

EXACT AMBIENT DIMENSIONS FOR SATURATED ICUBES

SCOTT DUKE KOMINERS

ABSTRACT. We determine the least n for which $\mathbb{Z}^n$ contains r pairwise orthogonal integral vectors of common squared Euclidean norm N whose $\mathbb{Z}$ -span is a direct summand of $\mathbb{Z}^n$. Equivalently, this is the least n for which I_n primitively represents NI_r . For each fixed r , the least ambient dimension that works simultaneously for every $N \geq 1$ is $r + 4\lceil r/4 \rceil$, and every N divisible by 8 attains this bound.

1. THE CLASSIFICATION

By an *integral r -frame of norm N* in $\mathbb{Z}^n$ we mean an ordered r -tuple $(v_1, \dots, v_r)$ such that $v_i \cdot v_j = N\delta_{ij}$. Thus such a frame's vectors are pairwise orthogonal and have common squared Euclidean norm N . Taking them as the edges issuing from the origin gives an r -dimensional cube of side length $\sqrt{N}$ whose vertices all lie in $\mathbb{Z}^n$. Following the icube literature, we accordingly call such a frame an *r -icube*.

A sublattice $L \subseteq \mathbb{Z}^n$ is *saturated* if $\mathbb{Z}^n/L$ is torsion-free, or equivalently—since every finitely generated torsion-free abelian group is free—if L is a direct summand of $\mathbb{Z}^n$; we say that a frame is saturated if its $\mathbb{Z}$ -span is. For fixed positive integers N and r , we seek the least ambient dimension of a saturated r -icube of norm N .

Write $I_n = x_1^2 + \dots + x_n^2$, and let $X \in \mathbb{Z}^{n \times r}$ have columns $v_1, \dots, v_r$. The r -frame condition is then

$$(1) \quad X^\top X = NI_r,$$

and the columns of X span a saturated sublattice precisely when the greatest common divisor of its $r \times r$ minors is 1; in this case X is called *primitive*.

2020 *Mathematics Subject Classification*. Primary 11E25; Secondary 11E12, 94B05.

Key words and phrases. primitive representation, integral quadratic form, saturated sublattice, icube, doubly even code, four-square identity.

I used LLMs to assist with exploration, computation, analysis, and synthesis in the preparation of this article, particularly GPT-5.6 Sol and Claude Fable 5 (accessed in part via Poe with the support of Quora, where I am an advisor). In particular, the problem considered here was first developed as part of an experiment in LLM-aided problem search, and then expanded upon through my own knowledge and thinking around questions of lattice representations. The final methods, analysis, and written form are my own; and of course any errors remain my responsibility. This work was conducted while I was visiting the Technological Innovation, Entrepreneurship, and Strategic Management (TIES) Group at the MIT Sloan School of Management; I greatly appreciate their hospitality.

Thus I_n *primitively represents* NI_r precisely when (1) has a primitive integral solution X .¹

Let $p_N(r)$ denote the least ambient dimension of a saturated r -icube of norm N , i.e.,

$$p_N(r) := \min\{n : I_n \text{ primitively represents } NI_r\}.$$

We call N *Gaussian-primitive*, and write $\text{GP}(N)$, if it has a primitive representation $N = a^2 + b^2$ with $\gcd(a, b) = 1$. The classical formula for primitive representations by two squares [18, Theorem 6.3, p. 247] gives

$$(2) \quad \text{GP}(N) \iff [4 \nmid N \text{ and } p \nmid N \text{ for every prime } p \equiv 3 \pmod{4}].$$

The four conditions heading the table below are thus mutually exclusive and exhaustive for $N > 1$.

Theorem 1.1. *For every $r \geq 1$, we have $p_1(r) = r$. For $N > 1$ and $r \geq 2$, the complete table is*

		GP(N) holds	$\frac{4 \nmid N}{\text{GP}(N) \text{ fails}}$	$N \equiv 4 \pmod{8}$	$8 \mid N$
(3)	$r \equiv 0 \pmod{4}$	$2r$	$2r$	$2r$	$2r$
	$r \equiv 1 \pmod{4}$	$2r$	$2r + 1$	$2r + 2$	$2r + 3$
	$r \equiv 2 \pmod{4}$	$2r$	$2r$	$2r + 2$	$2r + 2$
	$r \equiv 3 \pmod{4}$	$2r$	$2r + 1$	$2r + 1$	$2r + 1$.

