Mathematical proof note

Nonexistence of Perfect Two-Error-Correcting Lee Codes

Yang Shifu
National Mobile Communications Research Laboratory and the Frontiers Science Center for Mobile Information Communication and Security, Southeast University, Nanjing 211189, China

Version 1.0 — October 16, 2026

Result overview

Perfect Lee codes attain the sphere-packing bound for additive errors of bounded total symbol magnitude. This note resolves the radius-two case of the Golomb–Welch conjecture for arbitrary code subsets. No perfect two-error-correcting Lee code exists in the integer lattice $\mathbb{Z}^n$ for any $n \geq 3$, without assumptions of linearity, periodicity, or lattice structure. The proof places all local counts on one translation-invariant binary codeword process. Exact convolution moments and congruences modulo three and five determine the admissible local distributions. In the remaining dimension classes, a codeword-anchored deficit grows by a factor of three under successive dyadic dilations while remaining uniformly bounded, which yields a contradiction after finitely many scales. The result also gives the complete radius-two existence classification over cyclic alphabets of size at least five and a uniform relative gap below the sphere-packing bound at every fixed length $n \geq 3$.

Proof architecture

The argument has four load-bearing stages. First, the same codeword set tiles every integer dilation of the radius-two Lee sphere whose scale is coprime to the sphere cardinality. Second, symmetric convolution masks give three exact second-moment identities; the moment at scale 2^j retains a conditional term from scale 2^{j+1}. Third, reduction modulo three either gives an immediate contradiction or fixes one of two five-state distributions, after which reduction modulo five excludes every dimension class with $5 \nmid n$. Finally, when $5 \mid n$, the conditional-moment deficit satisfies

$$\Delta_{j+1} \geq 3\Delta_j, \qquad \Delta_j \geq \frac{s-1}{s+1}, \qquad \Delta_j \leq s-1.$$

A finite number of dyadic scales is therefore sufficient. Every variable appearing below is evaluated on the same probability space, and no periodicity reduction is used.

1 Introduction

Lee-metric codes measure an error by its total symbol magnitude and provide a natural model for nonbinary error correction [1]. Their algebraic constructions and decoding methods have been

applied to constrained and partial-response channels, where the magnitudes of symbol changes carry information about the error mechanism [2]. For a code over the integer alphabet, a decoding sphere of radius two contains all additive error vectors with total absolute magnitude at most two. Perfectness requires these spheres to be disjoint and to cover every received word. The existence question therefore concerns equality in the sphere-packing bound and the joint compatibility of all decoding regions.

Golomb and Welch [3] formulated the conjecture that perfect Lee codes over $\mathbb{Z}^n$ do not exist when the dimension is at least three and the error-correcting radius is at least two. Their constructions establish perfect codes in dimensions one and two for every radius, and in every dimension for radius one. They also established nonexistence for sufficiently large radii at each fixed dimension. Radius two is the first case beyond single-error correction and requires a result uniform in the dimension. Horak and Kim [4] surveyed the conjecture, developed explicit large-radius bounds, and described algebraic conditions for translational Lee-sphere tilings.

Geometric arguments resolved several low-dimensional cases. Horak [5] proved nonexistence in dimensions three through five for every radius at least two, and established the radius-two result in dimension six in [6]. Algebraic methods provided a second direction. Horak and Grošek [7] excluded linear radius-two codes through dimension twelve by studying homomorphisms from the integer lattice to finite abelian groups. Kim [8] obtained a number-theoretic criterion for arbitrary radius-two codes in dimensions for which the sphere cardinality is prime. These results connected the existence problem to both local geometric restrictions and the arithmetic of $2n^2 + 2n + 1$.

Leung and Zhou [9] subsequently proved the nonexistence of lattice radius-two Lee tilings in every dimension $n \geq 3$. Their result also excludes arbitrary tilings when $2n^2 + 2n + 1$ is prime. A central feature of their proof is the study of multiplicities in two group-ring products, first modulo three and then modulo five. The resulting residue-class analysis supplies strong restrictions on the possible local counts. Closely related work has considered codes near the sphere-packing bound: Camarero and Martínez [10] constructed quasi-perfect radius-two Lee codes in arbitrarily large dimensions, while Zhou and Zhou [11] restricted almost perfect linear radius-two codes to a finite set of dimensions. These developments sharpen the distinction between correcting every error of Lee weight at most two and attaining perfect coverage.

For an arbitrary subset of $\mathbb{Z}^n$, the counting argument must accommodate spatial dependence and retain a common codeword indicator at all scales. Translation averaging provides such a setting: local codeword counts become integer-valued random variables on one probability space, and symmetric convolutions remain self-adjoint. The critical additional quantity is a codeword-conditioned moment linking scales a and $4a$. Its value can depend on a, so the second moment at one scale involves a quantity at the next scale. This dependence becomes the mechanism that completes the proof. Our formulation uses the same-code dilation principle of Horak and Kim [4, Theorem 24 and Corollary 25] and develops the modular counting approach of Leung and Zhou [9, Section 3] for this translation-invariant setting.

In this note, we prove the nonexistence of perfect two-error-correcting Lee codes over $\mathbb{Z}^n$ for every $n \geq 3$. A common translation average retains the binary codeword indicator and all exact decoding relations. Three second-moment identities then determine two five-state distributions after reduction modulo three, and reduction modulo five excludes eight further dimension classes. These distributions are derived explicitly from the coverage equations and their integer-valued counts.

For the remaining dimensions, we introduce a conditional-moment deficit that is bounded at every scale. Its second-moment relation forces a factor-of-three increase whenever the scale doubles.

We prove a strictly positive lower bound by conditioning a directional sum on a codeword; translation averaging counts each resulting mismatch exactly once. The two estimates complete the argument after finitely many scales and extend the modular method to arbitrary code subsets.

