CUBES OF INTEGRAL VECTORS IN DIMENSION FOUR

EMIL W. KISS, PÉTER KUTAS

Abstract. A system of \(m\) nonzero vectors in \(\mathbb{Z}^n\) is called an \(m\)-icube if they are pairwise orthogonal and have the same length. The paper describes \(m\)-icubes in \(\mathbb{Z}^4\) for \(2 \leq m \leq 4\) using Hurwitz integral quaternions, counts the number of them with given edge length, and proves that unlimited extension is possible in \(\mathbb{Z}^4\).

1. Introduction and main results

Two vectors are called twins if they are orthogonal, and have the same length. An \(m\)-icube in \(\mathbb{Z}^n\) is a sequence \((v_1, \ldots, v_m)\) of nonzero vectors in \(\mathbb{Z}^n\) that are twins pairwise. The common length of the vectors \(v_\ell\) is the edge length of the icube. By the norm of \(v_\ell\) we mean the square of its length. The main object of this paper is to study how icubes can be constructed, extended and counted. The paper [3] investigates these questions extensively in \(\mathbb{Z}^3\), using the number theory of quaternions.

For a trivial example, if the dimension is even, then every vector \((a_1, \ldots, a_n)\) has a twin, namely \((a_2, -a_1, a_4, -a_3, \ldots, a_n, -a_{n-1})\). Similarly, the rows of the matrix

\[
\begin{pmatrix}
  a & b & c & d & e & f & g & h \\
  b & -a & d & -c & f & -e & -h & g \\
  c & -d & -a & b & g & h & -e & -f \\
  d & c & -b & -a & h & -g & f & -e \\
  e & -f & -g & -h & a & b & c & d \\
  f & e & -h & g & -b & -a & -d & c \\
  g & h & e & -f & -c & d & -a & -b \\
  h & -g & f & e & -d & -c & b & -a \\
\end{pmatrix}
\]

form an 8-icube, proving that every 8-dimensional integral vector can be extended to an 8-icube. The above matrix comes from the multiplication table of Cayley-numbers. The \(4 \times 4\) minor in the upper left corner yields a 4-icube in dimension 4, extending an arbitrary element of \(\mathbb{Z}^4\).

Classical results of Hurwitz [6] and Radon [7] show, however, that a similar “permutational” extension is possible only in dimensions 1, 2, 4 and 8 (an interesting
approach using extraspecial 2-groups is given by Eckmann in [2]). To prove further extension theorems we have to explore the number-theoretic structure of the components of the vectors. An example for this type of argument is the Euler-matrix

\[
\begin{pmatrix}
m^2 + n^2 - p^2 - q^2 & -2mq + 2np & 2mp + 2nq \\
2mq + 2np & m^2 - n^2 + p^2 - q^2 & -2mn + 2pq \\
-2mp + 2nq & 2mn + 2pq & m^2 - n^2 - p^2 + q^2
\end{pmatrix},
\]

which is a “typical” 3-icube in dimension 3 (see [8] and [3]). We start with an extension theorem that generalizes Corollary 5.11 of [3].

**Theorem 1.1.** Let \((v_1, \ldots, v_{n-1})\) be an \(n-1\)-icube in \(\mathbb{Z}^n\), where \(n \geq 2\). If \(n\) is even, then this icube can be extended to an \(n\)-icube. If \(n\) is odd, then such an extension is possible if and only if the common length of the vectors \(v_\ell\) is an integer.

**Proof.** Let \(N\) denote the edge norm of \((v_1, \ldots, v_{n-1})\). By Proposition 1.3 of [3], if \(n\) is odd, then the edge length of any \(n\)-icube in \(\mathbb{Z}^n\) is an integer. Therefore an extension is only possible if \(n\) is even or if \(N\) is a square.

Define \(L\) to be the \(n \times (n - 1)\) matrix whose columns are \(v_1, \ldots, v_{n-1}\). Then \(L^T L = NI_{n-1}\) (where \(I_{n-1}\) denotes the identity matrix). The Cauchy-Binet formula therefore implies that

\[\det(L_1)^2 + \cdots + \det(L_n)^2 = N^{n-1},\]

where \(L_i\) is the minor of \(L\) obtained by deleting the \(i\)-th row.

Let \(M_i = (-1)^{n+i} \det(L_i)\). Add a last column to \(L\) whose entries are \(M_i/N^{(n-2)/2}\), and denote the resulting matrix by \(K\). Then the columns of \(L\) are pairwise orthogonal by the Laplace expansion theorem for determinants. The displayed formula above shows that \(K^T K = N I_n\). This implies that \(KK^T = N I_n\). Denote the rows of \(L\) by \(s_i\). We get that the scalar product of \(s_i\) by itself, which is an integer, equals \(N - M_i^2/N^{n-2}\). Therefore if \(n\) is even or if \(N\) is a square, then \(N^{(n-2)/2}\) divides \(M_i\), and the last column of \(K\) consists of integers. \(\square\)

Here are the main results of this paper.

**Theorem 1.2.** Every \(m\)-icube in \(\mathbb{Z}^4\) can be extended to a 4-icube for \(1 \leq m \leq 3\).

Of course, the only nontrivial case occurs when \(m = 2\), according to the statements above. The proof is found at the end of Section 3.