For $N > 1$ and $r = 1$,

$$(4) \quad p_N(1) = \begin{cases} 2 & \text{GP}(N) \text{ holds} \\ 3 & \text{GP}(N) \text{ fails and } N \not\equiv 0, 4, 7 \pmod{8} \\ 4 & N \equiv 4 \text{ or } 7 \pmod{8} \\ 5 & 8 \mid N. \end{cases}$$

The extremal consequence of Theorem 1.1 admits a particularly simple formulation in terms of

$$(5) \quad D(r) := r + 4 \left\lceil \frac{r}{4} \right\rceil.$$

Corollary 1.2. *For integers $n \geq r \geq 1$, the following are equivalent:*

- (1) I_n *primitively represents* NI_r for every $N \geq 1$;
- (2) I_n *primitively represents* $8I_r$;
- (3) $n \geq D(r)$.

Moreover, for every positive integer N divisible by 8, the form I_n *primitively represents* NI_r if and only if $n \geq D(r)$.

¹The saturation requirement we use here is stronger than the primitivity convention of [15], which calls an icube primitive when the greatest common divisor of all its entries is 1. For example, the columns of $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ form a 2-icube of norm 2 whose entries have greatest common divisor 1, but their span has index 2 in $\mathbb{Z}^2$ and is therefore not saturated.

Consequently,

$$(6) \quad \max_{N \geq 1} p_N(r) = D(r),$$

and every N divisible by 8 attains the maximum.

In icube language, Corollary 1.2 says that $\mathbb{Z}^n$ contains saturated r -icubes of every positive integral norm precisely when it contains such an icube of norm 8, and this occurs precisely when $n \geq D(r)$.

Outline of the proof. The proof matches lower bounds with explicit saturated frames. Section 2 establishes the baseline lower bound $n \geq 2r$: if a prime p divides N , then saturation keeps the columns independent modulo p , while (1) makes their image totally isotropic. For upper bounds, the identity block makes saturation automatic and reduces norm N to an orthogonal system of norm $N - 1$; Euler’s four-square identity supplies these systems in blocks of four, giving the form of $D(r)$. Section 3 uses Gaussian integers to settle rank 2 and build the even-rank cases, while determinant square classes supply the additional row in the relevant odd-prime, odd-rank cases. Section 4 treats $4 \mid N$: reduction modulo 2 gives a length- n doubly even code of dimension r , and its dimension bound—strengthened in one case by the forced presence of the all-ones word—gives the sharp lower bounds. Three- and four-square representations of $N - 1$ give matching constructions showing that the bounds are in fact attained. At the end of Section 4, these results are assembled along with the classical rank-1 criteria to prove Theorem 1.1 and Corollary 1.2.

Related work. Bernert and Reinhold recently determined the possible side lengths of d -dimensional cubes in $\mathbb{Z}^n$ without imposing a saturation condition [2]. Their problem therefore allows the lattice generated by the edge vectors to have torsion in the ambient quotient, whereas our problem requires that lattice to be a direct summand, and seeks the least possible ambient dimension.

An early study of integral icubes is due to Sárközy, who treated 3-icubes [22]; subsequent contributions include [9, 15, 10]. A related line motivated by discrete quantum computation appears in [8, 17]. Chamizo–Jiménez-Urroz [6] and Erdélyi–Maga–Zábrádi [7] instead study extension of prescribed frames in a fixed ambient dimension.

The case of primitive representation in rank 1 is classical: the two-square criterion is (2), and the primitive criteria for three, four, and five squares are recalled and synthesized in [1, Appendix A].

Meanwhile, rank 2 has several close precedents. Without primitivity, every positive-definite classical binary form is a sum of five squares of integral linear forms [19, 16, 12, 23]; see also [13, 14]. At the determinant level, [1, Appendix A] records that the possible discriminants D of saturated rank-2 sublattices of $\mathbb{Z}^4$ are exactly those with $D \not\equiv 0, 7, 12, 15 \pmod{16}$. Taking $D = N^2$ recovers the necessary condition $4 \nmid N$, but does not force the scalar Gram matrix NI_2 .

