triples whose components sum to 0 in $\mathbb{Z}/2^{r+1}\mathbb{Z}$. Then $\#H_0 = 8$ and $\#H = 4$. Showing sufficiency amounts to proving that if $\psi(\alpha) \in H$, then α is congruent to a sum of mth powers modulo 2^{r+1}. But if $\psi(\alpha) \in H$, then $\psi(\alpha)$ is one of

$$(\overline{0}, \overline{0}, \overline{0}) = \psi(0^m),$$
$$(\overline{2^r}, \overline{2^r}, \overline{0}) = \psi((1 + i + j)^m),$$
$$(\overline{2^r}, 0, \overline{2^r}) = \psi((1 + i + k)^m),$$
$$(\overline{0}, \overline{2^r}, \overline{2^r}) = \psi((1 + j + k)^m).$$

(These equalities come from (2)–(4) together with the fact that $2^r \mid V$ while $2^{r+1} \nmid V$.) Thus, for $\beta = 0, 1 + i + j, 1 + i + k$, or $1 + j + k$, we have that $\alpha - \beta^m$ is congruent to an integer modulo 2^{r+1}. Since every integer is congruent mod 2^{r+1} to a sum of fewer than 2^{r+1} terms 1^m, we conclude that α is congruent modulo 2^{r+1} to a sum of 2^{r+1} mth powers. □

5. Economizing mth powers

Keeping track of the estimates in the proof of Theorem 1.1(i) would lead one to a quantitative bound of the shape $\log g_{\mathbb{L}}(m) = O(m \log m)$. We now describe modifications to our argument that yield the following much sharper upper bound.

Theorem 5.1. *For all integers $m \geq 2$, we have $g_{\mathbb{L}}(m) = O(m \log m)$.*

While the arguments thus far have been essentially self-contained, the proof of Theorem 5.1 rests on the deep result of Vinogradov that $G(m) = O(m \log m)$, where $G(m)$ is the minimal number of nonnegative mth powers required to additively represent all *sufficiently large* positive integers. (See [23] for references.)

As before, let $v(m)$ denote the minimal v for which the conclusion of Proposition 2.1 holds. As observed in [4], it is essentially trivial that $v(m) \leq G(m) + 1$: Indeed, for any $n \in \mathbb{Z}$, and all sufficiently large $x_0 \in \mathbb{Z}_{>0}$ (depending on n, m), we can write

$x_0^m - n = x_1^m + x_2^m + \cdots + x_G^m$, where $G = G(m)$. Hence, $n = x_0^m - x_1^m - \cdots - x_G^m$ is a sum/difference of $G+1$ mth powers.

We can use the same idea to optimize the proof of Lemma 3.2. Suppose $\alpha \in \mathbb{L}$ is congruent to an integer modulo $2V$, so that

$$\alpha = a + 2V(bi + cj + dk)$$

with $a, b, c, d \in \mathbb{Z}$. As in the current proof, for some $a_0 \in \mathbb{Z}$, we have

$$\beta = a_0 + 2V(bi + cj + dk) \in \mathbb{L}_m[9v].$$

With A, B, a_1 as in eq. (5) of Lemma 3.2, we select $z \in \mathbb{Z}_{>0}$ so large that

$$2|a_1|z^m + a - a_0 = x_1^m + \cdots + x_G^m \tag{9}$$

for some nonnegative integers $x_1, \dots, x_G$. Then (recall that $a_1 < 0$)

$$\begin{aligned} a - a_0 &= 2a_1 z^m + x_1^m + \cdots + x_G^m \\ &= ((A+Bi)z)^m + ((A-Bi)z)^m + x_1^m + \cdots + x_G^m \in \mathbb{L}_m[G+2]. \end{aligned} \tag{10}$$

Hence,

$$\alpha = (a - a_0) + \beta \in \mathbb{L}_m[G + 2 + 9v].$$

As we saw in the last paragraph, it is permissible to take $v = G + 1$. So this reasoning shows that the conclusion of Lemma 3.2 holds with $w = 10G + 11$.

The proof of Theorem 1.1(i) shows that

$$g_{\mathbb{L}}(m) \le g_{\mathbb{L}/(2V)}(m) + w.$$

By the Chinese remainder theorem, with p^{e_p} the exact power of p dividing $2V$,

$$g_{\mathbb{L}/(2V)}(m) = \max_{p \mid 2V} g_{\mathbb{L}/(p^{e_p})}(m).$$

Suppose first that p is odd, so that $g_{\mathbb{L}/(p_p^e)}(m) = g_{\mathrm{M}_2(\mathbb{Z}/p^{e_p}\mathbb{Z})}(m)$. Vaserstein has shown [21, Theorem 3] that every element of $\mathrm{M}_2(\mathbb{Z})$ is a sum of at most $\frac{1}{2}(G(m)+9)$ mth powers. It follows immediately that $g_{\mathrm{M}_2(\mathbb{Z}/p^{e_p}\mathbb{Z})}(m) \le \frac{1}{2}(G(m)+9)$, so that