The following result, proved in Section 4, counts the number of \(m\)-icubes in \(\mathbb{Z}^4\). Denote by \(f_m(N)\) the number of \(m\)-icubes with edge norm \(N\) (that is, edge length \(\sqrt{N}\)) in \(\mathbb{Z}^4\). A famous theorem by Jacobi provides the value of \(f_1(N)\), we include it for
comparison. Let \( c_m = \frac{24 \cdot 2^m}{(4 - m)!} \), thus \( c_1 = 8, c_2 = 48, c_3 = 192 \) and \( c_4 = 384 \).

Furthermore, if \( p \) is a (positive) odd prime and \( k \geq 1 \), then define
\[
g(p^k) = \frac{(k + 1)p^k(p^2 - 1) - 2(p^{k+1} - 1)}{(p - 1)^2}.
\]

**Theorem 1.3.** Let \( g_m(N) = f_m(N)/c_m \). Then \( g_m \) is a multiplicative function for every \( 1 \leq m \leq 4 \), whose value on prime powers is given by the following formulae,

1. \( g_m(2^k) = 3 \) for every \( k \geq 1 \).
2. \( g_1(p^k) = \sigma(p^k) = (p^{k+1} - 1)/(p - 1) \) (this is Jacobi’s classical result) and \( g_3(p^k) = g_4(p^k) = g(p^k) \) (the function defined before the theorem).
3. If \( p \equiv 3 \pmod{4} \), then \( g_2(p^k) = g(p^k) \). If \( p \equiv 1 \pmod{4} \), then \( g_2(p^k) = (k + 1)p^k \).

In particular, we have that \( f_4(N) = 2f_3(N) \).

The proofs are based on a representation theorem of icubes using Hurwitz integral quaternions (see Theorems 3.5, 3.9, 4.2 and 4.4).

## 2. Integral Quaternions

We review some properties of integral quaternions. The general references are [1], [5] and [4], but we ask the reader to browse Section 2 of [3] for background, as we shall use the notation and the results introduced there. The norm of \( \alpha = a + bi + cj + dk \) is \( N(\alpha) = a^2 + b^2 + c^2 + d^2 \). This \( \alpha \) is a Hurwitz integral quaternion if \( 2a, 2b, 2c, 2d \) are all integers of the same parity. Hurwitz integral quaternions form a left Euclidean ring \( E \). The ring of quaternions with integral coefficients is denoted by \( L \) (these are the Lipschitz integral quaternions). The sign \( \alpha \mid \beta \) means: \( \alpha \) divides \( \beta \) on the left in \( E \). The ring \( E \) has 24 units. Every element \( \alpha \) of \( E \) has a left associate in \( L \) and a right associate in \( L \).

**Theorem 2.1** ([3], Theorem 2.7; see Theorem 377 of [4] and the note after the proof of Theorem 3 in Section 5.3 of [1]). An integral quaternion is irreducible in the ring \( E \) if and only if its norm is a prime in \( Z \). The only elements of \( E \) whose norm is 2 are \( 1 + i \) and its left associates. If \( p > 2 \) is a prime in \( Z \), then there exist exactly \( 24(p + 1) \) integral quaternions whose norm is \( p \).

**Lemma 2.2** ([3], Lemma 2.5). Suppose that \( \alpha \in E \) and \( p \in Z \) is a prime such that \( p \mid N(\alpha) \) but \( p \) does not divide \( \alpha \). Then \( \alpha \) can be written as \( \pi \alpha' \) where \( N(\pi) = p \), and this \( \pi \) is uniquely determined up to right association.

**Lemma 2.3** ([3], Lemma 2.6). Suppose that \( \theta, \eta, \pi \in E \) such that \( N(\pi) = p \) is a prime in \( Z \). If \( \pi \mid \theta, p \mid \theta \eta \) but \( p \) does not divide \( \theta \), then \( \pi \mid \eta \).

We shall reduce questions to quaternions having odd norm, using the following assertion.
Claim 2.4. Let \( \alpha = a + bi + cj + dk \in \mathbb{L} \).

1. There exists an element \( \beta \in \mathbb{L} \) such that \( \alpha = (1 + i)\beta \) if and only if \( a \equiv b \mod{2} \) and \( c \equiv d \mod{2} \). The analogous statements hold for \( 1 + j \) and \( 1 + k \).

2. If \( \alpha = (1 + i)\beta \) for some \( \beta \in \mathbb{L} \).

3. If \( N(\alpha) \equiv 4 \mod{8} \), then \( \alpha = (1 + i)\beta \) for some \( \beta \in \mathbb{L} \).

4. If \( N(\alpha) \equiv 2 \mod{8} \), then there is exactly one element \( \eta \in \{1 + i, 1 + j, 1 + k\} \) such that \( \alpha = \eta \beta \) for some \( \beta \in \mathbb{L} \).