Hunsucker defines primitivity by the greatest common divisor of the 2×2 minors; his Theorem 1 [11] specializes to

$$I_4 \text{ primitively represents } NI_2 \iff 4 \nmid N.$$

In Hunsucker's notation, $N(x^2 + y^2)$ has content N and primitive part $x^2 + y^2$, so his criterion says that N must be odd or twice an odd integer. The specialization to prime N is also proved by Budarina [3]; her earlier work treats primitively 2-universal forms of squarefree odd discriminant and class number 1 [5]. Oh-Yoon prove that I_6 primitively represents every positive-definite binary integral form, and that the least rank of a primitively 2-universal form is 6 [20, Theorem 2.4 and its proof]. Their rank-5 obstruction is formulated for general binary targets and does not single out the scalar forms NI_2 ; their local analysis contains a related dyadic exclusion for a split binary lattice over $\mathbb{Z}_2$ [21, Lemma 5.1]. For related local criteria and primitive odd m -universality, see also [4].

Together, the prior rank-2 results determine primitive representation by I_4 and show that I_6 primitively represents every binary target, but they do not decide the scalar problem for I_5 . The remaining rank-2 conclusion needed here is that I_5 does not primitively represent NI_2 when $4 \mid N$; Schinzel's theorem shows that this obstruction is particular to saturation.

To our knowledge, the prior literature has not determined the general values for $p_N(r)$ presented in (3), the formula (6) for the maximum over N , or the criterion in Corollary 1.2 reducing the all- N problem to $N = 8$. Our use of doubly even-code bounds to obtain sharp lower bounds under saturation also appears to be new. That said, the constituent ingredients are classical; our main contribution is in assembling them to give sharp ambient dimensions for every scalar target.

2. GENERAL BOUNDS AND CONSTRUCTIONS

If an integral $n \times r$ matrix X of rank r has Smith invariant factors $d_1 \mid \cdots \mid d_r$, then the greatest common divisor of its $r \times r$ minors is $d_1 \cdots d_r$. Thus X is primitive if and only if every d_i is 1, equivalently if and only if $X \bmod p$ has rank r for every prime p . This gives the following general lower bound.

Lemma 2.1. *If $N > 1$, then $p_N(r) \geq 2r$.*

Proof. Choose a prime $p \mid N$ and suppose that X satisfies (1). Primitivity makes $X \bmod p$ have rank r , while $X^\top X \equiv 0 \pmod{p}$ makes its image W satisfy $W \subseteq W^\perp$ in the nondegenerate dot-product space $\mathbb{F}_p^n$. Hence $r = \dim W \leq \dim W^\perp = n - r$. $\square$

The following identity-block construction enforces primitivity.

Lemma 2.2. *If $Y \in \mathbb{Z}^{m \times r}$ satisfies $Y^\top Y = (N - 1)I_r$, then*

$$X := \begin{pmatrix} I_r \\ Y \end{pmatrix} \in \mathbb{Z}^{(m+r) \times r}$$

is primitive and satisfies $X^\top X = NI_r$.

Proof. The Gram identity is immediate, and meanwhile the minors coming from the first r rows have determinant 1 by construction. $\square$

We shall also use that block-diagonal sums of primitive matrices are primitive, because the corresponding ambient quotient is the direct sum of the torsion-free quotient lattices.

For $a, b, c, d \in \mathbb{Z}$, let

$$(7) \quad H(a, b, c, d) := \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

Euler's four-square identity is

$$(8) \quad H(a, b, c, d)^\top H(a, b, c, d) = (a^2 + b^2 + c^2 + d^2)I_4.$$

Together with Lagrange's theorem and Lemma 2.2, this gives

$$(9) \quad p_N(r) \leq r + 4 \left\lceil \frac{r}{4} \right\rceil = D(r).$$

Indeed, choose $a, b, c, d \in \mathbb{Z}$ with $N - 1 = a^2 + b^2 + c^2 + d^2$, put $k = \lceil r/4 \rceil$, and let $Y \in \mathbb{Z}^{4k \times r}$ consist of any r columns of the block-diagonal sum of k copies of $H(a, b, c, d)$. Then $Y^\top Y = (N - 1)I_r$, so Lemma 2.2 gives a representation in $r + 4k$ rows and hence (9).