The coding consequences include a complete radius-two existence classification for cyclic alphabets of size at least five. We also obtain, at each fixed length at least three, a positive relative gap below the sphere-packing bound that is uniform in the alphabet size. A finite-alphabet approximation relates the normalized maximum code size to the optimal packing density on the integer alphabet, with an explicit boundary-loss estimate. These consequences follow from the main theorem, periodic lifting, and compactness of the space of codeword indicators.

Section 2 states the main theorem and develops the common translation model. Section 3 derives the local counts, exact moments, and modular relations. Sections 4 and 5 complete the dimension analysis. Section 6 gives the finite-alphabet classification and packing-density consequences, and Section 7 concludes the note.

2 Code Model and Main Result

In this section, we formulate perfect Lee decoding over the integer alphabet and introduce a translation-invariant representation of a hypothetical perfect code. This representation allows all subsequent expectations to be evaluated with respect to one probability measure.

2.1 Perfect Radius-Two Lee Codes

For $x, y \in \mathbb{Z}^n$, define the Lee distance by

$$d_{\mathrm{L}}(x, y) = \sum_{i=1}^{n} |x_i - y_i|. \tag{1}$$

For a nonnegative integer r, the corresponding Lee sphere is

$$B_r^n = \{x \in \mathbb{Z}^n : \|x\|_1 \le r\}, \qquad r \ge 0. \tag{2}$$

Throughout the proof, let

$$B = B_2^n, \qquad M = |B| = 2n^2 + 2n + 1, \tag{3}$$

$$V = \{0, \pm e_1, \dots, \pm e_n\}, \qquad s = |V| = 2n + 1, \tag{4}$$

where e_i is the ith coordinate vector. A code $C \subseteq \mathbb{Z}^n$ corrects every error in B when its distinct codewords have Lee distance at least five. It is perfect when, in addition, every $x \in \mathbb{Z}^n$ is within Lee distance two of a codeword. Thus its binary indicator $f = \mathbf{1}_C$ satisfies

$$\sum_{b \in B} f(x - b) = 1 \qquad (x \in \mathbb{Z}^n). \tag{5}$$

The main result determines the existence of such a code in every dimension at least three.

Theorem 2.1. *For every integer $n \ge 3$, there is no perfect two-error-correcting Lee code in $\mathbb{Z}^n$.*

2.2 Dilations and a Common Translation Average

For a function h on $\mathbb{Z}^n$, let $(S^v h)(x) = h(x - v)$ and define

$$Q_a = \sum_{b \in B} S^{ab}, \qquad T_a = \sum_{u \in V} S^{au}, \qquad a \geq 1. \tag{6}$$

A dilation has the form $aB = \{ab : b \in B\}$ and retains exactly M points. Operator powers such as T_a^2 denote repeated convolution. We first establish the dilation relation that supplies the required codeword separation at several scales.

Lemma 2.2. *If $f : \mathbb{Z}^n \to \{0, 1\}$ satisfies $Q_1 f = \mathbf{1}$, then*

$$Q_a f = \mathbf{1} \qquad \textit{whenever } \gcd(a, M) = 1. \tag{7}$$

Consequently, distinct codewords have no difference in $a(B_4^n \setminus \{0\})$ for any such a.

Proof. For a prime $p \nmid M$, the integer Laurent-polynomial identity modulo p gives $Q_p \equiv Q_1^p \pmod{p}$. Applying this identity to f yields

$$Q_p f \equiv M^{p-1} \equiv 1 \pmod{p}. \tag{8}$$

Every value of $Q_p f$ is a nonnegative integer, and hence is at least one. Since all shifts commute,

$$Q_1(Q_p f) = Q_p(Q_1 f) = M\mathbf{1}.$$

Each value on the left is the sum of M integers that are at least one. All summands equal one. As $0 \in B$, this determines $Q_p f$ at every point.

For composite a, apply the prime argument successively to bB after the relation has been established for b. Each intermediate set has cardinality M. Finally, $B_2^n - B_2^n = B_4^n$; a nonzero codeword difference in aB_4^n would produce an overlap between two translates of aB and contradict (7). □

We next average translates of one hypothetical code. This step preserves the binary values of the indicator and every pointwise coverage relation.

Lemma 2.3. *If (5) has a solution, its binary solution space supports a translation-invariant probability measure μ. For the origin indicator $F(\omega) = \omega(0)$,*

$$\mathbb{E}F = \rho := M^{-1}. \tag{9}$$

Finite symmetric sums of shifts are commuting self-adjoint operators on $L^2(\mu)$.

Proof. Let $\Omega \subseteq \{0, 1\}^{\mathbb{Z}^n}$ be the solution space of (5). It is compact because each covering equation is a closed condition involving finitely many coordinates. It is also invariant under $\tau_v \omega(x) = \omega(x - v)$. Starting from a solution ω_*, take a weakly convergent subsequence of the probability measures

$$\frac{1}{(2R + 1)^n} \sum_{v \in [-R,R]^n \cap \mathbb{Z}^n} \delta_{\tau_v \omega_*}. \tag{10}$$

For every fixed translation, the relative size of the symmetric difference of the original and translated averaging boxes tends to zero. The limit μ is therefore translation invariant and remains supported on Ω. Taking expectation in $Q_1 F = 1$ gives (9).

