

NO LATTICE TILING OF $\mathbb{Z}^{35}$ OR $\mathbb{Z}^{805}$ BY LEE BALLS OF RADIUS THREE

DEEP BHATTACHARJEE AND USHASHI BHATTACHARYA

ABSTRACT. We prove that there is no lattice tiling of $\mathbb{Z}^{35}$ or of $\mathbb{Z}^{805}$ by Lee balls of radius three. These were the only cases left open by Xiao and Zhou among the Lee balls of dimension at least three and radius at least two with fewer than 2^{30} points, so the lattice Golomb–Welch conjecture holds for all of them.

1. INTRODUCTION

For integers $n \geq 1$ and $r \geq 0$ the Lee ball of radius r in $\mathbb{Z}^n$ is

$$B^n(r) = \{a \in \mathbb{Z}^n : |a_1| + \cdots + |a_n| \leq r\}.$$

A *tiling* of $\mathbb{Z}^n$ by $B^n(r)$ is a set $T \subset \mathbb{Z}^n$ such that the translates $t + B^n(r)$ with $t \in T$ partition $\mathbb{Z}^n$, and it is a *lattice tiling* if T is a subgroup of $\mathbb{Z}^n$. Such tilings exist when $n \leq 2$ and when $r = 1$.¹ Golomb and Welch [6] conjectured that these are the only cases.

Conjecture A (Golomb–Welch). *For $n \geq 3$ and $r \geq 2$ there is no tiling of $\mathbb{Z}^n$ by $B^n(r)$.*

The conjecture is open, and so is its lattice form, in which only lattice tilings are considered. It holds for $3 \leq n \leq 5$ [7, 8] and for radii that are large compared with the dimension [15, 10]; the lattice form holds for radius two in every dimension [13]. We refer to the survey of Horak and Kim [10] for the history. A lattice tiling is the same thing as a perfect code in a finite abelian group [9], and in this form many further dimensions have been excluded for small radii by the polynomial method and by group-ring equations [11, 19, 21, 16, 20]. Xiao and Zhou [18] recently combined all these criteria with new ones and applied them to every pair (n, r) with $n \geq 3$, $r \geq 2$ and $|B^n(r)| < 2^{30}$. Of the 1358 such pairs they excluded 1356, and the two that remained are $(n, r) = (35, 3)$ and $(805, 3)$ [18, Theorem 5.1]. We settle both.

Theorem 1.1. *There is no lattice tiling of $\mathbb{Z}^{35}$ by $B^{35}(3)$, and there is no lattice tiling of $\mathbb{Z}^{805}$ by $B^{805}(3)$.*

2020 *Mathematics Subject Classification.* Primary 52C22; Secondary 05B45, 94B25, 05C25.

Key words and phrases. Golomb–Welch conjecture, Lee metric, perfect code, lattice tiling, group ring.

Corresponding author: Deep Bhattacharjee.

¹A lattice tiling by $B^n(r)$ is a lattice packing of translates of $B^n(r)$ with density one, so the question is the extreme case of the lattice packing problem for the Lee ball, the ℓ^1 counterpart of the Euclidean ball. For the Euclidean problem in dimensions four and seven, where the densest lattices are D_4 and E_7 , see [3, 4]; there the obstacle is to compare every packing with one lattice, whereas here it is to show that a single lattice cannot exist.

Corollary 1.2. *If $n \geq 3$, $r \geq 2$ and $|B^n(r)| < 2^{30}$, then $\mathbb{Z}^n$ has no lattice tiling by $B^n(r)$.*

Proof. This is Theorem 1.1 together with [18, Theorem 5.1]. $\square$

The balls in question have

$$|B^{35}(3)| = 59711 = 29^2 \cdot 71, \quad |B^{805}(3)| = 696845031 = 3 \cdot 29^2 \cdot 179 \cdot 1543.$$

Neither number is prime, so the theorem of Szegedy [17], which turns the nonexistence of lattice tilings into the nonexistence of all tilings when $|B^n(r)|$ is prime, does not apply, and Theorem 1.1 says nothing about tilings that are not lattice tilings. In the language of the degree–diameter problem [5], Theorem 1.1 says that no abelian group of order 59711 is generated by 35 elements in such a way that each of its elements is a sum of at most three of these generators and their negatives, and likewise for order 696845031 and 805 generators; in other words the abelian Cayley–Moore bound is not attained in degree 70 or in degree 1610 at diameter three (compare [18, Section 1]).²

The method. A lattice tiling of $\mathbb{Z}^n$ by $B^n(3)$ gives a finite abelian group G of order $|B^n(3)|$ and elements $g_1, \dots, g_n$ such that $a \mapsto \sum_j a_j g_j$ maps $B^n(3)$ bijectively onto G (Lemma 2.2). Summing a character over the ball gives a cubic identity in a group ring (Proposition 2.3), and projecting G onto $\mathbb{Z}/p$ for a prime p dividing $|G|$ turns it into conditions on the images of the g_j . This is the setting of [21, 18], and two features of the present cases defeat the projections used so far.

For $n = 805$ the conditions modulo $p = 29$ leave a very large number of possible distributions of the images, whose examination Xiao and Zhou estimated would take about two months of exhaustive search [18, Example 5.13]. We read off the coefficient of the identity element modulo 29^2 instead; it excludes all of them by one congruence (Section 5).

For $n = 35$ Xiao and Zhou found, for each of the two primes 71 and 29, a distribution of the images that satisfies every condition coming from that prime alone [18, Example 5.14]. We project onto $\mathbb{Z}/71 \times \mathbb{Z}/29$ at once, through a character with values in the dual numbers over the group ring $\mathbb{F}_{71}[\mathbb{Z}/29]$. The first-order part of the identity couples the two distributions and leads to a circulant linear system over $\mathbb{F}_{71}$ whose only solution is zero (Section 6). Figure 1 shows the order of the argument.

Theorem 1.1, with every step of Sections 2–6, has been formalized in the Lean 4 proof assistant (Section 7).

2. PERFECT CODES AND THE BALL IDENTITY

All groups in this paper are abelian and written additively, except the groups of units of rings. For $a \in \mathbb{Z}^n$ we write $|a| = |a_1| + \dots + |a_n|$, and $B^n = B^n(3)$.

Definition 2.1. Let G be a finite group and $g = (g_1, \dots, g_n) \in G^n$. Put $\varphi_g(a) = \sum_j a_j g_j$ for $a \in \mathbb{Z}^n$. We call g a *perfect code* in G if φ_g maps B^n bijectively onto G .