We also use the following sharper row counts. Suppose that $M = a^2 + b^2 + c^2$ and write $r = 4q + s$, with $0 \leq s \leq 3$. Use q copies of $H(a, b, c, 0)$ in mutually disjoint row sets; if $s = 2$ or 3 , retain s columns of one further copy, while if $s = 1$, place $(a, b, c)^\top$ directly in three new coordinates. This gives an integral Y with $Y^\top Y = MI_r$ in

$$(10) \quad r, \quad r + 2, \quad r + 2, \quad r + 1$$

rows according as $r \equiv 0, 1, 2, 3 \pmod{4}$. If M is a sum of four squares, the analogous row counts are

$$(11) \quad r, \quad r + 3, \quad r + 2, \quad r + 1.$$

3. RANK 2 AND ODD PRIMES

We first settle the rank-2 case of Theorem 1.1. The following Gaussian calculation constructs a primitive representation in four variables exactly when $4 \nmid N$; reduction modulo 2 then excludes representation by I_5 when $4 \mid N$.

Lemma 3.1. *For $N > 1$, we have*

$$p_N(2) = \begin{cases} 4 & 4 \nmid N \\ 6 & 4 \mid N. \end{cases}$$

Proof. Identify $\mathbb{Z}^4$ with $\mathbb{Z}[i]^2$. For $z, w \in \mathbb{Z}[i]$, the columns corresponding to (z, w) and $i(z, w)$ are orthogonal and both have squared norm $|z|^2 + |w|^2$. Their $\mathbb{Z}$ -span is the Gaussian submodule $\mathbb{Z}[i](z, w)$. If g generates the ideal $z\mathbb{Z}[i] + w\mathbb{Z}[i]$, then Smith normal form over the principal ideal domain $\mathbb{Z}[i]$ gives

$$\mathbb{Z}[i]^2/\mathbb{Z}[i](z, w) \simeq \mathbb{Z}[i] \oplus \mathbb{Z}[i]/(g).$$

Since $N > 0$, the element g is nonzero, and $\mathbb{Z}[i]/(g)$ is a finite abelian group that is torsion-free only when it is trivial. Thus the submodule is saturated over $\mathbb{Z}$ if and only if g is a unit, or equivalently $z\mathbb{Z}[i] + w\mathbb{Z}[i] = \mathbb{Z}[i]$; call such a pair *unimodular*.

Let $U(N)$ count ordered unimodular pairs (z, w) with $|z|^2 + |w|^2 = N$, and let $A(d)$ be the number of ideals of $\mathbb{Z}[i]$ of norm d . Let $r_4(N)$ denote the number of ordered representations of N by four squares. For each ideal $\mathfrak{a}$ of norm d , fix a generator $\alpha_{\mathfrak{a}}$. The pairs with gcd ideal $\mathfrak{a}$ are uniquely of the form $\alpha_{\mathfrak{a}}(z', w')$, where (z', w') is unimodular and has norm N/d ; changing the chosen generator only permutes these pairs. Summing over $\mathfrak{a}$ gives

$$(12) \quad r_4(N) = \sum_{d|N} A(d)U(N/d).$$

Meanwhile, Jacobi's formula says that

$$r_4(N) = 8 \sum_{\substack{d|N \\ 4 \nmid d}} d.$$

Set $f := r_4/8$ and $u := U/8$. Then (12) becomes $f = A * u$, where $*$ denotes Dirichlet convolution. Jacobi's formula makes f multiplicative, while unique factorization of ideals makes A multiplicative; because $A(1) = 1$, the convolution identity then means that u must be multiplicative as well. For a prime p , write $f_p(T) := \sum_{e \geq 0} f(p^e)T^e$, and define $A_p(T)$ and $u_p(T)$ similarly. The local factors and their quotients are

	$\frac{f_p(T)}{1+2T}$	$\frac{A_p(T)}{1-T}$	$u_p(T) = f_p(T)/A_p(T)$
$p = 2$	$\frac{1}{1-T}$	$\frac{1}{1-T}$	$1+2T$
$p \equiv 1 \pmod{4}$	$\frac{1}{(1-T)(1-pT)}$	$\frac{1}{(1-T)^2}$	$\frac{1-T}{1-pT}$
$p \equiv 3 \pmod{4}$	$\frac{1}{(1-T)(1-pT)}$	$\frac{1}{1-T^2}$	$\frac{1+T}{1-pT}$

Let χ_{-4} be the quadratic character modulo 4. Reading off coefficients gives

$$\begin{aligned} u(2) &= 2, & u(2^e) &= 0 & (e \geq 2), \\ u(p^e) &= p^{e-1}(p - \chi_{-4}(p)) & & & (p \text{ odd}, e \geq 1). \end{aligned}$$

Thus $U(N) > 0$ if and only if $4 \nmid N$. Lemma 2.1 now gives $p_N(2) = 4$ in that case.