On observables, $S^v H = H \circ \tau_v$ is unitary and has adjoint S^{-v}. Symmetric finite sums are consequently self-adjoint. Commutation follows from commutation of the coordinate shifts. □

Fix this measure for the rest of the proof, and write $f(x) = \omega(x)$ for an individual configuration, so $F = f(0)$. For $a = 2^j$, $j \geq 0$, define the origin counts

$$A_a = T_a F, \qquad B_a = T_{3a} F, \qquad D_a = T_{5a} F, \tag{11}$$

$$X_a = T_{2a} T_a F, \qquad Y_a = T_{4a} T_a F. \tag{12}$$

Each count also defines a field by evaluating the same expression at $x \in \mathbb{Z}^n$. Since M is odd and $3 \nmid M$, all dyadic scales and their triples satisfy Lemma 2.2. The count D_a is always an integer in $[0, s]$, and it is binary when $5 \nmid M$.

3 Convolution Counts and Exact Moments

In this section, we derive the identities shared by the counts in (11)–(12). The local separation conditions determine several indicator products exactly, which makes it possible to evaluate second moments while retaining the dependence between scales.

3.1 Local Counting Relations

Lemma 3.1. *For every dyadic a,*

$$T_a^2 + T_{2a} = 2Q_a + 2nI, \tag{13}$$

$$A_a B_a = F, \qquad F X_a = F, \tag{14}$$

$$F(T_{2a} T_{4a} F) = F, \tag{15}$$

$$0 \leq X_a \leq n + 1, \qquad F \leq A_a \leq Y_a \leq s. \tag{16}$$

Moreover,

$$\mathbb{E} A_a = \mathbb{E} B_a = \mathbb{E} D_a = s\rho, \tag{17}$$

$$\mathbb{E} X_a = \mathbb{E} Y_a = s^2 \rho. \tag{18}$$

Proof. At displacement zero, the coefficients of T_a^2 and T_{2a} are s and one. At $\pm 2ae_i$, they are one and one. At $\pm ae_i$ and $\pm ae_i \pm ae_k$ with $i \neq k$, they are two and zero. These are all possible displacements, proving (13).

For every admissible scale b, the count $T_b F$ is binary because $bV \subseteq bB$. If $A_a(x) = B_a(x) = 1$, the corresponding codewords lie in $x + aV$ and $x + 3aV$. Their difference belongs to aB_4^n, so Lemma 2.2 requires them to coincide. The intersection of the two sets is $\{x\}$, and hence $A_a B_a = F$.

After displacements are divided by a, the support of $T_{2a} T_a$ consists of

$$0, \quad \pm e_i, \quad \pm 2e_i, \quad \pm 3e_i, \quad \pm 2e_i \pm e_k \quad (i \neq k). \tag{19}$$

Only the displacements $\pm e_i$ have coefficient two; all other coefficients are one. Every nonzero displacement lies in B_3^n. If the origin is a codeword, separation excludes every other contributing position, which proves $F X_a = F$. Similarly, $T_{2a} T_{4a}$ has support $2a(V + 2V) \subseteq 2aB_3^n$ and constant coefficient one. Separation at scale $2a$ proves (15).

If $A_a(x) = 1$, its codeword excludes every other codeword contributing to $X_a(x)$ because the difference lies in aB_4^n. Thus $X_a(x) \le 2$. If $A_a(x) = 0$, at most one contributing codeword lies in $x + aB_2^n$. Every remaining contributing codeword has displacement type (3) or $(2, 1)$ after division by a, with exactly one odd coordinate. Two candidates with the same odd coordinate differ by $2aw$ with $\|w\|_1 \le 3$. Lemma 2.2 excludes such a pair at scale $2a$. There are n odd-coordinate classes, so $X_a \le n + 1$.

Finally, Y_a is the sum of s translates of the binary field A_a, including A_a itself. This gives the remaining bounds in (16). Translation invariance and the sums of the convolution coefficients give (17)–(18). □

3.2 Moments Coupling Adjacent Dyadic Scales

We retain the conditional moment at each scale by defining

$$Z_j = M\mathbb{E}[FY_{2^j}], \qquad \Delta_j = s - Z_j. \tag{20}$$

Since $\mathbb{P}(F = 1) = M^{-1}$, the quantity Z_j equals $\mathbb{E}[Y_{2^j} \mid F = 1]$. Thus Δ_j measures the difference between the largest possible count s and its mean at a codeword.

Lemma 3.2. *For every $j \ge 0$ and $a = 2^j$,*

$$1 \le Z_j \le s, \tag{21}$$
$$M\mathbb{E}X_a^2 = 12n^2 + 4n + 1, \tag{22}$$
$$M\mathbb{E}[A_aY_a] = 6n + 1, \tag{23}$$
$$M\mathbb{E}Y_a^2 = 12n^2 + 4n + Z_{j+1}. \tag{24}$$

Proof. The bounds on Z_j follow from $F \le Y_a \le s$ and $F^2 = F$. Applying (13) to the indicator gives

$$T_a^2F = 2 + 2nF - T_{2a}F. \tag{25}$$

Commutation and self-adjointness imply

$$\mathbb{E}X_a^2 = \langle T_a^2F, T_{2a}^2F\rangle,$$
$$\mathbb{E}Y_a^2 = \langle T_a^2F, T_{4a}^2F\rangle,$$

where $\langle H, J\rangle = \mathbb{E}[HJ]$. If U, W are the corresponding binary T counts, then $FU = FW = F$ and $\mathbb{E}U = \mathbb{E}W = s\rho$. Hence

$$\begin{aligned}\mathbb{E}[(2 + 2nF - U)(2 + 2nF - W)] \\ = 4 + (4n^2 - 4n - 4)\rho + \mathbb{E}[UW].\end{aligned} \tag{26}$$

For X_a, relation (15) gives $\mathbb{E}[UW] = \rho$. For Y_a, the mixed term is

$$\begin{aligned}\mathbb{E}[(T_{2a}F)(T_{8a}F)] &= \mathbb{E}[F(T_{2a}T_{8a}F)] \\ &= \rho Z_{j+1}.\end{aligned} \tag{27}$$

Using $4M + 4n^2 - 4n - 4 = 12n^2 + 4n$ in (26) proves (22) and (24). Also,

$$\begin{aligned}\mathbb{E}[A_a Y_a] &= \langle F, T_{4a} T_a^2 F \rangle \\ &= 2s\rho - \langle F, T_{4a} T_{2a} F \rangle + 2n\rho \\ &= (6n+1)\rho,\end{aligned}$$

which proves (23). □

Equation (27) identifies the term that connects consecutive scales. All its factors are evaluated in the same process, while Z_j and Z_{j+1} retain their separate values. The recurrence in Section 5 follows from comparing this exact mixed term with an integer upper bound for Y_a^2.