Proof. (1) can be shown by direct calculation. Since \( m^2 \equiv 1 \mod{8} \) for every odd integer \( m \), we see that \( N(\alpha) \) is divisible by 8 if and only if \( a, b, c, d \) are all even, so (2) holds. By the same argument, if \( 4 \mid N(\alpha) \), then \( a, b, c, d \) are all even, or are all odd. In the first case we have (3), since \( 2 = (1+i)(1-i) \). In the second case (3) also holds by (1). Now suppose that \( N(\alpha) \equiv 2 \mod{4} \). Then two numbers of \( a, b, c, d \) are even and two are odd. If \( a \equiv b \mod{2} \), then \( c \equiv d \mod{2} \), so (1) shows that \( 1 + i \) can be pulled out from \( \alpha \), but \( 1 + j \) and \( 1 + k \) cannot.

Next we investigate quaternions with integral coefficients having odd norm. Let \( K = \{1, i, j, k\} \), and write a general quaternion \( \alpha \in \mathbb{L} \) as \( a_1 + a_i + a_j + a_k \). For \( g \in K \) define

\[
S_g = \{a_1 + a_i + a_j + a_k \in \mathbb{L} \mid a_g \neq a_h \text{ for every } h \neq g, \text{ where } h \in K\}.
\]

So for example the elements of \( S_i \) are those where the coefficient of \( i \) is odd and the other coefficients are even, or vice versa. Let \(*\) denote the Klein-group multiplication on \( K \) (which is quaternion-multiplication, but disregards the signs). Call two nonzero quaternions twins if so are the vectors formed by their coefficients. The following claim summarizes well-known, easy facts.

Claim 2.5. Let \( \alpha, \beta \in \mathbb{L} \) with odd norm and \( 2\sigma = 1 + i + j + k \).

1. Both \( \alpha \) and \( \beta \) belong to exactly one of the sets \( S_g \). If they are twins, then they cannot belong to the same \( S_g \).

2. If \( N(\alpha) \equiv 1 \mod{4} \) then \( \alpha \in S_g \) if and only if \( \alpha \equiv g \mod{2} \) in \( \mathbb{L} \) if and only if \( \alpha \equiv g \mod{2} \) in \( \mathbb{E} \).

3. If \( N(\alpha) \equiv 3 \mod{4} \), then \( \alpha \in S_g \) if and only if \( \alpha \equiv 2\sigma - g \mod{2} \) in \( \mathbb{L} \) if and only if \( \alpha \equiv 2\sigma - g \mod{2} \) in \( \mathbb{E} \).

4. If \( \alpha \in S_g \) and \( \beta \in S_h \), then \( \alpha, \beta \in S_{gh} \).

5. If \( \alpha \in S_1 \) and \( \gamma \in \mathbb{E} \), then \( \gamma \in S_g \iff \alpha \gamma \in S_g \iff \gamma \alpha \in S_g \).

Proof. If \( N(\alpha) \equiv 1 \mod{4} \), then \( \alpha \) has exactly one odd component. If \( N(\alpha) \equiv 3 \mod{4} \), then \( \alpha \) has exactly one even component. Suppose that \( \alpha \) and \( \beta \) are twins in \( S_g \). Then \( N(\alpha) = N(\beta) \equiv 1 \mod{4} \) implies that the scalar product of the corresponding vectors is congruent to 1 modulo 2, which is impossible, since they are orthogonal. If \( N(\alpha) = N(\beta) \equiv 3 \mod{4} \), then this scalar product is congruent to 3 modulo 2, also a contradiction. This shows (1). The proofs of (2) – (4) are left to the reader.
Suppose that $\alpha \in S_1$ and $\alpha \gamma = \delta \in S_g$. Then $N(\alpha) \gamma = \overline{\alpha} \delta \in \mathbb{L}$. Since $N(\alpha)$ is odd, this implies that $\gamma \in \mathbb{L}$. The norm of $\gamma$ is odd, so (5) follows from (4).

Call a quaternion $\alpha$ primary if $\alpha \in S_1$ and $a_1 + a_i + a_j + a_k \equiv 1 (4)$. Obviously, if $\alpha \in S_1$, then exactly one of $\alpha$ and $-\alpha$ is primary.

**Claim 2.6.** The following hold.

1. If $\gamma \in \mathbb{E}$ has odd norm, then $\gamma$ has exactly one primary left associate, and exactly one primary right associate.
2. The primary quaternions form a semigroup under multiplication. Moreover, if the (left or right) quotient of two primary quaternions is in $\mathbb{E}$, then it is also primary.
3. Let $\alpha$ be a primary quaternion and $\varepsilon \in \mathbb{E}$ a unit. Then $\varepsilon \alpha \in \mathbb{L}$ (or $\alpha \varepsilon \in \mathbb{L}$) if and only if $\varepsilon \in Q = \{\pm 1, \pm i, \pm j, \pm k\}$.

**Proof.** Statement (3) clearly follows from Claim 2.5 (5). The rest of the proof is left to the reader.

We close this section with two counting results. Call a quaternion with integral coefficients primitive, if its coefficients are relatively prime.

**Claim 2.7** (Jacobi). Let $N > 1$ be odd. Then the number of primary primitive quaternions with norm $N$ is $h(N) = N \prod_p \left(1 + \left(1/p\right)\right)$, where $p$ runs over the prime divisors of $N$.

A pure quaternion is one with real part zero.

