

McMaster University

Advanced Optimization Laboratory



Title:

Primitive Point Packing

Authors:

Antoine Deza and Lionel Pournin

AdvOL-Report No. 2020/1

June 2020, Hamilton, Ontario, Canada

PRIMITIVE POINT PACKING

ANTOINE DEZA

McMaster University, Hamilton, Ontario, Canada

e-mail: deza@mcmaster.ca

LIONEL POURNIN

Université Paris 13, Villetaneuse, France

e-mail: lionel.pournin@univ-paris13.fr

ABSTRACT

A point in the d -dimensional integer lattice \mathbb{Z}^d is primitive when its coordinates are relatively prime. Two primitive points are multiples of one another when they are opposite, and for this reason, we consider half of the primitive points within the lattice, the ones whose first non-zero coordinate is positive. We solve the packing problem that asks for the largest possible number of such points whose absolute values of any given coordinate sum to at most a fixed integer k . We present several consequences of this result at the intersection of geometry, number theory, and combinatorics. In particular, we obtain an explicit expression for the largest possible diameter of a lattice zonotope contained in the hypercube $[0, k]^d$ and, conjecturally of any lattice polytope in that hypercube.

1. Introduction

Lattice polytopes appear in many branches of mathematics, as for instance in algebraic geometry where they are associated with certain toric varieties. It is noteworthy that, in relation with the study of these and similar objects, methods from combinatorics and algebraic geometry have been beneficial to both fields [1, 5, 10, 14, 23, 25]. Another branch of mathematics where lattice polytopes turn up is combinatorial optimization. In particular, they encode the feasible domain of a number of optimization problems [3, 7, 19, 20]. In this other context, an important quantity is the largest diameter a polytope can

possibly have in terms of a fixed combinatorial or geometric property. Here, by the diameter of a polytope, we mean the diameter of the graph made up of its vertices and edges. This quantity is tightly linked to the complexity of pivoting methods for solving the corresponding optimization problem and it has been extensively studied, for instance as a function of the dimension and number of facets of the polytope [15, 16, 19, 26]. However, as the disproof of the Hirsch conjecture [24] shows, its behavior remains elusive.

Yet another field where lattice polytopes appear, lies at the intersection of geometry and number theory [2, 6, 11, 12]. For instance, the density of primitive points—points whose coordinates are relatively prime—within the lattice \mathbb{Z}^d is equal to $1/\zeta(d)$, where ζ denotes Riemann’s zeta function [13, 17, 21]. From that observation, a sharp estimate for the largest possible diameter of a lattice zonotope contained in the hypercube $[0, k]^d$ when d is fixed and k grows large has been derived recently [9]. The case of zonotopes—polytopes obtained as a Minkowski sum of line segments—is particularly interesting in relation to the problem of the diameter of polytopes. Indeed, it is conjectured that the largest possible diameter of a lattice polytope contained in the hypercube $[0, k]^d$ is always achieved by a zonotope [8]. In the case of lattice zonotopes, the problem can be reformulated as follows in terms of primitive points.

Let \mathbb{P}^d be the set of the primitive points contained in \mathbb{Z}^d . Consider a subset \mathcal{X} of \mathbb{P}^d whose first non-zero coordinate of elements is positive and call

$$\kappa(\mathcal{X}) = \max \left\{ \sum_{x \in \mathcal{X}} |x_i| : 1 \leq i \leq d \right\},$$

where the coordinates of a point x from \mathbb{R}^d are denoted by x_1 to x_d . In other words, $\kappa(\mathcal{X})$ is the sum over all the points in \mathcal{X} of the absolute value of one of their coordinates for which that sum is the greatest. Using this quantity, we can ask the question of *how large the cardinality of \mathcal{X} can be under the requirement that $\kappa(\mathcal{X})$ does not exceed a given integer k* . Incidentally, the answer to this primitive point packing problem at the intersection of geometry, number theory, and combinatorics coincides with the largest possible diameter of a lattice zonotope contained in the hypercube $[0, k]^d$. In this article, we settle this problem completely by giving an explicit expression for its solution, thus also solving the question on the largest possible diameter of lattice zonotopes and, conjecturally, the more general one about lattice polytopes.