3.3 Congruences of the Convolution Counts

Lemma 3.3. *For every dyadic a, the following congruences hold pointwise:*

$$X_a \equiv 2s + 2nA_a - B_a \pmod 3, \tag{28}$$

$$Y_a + D_a \equiv 2s^3 - 4nX_a + (4n^2 + 2n)A_a \pmod 5. \tag{29}$$

Proof. Applying T_a to (25) gives

$$T_a^3 F = 2s - X_a + 2nA_a.$$

Applying it once more, and using the squared relations at a and $2a$, yields

$$\begin{aligned}T_a^4 F = {} & 2s^2 - T_{4a} F - 4n T_{2a} F \\ & + (4n^2 + 2n) F.\end{aligned}$$

Consequently,

$$T_a^5 F = 2s^3 - Y_a - 4nX_a + (4n^2 + 2n)A_a.$$

For integer-coefficient convolutions, $T_a^3 \equiv T_{3a} \pmod 3$ and $T_a^5 \equiv T_{5a} \pmod 5$. Substitution gives (28)–(29), with D_a treated as a nonnegative integer throughout. □

4 Dimensions Determined by Modular Counts

In this section, we combine the congruences with the exact moments. Reduction modulo three first restricts X_a to a small set of values. The resulting probability distributions then determine explicit positive gaps for eight residue classes modulo fifteen.

4.1 Reduction Modulo Three

Lemma 4.1. *A perfect code satisfying* (5) *cannot exist if $n \geq 3$ and $3 \mid n$. In the other two residue classes, the joint distribution of (F, A_a, B_a, X_a) is given in Table 1, where each probability is ρ times the displayed value.*

Proof. If $3 \mid n$, (28) gives $X_a \equiv 2 - B_a \pmod 3$. Therefore $L = X_a - 2 + B_a \geq 0$, and (17)–(18) give $\mathbb{E}L = 2n\rho$. Since

$$X_a^2 = (2 - B_a)^2 + L(X_a + 2 - B_a),$$

we obtain

$$\begin{aligned} \mathbb{E}X_a^2 &\leq 4 - 3s\rho + (n+3)2n\rho \\ &= (10n^2 + 8n + 1)\rho. \end{aligned} \tag{30}$$

This conflicts with (22), whose value exceeds the right-hand side by $2n(n-2)\rho > 0$.

For $n \equiv 1 \pmod 3$, define

$$P_1 = X_a^2 - 3X_a + 2(A_a + B_a - F),$$

and for $n \equiv 2 \pmod 3$, define

$$P_2 = X_a^2 - 5X_a + 4 + 2(A_a + B_a - 2F).$$

These expressions are nonnegative in their respective residue classes. Indeed, when $A_a = B_a = 0$, congruence (28) restricts X_a to $0, 3, 6, \ldots$ in the first case and $1, 4, 7, \ldots$ in the second. The relevant factors are $X_a(X_a - 3)$ and $(X_a - 1)(X_a - 4)$. When exactly one of A_a, B_a equals one, the factors are $(X_a - 1)(X_a - 2)$ and $(X_a - 2)(X_a - 3)$, which are nonnegative for integer X_a. If $F = 1$, (14) gives $A_a = B_a = X_a = 1$, and both expressions vanish.

The exact moments give, in the respective classes,

$$\begin{aligned} M\mathbb{E}P_1 &= 12n^2 + 4n + 1 - 3s^2 + 2(2s - 1) = 0, \\ M\mathbb{E}P_2 &= 12n^2 + 4n + 1 - 5s^2 + 4M + 4s - 4 = 0. \end{aligned}$$

A nonnegative random variable with mean zero vanishes almost surely, so only the corresponding roots can occur. The event $F = 1$ has probability ρ, and $A_aB_a = F$ gives probability $(s-1)\rho = 2n\rho$ for each event on which exactly one of A_a, B_a equals one.

To determine the two remaining masses, normalize probabilities by ρ. In the class $n \equiv 1 \pmod 3$, write them as p_0, p_3 according to the value of X_a. Normalization and the first moment give

$$p_0 + p_3 = M - 1 - 4n = 2n(n-1), \qquad 1 + 8n + 3p_3 = s^2.$$

Thus $p_3 = 4n(n-1)/3$ and $p_0 = 2n(n-1)/3$. In the class $n \equiv 2 \pmod 3$, the analogous masses satisfy

$$p_1 + p_4 = 2n(n-1), \qquad 1 + 10n + p_1 + 4p_4 = s^2.$$

Solving gives $p_4 = 2n(n-2)/3$ and $p_1 = (4n^2 - 2n)/3$, proving every entry in Table 1. □

4.2 Reduction Modulo Five

We now use the same five-state distribution to evaluate the right-hand side of (29). The argument needs only the mean and nonnegative integrality of D_a, so it applies uniformly across the eight classes considered below.

Table 1: Joint count distributions; each displayed probability is normalized by ρ.