²The statement concerns the word metric of the Cayley graph of G with respect to $\pm g_1, \dots, \pm g_n$: every element has word length at most three, and the lattice tiling asks that the shortest word be unique. This is the opposite extreme from the word metrics of hyperbolic groups, where the Cayley graph is negatively curved at large scale [1]; in an abelian group the ball of radius three is as small as it can be, and the tiling asks it to be exactly as large as $B^n(3)$.

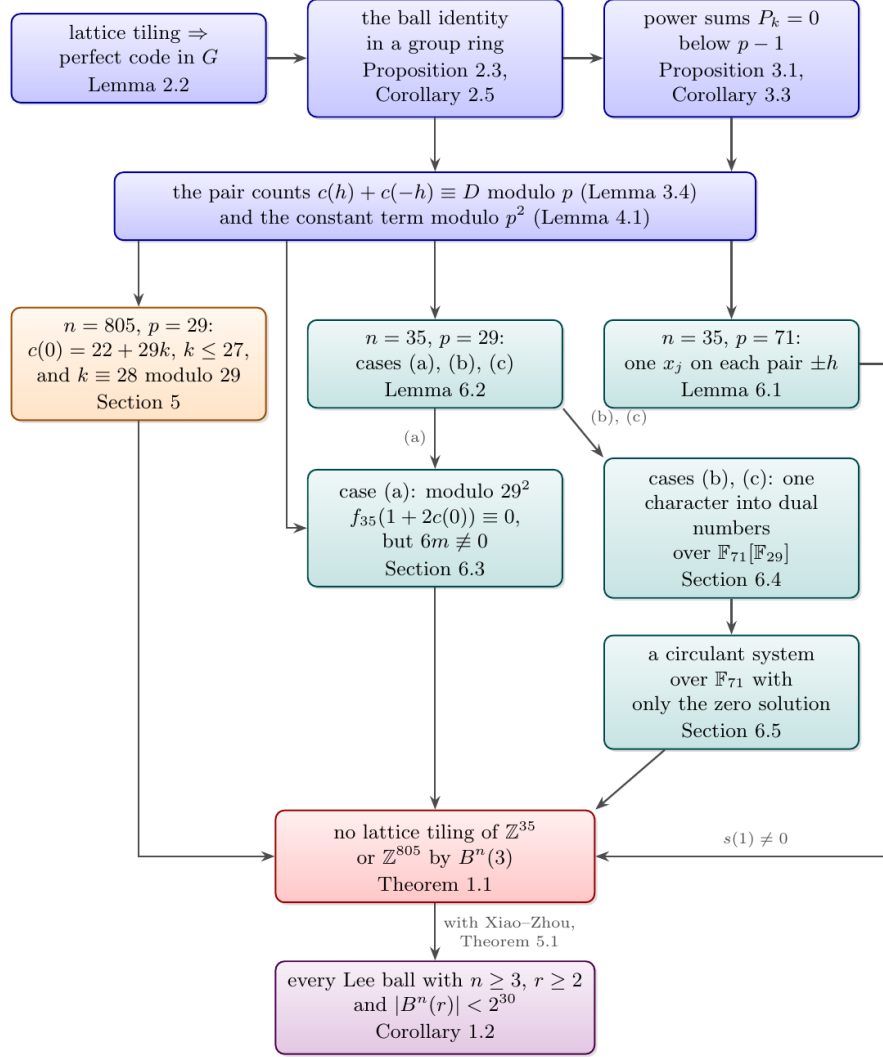


FIGURE 1. The order of the proof. Arrows point from a result to the results that use it.

Lemma 2.2. *Let $L \subseteq \mathbb{Z}^n$ be a subgroup such that the translates $l + B^n$, $l \in L$, partition $\mathbb{Z}^n$. Let $e_1, \dots, e_n$ be the unit vectors. Then $G = \mathbb{Z}^n/L$ is finite, $(e_1 + L, \dots, e_n + L)$ is a perfect code in G , and $|G| = |B^n|$.*

Proof. Here $\varphi_g(a) = a + L$. Every $x \in \mathbb{Z}^n$ lies in a translate $l + B^n$ with $l \in L$, and then $a = x - l \in B^n$ satisfies $\varphi_g(a) = x + L$; so φ_g maps B^n onto G , and G is finite. If $a, b \in B^n$ and $a - b \in L$, the point a lies in $0 + B^n$ and in $(a - b) + B^n$, because $a - (a - b) = b \in B^n$. The translates are disjoint, so $a - b = 0$. Hence φ_g is injective on B^n , and $|G| = |B^n|$. $\square$

Figure 2 shows the ball $B^3(3)$, the tile of the three-dimensional case.

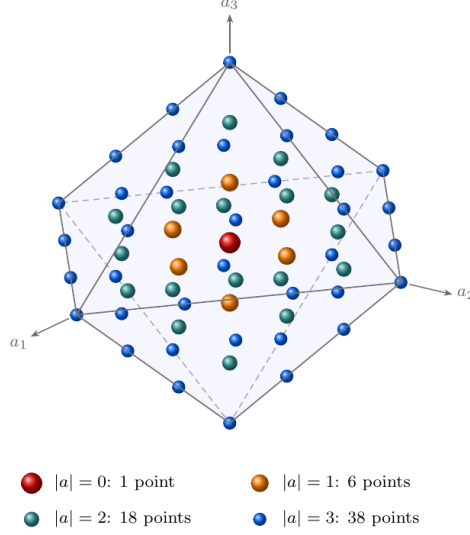


FIGURE 2. The Lee ball $B^3(3)$: the 63 points of $\mathbb{Z}^3$ in the octahedron $|a_1| + |a_2| + |a_3| \leq 3$, shaded by $|a|$. A lattice tiling translates it by the points of a subgroup L ; the quotient $\mathbb{Z}^3/L$ then has one element for each point of the ball.

The next identity is the source of all the conditions used below. Let f_n be the polynomial

$$f_n(X) = X^3 + 3X^2 + 2X - 6nX = X(X+1)(X+2) - 6nX.$$

Proposition 2.3. *Let R be a commutative ring, Γ a group, $\chi: \Gamma \rightarrow R^\times$ a homomorphism, and $z_1, \dots, z_n \in \Gamma$. For $i = 1, 2, 3$ put $T_i = 1 + \sum_j (\chi(iz_j) + \chi(-iz_j))$. Then*

$$(2.1) \quad 6 \sum_{a \in B^n} \chi\left(\sum_j a_j z_j\right) = T_1^3 + 3T_1T_2 + 2T_3 - 6nT_1.$$

Proof. Put $u_j = \chi(z_j)$ and $v_j = \chi(-z_j)$, so that $u_j v_j = 1$ and $\chi(\sum_j a_j z_j) = \prod_j u_j^{a_j}$, where $u_j^{-1} = v_j$. Consider multisets of the letters $u_1, \dots, u_n$ and $v_1, \dots, v_n$, and say that a multiset contains a *pair* if it contains both u_j and v_j for some j . A multiset M of size k without a pair corresponds to the point $a \in \mathbb{Z}^n$ with a_j equal to the multiplicity of u_j minus that of v_j ; this is a bijection onto the points with $|a| = k$, and the product of the elements of M is $\prod_j u_j^{a_j}$.