Let us describe our main results in more details. Following the notation introduced in [9], we refer to the solution to our packing problem as

$$\delta_z(d, k) = \max_{\mathcal{X} \in \mathbb{P}_\circ^d} \{|\mathcal{X}| : \kappa(\mathcal{X}) \leq k\}.$$

Here \mathbb{P}_\circ^d is the subset of \mathbb{P}^d made up of the points whose first non-zero coordinate is positive. Note that an expression for $\delta_z(d, k)$ is already known when k is less than $2d$. Indeed, it is proven in [8] that, in this case,

$$(1) \quad \delta_z(d, k) = \left\lfloor \frac{(k+1)d}{2} \right\rfloor.$$

Denote by $B(d, p)$ the ball of radius p for the 1-norm, centered on the origin of \mathbb{R}^d . Note that this ball is a cross-polytope, the polytope dual to the hypercube. Our first result, which we prove in Section 2 provides the cardinality of the intersection of $B(d, p)$ with \mathbb{P}_\circ^d and the value of κ at that intersection.

THEOREM 1.1: *For any positive integers d and p ,*

- (i) $|B(d, p) \cap \mathbb{P}_\circ^d| = \frac{1}{2} \sum_{j=1}^d 2^j \binom{d}{j} \sum_{i=j}^p c_\psi(i, j)$, and
- (ii) $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) = \frac{1}{2} \sum_{j=1}^d 2^j \binom{d}{j} \sum_{i=j}^p i c_\psi(i, j)$,

where

$$c_\psi(p, d) = \frac{1}{(d-1)!} \sum_{i=1}^d s(d, i) J_{i-1}(p).$$

In the statement of this theorem, $s(d, i)$ stands for Stirling's numbers of the first kind and $J_i(p)$ for Jordan's totient function, whose precise definitions will be recalled in Section 2. The number of lattice points contained in a lattice polytope is related to certain invariants of the associated toric variety [22] and expressions for that number have been obtained in particular cases. For instance, a formula for the number of lattice points contained in the dilates by a positive integer of the cross-polytope $B(d, 1)$ is known [4]. In this light, it is noteworthy that Theorem 1.1 provides an expression for the number of primitive points contained in these dilates. Indeed, the intersection of $B(d, p)$ with \mathbb{P}^d is twice as large as its intersection with \mathbb{P}_\circ^d .

Theorem 1.1 also solves our primitive point packing problem for special values of k . Indeed, it is shown in [9] that the intersection of $B(d, p)$ with \mathbb{P}_\circ^d is the

unique subset of \mathbb{P}_\circ^d of cardinality $\delta_z(d, k)$ when

$$k = \kappa(B(d, p) \cap \mathbb{P}_\circ^d).$$

Hence, for these values of k , Theorem 1.1 provides an expression for $\delta_z(d, k)$. Now consider the piecewise-linear map $k \mapsto \lambda(d, k)$ that interpolates $\delta_z(d, k)$ linearly between any two consecutive such values of k . It follows from Theorem 1.1 that, when k is between $\kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$ and $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ the slope of the interpolation is d/p . More precisely, for these values of k ,

$$\frac{\lambda(d, k) - |B(d, p-1) \cap \mathbb{P}_\circ^d|}{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)} = \frac{d}{p}.$$

We will prove throughout Sections 3, 4, and 5 that $\delta_z(d, k)$ is equal to $\lfloor \lambda(d, k) \rfloor$ except for a few notable, but infrequent cases.

THEOREM 1.2: *For any fixed d , the maps $k \mapsto \delta_z(d, k)$ and $k \mapsto \lfloor \lambda(d, k) \rfloor$ coincide, except on an infinite subset \mathbb{E} of $\mathbb{N} \setminus \{0\}$ such that,*

$$\lim_{k \rightarrow \infty} \frac{|\mathbb{E} \cap [1, k]|}{k^{1/(d-1)}} = 0.$$

In addition, $k \mapsto \delta_z(d, k)$ coincides, on \mathbb{E} , with $k \mapsto \lfloor \lambda(d, k) \rfloor - 1$.