$n \bmod 3$	(F, A_a, B_a)	X_a	Probability$/\rho$
1	$(1,1,1)$	1	1
	$(0,1,0)$	2	$2n$
	$(0,0,1)$	2	$2n$
	$(0,0,0)$	0	$2n(n-1)/3$
	$(0,0,0)$	3	$4n(n-1)/3$
2	$(1,1,1)$	1	1
	$(0,1,0)$	2	$2n$
	$(0,0,1)$	3	$2n$
	$(0,0,0)$	1	$(4n^2-2n)/3$
	$(0,0,0)$	4	$2n(n-2)/3$

Lemma 4.2. *A perfect code satisfying* (5) *cannot exist if* $n \geq 3$, $3 \nmid n$, *and* $5 \nmid n$.

Proof. Fix $a = 1$ and suppress this subscript. Let r be the least nonnegative residue of $2s^3 - 4nX + (4n^2 + 2n)A$ modulo five. Define

$$w(0), \ldots, w(4) = (0, 2, 3, 3, 2), \qquad H(y) = \frac{5y - y^2}{2}.$$

For any nonnegative integer y, $H(y) \leq w(y \bmod 5)$. Reducing a residue by one increases w by at most two. Since $Y + D \equiv r \pmod 5$ and $D \geq 0$, these observations imply

$$Y + D \geq r, \tag{31}$$

$$H(Y) \leq w(r) + 2D. \tag{32}$$

Also, (18), (24), and $Z_1 \leq s$ yield

$$\begin{aligned} M\mathbb{E}H(Y) &= 4n^2 + 8n + \frac{5 - Z_1}{2} \\ &\geq 4n^2 + 7n + 2. \end{aligned} \tag{33}$$

Taking expectations in (31) requires

$$\Gamma_{\mathrm{I}}(n) := M\mathbb{E}r - s^2 - s \leq 0, \tag{34}$$

whereas (32) and (33) require

$$\Gamma_{\mathrm{II}}(n) := 4n^2 + 7n + 2 - M\mathbb{E}w(r) - 2s \leq 0. \tag{35}$$

The probabilities in Table 1 evaluate these quantities exactly. Table 2 lists all five values of r in the order of the corresponding rows of Table 1. Their weighted sums give the displayed gaps, using test I from (34) or test II from (35).

For example, if $n \equiv 1 \pmod 3$ and $n \equiv 1 \pmod 5$, then $r \equiv 4 + X + A \pmod 5$. Its values on the five rows of Table 1 are $1, 2, 1, 4, 2$, respectively. Hence

$$M\mathbb{E}r = 1 + 6n + \frac{16n(n-1)}{3},$$

Table 2: Modulo-five residues in the order of Table 1, the resulting positive gaps, and the smallest admissible dimensions.

$n \bmod 3$	$n \bmod 5$	$(r_1, r_2, r_3, r_4, r_5)$	Test	$\Gamma(n)$	n_0
1	1	$(1, 2, 1, 4, 2)$	I	$(4n^2 - 16n - 3)/3$	16
1	2	$(2, 4, 4, 0, 1)$	II	$(4n^2 - 7n - 9)/3$	7
1	3	$(1, 4, 2, 1, 0)$	II	$(8n^2 - 17n - 6)/3$	13
1	4	$(4, 3, 1, 3, 0)$	II	$2n^2 - 5n - 2$	4
2	1	$(1, 2, 2, 0, 3)$	II	$2n^2 - 5n - 2$	11
2	2	$(2, 4, 1, 2, 3)$	I	$2n(n - 2)/3$	17
2	3	$(1, 4, 0, 4, 3)$	I	$(10n^2 - 14n - 3)/3$	8
2	4	$(4, 3, 0, 2, 4)$	I	$(4n^2 - 20n + 6)/3$	14

which gives $\Gamma_{\mathrm{I}}(n) = (4n^2 - 16n - 3)/3$. The other rows follow by the same finite substitution.

For every row in Table 2, the quadratic gap has positive leading coefficient, positive value at the smallest admissible dimension n_0, and positive derivative at n_0. It remains positive for all $n \geq n_0$, contradicting the required inequality in (34) or (35). □

5 A Finite-Scale Contradiction for the Remaining Dimensions

In this section, we treat the multiples of five by retaining the whole sequence of conditional moments in (20). The moment comparison forces the deficits to grow, and a directional counting argument gives a uniform positive lower bound. Their combination completes the proof of Theorem 2.1.

5.1 Growth of the Conditional-Moment Deficit

If $5 \mid n$, then $M \equiv 1 \pmod 5$. Thus $5a$ is an admissible scale for every dyadic a, and D_a is binary. This additional separation is used in both lemmas below.

Lemma 5.1. *If* $5 \mid n$*, then*

$$\Delta_{j+1} \geq 3\Delta_j, \qquad 0 \leq \Delta_j \leq s - 1 \qquad (j \geq 0). \tag{36}$$

Proof. Fix $a = 2^j$ and suppress the subscript on A, D, Y. Equation (29) reduces to $Y + D \equiv 2 \pmod 5$. As D is binary, the integer

$$L = Y - 2 + D$$

is nonnegative. The means and the mixed moment give

$$\mathbb{E}L = 2n\rho, \tag{37}$$

$$\mathbb{E}[AL] = (2n - 1)\rho + \mathbb{E}[AD]. \tag{38}$$

Since $AD \geq F$ and $AL \leq L$, equations (37)–(38) imply equality in both comparisons. Therefore

$$AD = F, \qquad AL = L \qquad \text{almost surely.} \tag{39}$$

We use these equalities to bound the exact identity

$$Y^2 = (2 - D)^2 + L(Y + 2 - D).$$

If $A = 0$, then $L = 0$. If $A = D = 1$, then $F = 1$ and $Y + 1 \le s + 1$. If $A = 1, D = 0$, then $F = 0$ and $Y \equiv 2 \pmod 5$. Since $s \equiv 1 \pmod 5$ and $Y \le s$, it follows that $Y \le s - 4$. Thus

$$L(Y + 2 - D) \le (s - 2)L + 3FL. \tag{40}$$

The identity $\mathbb{E}[FL] = \rho(Z_j - 1)$ now yields

$$\begin{aligned} M\mathbb{E}Y^2 &\le 4M - 3s + (s - 2)2n + 3(Z_j - 1) \\ &= 12n^2 - 2 + 3Z_j. \end{aligned} \tag{41}$$