Let h_k be the sum, over all multisets M of size k , of the product of the elements of M , and let $p_i = \sum_j (u_j^i + v_j^i)$. The multisets of size 2 with a pair are the n multisets $\{u_j, v_j\}$, each with product 1. A multiset of size 3 with a pair is $\{u_j, v_j, w\}$ for one index j and one letter w , these are distinct for distinct (j, w) , and the product is w . Hence

$$\sum_{a \in B^n} \prod_j u_j^{a_j} = 1 + p_1 + (h_2 - n) + (h_3 - np_1).$$

Newton's identities give $2h_2 = p_1^2 + p_2$ and $6h_3 = p_1^3 + 3p_1p_2 + 2p_3$ in the polynomial ring over $\mathbb{Z}$ in the $2n$ letters, hence in R . Six times the right side above is therefore

$$6 + 6p_1 + 3p_1^2 + 3p_2 - 6n + p_1^3 + 3p_1p_2 + 2p_3 - 6np_1,$$

which is $T_1^3 + 3T_1T_2 + 2T_3 - 6nT_1$ for $T_i = 1 + p_i$. $\square$

With Γ trivial, (2.1) reads $6|B^n| = f_n(2n+1)$. For instance $|B^{35}| = f_{35}(71)/6 = 59711$ and $|B^{805}| = f_{805}(1611)/6 = 696845031$.

Lemma 2.4. *Let g be a perfect code in G , let $\psi: G \rightarrow \Gamma$ be a surjective homomorphism onto a finite group Γ , and let $F: \Gamma \rightarrow M$ be a map to a group M . Then*

$$\sum_{a \in B^n} F\left(\sum_j a_j \psi(g_j)\right) = \frac{|G|}{|\Gamma|} \sum_{\gamma \in \Gamma} F(\gamma).$$

Proof. The argument of F is $\psi(\varphi_g(a))$, and φ_g maps B^n bijectively onto G , so the left side is $\sum_{x \in G} F(\psi(x))$. Each fibre of ψ has $|G|/|\Gamma|$ elements. $\square$

For a commutative ring k and a finite group Γ we write $k[\Gamma]$ for the group ring, with basis elements $[\gamma]$, $\gamma \in \Gamma$, multiplied by $[\gamma][\gamma'] = [\gamma + \gamma']$. Its unit element is $[0]$, and we write $S_\Gamma = \sum_{\gamma \in \Gamma} [\gamma]$. For $F \in k[\Gamma]$ we write $F(\gamma)$ for the coefficient of $[\gamma]$.

Corollary 2.5. *Let g be a perfect code in G , let $\psi: G \rightarrow \Gamma$ be surjective, and put $x_j = \psi(g_j)$.*

- (1) *If $\chi: \Gamma \rightarrow R^\times$ is a homomorphism into the units of a commutative ring and $T_i = 1 + \sum_j (\chi(ix_j) + \chi(-ix_j))$, then*

$$(2.2) \quad 6 \frac{|G|}{|\Gamma|} \sum_{\gamma \in \Gamma} \chi(\gamma) = T_1^3 + 3T_1T_2 + 2T_3 - 6nT_1.$$

- (2) *In $k[\Gamma]$, with $T_i = [0] + \sum_j ([ix_j] + [-ix_j])$,*

$$(2.3) \quad 6 \frac{|G|}{|\Gamma|} S_\Gamma = T_1^3 + 3T_1T_2 + 2T_3 - 6nT_1.$$

Proof. Apply Proposition 2.3 with $z_j = x_j$ and then Lemma 2.4 with $F = \chi$. Part (2) is the case $R = k[\Gamma]$, $\chi(\gamma) = [\gamma]$. $\square$

Lemma 2.6. *If a prime p divides $|G|$, there is a surjective homomorphism $G \rightarrow \mathbb{Z}/p$.*

Proof. Write G as a direct sum of cyclic groups of prime power order. Since p divides $|G|$, one summand is $\mathbb{Z}/p^e$ with $e \geq 1$; project onto it and reduce modulo p . $\square$

3. POWER SUMS MODULO A PRIME

Throughout this section g is a perfect code in a group G with $|G| = |B^n|$, p is a prime dividing $|G|$, and $\psi: G \rightarrow \mathbb{F}_p = \mathbb{Z}/p$ is surjective. We put

$$\begin{aligned} x_j &= \psi(g_j), & m &= \frac{|G|}{p}, & c(h) &= \#\{j : x_j = h\} \quad (h \in \mathbb{F}_p), \\ P_k &= \sum_j (x_j^k + (-x_j)^k) \in \mathbb{F}_p, \end{aligned}$$

with $0^0 = 1$. For odd k the two terms of each summand cancel, so $P_k = 0$. For $F \in \mathbb{F}_p[\mathbb{F}_p]$ and $k \geq 0$ we define the moment $M_k(F) = \sum_{h \in \mathbb{F}_p} F(h)h^k \in \mathbb{F}_p$. Expanding $(h + h')^k$ gives

$$(3.1) \quad M_k(FF') = \sum_{i=0}^k \binom{k}{i} M_i(F) M_{k-i}(F').$$

For $T_i = [0] + \sum_j ([ix_j] + [-ix_j])$ we have $M_0(T_i) = 2n + 1$ and $M_k(T_i) = i^k P_k$ for $k \geq 1$.