**Lemma 2.8** (see [3], Theorem 4.2). Let $\theta \in \mathbb{E}$ be a primitive pure quaternion whose norm is a square. Then $\theta$ can be written as $\gamma i \overline{\gamma}$ for some $\gamma \in \mathbb{E}$. Here $\gamma$ is uniquely determined in the sense that any two such elements $\gamma$ are right associates via a unit in $\{1, -1, i, -i\}$.

**Claim 2.9.** Let $N > 1$ be odd. Then the number of primary quaternions $\gamma$ with norm $N$ such that $\gamma i \overline{\gamma}$ is primitive is $q(N) = N \prod_p \left(1 - (s_p/p)\right)$, where $p$ runs over the prime divisors of $N$ and $s_p \in \{1, -1\}$ is congruent to $p$ modulo 4.

(In other words, $s_p = (-1)^{(p-1)/2} = (−1/p)$ as a Legendre-symbol).

**Proof.** Theorem 4.8 in [3] implies that the number of primitive vectors $(x, y, z)$ with norm $N^2$ is $6q(N)$. By Lemma 2.8, the quaternions corresponding to such vectors can be written as $\theta = \gamma i \overline{\gamma}$ for some $\gamma \in \mathbb{E}$. Conjugacy with the units in $\mathbb{E}$ yields an equivalence relation on the set of all such elements $\theta$. The fact that $\theta$ is primitive, but not a unit implies that at least two of its components are nonzero. Therefore each conjugacy class has 12 elements (the stabilizer is just $\{1, −1\}$ in each case). It is sufficient to show that exactly two of these conjugates can be written in the form $\gamma i \overline{\gamma}$ such that $\gamma$ is primary.
If $\theta = \gamma i \overline{\gamma}$, then Claim 2.6 shows that $\gamma = \varepsilon \alpha$, where $\varepsilon$ is a unit and $\alpha$ is primary. Therefore $\theta$ has a conjugate of the required form, namely $\alpha i \overline{\alpha}$. Exactly one of $\beta = \pm i a \overline{a}$ is primary, and $\beta i \overline{\beta} = i b \overline{b}$ is a conjugate of $\theta$ that is different from $\theta$.

Conversely, suppose that $\theta$ has two conjugates $\theta_1 = \gamma_1 i \overline{\gamma_1}$ and $\theta_2 = \gamma_2 i \overline{\gamma_2}$ such that $\gamma_1$ and $\gamma_2$ are primary. Thus $\theta_2 = \varepsilon \gamma_1 i$ for some unit $\varepsilon$. By the uniqueness statement of Lemma 2.8, $\varepsilon \gamma_1 = \gamma_2 \rho$ for some $\rho \in \{1, -1, i, -i\}$. Claim 2.6 shows that $\varepsilon \in Q$, and Claim 2.5 (5) gives that $\varepsilon = \pm 1$. If $\varepsilon = -1$, then $\theta_1 = \theta_2$. If $\varepsilon = \pm i$, then $\theta_2 = i \theta_1 i$. □

There is an alternative argument for the previous statement: the reader may go through the proof of Theorem 4.8 in [3], and modify it in such a way that only primary prime factors are used when building $\gamma$.

3. Construction and extension

We shall speak about $m$-icubes $(\alpha_1, \ldots, \alpha_m)$ in $\mathbb{E}$ and in $\mathbb{L}$, meaning that this is a sequence of simultaneous twins such that each $\alpha_\ell$ lies in $\mathbb{E}$ or in $\mathbb{L}$, respectively.

**Lemma 3.1.** The quaternions $\alpha$ and $\beta$ are twins if and only if their norms are equal, and $\overline{\alpha} \beta = -\overline{\beta} \alpha$ (or equivalently, $\alpha \overline{\beta} = - \beta \overline{\alpha}$) holds.

**Proof.** If $\alpha = a_1 + a_2 i + a_3 j + a_4 k$ and $\beta = b_1 + b_2 i + b_3 j + b_4 k$, then the real part of $\alpha \beta$ is $a_1 b_1 - a_2 b_2 - a_3 b_3 + a_4 b_4$. Therefore the vectors corresponding to $\alpha$ and $\beta$ are orthogonal if and only if the real part of $\overline{\alpha} \beta$ is zero (if and only if the real part of $\overline{\beta} \alpha$ is zero). However, the real part of a quaternion is zero if and only if its conjugate is its negative. □

**Corollary 3.2.** If $\gamma \neq 0$, then $\alpha$ and $\beta$ are twins if and only if $\alpha \gamma$ and $\beta \gamma$ are twins if and only if $\gamma \alpha$ and $\gamma \beta$ are twins. □

**Lemma 3.3.** Let $\alpha, \beta \in \mathbb{E}$ be twins and $p \in \mathbb{Z}$ be a prime dividing $N(\alpha) = N(\beta)$. Then there exists a quaternion $\pi \in \mathbb{E}$ with norm $p$ such that either $\pi$ divides both $\alpha$ and $\beta$ on the left, or $\pi$ divides both $\alpha$ and $\beta$ on the right. If $\beta \overline{\alpha}$ is divisible by $p$, then the second case surely holds.