Note that the set \mathbb{E} of exceptions depends on the dimension. We will determine it explicitly in every dimension: it is given at the end of Section 4 when $d > 2$, and at the end of Section 5 when $d = 2$. The dependence of \mathbb{E} on d is consistent over all the dimensions above 2, but as we shall see, its form and its density within \mathbb{N} are slightly different in the 2-dimensional case.

The proof of theorem 1.2 will be split into first establishing an upper bound on $\delta_z(d, k)$, and then proving that this bound is exact by constructing sets of primitive points that achieve it. The upper bound is proven in Section 3. The general machinery we use to show that this bound is sharp is given in Section 4 together with sets of primitive points that achieve it in all dimensions greater than 2. The construction for the 2-dimensional case is given in Section 5.

Recall that, when $1 \leq k < 2d$, our expression for $\delta_z(d, k)$ simplifies to (1). Note, in particular that the bounds of this range for k are $|B(d, 1) \cap \mathbb{P}_\circ^d|$ and $|B(d, 2) \cap \mathbb{P}_\circ^d|$. We report in Table 1 the first values of $\delta_z(d, k)$ such that k is at least $2d$. In this table, the bold numbers are the values of $\delta_z(d, k)$ that coincide, for some integer p , with the cardinality of $B(d, p) \cap \mathbb{P}_\circ^d$ and the starred values

d	$k - 2d$														
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	4	5	6	6	7	8	8	8*	9	10	10	10*	11	12	12
3	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
4	17	18	20	21	22	24	25	26	28	29	30	32	33	34	36
5	26	28	30	31	33	35	36	38	40	41	43	45	46	48	50
6	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66

Table 1. Some values of $\delta_z(d, k)$.

are the ones such that k belongs to \mathbb{E} . Note that, when d is equal to 3, the smallest number in \mathbb{E} is 135 and it already lies way outside of the table.

We will also study the sets of points that solve our primitive point packing problem. Surprisingly, there exist values of d and k such that $\delta_z(d, k)$ is not achieved by a set of primitive points between $B(d, p - 1) \cap \mathbb{P}_\circ^d$ and $B(d, p) \cap \mathbb{P}_\circ^d$ in terms of inclusion, where p is the smallest integer such that k is less than $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. We will obtain, in Section 6, the following characterization for the values of d and k such that this phenomenon occurs. Note in particular, that this phenomenon only happens when d is equal to 2.

THEOREM 1.3: *Consider the smallest integer p such that $k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. If d is greater than 2, then any subset \mathcal{X} of \mathbb{P}_\circ^d of cardinality $\delta_z(d, k)$ such that $\kappa(\mathcal{X})$ does not exceed k must satisfy*

$$(2) \quad B(d, p - 1) \cap \mathbb{P}_\circ^d \subset \mathcal{X} \subset B(d, p) \cap \mathbb{P}_\circ^d.$$

If, on the other hand, d is equal to 2, then there exists a subset \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$ that satisfies (2) if and only if $p = 2$, or p is odd, or $p/2$ is even, or the following two conditions hold.

- (i) $k - \kappa(B(2, p - 1) \cap \mathbb{P}_\circ^2)$ is distinct from $p/2 + 1$,
- (ii) $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k$ is distinct from $p/2 - 1$.

We further show in Section 6 that the unicity result from [9] that we mention above singles out every value of k such that there is a unique set of primitive points that solves our packing problem.

THEOREM 1.4: *There exists a unique subset \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$ if and only if $k = \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ for some p .*

We conclude the article, by gathering in Section 7 a number of asymptotic estimates. Among them, we derive from Theorem 1.1 asymptotic estimates for $|B(d, p) \cap \mathbb{P}_\circ^d|$ in terms of $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ when p is fixed and d goes to infinity. This complements the result from [9] on the asymptotic behavior of $\delta_z(d, k)$. We also obtain an exact asymptotic estimate of the number of primitive points of 1-norm p contained in the positive orthant $]0, +\infty[^d$, for any fixed d , when p goes to infinity. Note that these points are a special case of integer compositions [18], the compositions of p into d relatively prime integers.