Proposition 3.1. *Let $v \geq 1$, and suppose that $P_k = 0$ for $1 \leq k < v$. Then $\kappa_n(v) P_v = 6m \sum_{h \in \mathbb{F}_p} h^v$, where*

$$\kappa_n(v) = 3(2n+1)^2 + 3(2n+1)(1+2^v) + 2 \cdot 3^v - 6n.$$

Proof. Call F flat if $M_k(F) = 0$ for $1 \leq k < v$. By (3.1) a product of flat elements is flat, and for flat F, F' we have $M_v(FF') = M_0(F)M_v(F') + M_v(F)M_0(F')$. The T_i are flat by hypothesis, so

$$\begin{aligned} M_v(T_1^3) &= 3(2n+1)^2 P_v, & M_v(T_1 T_2) &= (2n+1)(1+2^v) P_v, \\ M_v(T_3) &= 3^v P_v, & M_v(T_1) &= P_v. \end{aligned}$$

Apply M_v to (2.3) with $k = \Gamma = \mathbb{F}_p$; the left side becomes $6m \sum_h h^v$. $\square$

Lemma 3.2. $\sum_{h \in \mathbb{F}_p} h^v = 0$ for $1 \leq v < p-1$, and $\sum_{h \in \mathbb{F}_p} h^{p-1} = -1$.

Proof. If $1 \leq v < p-1$, a generator u of the cyclic group $\mathbb{F}_p^\times$ has $u^v \neq 1$, and $\sum_h h^v = \sum_h (uh)^v = u^v \sum_h h^v$. If $v = p-1$, then $h^v = 1$ for $h \neq 0$. $\square$

Corollary 3.3. *Let $2 \leq L \leq p-1$, and suppose that $\kappa_n(v) \neq 0$ in $\mathbb{F}_p$ for every even v with $2 \leq v < L$. Then $P_k = 0$ for $1 \leq k < L$.*

Proof. By induction on k . For odd k we have seen that $P_k = 0$. For even $k < L$, Proposition 3.1 with $v = k$ and Lemma 3.2 give $\kappa_n(k) P_k = 0$. $\square$

When all power sums below $p-1$ vanish, the distribution of the x_j is almost determined.

Lemma 3.4. *Suppose that $P_k = 0$ for $1 \leq k < p-1$, and let $D \in \{0, \dots, p-1\}$ be the integer with $D \equiv -P_{p-1} \pmod{p}$.*

- (1) $c(h) + c(-h) \equiv D \pmod{p}$ for every $h \neq 0$, and $2c(0) \equiv 2n + D \pmod{p}$.
- (2) $(p-1)D + 2c(0) \leq 2n$, and if equality holds, then $c(h) + c(-h) = D$ for every $h \neq 0$.

Proof. (1) Let $F = T_1 - (2n+1)[0]$, so that $F(h) = c(h) + c(-h) - 2n \delta_{h,0}$, $M_0(F) = 0$ and $M_k(F) = P_k$ for $k \geq 1$. Fix $h \in \mathbb{F}_p$. Expanding $(h' - h)^{p-1}$ by the binomial theorem gives

$$\sum_{h'} F(h') (h' - h)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (-h)^{p-1-i} M_i(F) = M_{p-1}(F) = P_{p-1}.$$

On the other hand $(h' - h)^{p-1}$ is 1 for $h' \neq h$ and 0 for $h' = h$, so the left side is $M_0(F) - F(h) = -F(h)$. Thus $F(h) \equiv D$ for every h , which is (1).

(2) Every j with $x_j \neq 0$ is counted in exactly two of the numbers $c(h) + c(-h)$ with $h \neq 0$, so these $p-1$ numbers add up to $2n - 2c(0)$. Each of them is a

nonnegative integer congruent to D modulo p , and $0 \leq D < p$, so each is at least D . $\square$

4. THE CONSTANT TERM MODULO p^2

The identity (2.3) holds over $\mathbb{Z}$, so it can be read modulo p^2 . When the pair counts are divisible by p , its coefficient at $[0]$ gives one more congruence.

Lemma 4.1. *Keep the notation of Section 3, and assume $p \geq 5$. If p divides $c(h) + c(-h)$ for every $h \neq 0$, then*

$$6m \equiv f_n(1 + 2c(0)) \pmod{p^2}.$$

Proof. Work in $(\mathbb{Z}/p^2)[\mathbb{F}_p]$. As $p \geq 5$, the numbers $i = 1, 2, 3$ are invertible modulo p , and the coefficient of T_i at h is $\delta_{h,0} + c(i^{-1}h) + c(-i^{-1}h)$. At $h = 0$ this is $A = 1 + 2c(0)$, and at $h \neq 0$ it is divisible by p . Hence $T_i = A[0] + pW_i$ with $W_i(0) = 0$. Since $p^2 = 0$,

$$T_1^3 + 3T_1T_2 + 2T_3 - 6nT_1 = f_n(A)[0] + p((3A^2 + 3A - 6n)W_1 + 3AW_2 + 2W_3),$$

and the second term has coefficient 0 at $[0]$. The left side of (2.3) is $6mS_{\mathbb{F}_p}$, whose coefficient at $[0]$ is $6m$. $\square$

TABLE 1. The values of $\kappa_{805}(v)$ and $\kappa_{35}(v)$ modulo 29 for even v .

v	2	4	6	8	10	12	14	16	18	20	22	24	26	28
$\kappa_{805}(v) \bmod 29$	24	19	23	23	24	8	25	10	15	11	11	10	26	9
$\kappa_{35}(v) \bmod 29$	17	20	27	10	1	3	5	17	14	7	24	4	2	0

5. DIMENSION 805

Proof of Theorem 1.1 for $n = 805$. Suppose that a lattice tiling exists. Lemma 2.2 gives a perfect code g in a group G of order 696845031, and Lemma 2.6 gives a surjection $\psi: G \rightarrow \mathbb{F}_{29}$. We use the notation of Section 3 with $p = 29$, so $m = |G|/29 = 24029139 = 29 \cdot 828591$.

Step 1: $P_k = 0$ for $1 \leq k \leq 28$. Modulo 29 we have $n \equiv 22$, $2n + 1 \equiv 16$ and $3 \equiv 2^5$, so with $z = 2^v$,

$$\kappa_{805}(v) \equiv 3 \cdot 16^2 + 3 \cdot 16(1 + z) + 2z^5 - 6 \cdot 22 \equiv 2z^5 + 19z + 17 \pmod{29}.$$

Table 1 lists these values for even $v \leq 28$; none is zero. Corollary 3.3 with $L = 28$ gives $P_k = 0$ for $1 \leq k < 28$. Proposition 3.1 with $v = 28$ and Lemma 3.2 give $9P_{28} = -6m = 0$, since 29 divides m . Hence $P_{28} = 0$.

Step 2: the counts. Lemma 3.4 applies with $D = 0$: 29 divides $c(h) + c(-h)$ for every $h \neq 0$, and $2c(0) \equiv 2n$, so $c(0) \equiv 22 \pmod{29}$. Since $0 \leq c(0) \leq 805 = 22 + 29 \cdot 27$, we can write $c(0) = 22 + 29k$ with $0 \leq k \leq 27$.