**Proof.** If $p \mid \alpha$, then every $\pi \in \mathbb{E}$ with norm $p$ divides $\alpha$ both on the left and on the right, since $p = \pi \overline{\pi} = \pi \overline{\pi}$ (and such an element exists by Theorem 2.1). If $\alpha$ is not divisible by $p$, then Lemma 2.2 yields a left divisor $\pi_1 \in \mathbb{E}$ with norm $p$. Applying this lemma to $\overline{\pi}$ we get a right divisor $\pi_2$ of $\alpha$ with norm $p$. Similarly, $\beta$ has a left divisor $\pi_3$ and a right divisor $\pi_4$ of norm $p$. We also see that if $\alpha$ or $\beta$ is divisible by $p$, then $\pi_1 = \pi_3$ and $\pi_2 = \pi_4$ can be achieved, so the statement of the lemma holds both on the left and on the right.

Thus we can assume that $\alpha$ and $\beta$ are not divisible by $p$. By Lemma 3.1, we have $\alpha \overline{\beta} = - \beta \overline{\alpha}$. Suppose first that this quaternion is not divisible by $p$. The
uniqueness statement of Lemma 2.2 can be applied to \( \alpha \beta = -\beta \alpha \), so \( \pi_1 \) and \( \pi_3 \) are right associates, and the statement of the lemma holds on the left.

If \( \alpha \beta = -\beta \alpha \) is divisible by \( p \), then apply Lemma 2.3 to \( \pi = \pi_2 \), \( \theta = \alpha \), \( \eta = \beta \). We get that \( \pi_2 \mid \beta \), so \( \pi_2 \) is a right divisor of \( \beta \), too, and the statement of the lemma holds on the right. \( \square \)

**Lemma 3.4.** Let \( \alpha_1, \ldots, \alpha_m \in \mathbb{E} \) be pairwise twins and \( p \in \mathbb{Z} \) a prime dividing their common norm. Then there exists a quaternion \( \pi \in \mathbb{E} \) with norm \( p \) such that either \( \pi \) divides every \( \alpha_\ell \) on the left, or \( \pi \) divides every \( \alpha_\ell \) on the right.

**Proof.** Lemma 2.2 yields a left divisor \( \pi_\ell \) of \( \alpha_\ell \) and a right divisor \( \rho_\ell \) of \( \alpha_\ell \) with norm \( p \). If \( p \) does not divide \( \alpha_\ell \), then \( \pi_\ell \) and \( \rho_\ell \) are essentially unique, otherwise they can be chosen arbitrarily. Thus we can disregard those \( \alpha_\ell \) that are divisible by \( p \), and can assume (to simplify notation) that no \( \alpha_\ell \) is divisible by \( p \).

Consider the complete graph on \( \{1, 2, \ldots, m\} \). Color the edge \( \{u, v\} \) to Lilac if \( \pi_u \) and \( \pi_v \) are right associates, and to Red if \( \rho_u \) and \( \rho_v \) are left associates (any edge can carry both colors). The previous lemma shows that every edge has a color. By uniqueness, the lilac edges, as well as the red edges yield a transitive relation. This implies by an elementary graph-theoretic argument that either every edge is lilac, or every edge is red. \( \square \)

Recall that \( \mathbb{Q} = \{\pm 1, \pm i, \pm j, \pm k\} \). We characterize icubes in \( \mathbb{E} \) first.

**Theorem 3.5.** Let \( (\alpha_1, \ldots, \alpha_m) \) be an \( m \)-icube in \( \mathbb{E} \). Then there exist \( \gamma, \delta \in \mathbb{E} \) and an \( m \)-icube \( (\varepsilon_1, \ldots, \varepsilon_m) \in \mathbb{Q}^m \) such that \( \varepsilon_1 = 1 \) and \( \alpha_\ell = \gamma \varepsilon_\ell \delta \) for every \( 1 \leq \ell \leq m \). Conversely, every such \( (\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta) \) is an \( m \)-icube in \( \mathbb{E} \).

**Proof.** Corollary 3.2 implies that \( (\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta) \) is an \( m \)-icube. Conversely, suppose that \( C = (\alpha_1, \ldots, \alpha_m) \) is an \( m \)-icube in \( \mathbb{E} \). Applying Lemma 3.4 and Corollary 3.2 several times successively we see that \( C = (\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta) \) for some \( \gamma, \delta \in \mathbb{E} \) and units \( \varepsilon_\ell \in \mathbb{E} \). Replacing \( \gamma \) by \( \gamma \varepsilon_1 \) we can assume that \( \varepsilon_1 = 1 \). Then \( (\varepsilon_1, \ldots, \varepsilon_m) \) is an \( m \)-icube by Corollary 3.2. Since 1 and \( \varepsilon_\ell \) are twins, the real part of each \( \varepsilon_\ell \) is zero for \( \ell \geq 2 \), and therefore \( \varepsilon_\ell \) has integer coefficients. \( \square \)

To prove extension results we have to characterize icubes in \( \mathbb{L} \). To count them, we need uniqueness in the above decomposition. To achieve these ends we reduce the problem to icubes with odd norm. The next statement is clear by Claim 2.4.