If $4 \mid N$, then reduction modulo 2 of a primitive representation in four or five rows would induce a doubly even code of dimension 2. Indeed, primitivity

makes the reduction have dimension 2, and an integral square is congruent modulo 4 to 0 or 1 according as the integer is even or odd. Thus, for $\xi \in \mathbb{F}_2^2$, its coordinatewise lift $\tilde{\xi} \in \{0, 1\}^2$, and $z = X\tilde{\xi}$, we have

$$\text{wt}(z \bmod 2) \equiv z^\top z = N\tilde{\xi}^\top \tilde{\xi} \equiv 0 \pmod{4}.$$

No such 2-dimensional code exists: at length 4 there is only one nonzero word whose weight is divisible by 4, while two distinct words of weight 4 in length 5 have sum of weight 2. Thus $p_N(2) \geq 6$, while (9) gives $p_N(2) \leq 6$. $\square$

The condition $\text{GP}(N)$ is the usual criterion for a primitive vector $(a, b) \in \mathbb{Z}^2$ of squared norm N . Placing r copies of such a vector in disjoint coordinate pairs gives

$$(13) \quad p_N(r) = 2r \quad (N > 1 \text{ under } \text{GP}(N)),$$

by Lemma 2.1. Direct sums of the representations in Lemma 3.1 likewise give $p_N(r) = 2r$ whenever $4 \nmid N$ and r is even.

Lemma 3.2. *Suppose that r is odd and a prime $p \equiv 3 \pmod{4}$ divides N . Then $p_N(r) \geq 2r + 1$.*

Proof. Equality in Lemma 2.1 would give a maximal totally isotropic r -space in $(\mathbb{F}_p^{2r}, I_{2r})$. A nondegenerate form of dimension $2r$ with such a subspace is hyperbolic. Its determinant square class is that of the hyperbolic Gram matrix $\begin{pmatrix} 0 & I_r \\ I_r & 0 \end{pmatrix}$, namely $(-1)^r$. On the other hand, I_{2r} has determinant square class 1. Since r is odd and -1 is a nonsquare in $\mathbb{F}_p$, this is impossible. $\square$

When $4 \nmid N$, $r \geq 3$ is odd, and a prime $p \equiv 3 \pmod{4}$ divides N , the lower bound in Lemma 3.1 is attained: Choose a four-square representation of $N - 1$, take three columns of the corresponding matrix $H(a, b, c, d)$, and apply Lemma 2.2 to obtain a primitive representation of NI_3 in seven rows. Adding $(r - 3)/2$ copies of the rank-2 representation furnished by Lemma 3.1 uses $4 \cdot (r - 3)/2$ additional rows, for a total of

$$7 + 4 \frac{r - 3}{2} = 2r + 1.$$

4. THE DYADIC CASES

Let $\mathcal{E}_n$ denote the even-weight subspace of $\mathbb{F}_2^n$:

$$\mathcal{E}_n := \{x \in \mathbb{F}_2^n : \text{wt}(x) \equiv 0 \pmod{2}\}$$

and define

$$(14) \quad q_n(x) := \frac{\text{wt}(x)}{2} \pmod{2} \quad (x \in \mathcal{E}_n).$$

The polar form of q_n is the restriction of the standard dot product:

$$(15) \quad q_n(x + y) + q_n(x) + q_n(y) = x \cdot y.$$

A linear code $C \subseteq \mathbb{F}_2^n$ is *doubly even* exactly when $C \subseteq \mathcal{E}_n$ and q_n vanishes on C .

Write $\kappa(n)$ for the largest possible dimension of a doubly even binary code of length n . The value $\kappa(n)$ is standard in coding theory; we include a short proof tailored to the present application, together with the additional assertion for $n \equiv 4 \pmod{8}$ needed below; the latter is closely related to the usual extension properties of doubly even codes.

Lemma 4.1. *For $n \geq 1$,*

$$(16) \quad \begin{array}{c|cccc} n \bmod 8 & 0 & 1 & 2 & 3 \\ \hline \kappa(n) & n/2 & (n-1)/2 & (n-2)/2 & (n-3)/2 \\ \hline n \bmod 8 & 4 & 5 & 6 & 7 \\ \hline \kappa(n) & (n-2)/2 & (n-3)/2 & (n-2)/2 & (n-1)/2. \end{array}$$

If $n \equiv 4 \pmod{8}$ and C is doubly even with $\dim C = \kappa(n)$, then the all-ones word $\mathbf{1}$ belongs to C .