2. The number of primitive points in a cross-polytope

Consider the isometry σ of \mathbb{R}^d that permutes the coordinates cyclically as

$$\sigma : \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{d-1} \\ x_d \end{bmatrix} \mapsto \begin{bmatrix} x_d \\ x_1 \\ \vdots \\ x_{d-2} \\ x_{d-1} \end{bmatrix}.$$

Further consider the map τ that sends a vector x of \mathbb{R}^d to $\sigma(x)$ when x_d is non-negative and to $-\sigma(x)$ otherwise. In the remainder of the article, C denotes the cyclic group generated by τ . Observe that C has order d . For any point x contained in \mathbb{R}^d , we denote by $C \cdot x$ the orbit of x under the action of C on \mathbb{R}^d . Note that all the elements of $C \cdot x$ have the same 1-norm and, when x is primitive, $C \cdot x$ is a subset of \mathbb{P}^d . In addition, observe that the intersection of $B(d, p)$ and \mathbb{P}_\circ^d is invariant under the action of C on \mathbb{R}^d .

We first recall a proposition on the relation between $\kappa(\mathcal{X})$ and the 1-norms of the elements of \mathcal{X} , that is used implicitly in [9].

PROPOSITION 2.1: *For any subset \mathcal{X} of \mathbb{P}_\circ^d ,*

$$\kappa(\mathcal{X}) \geq \frac{1}{d} \sum_{x \in \mathcal{X}} \|x\|_1,$$

with equality if and only if \mathcal{X} is invariant under the action of C on \mathbb{R}^d .

Now denote by $c_\psi(p, d)$ the number of primitive points of 1-norm p and dimension d contained in the positive orthant:

$$c_\psi(p, d) = \left| \left\{ x \in \mathbb{P}^d \cap]0, +\infty[^d : \|x\|_1 = p \right\} \right|.$$

This quantity makes it possible to express as follows the sum over the intersection $B(d, p) \cap \mathbb{P}_\circ^d$ of any map that is well-behaved relative to the 1-norm.

LEMMA 2.2: *For any map $f : \mathbb{N} \rightarrow \mathbb{R}$ and any positive integer p ,*

$$\sum f(\|x\|_1) = \sum_{j=1}^d 2^j \binom{d}{j} \sum_{i=j}^p f(i) c_\psi(i, j),$$

where the sum in the left-hand side is over the primitive points x in $B(d, p)$.

Proof. Consider the sphere $S(d, i)$ of radius i for the 1-norm, centered at the origin of \mathbb{R}^d . In other words, $S(d, i)$ is the boundary of $B(d, i)$.

Let us first count the number of primitive points contained in $S(d, i)$. As $B(d, i)$ is a cross polytope, $c_\psi(i, j)$ is precisely the number of primitive points contained in the relative interior of one of its faces of dimension $j - 1$.

We therefore immediately obtain

$$|S(d, i) \cap \mathbb{P}^d| = \sum_{j=1}^d 2^j \binom{d}{j} c_\psi(i, j).$$

where the coefficient of $c_\psi(i, j)$ in the right-hand side is the number of the faces of dimension $j - 1$ of a cross-polytope.

Now observe that by construction, the intersection of $B(d, p)$ with \mathbb{P}^d is partitioned into the sets $S(d, i) \cap \mathbb{P}^d$ where i ranges from 1 to p . Hence,

$$\sum f(\|x\|_1) = \sum_{i=1}^p f(i) \sum_{j=1}^d 2^j \binom{d}{j} c_\psi(i, j),$$

where the sum in the left-hand side is over the primitive points x in $B(d, p)$. Exchanging the two sums in the right-hand side and noticing that $c_\psi(i, j)$ vanishes when i is less than j completes the proof. ■

Note that the cardinality of the intersection $B(d, p) \cap \mathbb{P}^d$ can be obtained from Lemma 2.2 by using, for f , the map that sends every natural integer to 1. By symmetry, the cardinality of $B(d, p) \cap \mathbb{P}_\circ^d$ is half of that quantity. In addition, since the intersection of $B(d, p)$ with \mathbb{P}_\circ^d is invariant under the action of C on \mathbb{R}^d , it follows from Proposition 2.1 that

$$d\kappa(B(d, p) \cap \mathbb{P}_\circ^d) = \sum \|x\|_1,$$

where the sum in the right-hand side is over the points x in that intersection. As above, that sum is half the sum of the 1-norms of the points in $B(d, p) \cap \mathbb{P}^d$,

that can be obtained from Lemma 2.2 by using for f , the identity map on \mathbb{N} . According to this discussion, we obtain the following.