**Claim 3.6.** Suppose that \( N = 2^n D \) where \( n \geq 2 \) and \( D \) is odd. Then every \( m \)-icube \( (\alpha_1, \ldots, \alpha_m) \) in \( \mathbb{L} \) with edge norm \( N \) can be written uniquely as

\[
((1 + i)^{n-1} \beta_1, \ldots, (1 + i)^{n-1} \beta_m),
\]

where \( (\beta_1, \ldots, \beta_m) \) is also an \( m \)-icube in \( \mathbb{L} \). Thus \( f_m(N) = f_m(2D) \). \( \square \)
Claim 3.7. Let $N = 2D$ where $D$ is odd. Then every $m$-cube $(\alpha_1, \ldots, \alpha_m)$ in $L$ with edge norm $N$ can be written uniquely as $(\eta \beta_1, \ldots, \eta \beta_m)$, where $(\beta_1, \ldots, \beta_m)$ is an $m$-cube in $L$ and $\eta \in \{1 + i, 1 + j, 1 + k\}$. Therefore $f_m(N) = 3f_m(D)$.

Proof. By the proof of Claim 2.4 we see that exactly two of the components of every $\alpha_\ell$ are even. Since the vectors corresponding to $\alpha_1, \ldots, \alpha_m$ are pairwise orthogonal, looking at the scalar products modulo 2 we see that these two-element subsets of the indices are either equal or disjoint. Thus (1) of Claim 2.4 shows that the same element of $\{1 + i, 1 + j, 1 + k\}$ can be pulled out of each $\alpha_i$ on the left. This shows that every $m$-cube of edge norm $D$ yields exactly three $m$-cubes of edge norm $2D$. □

To each $m$-cube $(\alpha_1, \ldots, \alpha_m)$ with odd edge norm assign the unique sequence $(g_1, \ldots, g_m)$ with the property that $\alpha_\ell \in S_{g_\ell}$ for every $1 \leq \ell \leq m$ (see Claim 2.5). This sequence is called the type of $(\alpha_1, \ldots, \alpha_m)$. By Claim 2.5 (1), the elements $g_\ell \in K$ are pairwise different. Call an $m$-cube $(\alpha_1, \ldots, \alpha_m)$ orderly, if its type is (1) or (1, i), or (1, i, j), or (1, i, j, k), depending on $m$.

Permuting the components of vectors preserves norm as well as orthogonality. If $(g_1, \ldots, g_m)$ and $(h_1, \ldots, h_m)$ are types, then one can fix a permutation $r$ of $K$ that maps each $h_\ell$ to $g_\ell$. This permutation induces a bijection on $L$:

$$a = a_1 + a_i + a_j j + a_k k \mapsto r(a) = a_{r(1)} + a_{r(i)} i + a_{r(j)} j + a_{r(k)} k.$$

If $(\alpha_1, \ldots, \alpha_m)$ has type $(g_1, \ldots, g_m)$, then $(r(\alpha_1), \ldots, r(\alpha_m))$ has type $(h_1, \ldots, h_m)$, so the number of $m$-cubes of type $(g_1, \ldots, g_m)$ does not depend on $(g_1, \ldots, g_m)$. The number of possible types is $4 \cdot 3 \cdot \ldots \cdot (4 - m + 1) = 24/(4 - m)!$. Hence:

Claim 3.8. Let $N$ be odd. Then $f_m(N) = 24M/(4 - m)!$, where $M$ is the number of orderly $m$-cubes with edge norm $N$. □

Theorem 3.9. Let $\gamma$ and $\delta$ be primary quaternions, and $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm i$, $\varepsilon_3 = \pm j$ and $\varepsilon_4 = \pm k$. Then $(\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta)$ is an orderly $m$-cube in $L$. Conversely, every orderly $m$-cube in $L$ with odd edge norm can be obtained this way.

Proof. Since $\gamma$ and $\delta$ are primary, $(\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta)$ is orderly by (4) of Claim 2.5. Conversely, suppose that $C$ is an orderly $m$-cube in $L$ with odd edge norm. Apply Lemma 3.4 successively, but in every step make sure that $\pi$ is primary (this can be done by Claim 2.6). Claim 2.5 ensures that after pulling out $\pi$ we get an orderly cube in $L$. Thus we get a representation $C = (\gamma \varepsilon_1 \delta, \ldots, \gamma \varepsilon_m \delta)$, where $\gamma$ and $\delta$ are primary. Since $(\varepsilon_1, \ldots, \varepsilon_m)$ is orderly, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm i$, $\varepsilon_3 = \pm j$ and $\varepsilon_4 = \pm k$. □
To deal with the case \( m = 3 \) and \( m = 4 \) we prove uniqueness in Theorem 3.9. We keep the notation that \( \varepsilon_1 = \pm 1, \varepsilon_2 = \pm i, \varepsilon_3 = \pm j \) and \( \varepsilon_4 = \pm k \).

**Lemma 4.1.** Suppose that \( \gamma_1 \varepsilon_1 \delta_1 = \gamma_2 \varepsilon_2 \delta_2 \) for \( \ell = u, v \) and \( N(\gamma_1 \delta_1) = N(\gamma_2 \delta_2) \neq 0 \). Then \( \overline{\gamma_1} \gamma_2 \) permutes with \( \varepsilon_u \overline{\varepsilon_v} \).