$$g_{\mathbb{L}/(p^{e_p})}(m) \ll G(m). \tag{11}$$

Now suppose that $p = 2$. For $e_2 \le 2$, the pigeonhole argument seen in the proof of Theorem 1.1(i) implies that every element of $\mathbb{L}/(2^{e_2})$ that is a sum of mth powers is a sum of at most $\#\mathbb{L}/(2^{e_2}) = 2^{4e_2} \le 2^8$ mth powers. So assume that $e_2 > 2$. Let $\alpha \in \mathbb{L}$ and suppose that α is congruent to a sum of mth powers modulo 2^{e_2}. By the proof of Lemma 4.3, we can choose $\beta \in \mathbb{L}$ with $\alpha - \beta^m$ congruent to an integer modulo 2^{e_2}. (Notice that $e_2 = r + 1$, and that the condition $e_2 > 2$ forces us to be in case (iii) of that lemma.) That integer is congruent, modulo 2^{e_2}, to a sum of $G(m)$ mth powers. Hence, α is congruent mod 2^{e_2} to a sum of $G(m)+1$ mth powers. We conclude that (11) holds for $p = 2$ as well. Therefore, $g_{\mathbb{L}/(2V)}(m) \ll G(m)$. Since also $w \ll G(m)$, it follows that

$$g_{\mathbb{L}}(m) \ll G(m) \ll m \log m,$$

as desired.

6. A concluding word on generalizations

The proof of Theorem 1(i) is reasonably robust. For example, let a and b be arbitrary nonzero integers. Consider the generalized Lipschitz quaternion ring $\mathbb{L}^{a,b}$ (say) with $\mathbb{Z}$-basis elements $1, i, j, k$ satisfying $i^2 = a$, $j^2 = b$, $ij = -ji = k$. (Thus, $k^2 = -ab$.). The proof of Theorem 1(i) can be adapted to prove Waring's conjecture for all these rings. In fact, as we now demonstrate, $g_{\mathbb{L}^{a,b}}(m)$ is bounded by a constant depending only on m (and not on the choice of a, b).

We will show that every element of $\mathbb{L}^{a,b}$ that is congruent to an integer modulo $m!$ can be written as the sum of w mth powers, where w is bounded entirely in terms of m. Once this is proved, following the proof of Theorem 1(i) gives that

$$g_{\mathbb{L}^{a,b}}(m) \leq w + g_{\mathbb{L}^{a,b}/(m!)}(m) \leq w + \#\mathbb{L}^{a,b}/(m!) = w + m!^4,$$

and so $g_{\mathbb{L}^{a,b}}(m)$ is also bounded in terms of m. In what follows, we use Im for the pure part of an element of $\mathbb{L}^{a,b}$ and Re for the real component.

In the course of proving Proposition 2.1, we showed the existence of a polynomial identity

$$m!X + C_m = \sum_{\ell=1}^{2^{m-1}} \pm(s_\ell + X)^m,$$

where $C_m \in \mathbb{Z}$ and each $s_\ell \in \{0, 1, 2, \ldots, m-1\}$. Suppose that $\alpha \in \mathbb{L}^{a,b}$ and that α is congruent to an integer modulo $m!$. Then $\alpha = A + m!(Bi + Cj + Dk)$ for some $A, B, C, D \in \mathbb{Z}$. Plugging $X = Bi + Cj + Dk$ into the above identity, we see that

$$\begin{aligned} m!(Bi + Cj + Dk) &= \mathrm{Im} \sum_{\ell=1}^{2^{m-1}} \pm(s_\ell + Bi + Cj + Dk)^m \\ &= \sum_{\ell=1}^{2^{m-1}} \mathrm{Im}(\pm(s_\ell + Bi + Cj + Dk)^m) = \sum_{\ell=1}^{2^{m-1}} \mathrm{Im}((s_\ell \pm (Bi + Cj + Dk))^m). \end{aligned}$$

Therefore

$$\beta := \sum_{\ell=1}^{2^{m-1}} (s_\ell \pm (Bi + Cj + Dk))^m$$

has the same pure part as α, and $\beta \in \mathbb{L}_m^{a,b}[2^{m-1}]$. Write

$$\beta = A_0 + m!(Bi + Cj + Dk).$$

At least one of $a, b, -ab$ is negative. Suppose $a < 0$; the other cases are similar. Then $\mathbb{Z}[i]$ is isomorphic to the ring $\mathbb{Z}[\sqrt{|a|} \cdot \sqrt{-1}] \subset \mathbb{C}$. Reasoning with complex arguments as in the proof of Lemma 3.2, we can find an $A_1 + B_1 i \in \mathbb{Z}[i]$ with $a_1 := \mathrm{Re}((A_1 + B_1 i)^m) < 0$. Arguing as in the last section (cf. equations (9), (10)),

$$A - A_0 \in \mathbb{L}_m^{a,b}[G + 2],$$

where $G = G(m)$. Thus,

$$\alpha = A - A_0 + \beta \in \mathbb{L}_m^{a,b}[G + 2 + 2^{m-1}],$$

and we may take $w = G + 2 + 2^{m-1}$.