PROPOSITION 2.3: *For any positive integers d and p ,*

$$(i) \quad |B(d, p) \cap \mathbb{P}_\circ^d| = \frac{1}{2} \sum_{j=1}^d 2^j \binom{d}{j} \sum_{i=j}^p c_\psi(i, j), \text{ and}$$

$$(ii) \quad \kappa(B(d, p) \cap \mathbb{P}_\circ^d) = \frac{1}{2d} \sum_{j=1}^d 2^j \binom{d}{j} \sum_{i=j}^p i c_\psi(i, j).$$

It is noteworthy that, as a consequence of this proposition,

$$\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) = \frac{p |S(d, p) \cap \mathbb{P}_\circ^d|}{d},$$

where $S(d, p)$ is the sphere of radius p for the 1-norm, centered at the origin of \mathbb{R}^d . We now derive a formula for $c_\psi(p, d)$. Let us denote by J_q Jordan's totient function; that is, for any two positive integers p and q ,

$$J_q(p) = p^q \prod_{n|p} \left(1 - \frac{1}{n^q}\right),$$

where, in this expression, n ranges over prime numbers. We also denote by $s(d, i)$ Stirling's numbers of the first kind. Let us recall that these numbers can be computed using the recurrence

$$s(d+1, i) = -ds(d, i) + s(d, i-1),$$

with $s(i, i) = 1$ for all $i \in \mathbb{N}$ and $s(d, 0) = 0$ when d is positive.

THEOREM 2.4: $c_\psi(p, d) = \frac{1}{(d-1)!} \sum_{i=1}^d s(d, i) J_{i-1}(p).$

Proof. First observe that

$$\binom{p-1}{d-1} = \sum_{q|p} c_\psi\left(\frac{p}{q}, d\right).$$

Indeed, the left-hand side of this equality is the number of the lattice points of 1-norm p contained in the positive orthant $]0, +\infty[^d$ or, equivalently, the number of compositions of p into d integers. Dividing each of these points by the greatest common divisor of its coordinates results in a set of primitive points whose number is the right-hand side of the equality.

By Möbius' inversion formula,

$$(3) \quad c_\psi(p, d) = \sum_{q|p} \mu(q) \binom{p/q - 1}{d - 1}$$

where μ denotes Möbius' function. By definition of Stirling's numbers of the first kind, the following holds when d is positive.

$$(4) \quad \binom{p/q - 1}{d - 1} = \frac{1}{(d - 1)!} \sum_{i=1}^d s(d, i) \left(\frac{p}{q}\right)^{i-1}.$$

Combining (3) with (4), and permuting the sums yields

$$c_\psi(p, d) = \frac{1}{(d - 1)!} \sum_{i=1}^d s(d, i) \sum_{q|p} \mu(q) \left(\frac{p}{q}\right)^{i-1}.$$

Since Jordan's totient function satisfies

$$\sum_{q|p} J_i(q) = p^i,$$

Möbius' inversion formula provides the desired result. \blacksquare

Theorem 1.1 immediately follows from Proposition 2.3 and Theorem 2.4.

3. Upper bounds on $\delta_z(d, k)$

We first establish the following upper bound, and provide some information on the subsets of \mathbb{P}_\circ^d that achieve it in a special case.

LEMMA 3.1: *Consider a subset \mathcal{X} of \mathbb{P}_\circ^d . If $\kappa(\mathcal{X})$ is at most k , then \mathcal{X} has cardinality at most $\lfloor \lambda(d, k) \rfloor$. If in addition,*

- (i) \mathcal{X} has cardinality exactly $\lfloor \lambda(d, k) \rfloor$,
- (ii) d is a proper divisor of p ,
- (iii) p/d a divisor of $k - \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d)$,

where p is the smallest integer such that $k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$, then

$$B(d, p - 1) \cap \mathbb{P}_\circ^d \subset \mathcal{X} \subset B(d, p) \cap \mathbb{P}_\circ^d.$$