**Proof.** Multiply the first equation by the conjugate of the second. We obtain that \( N(\delta_1) \gamma_1 \varepsilon_u \overline{\varepsilon_v} \overline{\gamma_1} = N(\delta_2) \gamma_2 \varepsilon_u \overline{\varepsilon_v} \overline{\gamma_2} \). Now multiply on the left by \( \overline{\gamma_1} \) and on the right by \( \gamma_2 \), and then simplify by \( N(\gamma_1 \delta_1) = N(\gamma_2 \delta_2) \). \( \square \)

An \( m \)-icube is called **primitive**, if the \( 4m \) components of its \( m \) vectors have no common divisor other than \( \pm 1 \).

**Theorem 4.2.** Suppose that \( m \geq 3 \) and \( (\gamma_1 \varepsilon_1 \delta_1, \ldots, \gamma_1 \varepsilon_m \delta_1) = (\gamma_2 \varepsilon_1 \delta_2, \ldots, \gamma_2 \varepsilon_m \delta_2) \) are two representations of an icube given by Theorem 3.9, where \( \gamma_1 \) and \( \gamma_2 \) are primitive. Then \( \gamma_1 = \gamma_2 \) and \( \delta_1 = \delta_2 \). Furthermore, such an icube \( (\gamma_1 \varepsilon_1 \delta_1, \ldots, \gamma_1 \varepsilon_m \delta_1) \) is primitive if and only if \( \gamma_1 \) and \( \delta_1 \) are both primitive.

**Proof.** Lemma 4.1 shows that \( \overline{\gamma_1} \gamma_2 \) permutes with \( \varepsilon_u \overline{\varepsilon_v} = \pm i \) and with \( \varepsilon_1 \overline{\varepsilon_3} = \pm j \). Therefore \( d = \overline{\gamma_1} \gamma_2 \) is a real number. As \( \gamma_1 \) and \( \gamma_2 \) are primary, \( d \in \mathbb{Z} \). We have \( d \gamma_1 = N(\gamma_1) \gamma_2 \). Since \( \gamma_1 \) and \( \gamma_2 \) are primitive, the gcd of the coefficients of the two sides of this equation is \( N(\gamma_1) = \pm d \). Therefore \( \gamma_2 = \pm \gamma_1 \). Since they are primary, they are equal. Then \( \gamma_1 \varepsilon_1 \delta_1 = \gamma_2 \varepsilon_1 \delta_2 \) yields \( \delta_1 = \delta_2 \).

Now let \( C = (\gamma_1 \varepsilon_1 \delta_1, \ldots, \gamma_1 \varepsilon_m \delta_1) \) such that \( \gamma_1 \) and \( \delta_1 \) are primitive and assume to get a contradiction that \( C \) is not primitive. Write \( C \) as \( cC' \), where \( c > 1 \) and \( C' \) is a primitive \( m \)-icube. Then \( C' \) can be represented as \( (\gamma_3 \varepsilon_1 \delta_3, \ldots, \gamma_3 \varepsilon_m \delta_3) \), where \( \gamma_3 \) must be primitive, so \( C \) has a representation \( C = (\gamma_3 \varepsilon_1 (c \delta_3), \ldots, \gamma_3 \varepsilon_m (c \delta_3)) \). Here \( c \delta_3 \) is also primary, since \( c \) is a positive odd integer. The uniqueness statement proved in the previous paragraph shows that \( \delta_1 = c \delta_3 \), contradicting the assumption that \( \delta_1 \) is primitive. \( \square \)

**Corollary 4.3.** Suppose that \( m \geq 3 \) and \( N \) is an odd integer. Then the number of orderly, primitive \( m \)-icubes with edge norm \( N \) is

\[
k(N) = 2^m \sum_{d|N} h(d) h(N/d) .
\]

Here \( h(d) = d \prod_p \left( 1 + \frac{1}{p} \right) \), where \( p \) runs over the prime divisors of \( d \).

**Proof.** Recall that \( h(d) \) is the number of primitive, primary quaternions with norm \( d \) by Claim 2.7. Consider the unique representation given by Theorem 4.2, and let \( d = N(\gamma_1) \). Then \( N(\delta_1) = N/d \). These two quaternions can be chosen \( h(d) h(N/d) \) ways, and \( d \) can be any divisor of \( N \). Finally, there are \( 2^m \) possibilities to chose the signs of \( \varepsilon_1, \ldots, \varepsilon_m \). \( \square \)
We can now compute $f_4$ as stated in Theorem 1.3. Fix $m = 4$ and write $N = 2^nD$, where $D$ is odd. By Claims 3.6 and 3.7 we have that $f_4(N) = 3f_4(D)$ if $n \geq 1$. Next Claim 3.8 shows that $f_4(D) = 24M$, where $M$ is the number of orderly $m$-icubes with edge norm $D$. Finally, each orderly $m$-cube can be written uniquely as $C = cC'$, where $c$ is a positive integer and $C'$ is primitive. Clearly, $c \mid D^2$, and therefore

$$M = \sum_{c^2 \mid N} k(N/c^2),$$

where $k$ is the function defined in Corollary 4.3 for $m = 4$. Thus

$$f_4(D) = (16 \cdot 24) \sum_{c^2 \mid N} \sum_{d \mid (N/c^2)} h(d)h(N/(c^2d)).$$

It is a well-known fact that the convolution of multiplicative functions is multiplicative. Since $h$ is obviously multiplicative, so is $k/16$, which is the convolution of $h$ by itself. The function assigning 1 to squares and 0 to all other integers is also multiplicative, so the double sum above (which is $f_4(D)/384$) is also multiplicative for odd values of $D$. Finally the remarks at the beginning of this argument show that $f_4(N)/384$ is multiplicative on the set of positive integers.