Step 3: modulo 29^2 . By Lemma 4.1, $6m \equiv f_{805}(A) \pmod{29^2}$ with $A = 1 + 2c(0) = 45 + 58k$. For integers a and y ,

$$f_n(a + y) = f_n(a) + yf'_n(a) + y^2(3a + 3) + y^3, \quad f'_n(X) = 3X^2 + 6X + 2 - 6n.$$

Take $a = 45$ and $y = 58k$; the last two terms are divisible by 29^2 . Here $f_{805}(45) = -120060 \equiv 29 \cdot 7$ and $f'_{805}(45) = 1517 \equiv 9 \pmod{29}$, so $f_{805}(A) \equiv 29(7 + 18k) \pmod{29^2}$. On the other side $6m = 29 \cdot 4971546$ with $4971546 \equiv 18 \pmod{29}$.

Therefore $7 + 18k \equiv 18$, that is $18k \equiv 11 \pmod{29}$. As $18 \cdot 21 \equiv 1$, this gives $k \equiv 11 \cdot 21 \equiv 28 \pmod{29}$, which contradicts $0 \leq k \leq 27$. $\square$

Without the bound $c(0) \leq n$ the congruence of Step 3 has the solution $c(0) = 834$; it is the size of G relative to n , through $c(0) \leq n$, that closes the case.

6. DIMENSION 35

Suppose that a lattice tiling of $\mathbb{Z}^{35}$ by $B^{35}(3)$ exists. By Lemma 2.2 there is a perfect code g in a group G of order $59711 = 71 \cdot 29^2$, and by Lemma 2.6 there are surjections $\psi_1: G \rightarrow \mathbb{F}_{71}$ and $\psi_2: G \rightarrow \mathbb{F}_{29}$. We put

$$\begin{aligned} x_j &= \psi_1(g_j) \in \mathbb{F}_{71}, & y_j &= \psi_2(g_j) \in \mathbb{F}_{29}, \\ c_{71}(h) &= \#\{j : x_j = h\}, & c_{29}(t) &= \#\{j : y_j = t\}. \end{aligned}$$

6.1. The prime 71.

Lemma 6.1. $c_{71}(0) = 0$, and $c_{71}(h) + c_{71}(-h) = 1$ for every $h \neq 0$. Consequently $x_j \neq 0$ for every j , and $x_j \neq \pm x_k$ for $j \neq k$.

Proof. We apply Section 3 with $p = 71$ and $m = 841$. Since $2n + 1 = 71$ and $6n = 210 \equiv -3 \pmod{71}$, we have $\kappa_{35}(v) \equiv 2 \cdot 3^v + 3 = 3(2 \cdot 3^{v-1} + 1)$. If this vanished, then $3^{v-1} \equiv -2^{-1} \equiv -36 = -6^2$. But 3 is a square modulo 71, because $\left(\frac{3}{71}\right) = -\left(\frac{71}{3}\right) = -\left(\frac{2}{3}\right) = 1$, while -1 is not, because $71 \equiv 3 \pmod{4}$. So $\kappa_{35}(v) \neq 0$ for every $v \geq 1$, and Corollary 3.3 with $L = 70$ gives $P_k = 0$ for $1 \leq k < 70$. For $v = 70$ we have $\kappa_{35}(70) \equiv 2 + 3 = 5$ by Fermat's theorem, and $6m = 5046 \equiv 5$, so Proposition 3.1 and Lemma 3.2 give $5P_{70} = -5$, that is $P_{70} = -1$ and $D = 1$.

By Lemma 3.4, $2c_{71}(0) \equiv 2n + 1 = 71 \equiv 0$, and $c_{71}(0) \leq 35$, so $c_{71}(0) = 0$. Then $(p - 1)D + 2c_{71}(0) = 70 = 2n$, and the equality case of Lemma 3.4 gives $c_{71}(h) + c_{71}(-h) = 1$ for $h \neq 0$. If $x_j = \pm x_k$ for some $j \neq k$, then $h = x_j \neq 0$ has $c_{71}(h) + c_{71}(-h) \geq 2$, since $h \neq -h$. $\square$

6.2. The prime 29.

Lemma 6.2. *One of the following holds.*

- (a) 29 divides $c_{29}(t) + c_{29}(-t)$ for every $t \neq 0$, and $c_{29}(0) \in \{6, 35\}$.
- (b) $c_{29}(t) + c_{29}(-t) = 1$ for every $t \neq 0$, and $c_{29}(0) = 21$.
- (c) $c_{29}(t) + c_{29}(-t) = 2$ for every $t \neq 0$, and $c_{29}(0) = 7$.

Proof. We apply Section 3 with $p = 29$ and $m = 2059 = 29 \cdot 71$. Modulo 29 we have $2n + 1 \equiv 13$ and $6n \equiv 7$, so with $z = 2^v$,

$$\kappa_{35}(v) \equiv 3 \cdot 13^2 + 3 \cdot 13(1 + z) + 2z^5 - 7 \equiv 2z^5 + 10z + 17 \pmod{29}.$$

By Table 1 these values are nonzero for even $v \leq 26$, so Corollary 3.3 with $L = 28$ gives $P_k = 0$ for $1 \leq k < 28$. (The value at $v = 28$ is zero, so P_{28} is not determined.) Let D be as in Lemma 3.4. Then $28D + 2c_{29}(0) \leq 70$, so $D \leq 2$, and $2c_{29}(0) \equiv 70 + D \pmod{29}$.

If $D = 0$, then $c_{29}(0) \equiv 35 \equiv 6$ and $c_{29}(0) \leq 35$, which is (a). If $D = 1$, then $2c_{29}(0) \equiv 13$, so $c_{29}(0) \equiv 21$, while $2c_{29}(0) \leq 42$; hence $c_{29}(0) = 21$, equality holds in Lemma 3.4(2), and we are in (b). If $D = 2$, then $2c_{29}(0) \equiv 14$, so $c_{29}(0) \equiv 7$, while $2c_{29}(0) \leq 14$; hence $c_{29}(0) = 7$ and we are in (c). $\square$

Figure 3 shows the distributions of Lemma 6.1 and of case (c).