Comparison with (24) gives

$$3Z_j - Z_{j+1} \ge 4n + 2 = 2s,$$

which is equivalent to the first inequality in (36). The remaining bounds follow from (21). □

5.2 A Positive Deficit From Codeword-Conditioned Counting

Growth alone permits an identically zero sequence. We next rule out that possibility by comparing the decoding counts at two nearby scaled locations. Conditioning the directional sum on a codeword prevents repeated counting of the same mismatch.

Lemma 5.2. *If* $5 \mid n$*, then*

$$\Delta_j \ge \frac{s - 1}{s + 1} \qquad (j \ge 0). \tag{42}$$

Proof. Fix $a = 2^j$ and define

$$\begin{aligned} U &= T_{4a}F, & V_2 &= T_{2a}F, & D &= T_{5a}F, \\ J &= U - A_a, & E_4 &= U(1 - A_a), & E_5 &= D(1 - V_2). \end{aligned}$$

Each of E_4, E_5 is binary and records a mismatch between two counts in the same configuration.

Let x be a codeword and $w \in V \setminus \{0\}$. Suppose both $E_4(x + 4aw)$ and $E_5(x + 5aw)$ vanish. The codeword at x gives $U(x + 4aw) = D(x + 5aw) = 1$. Hence there are codewords

$$c = x + 4aw - au, \qquad d = x + 5aw - 2av, \qquad u, v \in V. \tag{43}$$

Their difference lies in aB_4^n, so Lemma 2.2 requires $c = d$, or $w + u = 2v$. For $w \in \{\pm e_1, \dots, \pm e_n\}$, the only solutions are $(u, v) = (w, w)$ and $(-w, 0)$. The first produces the codeword $x + 3aw$, violating separation at scale a. The second produces $x + 5aw$, violating separation at scale $5a$. Consequently, for every configuration and every x,

$$\begin{aligned} f(x) \le\ & f(x)E_4(x + 4aw) \\ & + f(x)E_5(x + 5aw). \end{aligned} \tag{44}$$

Sum over all $s-1$ nonzero directions while retaining the factor $f(x)$. Translation invariance gives

$$\begin{aligned}\sum_{w\neq 0}\mathbb{E}[FE_4(4aw)] &= \mathbb{E}\left[E_4\sum_{w\neq 0}f(-4aw)\right]\\ &= \mathbb{E}[E_4(U-F)] = \mathbb{E}E_4. \end{aligned}\tag{45}$$

Indeed, $E_4 = 1$ implies $U = 1$ and $A_a = F = 0$. The corresponding calculation for E_5 gives

$$\sum_{w\neq 0}\mathbb{E}[FE_5(5aw)] = \mathbb{E}[E_5(D-F)] = \mathbb{E}E_5.$$

Thus (44) implies

$$(s-1)\rho \le \mathbb{E}E_4 + \mathbb{E}E_5. \tag{46}$$

Since U and A_a are binary and have the same mean, self-adjointness yields

$$\begin{aligned}\mathbb{E}E_4 &= s\rho - \mathbb{E}[UA_a] = \Delta_j\rho,\\ \mathbb{E}|J| &= 2\mathbb{E}E_4. \end{aligned}\tag{47}$$

Equations (25) and (29), with $5 \mid n$, imply

$$T_aJ = Y_a - T_a^2F \equiv V_2 - D \pmod 5.$$

If the binary variables V_2, D differ, the integer T_aJ is nonzero. It follows pointwise that

$$|V_2 - D| \le |T_aJ| \le T_a|J|.$$

Their equal means then give

$$\mathbb{E}E_5 = \tfrac{1}{2}\mathbb{E}|D-V_2| \le \tfrac{s}{2}\mathbb{E}|J| = s\mathbb{E}E_4. \tag{48}$$

Substituting (47)–(48) into (46) proves (42). □

5.3 Completion of the Main Proof

Proof. Suppose (5) holds for some $n \ge 3$. Lemma 4.1 excludes $3 \mid n$, and Lemma 4.2 excludes $3 \nmid n$ with $5 \nmid n$. The remaining dimensions satisfy $n \equiv 5$ or $10 \pmod{15}$. Choose an integer K such that $3^K > s+1$. Lemmas 5.1 and 5.2 imply

$$s-1 \ge \Delta_K \ge 3^K\Delta_0 \ge \frac{3^K(s-1)}{s+1} > s-1, \tag{49}$$

a contradiction. These cases exhaust all $n \ge 3$. □

For the last branch, all required counts use the finite scale set

$$\mathcal{A}_K = \{c2^j : c \in \{1,3,5\},\ 0 \le j \le K+3\}, \tag{50}$$

where $K = \lfloor \log_3(s+1) \rfloor + 1$. For $5 \mid n$, every member of (50) is coprime to M. Thus $O(\log n)$ successive dyadic levels suffice to complete this branch.

6 Finite-Alphabet Codes and Packing Density

In this section, we derive the coding consequences of Theorem 2.1. Periodic lifting first gives a strict finite-alphabet sphere-packing bound and an exact existence classification. A common limiting argument then gives a relative packing gap uniform in the alphabet size and a quantitative comparison between finite and integer alphabets.