Proof. The radical of the polar form on $\mathcal{E}_n$ is trivial when n is odd. When n is even, it is $R = \langle \mathbf{1} \rangle$, and

$$(17) \quad q_n(\mathbf{1}) = \frac{n}{2} \pmod{2}.$$

The Gauss sum of q_n is

$$(18) \quad \sum_{x \in \mathcal{E}_n} (-1)^{q_n(x)} = \operatorname{Re}((1+i)^n) = 2^{n/2} \cos\left(\frac{n\pi}{4}\right).$$

For a nondegenerate quadratic space of dimension $2m$ over $\mathbb{F}_2$, the Gauss sum is $(-1)^{\operatorname{Arf}(q)} 2^m$, and the maximal totally singular dimension is m or $m-1$ according as the Arf invariant is 0 or 1. When n is odd, $\mathcal{E}_n$ has dimension $n-1$ and is nondegenerate. The sign in (18) is positive for $n \equiv 1, 7 \pmod{8}$ and negative for $n \equiv 3, 5 \pmod{8}$, giving the four odd entries of (16).

Suppose that n is even. If $n \equiv 2 \pmod{4}$, then $q_n(\mathbf{1}) = 1$, so $\mathbf{1}$ is not singular. A totally singular subspace therefore meets R trivially and projects injectively to an isotropic subspace of the nondegenerate symplectic space $\mathcal{E}_n/R$, giving dimension at most $(n-2)/2$. If $n \equiv 0 \pmod{4}$, then $q_n(x + \mathbf{1}) = q_n(x)$ for every $x \in \mathcal{E}_n$, so q_n descends to a nondegenerate quadratic form on $\mathcal{E}_n/R$. Its Gauss sum is half of (18), so its Arf invariant is 0 for $n \equiv 0 \pmod{8}$ and 1 for $n \equiv 4 \pmod{8}$. The quotient has dimension $n-2$, so its Witt index is $(n-2)/2$ in the first case and $(n-4)/2$ in the second. Adjoining the singular radical gives the remaining entries of (16).

For attainment, write $n = 8\ell + t$, where $0 \leq t \leq 7$. Take the direct sum of ℓ copies of the doubly even extended binary Hamming $[8, 4, 4]$ code and a residual code C_t . Let C_t be the zero code of length t for $t = 0, 1, 2, 3$, set $C_5 = \{(c, 0) : c \in C_4\}$, and let C_4, C_6, C_7 be generated respectively by

$$(1 \ 1 \ 1 \ 1), \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

The displayed rows are independent, and every nonzero word in each residual code has weight 4. The residual dimensions for $t = 0, \dots, 7$ are therefore $0, 0, 0, 0, 1, 1, 2, 3$, which attains every entry of (16). Finally, if $n \equiv 4 \pmod{8}$ and $\dim C = n/2 - 1$, then the quotient $\mathcal{E}_n/R$ has Witt index $n/2 - 2$. If C did not contain R , then we must have $C \cap R = 0$, so its image in the quotient would be a totally singular space of dimension $n/2 - 1$, a contradiction. Hence $\mathbf{1} \in C$. $\square$

Proposition 4.2. *Suppose that $4 \mid N$ and $r \geq 2$. According as $r \equiv 0, 1, 2, 3 \pmod{4}$, we have*

$$p_N(r) \geq 2r, \quad 2r+2, \quad 2r+2, \quad 2r+1.$$

If moreover $8 \mid N$ and $r \equiv 1 \pmod{4}$, then $p_N(r) \geq 2r+3$.

Proof. Let X be primitive with $X^\top X = NI_r$. Its reduction modulo 2 has rank r . For $u \in \mathbb{F}_2^r$, lift u to $\tilde{u} \in \{0, 1\}^r$ and put $z = X\tilde{u}$. Then

$$\text{wt}(z \bmod 2) \equiv z^\top z = N\tilde{u}^\top \tilde{u} \equiv 0 \pmod{4}.$$

Thus the image of $X \bmod 2$ is a doubly even code of dimension r , and $r \leq \kappa(n)$. Since $n \geq 2r$, reading (16) from $n = 2r$ upward shows that the first possible n is $2r, 2r+2, 2r+2$, or $2r+1$, according as $r \equiv 0, 1, 2$, or $3 \pmod{4}$.