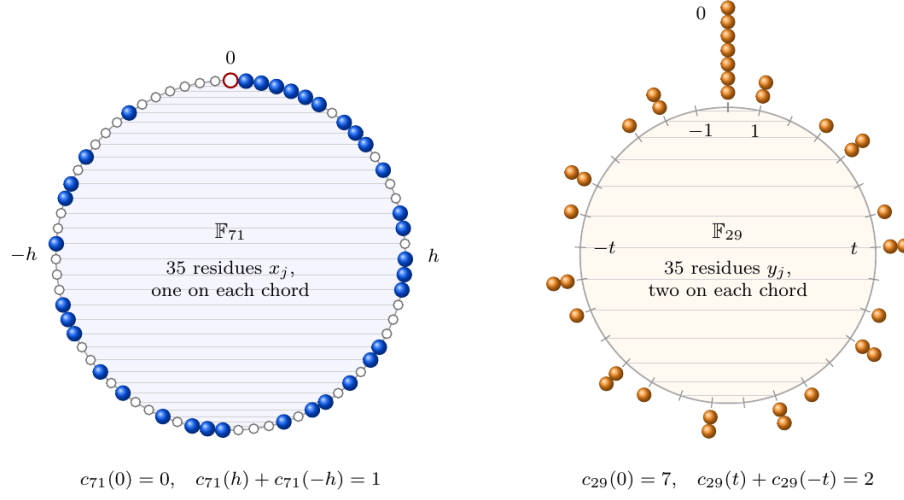


FIGURE 3. Left: the 35 residues x_j in $\mathbb{F}_{71}$; each pair $\{h, -h\}$ with $h \neq 0$ carries exactly one of them (Lemma 6.1). Right: the residues y_j in $\mathbb{F}_{29}$ in case (c) of Lemma 6.2; 0 carries seven of them and each pair $\{t, -t\}$ with $t \neq 0$ carries two. Each picture alone is compatible with the projected identity (2.3) (Remark 6.3).

6.3. Case (a). By Lemma 4.1 with $p = 29$, $6m = 12354 \equiv 580 \pmod{841}$ would be congruent to $f_{35}(1 + 2c_{29}(0))$. But $f_{35}(13) = 13 \cdot 14 \cdot 15 - 210 \cdot 13 = 0$ and $f_{35}(71) = 71(72 \cdot 73 - 210) = 6 \cdot 71 \cdot 841 \equiv 0$. Since $580 \not\equiv 0 \pmod{841}$, case (a) is impossible.

6.4. The joint projection. In cases (b) and (c) we have $c_{29}(t) + c_{29}(-t) = D$ for every $t \neq 0$, with $D = 1$ and $c_{29}(0) = 21$, or $D = 2$ and $c_{29}(0) = 7$. Let $\Gamma = \mathbb{F}_{71} \times \mathbb{F}_{29}$ and $\psi = (\psi_1, \psi_2): G \rightarrow \Gamma$. The image of ψ is a subgroup of the cyclic group Γ of order 2059 whose order is divisible by 71 and by 29, because both projections are onto; so ψ is surjective and $|G|/|\Gamma| = 29$.

Let $R_0 = \mathbb{F}_{71}[\mathbb{F}_{29}]$ and let $\Lambda = R_0[\varepsilon]/(\varepsilon^2)$ be the ring of dual numbers over R_0 . The map

$$\chi(s, t) = [t](1 + s\varepsilon) = [t] + s[t]\varepsilon, \quad (s, t) \in \Gamma,$$

is a homomorphism $\Gamma \rightarrow \Lambda^\times$, because $(1 + s\varepsilon)(1 + s'\varepsilon) = 1 + (s + s')\varepsilon$. The left side of (2.2) is

$$6 \cdot 29 \sum_{t \in \mathbb{F}_{29}} [t] \left(71 + \left(\sum_{s \in \mathbb{F}_{71}} s \right) \varepsilon \right) = 0,$$

because $71 = 0$ and $\sum_{s \in \mathbb{F}_{71}} s = 71 \cdot 35 = 0$ in $\mathbb{F}_{71}$. On the right side $T_i = U_i + N_i\varepsilon$ with

$$U_i = [0] + \sum_j ([iy_j] + [-iy_j]), \quad N_i = i \sum_j x_j ([iy_j] - [-iy_j]) \quad \text{in } R_0.$$

Taking the coefficient of ε in (2.2) gives

$$(6.1) \quad 3U_1^2 N_1 + 3(U_1 N_2 + U_2 N_1) + 2N_3 - 6nN_1 = 0.$$

The coefficient of U_i at t is $\delta_{t,0} + c_{29}(i^{-1}t) + c_{29}(-i^{-1}t)$, which equals $1 + 2c_{29}(0)$ at $t = 0$ and D at $t \neq 0$. Hence $U_i = A[0] + DS$ with $S = S_{\mathbb{F}_{29}}$ and $A = 1 + 2c_{29}(0) - D$. Since $S[t] = S$ for every t , we get $SN_i = 0$, and (6.1) becomes

$$(6.2) \quad (3A^2 + 3A - 6n)N_1 + 3AN_2 + 2N_3 = 0.$$

For $t \in \mathbb{F}_{29}$ put

$$s(t) = \sum_{j: y_j=t} x_j - \sum_{j: y_j=-t} x_j \in \mathbb{F}_{71}.$$

The coefficient of N_i at t is $i s(i^{-1}t)$. In $\mathbb{F}_{29}$ we have $2^{-1} = 15$ and $3^{-1} = 10$, so (6.2) says that

$$(6.3) \quad (3A^2 + 3A - 6n)s(t) + 6As(15t) + 6s(10t) = 0 \quad \text{for every } t \in \mathbb{F}_{29}.$$

In case (b), $A = 42$, and the coefficients are $5208 \equiv 25$, $252 \equiv 39$ and 6 modulo 71 . In case (c), $A = 13$, and they are $336 \equiv 52$, $78 \equiv 7$ and 6 . Multiplying by $12 = 6^{-1}$ in $\mathbb{F}_{71}$, we obtain

$$(6.4) \quad as(t) + bs(15t) + s(10t) = 0 \quad \text{for every } t \in \mathbb{F}_{29},$$

with $(a, b) = (16, 42)$ in case (b) and $(a, b) = (56, 13)$ in case (c).

6.5. A circulant system. The residue 2 is a primitive root modulo 29: $2^4 = 16 \neq 1$, $2^7 = 128 \equiv 12$ and $2^{14} \equiv 144 \equiv -1$, so the order of 2 divides 28 but not 14 or 4. Hence $15 = 2^{-1}$ has order 28, $15^{14} = -1$, and $15^5 = 2^{-5} = 3^{-1} = 10$, since $2^5 = 32 \equiv 3$. Put $\mu_k = s(15^k)$ for $k \in \mathbb{Z}$. Then $\mu_{k+28} = \mu_k$, and since $s(-t) = -s(t)$, also $\mu_{k+14} = -\mu_k$. Taking $t = 15^k$ in (6.4) gives

$$(6.5) \quad a\mu_k + b\mu_{k+1} + \mu_{k+5} = 0 \quad \text{for every } k.$$

Figure 4 shows these relations on the orbit of 1.