6.1 Periodic Lifting and the Sphere-Packing Bound

For $q \geq 5$, write $\pi_q : \mathbb{Z}^n \to \mathbb{Z}_q^n$ for coordinatewise reduction. For representatives $x_i, y_i \in \{0, \ldots, q-1\}$, the Lee distance is

$$d_{L,q}(x, y) = \sum_{i=1}^{n} \min\{|x_i - y_i|, q - |x_i - y_i|\}. \tag{51}$$

The radius-two sphere consists of the reductions of the vectors in B. This reduction is injective: two such vectors differ by at most four in each coordinate, so their difference cannot be a nonzero element of $q\mathbb{Z}^n$. Surjectivity follows by choosing a minimum-magnitude representative for each symbol error. Thus every finite-alphabet decoding sphere has cardinality M.

If $C \subseteq \mathbb{Z}_q^n$ has minimum Lee distance at least five, its lift $\widetilde{C} = \pi_q^{-1}(C)$ has minimum integer Lee distance at least five. Distinct words reducing to different codewords are separated by (51); distinct lifts of the same codeword differ by a nonzero vector in $q\mathbb{Z}^n$. Conversely, a $q\mathbb{Z}^n$-periodic integer code of minimum Lee distance at least five reduces to a finite-alphabet code with the same minimum-distance requirement. This gives the periodic correspondence used in the following consequence [4, Proposition 1].

Corollary 6.1. *For $n \geq 3$ and $q \geq 5$, every code $C \subseteq \mathbb{Z}_q^n$ with minimum Lee distance at least five satisfies*

$$|C|(2n^2 + 2n + 1) \leq q^n - 1. \tag{52}$$

In particular, a perfect two-error-correcting Lee code does not exist for these parameters.

Proof. Disjoint radius-two spheres give $M|C| \leq q^n$. Equality would make every received word have a unique representation $c + \pi_q(b)$ with $c \in C$ and $b \in B$. Lifting this representation gives an exact cover of $\mathbb{Z}^n$ by the translates of B centered at $\widetilde{C}$, contradicting Theorem 2.1. Both sides are integers, which gives (52). □

The alphabet threshold also fixes the size of the decoding region: $q \geq 5$ keeps the two opposite errors of magnitude two distinct. Within this range, the low-dimensional constructions and Theorem 2.1 give a complete classification.

Corollary 6.2. *Let $q \geq 5$ and $n \geq 1$. A perfect two-error-correcting Lee code in $\mathbb{Z}_q^n$ exists if and only if*

$$(n = 1 \text{ and } 5 \mid q) \quad \text{or} \quad (n = 2 \text{ and } 13 \mid q). \tag{53}$$

Proof. For $n = 1$, perfectness requires $5|C| = q$, and the multiples of five give a perfect code whenever $5 \mid q$. For $n = 2$, perfectness requires $13|C| = q^2$, so the primality of thirteen implies $13 \mid q$.

To prove sufficiency in dimension two, assume $13 \mid q$ and define the homomorphism

$$\phi : \mathbb{Z}_q^2 \to \mathbb{Z}_{13}, \qquad \phi(x, y) = x + 5y \pmod{13}.$$

The images of the thirteen radius-two error vectors are

$$0, \quad \pm 1, \quad \pm 5, \quad \pm 2, \quad \pm 10, \quad \pm 1 \pm 5,$$

which are exactly the thirteen elements of $\mathbb{Z}_{13}$. Every received word therefore has a unique radius-two error vector with the same ϕ-value, and subtracting that error places the word in $\ker \phi$. Thus $\ker \phi$ is perfect. Theorem 2.1 and Corollary 6.1 exclude all $n \geq 3$, proving (53). □

6.2 A Relative Gap Uniform in the Alphabet Size

Let $A_L(n, 5; q)$ be the largest size of a code in $\mathbb{Z}_q^n$ with minimum Lee distance at least five. To compare these finite-alphabet codes, consider the compact space

$$\Omega_{\text{pack}} = \{\omega \in \{0, 1\}^{\mathbb{Z}^n} : Q_1\omega(x) \leq 1 \text{ for every } x \in \mathbb{Z}^n\}. \tag{54}$$

Let $\mathcal{M}_n$ be its translation-invariant probability measures, and set

$$\alpha_n = \max_{\mu \in \mathcal{M}_n} \mathbb{E}_\mu F. \tag{55}$$

Compactness follows from the finite-coordinate inequalities in (54). The translation-invariance equations define a closed set of probability measures, and $\mu \mapsto \mathbb{E}_\mu F$ is continuous. Hence the maximum in (55) is attained. Averaging the translates of $5\mathbb{Z}^n$ gives $\alpha_n \geq 5^{-n}$, whereas $Q_1 F \leq 1$ gives $\alpha_n \leq M^{-1}$.

This density also bounds arbitrary integer-alphabet codes. For an integer code C of minimum Lee distance at least five, define its upper uniform density by

$$\overline{d}(C) = \limsup_{R \to \infty} \sup_{x \in \mathbb{Z}^n} \frac{|C \cap (x + [-R, R]^n)|}{(2R + 1)^n}. \tag{56}$$

Choose translated boxes whose densities converge to (56) and average the indicator as viewed from the locations in each box. A convergent subsequence gives an element of $\mathcal{M}_n$ with origin mean $\overline{d}(C)$, by the same boundary estimate as in Lemma 2.3. Consequently $\overline{d}(C) \leq \alpha_n$. The periodic construction below shows that these densities approach α_n, identifying (55) with the optimal integer-alphabet packing density.

Proposition 6.3. *For every fixed $n \geq 3$, there exists $\epsilon_n > 0$ such that*

$$\frac{MA_L(n, 5; q)}{q^n} \leq 1 - \epsilon_n \qquad \text{for every } q \geq 5. \tag{57}$$

One may take $\epsilon_n = 1 - M\alpha_n$.