Proof. Assume that $\kappa(\mathcal{X}) \leq k$. We further assume without loss of generality that $|\mathcal{X}|$ is equal to $\delta_z(d, k)$. Let p be the smallest integer such that k is less than $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. It follows that $\kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d) \leq k$ and therefore,

$$|B(d, p - 1) \cap \mathbb{P}_\circ^d| \leq \delta_z(d, k).$$

Since the right-hand side of this inequality is also the cardinality of \mathcal{X} , we can consider a subset \mathcal{X}^* of \mathcal{X} with the same cardinality than $B(d, p-1) \cap \mathbb{P}_\circ^d$. We can also require that the sum of the 1-norms of the points in \mathcal{X}^* is as small as possible. We then consider a bijection $\psi : B(d, p-1) \cap \mathbb{P}_\circ^d \rightarrow \mathcal{X}^*$. We can assume without loss of generality that the restriction of ψ to $B(d, p-1) \cap \mathcal{X}$ is the identity. By this assumption, the 1-norm of an element y of $B(d, p-1) \cap \mathbb{P}_\circ^d$ is at most that of its image by ψ . Indeed, either $\psi(y)$ coincides with y or it is outside of $B(d, p-1)$. In the latter case, the 1-norm of $\psi(y)$ is at least p , while the 1-norm of y is at most $p-1$. According to Proposition 2.1,

$$\kappa(\mathcal{X}) \geq \frac{1}{d} \sum_{x \in \mathcal{X}} \|x\|_1$$

and, as $B(d, p-1) \cap \mathbb{P}_\circ^d$ is invariant under the action of C on \mathbb{R}^d ,

$$\kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) = \frac{1}{d} \sum \|y\|_1,$$

where the sum in the right-hand side of this equality is over the points y contained in $B(d, p-1) \cap \mathbb{P}_\circ^d$. Since ψ cannot make 1-norms decrease,

$$\kappa(\mathcal{X}) \geq \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) + \frac{1}{d} \sum_{\substack{x \in \mathcal{X} \\ x \notin \mathcal{X}^*}} \|x\|_1.$$

In addition, if $B(d, p-1) \cap \mathbb{P}_\circ^d$ and \mathcal{X}^* do not coincide, then this inequality is strict. As all the points in $\mathcal{X} \setminus \mathcal{X}^*$ have 1-norm at least p ,

$$(5) \quad \kappa(\mathcal{X}) \geq \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) + p \frac{|\mathcal{X}| - |B(d, p-1) \cap \mathbb{P}_\circ^d|}{d}.$$

Note that this inequality is strict as soon as a point in $\mathcal{X} \setminus \mathcal{X}^*$ has 1-norm greater than p or $B(d, p-1) \cap \mathbb{P}_\circ^d$ does not coincide with \mathcal{X}^* . As $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \delta_z(d, k)$, we obtain from (5) the desired upper bound on $|\mathcal{X}|$.

Now assume that d is a proper divisor of p and that p/d is a divisor of $k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$. Observe that, in this case, $\lambda(d, k)$ is an integer. Therefore, if \mathcal{X} has cardinality $\lfloor \lambda(d, k) \rfloor$, then (5) must be an equality. In this case, as we discussed above, $B(d, p-1) \cap \mathbb{P}_\circ^d$ must coincide with \mathcal{X}^* . In other words, $B(d, p-1) \cap \mathbb{P}_\circ^d$ is a subset of \mathcal{X} . In addition, all the points in $\mathcal{X} \setminus \mathcal{X}^*$ must have 1-norm at most p . It follows that \mathcal{X} is a subset of $B(d, p) \cap \mathbb{P}_\circ^d$. ■

It is an immediate consequence, of Lemma 3.1 that $\delta_z(d, k) \leq \lfloor \lambda(d, k) \rfloor$ for all d and k . We can refine this bound as follows.

LEMMA 3.2: Consider the smallest integer p such that $k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. If d is a proper divisor of p and either

- (i) $k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$ is equal to p/d , or
- (ii) $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k$ is equal to p/d ,

then $\delta_z(d, k)$ cannot be equal to $\lfloor \lambda(d, k) \rfloor$.