It remains to sharpen the bound when $8 \mid N$ and $r = 4k+1$. At the only remaining candidate $n = 2r+2 = 8k+4$, the code has maximum dimension, so Lemma 4.1 gives $\mathbf{1}$ in its image. Choose $u \in \mathbb{F}_2^r$ such that $(X \bmod 2)u = \mathbf{1}$. Every coordinate of the corresponding vector $z = X\tilde{u}$ is odd, and hence

$$z^\top z \equiv n \equiv 4 \pmod{8}$$

(using the fact that every odd square is congruent to 1 modulo 8). But $z^\top z = N\tilde{u}^\top \tilde{u}$ is divisible by 8, a contradiction. $\square$

The bounds in Proposition 4.2 are sharp: If $N \equiv 4 \pmod{8}$, then $N-1 \equiv 3 \pmod{8}$ and hence, by Legendre's three-square theorem, is a sum of three squares. Applying Lemma 2.2 to the row counts in (10) gives, according as $r \equiv 0, 1, 2, 3 \pmod{4}$,

$$(19) \quad 2r, \quad 2r+2, \quad 2r+2, \quad 2r+1.$$

If $8 \mid N$, then $N-1 \equiv 7 \pmod{8}$ is not a sum of three squares by Legendre's theorem but is a sum of four squares by Lagrange's theorem. Thus (11) gives

$$(20) \quad 2r, \quad 2r+3, \quad 2r+2, \quad 2r+1.$$

Proof of Theorem 1.1. For $N = 1$, we have $p_1(r) \geq r$ a priori, while $X = I_r$ gives equality.

For $N > 1$ and $r \geq 2$, equation (13) gives the first column of (3). For the second column of (3), direct sums of the rank-2 representations in Lemma 3.1 give $2r$ rows when r is even. When r is odd, failure of $\text{GP}(N)$ supplies a prime $p \equiv 3 \pmod{4}$ dividing N ; Lemma 3.2 and the seven-row rank-3

construction above give $2r + 1$. Proposition 4.2, together with the attainment recorded in (19) and (20), gives the final two columns of (3).

It remains to consider the case $r = 1$. Factorization in $\mathbb{Z}[i]$ gives a primitive representation by two squares exactly when $\text{GP}(N)$ holds. A primitive representation by three squares exists if and only if $N \not\equiv 0, 4, 7 \pmod{8}$, and one by four squares exists if and only if $8 \nmid N$ (again, for a synthesis of these classical primitive representation results, see [1, Appendix A]). Finally, Lagrange’s theorem gives $N - 1 = a^2 + b^2 + c^2 + d^2$, so $N = 1^2 + a^2 + b^2 + c^2 + d^2$ is a primitive representation by five squares. Taking the least available number of squares gives (4). $\square$

Proof of Corollary 1.2. The implication (1) $\Rightarrow$ (2) is immediate. Equation (9), followed if necessary by adjoining zero rows, gives (3) $\Rightarrow$ (1); adjoining such rows preserves the greatest common divisor of the maximal minors. Theorem 1.1 gives $p_N(r) = D(r)$ whenever $8 \mid N$. Taking $N = 8$ proves (2) $\Rightarrow$ (3), and the same identity proves the final assertion. $\square$

Remark 4.3. For $r \equiv 1 \pmod{4}$, the code bound falls one coordinate short of $D(r)$. At the remaining candidate, saturation makes the binary image a maximum-dimensional doubly even code, so it contains $\mathbf{1}$. A coefficient vector mapping to $\mathbf{1}$ lifts to an integral combination with every coordinate odd, hence squared norm 4 modulo 8, contradicting the hypothesis $8 \mid N$. Without saturation the binary image may have dimension below r , so this obstruction need not apply.