Let V be the $\mathbb{F}_{71}$ -vector space of sequences $(\mu_k)_{k \in \mathbb{Z}}$ of period 28, and let σ be the shift, $(\sigma\mu)_k = \mu_{k+1}$. It is invertible, with $\sigma^{-1} = \sigma^{27}$. For our μ the set I of polynomials $Q \in \mathbb{F}_{71}[X]$ with $Q(\sigma)\mu = 0$ is an ideal. It contains $Q = X^5 + bX + a$ by (6.5), and $X^{14} + 1$. Applying $\sigma^5\mu = -(a + b\sigma)\mu$ three times gives $\sigma^{15}\mu = -(a + b\sigma)^3\mu$, while $\sigma^{15}\mu = \sigma\sigma^{14}\mu = -\sigma\mu$. So I also contains $C = (a + bX)^3 - X$. All congruences below are modulo 71.

In case (b), $C = 35X^3 - 31X^2 + 21X - 22$ and I contains $\tilde{C} = -2C = X^3 - 9X^2 + 29X - 27$. Division with remainder gives

$$Q = (X^2 + 9X - 19)\tilde{C} + 21X(X + 6), \quad \tilde{C} = (X - 15)X(X + 6) - 23(X - 5).$$

Hence $X(X + 6) \in I$, and then $X - 5 \in I$. As σ is invertible, $(\sigma + 6)\mu = 0$ and $(\sigma - 5)\mu = 0$; subtracting, $11\mu = 0$, so $\mu = 0$.

In case (c), $C = -4X^3 - 8X^2 - 30X + 33$ and I contains $\tilde{C} = -18C = X^3 + 2X^2 - 28X - 26$. Here

$$Q = (X^2 - 2X + 32)\tilde{C} - 23(X - 14)^2, \quad \tilde{C} = (X + 30)(X - 14)^2 - 23(X + 16).$$

Hence $(X - 14)^2 \in I$, and then $X + 16 \in I$. So $\sigma\mu = -16\mu$, and $0 = (\sigma - 14)^2\mu = 30^2\mu = 48\mu$; again $\mu = 0$.

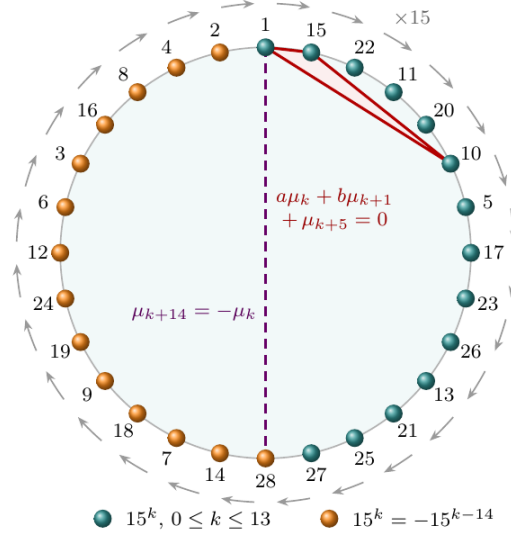


FIGURE 4. The cyclic group $\mathbb{F}_{29}^\times$ as the orbit 15^k , $0 \leq k \leq 27$. Each relation (6.5) joins the values of s at 15^k , $15^{k+1} = 2^{-1} \cdot 15^k$ and $15^{k+5} = 3^{-1} \cdot 15^k$ (one instance drawn), and opposite points 15^k and $15^{k+14} = -15^k$ carry opposite values of s .

6.6. End of the proof.

Proof of Theorem 1.1 for $n = 35$. Cases (a), (b) and (c) of Lemma 6.2 exhaust the possibilities. Case (a) is impossible, and in cases (b) and (c) we have shown that $\mu = 0$, in particular $s(1) = \mu_0 = 0$. The set $J = \{j : y_j = \pm 1\}$ has $c_{29}(1) + c_{29}(-1) = D$ elements, and $s(1) = \sum_{j \in J} \pm x_j$. If $D = 1$, then $s(1) = \pm x_j$ for one j , which is nonzero by Lemma 6.1. If $D = 2$, then $s(1) = \pm x_j \pm x_k$ with $j \neq k$, which is nonzero because $x_j \neq \pm x_k$ by Lemma 6.1. Either way $s(1) \neq 0$, a contradiction. $\square$

Remark 6.3. Case (b) can also be excluded without the prime 71. In cases (b) and (c) the element T_i of (2.3) for $\Gamma = \mathbb{F}_{29}$ is $A[0] + DS$ with integer coefficients, and $S^2 = 29S$, so the right side of (2.3) is $f_{35}(A)[0]$ plus an integer multiple of S . Comparing the coefficients at $[0]$ and $[1]$ with those of the left side $6mS$ gives $f_{35}(A) = 0$. For $A > 0$ this means $(A+1)(A+2) = 210$, that is $A = 13$, which rules out case (b), where $A = 42$. Case (c) passes: with $A = 13$ and $D = 2$ the right side is exactly $12354S = 6mS$. Likewise the distribution of Lemma 6.1 gives $T_i = S_{\mathbb{F}_{71}}$ and a right side $5046 S_{\mathbb{F}_{71}} = 6 \cdot 841 S_{\mathbb{F}_{71}}$, as required. So each of the two distributions of Figure 3 satisfies the projected identity (2.3) exactly, as Xiao and Zhou observed [18, Example 5.14], and only the joint projection of Section 6.4 sees that they cannot occur together.

7. FORMAL VERIFICATION

Theorem 1.1 has been formalized in Lean 4 [12] with the Mathlib library [14]. The formal statement defines a lattice tiling of $\mathbb{Z}^n$ by $B^n(r)$ as a subgroup L of $\mathbb{Z}^n$ such that every $x \in \mathbb{Z}^n$ has exactly one $l \in L$ with $\sum_j |x_j - l_j| \leq r$, and it

asserts that no such subgroup exists for $(n, r) = (35, 3)$ or $(805, 3)$. The proof follows Sections 2–6. Lemma 2.2, Proposition 2.3 for an arbitrary commutative ring, Lemmas 2.4 and 2.6, Proposition 3.1, Lemmas 3.2 and 3.4, Lemma 4.1 for $p = 29$, and the arguments of Sections 5 and 6 are proved there, and the finite computations in $\mathbb{F}_{29}$, $\mathbb{F}_{71}$ and $\mathbb{Z}/841$, among them Table 1, are checked by the kernel. Two steps are argued differently there: the left side of (2.2) in Section 6.4 is shown to vanish by pairing each element x of a fibre of ψ_2 with $2x_0 - x$ for a fixed x_0 in that fibre, and the system (6.5) is solved by an explicit linear combination of its twenty-eight equations. Both theorems depend only on the standard axioms of Lean, namely propositional extensionality, choice and quotient soundness. The numbers in Sections 5 and 6 were also recomputed independently by the programs archived with the formalization [2].