The proof above clearly shows that $f_4(2^n) = 384 \cdot 3$ for $n \geq 1$. If $p$ is an odd prime, then it is a routine calculation to prove, using the last displayed formula, that the value of $f_4(p^n)$ is the one given in (2) of Theorem 1.3. This somewhat complicated summation is left to the reader.

To show that $f_3(N) = f_4(N)/2$ one can either go through the argument above with $m = 3$, or invoke Theorem 1.1 (stating that each 3-icube has exactly two extensions in dimension 4). To compute $f_2(N)$ we need to improve Theorem 3.9, since uniqueness does not hold for $m = 2$.

**Theorem 4.4.** Every orderly 2-icube in $L$ with odd edge norm can be written in the from $(\gamma \varepsilon_1 \delta, \gamma \varepsilon_2 \delta)$, where $\gamma$ and $\delta \in L$ are primary quaternions such that $\gamma i \bar{\gamma}$ is primitive and $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm i$. Here $\gamma$ and $\delta$ are uniquely determined. Such an icube is primitive if and only if $\delta$ is primitive as well.

**Proof.** Theorem 3.9 yields a decomposition $C = (\gamma \varepsilon_1 \delta, \gamma \varepsilon_2 \delta)$. Suppose that $\gamma i \bar{\gamma}$ is divisible by a prime $p$. Apply Lemma 3.3 to $\alpha = \gamma$ and $\beta = \gamma i$. We get that there is a primary $\pi$ with norm $p$ that divides both $\gamma$ and $\gamma i$ on the right. Let $\gamma = \gamma_1 \pi$ (so $\gamma_1$ is primary). Now $\gamma i = \gamma_1 \pi i$ is right divisible by $\pi$, so the uniqueness statement of Lemma 2.2 shows that $\pi i = \varepsilon \pi$ for some unit $\varepsilon$. As $\pi$ is primary, Claim 2.6 gives that $\varepsilon \in Q$, so $\varepsilon \in S$, by Claim 2.5, that is, $\varepsilon = \pm i$. Therefore we can write $C$ as $(\gamma_1 \varepsilon_1 (\pi \delta), \gamma_1 (\pm \varepsilon_2 (\pi \delta)))$. Applying this several times we get a representation where $\gamma i \bar{\gamma}$ is primitive.

Suppose that $C = (\alpha_1, \alpha_2) = (\gamma_1 \varepsilon_1 \delta_1, \gamma_1 \varepsilon_2 \delta_1) = (\gamma_2 \varepsilon_1 \delta_2, \gamma_2 \varepsilon_2 \delta_2)$ are two representations such that $\gamma i \bar{\gamma}$ are both primitive. Then $\alpha_2 \bar{\alpha_1} = N(\delta_1 \gamma i (\varepsilon_2 \bar{\pi_1} \gamma_\ell \bar{\pi_2})$. Here
$\varepsilon_2 \overline{\varepsilon_1} = \pm i$, and therefore this quaternion determines $N(\delta_1)$ as the positive gcd of its coefficients. Thus $N(\delta_1) = N(\delta_2)$ and $\gamma_1 \overline{\gamma_1} = \gamma_2 \overline{\gamma_2}$. The uniqueness statement of Lemma 2.8 shows that $\gamma_1 = \gamma_2$, since both are primary. Thus $\delta_1 = \delta_2$ as well. The uniqueness statement in the last sentence of the theorem can be proved exactly as in Theorem 4.2.

□

Corollary 4.5. Suppose that $N$ is an odd integer. Then the number of orderly, primitive 2-icubes with edge norm $N$ is

$$k_2(N) = 4 \sum_{d|N} q(d)h(N/d),$$

where $p$ runs over the prime divisors of $d$ and the functions $q$ and $h$ are given by Claim 2.9 and Claim 2.7, respectively.

Proof. Consider the unique representation given by Theorem 4.4, and let $d = N(\gamma_1)$. Then $N(\delta_1) = N/d$. These two quaternions can be chosen $q(d)h(N/d)$ ways by the claims quoted in the corollary, and $d$ can be any divisor of $N$. Finally, there are 4 possibilities to choose the signs of $\varepsilon_1$ and $\varepsilon_2$.

□

To compute $f_2$ as stated in Theorem 1.3 we mimic the argument presented above for $f_4$. The reduction to odd norm is the same, and if $D$ is odd, then we get that

$$f_2(D) = (4 \cdot 12) \sum_{c^2|N} \sum_{d|(N/c^2)} q(d)h\left(\frac{N}{(c^2d)}\right).$$

Again, the details of the summation are left to the reader.

References


(Emil W. Kiss) EÖTVÖS UNIVERSITY, DEPARTMENT OF ALGEBRA AND NUMBER THEORY, 1117 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/c, HUNGARY

E-mail address, Emil W. Kiss: ewkiss@math.elte.hu
E-mail address, Péter Kutas: kutasp@gmail.com