What about part (ii) of Theorem 1.1? For general a, b, we do not have as satisfactory a characterization of $\mathbb{L}_m^{a,b}[\infty]$ as in the special case $a = b = -1$. We still have the local-global principle: An element of $\mathbb{L}^{a,b}$ belongs to $\mathbb{L}_m^{a,b}[\infty]$ precisely when its reduction mod p^e belongs to $(\mathbb{L}^{a,b}/(p^e))_m[\infty]$ for all prime powers p^e. (The proof is the same as before,

with $m!$ now replacing $2V$.) The results of [5, §4] show that $\mathbb{L}^{a,b}/(p^e) \cong \mathrm{M}_2(\mathbb{Z}/p^e\mathbb{Z})$ when $p \nmid 2ab$, which implies (see the proof of Lemma 4.2) that those primes do not contribute any restriction. It would seem an interesting problem to determine the restrictions imposed by those primes $p \mid 2ab$.

Acknowledgments

The author is supported by NSF award DMS-1402268. Enrique Treviño and the anonymous referee contributed several helpful comments; in particular, the referee suggested the simple proof of Lemma 3.1 included here. The author would also like to thank Ariel Pacetti and Fernando Rodriguez Villegas for making available their `qalg` scripts for `GP/PARI`, which were instrumental in discovering Theorem 1(ii).

References

[1] J. H. E. Cohn, *Waring's problem in quadratic number fields*, Acta Arith. **20** (1972), 1–16, addendum in **23** (1973), 417–418.
[2] A. Cooke, S. Hamblen, and S. Whitfield, *Sums of squares in quaternion rings*, Involve **10** (2017), 651–664.
[3] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly **78** (1971), 10–36.
[4] W. H. J. Fuchs and E. M. Wright, *The 'easier' Waring problem*, Quart. J. Math., Oxford Ser. **10** (1939), 190–209.
[5] J. M. Grau, C. Miguel, and A. M. Oller-Marcén, *On the structure of quaternion rings over $\mathbb{Z}/n\mathbb{Z}$*, Adv. Appl. Clifford Algebr. **25** (2015), 875–887.
[6] M. Griffin and M. Krusemeyer, *Matrices as sums of squares*, Linear and Multilinear Algebra **5** (1977/78), 33–44.
[7] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). Dem Andenken an Hermann Minkowski gewidmet*, Math. Ann. **67** (1909), 281–300.
[8] J.-R. Joly, *Sommes de puissances d-ièmes dans un anneau commutatif*, Acta Arith. **17** (1970), 37–114.
[9] Y.-R. Liu and T.-D. Wooley, *The unrestricted variant of Waring's problem in function fields*, Funct. Approx. Comment. Math. **37** (2007), 285–291.
[10] M. Newman, *Sums of squares of matrices*, Pacific J. Math. **118** (1985), 497–506.
[11] I. Niven, *A note on the number theory of quaternions*, Duke Math. J. **13** (1946), 397–400.
[12] R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, Quart. J. Math. **4** (1933), 52–63.
[13] A. R. Rajwade, *Squares*, London Mathematical Society Lecture Note Series, vol. 171, Cambridge University Press, Cambridge, 1993.
[14] D. R. Richman, *The Waring problem for matrices*, Linear and Multilinear Algebra **22** (1987), 171–192.
[15] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. J. Math. **66** (1944), 122–136.
[16] ———, *Sums of mth powers of algebraic integers*, Ann. of Math. (2) **46** (1945), 313–339.
[17] R. M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arith. **6** (1960/1961), 447–468.
[18] L. N. Vaserstein, *On the sum of powers of matrices*, Linear and Multilinear Algebra **21** (1987), 261–270.
[19] ———, *Waring's problem for algebras over fields*, J. Number Theory **26** (1987), 286–298.
[20] ———, *Waring's problem for commutative rings*, J. Number Theory **26** (1987), 299–307.
[21] ———, *Noncommutative number theory*, Algebraic K-theory and algebraic number theory (Honolulu, HI, 1987), Contemp. Math., vol. 83, Amer. Math. Soc., Providence, RI, 1989, pp. 445–449.
[22] ———, *Ramsey's theorem and Waring's problem for algebras over fields*, The arithmetic of function fields (Columbus, OH, 1991), Ohio State Univ. Math. Res. Inst. Publ., vol. 2, de Gruyter, Berlin, 1992, pp. 435–441.
[23] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*, Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–340.
[24] V. Veselý, *O jedné obdobě Waringova problému*, Časopis pro pěstování matematiky a fysiky **62** (1933), 123–127.
[25] E. Waring, *Meditationes algebraicæ*, American Mathematical Society, Providence, RI, 1991.

[26] E. M. Wright, *An easier Waring's problem*, J. London Math. Soc. **9** (1934), 267–272.
[27] ———, *The Tarry-Escott and the "easier" Waring problems*, J. Reine Angew. Math. **311/312** (1979), 170–173.

Department of Mathematics, University of Georgia, Athens, GA 30602

E-mail address: pollack@uga.edu