Proof. Suppose $\alpha_n = M^{-1}$, and choose a maximizing measure in (55). The nonnegative random variable $1 - Q_1 F$ has mean zero and therefore vanishes almost surely. Translation invariance gives the same equality at each $x \in \mathbb{Z}^n$. Since this set of locations is countable, all covering equalities hold simultaneously on a probability-one set of configurations. Each such configuration would be a perfect code, in contradiction to Theorem 2.1. It follows that $\epsilon_n = 1 - M\alpha_n > 0$.

For a finite-alphabet code, lift to a $q\mathbb{Z}^n$-periodic packing and average over its q^n translates. This produces an element of $\mathcal{M}_n$ whose mean is $|C|/q^n$. The definition of α_n now proves (57). □

For fixed block length, Proposition 6.3 rules out approaching equality in the sphere-packing bound by increasing the alphabet size. Its constant is determined by the optimal packing density at that length. The next result makes the connection with finite alphabets quantitative.

Proposition 6.4. *For every $n \geq 1$ and $q \geq 5$,*

$$\alpha_n \left(1 - \frac{4}{q}\right)^n \leq \frac{A_L(n, 5; q)}{q^n} \leq \alpha_n. \tag{58}$$

Consequently,

$$0 \leq \alpha_n - \frac{A_L(n, 5; q)}{q^n} \leq \frac{4n\alpha_n}{q}, \qquad \lim_{q\to\infty} \frac{A_L(n, 5; q)}{q^n} = \alpha_n. \tag{59}$$

Proof. The upper bound is the periodic-lifting argument above. For the lower bound, take a measure attaining (55) and consider the integer box

$$W_q = \{2, 3, \ldots, q - 3\}^n,$$

which has $(q - 4)^n$ points. The expected number of codewords in this box is $\alpha_n(q - 4)^n$, so some configuration contains at least this many. Keep these codewords and repeat them with period q in every coordinate.

Words in the same copy remain separated by at least five. For two different copies, at least one coordinate receives a nonzero multiple of q; the two retained coordinate values differ by at most $q - 5$. Their separation in that coordinate is therefore at least five. The periodic set is a valid radius-two packing, and its reduction modulo q has at least $\alpha_n(q - 4)^n$ codewords. This proves (58). Finally, $1 - (1 - x)^n \leq nx$ for $0 \leq x \leq 1$ gives (59). □

In dimensions one and two the perfect integer codes give $\alpha_1 = 1/5$ and $\alpha_2 = 1/13$; for every higher fixed dimension, Proposition 6.3 gives $M\alpha_n < 1$.

7 Conclusion

In this note, we have proved the nonexistence of perfect two-error-correcting Lee codes in $\mathbb{Z}^n$ for every $n \geq 3$. A common translation average preserves the codeword indicator and the exact coverage equations at every required scale. Local separation determines the convolution moments, and the modulo-three and modulo-five relations reduce the possible count distributions. For the remaining dimensions, codeword-conditioned directional counting gives a positive deficit whose dyadic growth contradicts its boundedness.

The theorem completes the radius-two existence classification over the integer alphabet and, together with the low-dimensional constructions, over every cyclic alphabet of size at least five. At each fixed length at least three, compactness also gives a positive relative gap below the finite-alphabet sphere-packing bound, uniformly in the alphabet size. The finite-alphabet approximation shows that normalized optimal code sizes converge to the integer packing density with an explicit boundary-loss estimate.

Sources

[1] C. Y. Lee, "Some properties of nonbinary error-correcting codes," *IRE Trans. Inf. Theory*, vol. 4, no. 2, pp. 77–82, Jun. 1958, doi: 10.1109/TIT.1958.1057446.

[2] R. M. Roth and P. H. Siegel, "Lee-metric BCH codes and their application to constrained and partial-response channels," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1083–1096, Jul. 1994, doi: 10.1109/18.335966.

[3] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominoes," *SIAM J. Appl. Math.*, vol. 18, no. 2, pp. 302–317, Mar. 1970, doi: 10.1137/0118025.

[4] P. Horak and D. Kim, "50 years of the Golomb–Welch conjecture," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 3048–3061, Apr. 2018, doi: 10.1109/TIT.2017.2786675.

[5] P. Horak, "Tilings in Lee metric," *Eur. J. Combin.*, vol. 30, no. 2, pp. 480–489, Feb. 2009, doi: 10.1016/j.ejc.2008.04.007.

[6] P. Horak, "On perfect Lee codes," *Discrete Math.*, vol. 309, no. 18, pp. 5551–5561, Sep. 2009, doi: 10.1016/j.disc.2008.03.019.

[7] P. Horak and O. Grošek, "A new approach towards the Golomb–Welch conjecture," *Eur. J. Combin.*, vol. 38, pp. 12–22, May 2014, doi: 10.1016/j.ejc.2013.10.010.

[8] D. Kim, "Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions," *Eur. J. Combin.*, vol. 63, pp. 1–5, Jun. 2017, doi: 10.1016/j.ejc.2017.01.007.

[9] K. H. Leung and Y. Zhou, "No lattice tiling of $\mathbb{Z}^n$ by Lee sphere of radius 2," *J. Combin. Theory, Ser. A*, vol. 171, Art. no. 105157, Apr. 2020, doi: 10.1016/j.jcta.2019.105157.

[10] C. Camarero and C. Martínez, "Quasi-perfect Lee codes of radius 2 and arbitrarily large dimension," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1183–1192, Mar. 2016, doi: 10.1109/TIT.2016.2517069.

[11] Z. Zhou and Y. Zhou, "Almost perfect linear Lee codes of packing radius 2 only exist for small dimensions," *IEEE Trans. Inf. Theory*, vol. 70, no. 6, pp. 3965–3980, Jun. 2024, doi: 10.1109/TIT.2023.3341954.