REFERENCES

1. M. Aka, A. Musso, and A. Wieser, *Equidistribution of rational subspaces and their shapes*, Ergodic Theory Dynam. Systems **44** (2024), 2009–2062, doi:10.1017/etds.2023.107.
2. C. Bernert and J. Reinhold, *Side lengths of cubes with vertices in $\mathbb{Z}^n$* , 2026, arXiv:2602.22202.
3. N. Budarina, *Primitive two-dimensional prime-universality of quadratic forms*, J. Pure Appl. Algebra **229** (2025), no. 6, Art. 107968, doi:10.1016/j.jpaa.2025.107968.
4. ———, *Primitive odd m -universality of quadratic forms with odd square-free determinant*, J. Algebra Appl. (2026), doi:10.1142/S0219498827502720.
5. N. V. Budarina, *On primitively 2-universal quadratic forms*, St. Petersburg Math. J. **23** (2012), no. 3, 435–458.
6. F. Chamizo and J. Jiménez-Urroz, *Extendable orthogonal sets of integral vectors*, Res. Math. Sci. **9** (2022), Art. 59, doi:10.1007/s40687-022-00357-9.
7. M. Erdélyi, P. Maga, and G. Zábrádi, *Extensions of integral orthoregular sets and icubes*, 2025, arXiv:2508.01196.
8. L. N. Gatti and J. Lacalle, *A model of discrete quantum computation*, Quantum Inf. Process. **17** (2018), no. 8, Art. 192, doi:10.1007/s11128-018-1956-0.
9. L. M. Goswick, E. W. Kiss, G. Moussong, and N. Simányi, *Sums of squares and orthogonal integral vectors*, J. Number Theory **132** (2012), no. 1, 37–53, doi:10.1016/j.jnt.2011.07.001.
10. M. Horváth, *Cubic sublattices*, Discrete Comput. Geom. **71** (2024), no. 4, 1369–1380, doi:10.1007/s00454-023-00535-8.
11. J. L. Hunsucker, *Primitive representation of a binary quadratic form as a sum of four squares*, Acta Arith. **19** (1971), 321–325, doi:10.4064/aa-19-4-321-325.
12. B. M. Kim, M.-H. Kim, and B.-K. Oh, *2-universal positive definite integral quinary quadratic forms*, Integral Quadratic Forms and Lattices, Contemp. Math., vol. 249, American Mathematical Society, 1999, pp. 51–62.
13. M.-H. Kim and B.-K. Oh, *Bounds for quadratic Waring’s problem*, Acta Arith. **104** (2002), 155–164, doi:10.4064/aa104-2-5.

14. ———, *Representations of integral quadratic forms by sums of squares*, Math. Z. **250** (2005), no. 2, 427–442, doi:10.1007/s00209-005-0761-5.
15. E. W. Kiss and P. Kutas, *Cubes of integral vectors in dimension four*, Studia Sci. Math. Hungar. **49** (2012), no. 4, 525–537, doi:10.1556/SScMath.49.2012.4.1225.
16. C. Ko, *On the representation of a quadratic form as a sum of squares of linear forms*, Quart. J. Math. **os-8** (1937), no. 1, 81–98, doi:10.1093/qmath/os-8.1.81.
17. J. Lacalle and L. N. Gatti, *Discrete quantum computation and Lagrange’s four-square theorem*, Quantum Inf. Process. **19** (2020), no. 1, Art. 34, doi:10.1007/s11128-019-2528-7.
18. R. A. Mollin, *Fundamental number theory with applications*, 2nd ed., Discrete Mathematics and Its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2008, doi:10.1201/b15895.
19. L. J. Mordell, *A new Waring’s problem with squares of linear forms*, Quart. J. Math. **os-1** (1930), no. 1, 276–288, doi:10.1093/qmath/os-1.1.276.
20. B.-K. Oh and J. Yoon, *Primitively 2-universal senary integral quadratic forms*, J. Number Theory **264** (2024), 148–183, doi:10.1016/j.jnt.2024.05.006.
21. ———, *Minimal rank of primitively n -universal integral quadratic forms over local rings*, Ramanujan J. **71** (2026), Art. 1, doi:10.1007/s11139-026-01449-8.
22. A. Sárközy, *Lattice cubes in 3-space*, Mat. Lapok **12** (1961), 232–245.
23. A. Schinzel, *A positive definite binary quadratic form as a sum of five squares of linear forms (completion of Mordell’s proof)*, Bull. Polish Acad. Sci. Math. **61** (2013), no. 1, 23–26, doi:10.4064/ba61-1-3.

HARVARD BUSINESS SCHOOL; DEPARTMENT OF ECONOMICS AND CENTER OF MATHEMATICAL SCIENCES AND APPLICATIONS, HARVARD UNIVERSITY; AND A16Z CRYPTO
Email address: `kominers@fas.harvard.edu`