Data and code availability. The L^AT_EX source of the paper, the Lean 4 formalisation of Theorem 1.1 described in Section 7, and the C, C++, Python, Julia and shell programs that recompute the finite quantities of Sections 5 and 6 are archived at Zenodo under doi:10.5281/zenodo.23398805 [2]; the paper is available at <https://github.com/creelie/refactored-waddle/blob/main/preprintGolombWelchRadiusThree/GolombWelchRadiusThree.pdf>. Deep Bhattacharjee carried out the computations and the Lean, Julia, C, C++, Python and shell verifications, and the proofs and the text were drafted, with AI assistance (Claude, Anthropic); both authors approved the final version.

Ethical declarations. Funding: none. Competing interests: none.

REFERENCES

- [1] D. Bhattacharjee, *Establishing equivariant class [O] for hyperbolic groups*, Asian Res. J. Math. **18** (2022), no. 11, 362–369, doi:10.9734/arjom/2022/v18i11615.
- [2] D. Bhattacharjee and U. Bhattacharya, *No lattice tiling of $\mathbb{Z}^{35}$ or $\mathbb{Z}^{805}$ by Lee balls of radius three: Lean formalization and programs*, Zenodo, 2026, doi:10.5281/zenodo.23398805.
- [3] D. Bhattacharjee, U. Bhattacharya and S. Bhattacharya, *The sphere packing problem in dimension 4*, Preprints.org, 2026, doi:10.20944/preprints202606.0856.v11.
- [4] D. Bhattacharjee, U. Bhattacharya and S. Bhattacharya, *The sphere packing problem in dimension 7*, Preprints.org, 2026, doi:10.20944/preprints202606.1534.v9.
- [5] R. Dougherty and V. Faber, *The degree-diameter problem for several varieties of Cayley graphs I: the abelian case*, SIAM J. Discrete Math. **17** (2004), 478–519, doi:10.1137/S0895480100372899.
- [6] S. W. Golomb and L. R. Welch, *Perfect codes in the Lee metric and the packing of polyominoes*, SIAM J. Appl. Math. **18** (1970), 302–317, doi:10.1137/0118025.
- [7] S. Gravier, M. Mollard and C. Payan, *On the non-existence of 3-dimensional tiling in the Lee metric*, European J. Combin. **19** (1998), 567–572, doi:10.1006/eujc.1998.0211.
- [8] P. Horak, *Tilings in Lee metric*, European J. Combin. **30** (2009), 480–489, doi:10.1016/j.ejc.2008.04.007.
- [9] P. Horak and B. F. AlBdaiwi, *Diameter perfect Lee codes*, IEEE Trans. Inform. Theory **58** (2012), 5490–5499, doi:10.1109/TIT.2012.2196257.
- [10] P. Horak and D. Kim, *50 years of the Golomb–Welch conjecture*, IEEE Trans. Inform. Theory **64** (2018), 3048–3061, doi:10.1109/TIT.2017.2786675.
- [11] D. Kim, *Nonexistence of perfect 2-error-correcting Lee codes in certain dimensions*, European J. Combin. **63** (2017), 1–5, doi:10.1016/j.ejc.2017.01.007.
- [12] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. 12699, Springer, 2021, pp. 625–635, doi:10.1007/978-3-030-79876-5_37.

- [13] K. H. Leung and Y. Zhou, *No lattice tiling of $\mathbb{Z}^n$ by Lee sphere of radius 2*, J. Combin. Theory Ser. A **171** (2020), 105157, doi:10.1016/j.jcta.2019.105157.
- [14] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381, doi:10.1145/3372885.3373824.
- [15] K. A. Post, *Nonexistence theorems on perfect Lee codes over large alphabets*, Inform. and Control **29** (1975), 369–380, doi:10.1016/S0019-9958(75)80005-2.
- [16] C. Qureshi, *On the non-existence of linear perfect Lee codes: the Zhang–Ge condition and a new polynomial criterion*, European J. Combin. **83** (2020), 103022, doi:10.1016/j.ejc.2019.103022.
- [17] M. Szegedy, *Algorithms to tile the infinite grid with finite clusters*, in: Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS 1998), IEEE, 1998, pp. 137–145, doi:10.1109/SFCS.1998.743437.
- [18] A. Xiao and Y. Zhou, *On the lattice tilings by Lee balls: Q -polynomials, group-ring equations, and a decision algorithm*, arXiv:2610.19775, 2026.
- [19] T. Zhang and G. Ge, *Perfect and quasi-perfect codes under the l_p metric*, IEEE Trans. Inform. Theory **63** (2017), 4325–4331, doi:10.1109/TIT.2017.2685424.
- [20] T. Zhang and G. Ge, *On linear diameter perfect Lee codes with distance 6*, J. Combin. Theory Ser. A **201** (2024), 105816, doi:10.1016/j.jcta.2023.105816.
- [21] T. Zhang and Y. Zhou, *On the nonexistence of lattice tilings of $\mathbb{Z}^n$ by Lee spheres*, J. Combin. Theory Ser. A **165** (2019), 225–257, doi:10.1016/j.jcta.2019.02.008.

FORMERLY, ELECTRO-GRAVITATIONAL SPACE PROPULSION LABORATORY (EGSPL),
 BHUBANESWAR, ODISHA 751030, INDIA; FORMERLY, UNIVERSITY OF CALCUTTA, SENATE HOUSE,
 87/1 COLLEGE STREET, KOLKATA 700073, WEST BENGAL, INDIA

Email address: `itsdeep@live.com`

Email address: `d.bhattacharjee@erl-forschung.de`

URL: `https://orcid.org/0000-0003-0466-750X`

FORMERLY, NATIONAL TAIWAN UNIVERSITY, TAIPEI 106319, TAIWAN

Email address: `rai.bhattacharya.in@gmail.com`

URL: `https://orcid.org/0009-0002-2254-3914`