Proof. Consider a subset \mathcal{X} of \mathbb{P}_\circ^d such that $\kappa(\mathcal{X})$ is at most k . Assume that \mathcal{X} has cardinality exactly $\lfloor \lambda(d, k) \rfloor$. Hence, by the definition of $\lambda(d, k)$,

$$(6) \quad |\mathcal{X}| = |B(d, p-1) \cap \mathbb{P}_\circ^d| + \left\lfloor \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor.$$

Further assume that d is a proper divisor of p and let us reach a contradiction in each of the two special cases considered in the statement of the lemma.

We first treat the case when

$$(7) \quad k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) = \frac{p}{d}.$$

In this case, by Lemma 3.1, $B(d, p-1) \cap \mathbb{P}_\circ^d$ is a subset of \mathcal{X} , which in turn is contained in $B(d, p)$. Combining (6) with (7), we obtain that

$$|\mathcal{X}| = |B(d, p-1) \cap \mathbb{P}_\circ^d| + 1.$$

In other words, \mathcal{X} contains exactly one element x of $B(d, p) \cap \mathbb{P}_\circ^d$. According to (7) and to Proposition 2.1, the absolute value of all the coordinates of x must be equal to p/d . Since d is a proper divisor of p , x cannot be primitive. This contradiction shows that $\delta_z(d, k)$ cannot coincide with $\lfloor \lambda(d, k) \rfloor$.

Now, assume that d is a proper divisor of p and that

$$(8) \quad \kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k = \frac{p}{d}.$$

Recall that, according to Proposition 2.3,

$$(9) \quad \kappa(B(d, p) \cap \mathbb{P}_\circ^d) - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) = \frac{p|S(d, p) \cap \mathbb{P}_\circ^d|}{d}.$$

Combining the equalities (6), (8), and (9) yields

$$|\mathcal{X}| = |B(d, p) \cap \mathbb{P}_\circ^d| - 1.$$

Again, it follows from Lemma 3.1 that $B(d, p-1) \cap \mathbb{P}_\circ^d$ is a subset of \mathcal{X} , and \mathcal{X} a subset of $B(d, p) \cap \mathbb{P}_\circ^d$. Hence, \mathcal{X} is obtained by removing a single point of 1-norm p from $B(d, p) \cap \mathbb{P}_\circ^d$. According to (8) and to Proposition 2.1, the absolute value of all the coordinates of x must be equal to p/d and, since d

is a proper divisor of p , x cannot be a primitive point. It follows from this contradiction, that $\delta_z(d, k)$ is not equal to $\lfloor \lambda(d, k) \rfloor$. ■

In the 2-dimensional case, we can further refine our bound as follows.

LEMMA 3.3: *Consider the smallest integer p such that $k < \kappa(B(2, p) \cap \mathbb{P}_\circ^2)$. If p is a multiple of 4 and $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is an odd multiple of $p/2$, then $\delta_z(2, k)$ cannot be equal to $\lfloor \lambda(d, k) \rfloor$.*

Proof. Assume that p is a multiple of 4 and $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ an odd multiple of $p/2$. Consider a subset \mathcal{X} of \mathbb{P}_\circ^d such that $\kappa(\mathcal{X})$ is not greater than k . We proceed as in the proof of Lemma 3.2 by assuming that

$$(10) \quad |\mathcal{X}| = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \left\lfloor \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2} \right\rfloor,$$

and we aim for a contradiction.

According to Lemma 3.1, \mathcal{X} admits $B(2, p-1) \cap \mathbb{P}_\circ^2$ as a subset and is itself a subset of $B(2, p) \cap \mathbb{P}_\circ^2$. Denote by \mathcal{Y} the set of the points of 1-norm p contained in \mathcal{X} . Since $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ an odd multiple of $p/2$, it follows from (10) that the cardinality of \mathcal{Y} is odd. It also follows from (10) that

$$|\mathcal{Y}| = \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2}.$$

Therefore, as $\kappa(\mathcal{X}) \leq k$ and as the points in \mathcal{Y} have 1-norm p ,

$$\kappa(\mathcal{X}) \leq \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{1}{2} \sum_{x \in \mathcal{Y}} \|x\|_1.$$

Observe that, by Proposition 2.1 the opposite inequality holds. Hence, according to the same proposition, \mathcal{X} is invariant under the action of C on \mathbb{R}^2 . Since $\mathcal{X} \setminus \mathcal{Y}$ is also invariant under that action, then so is \mathcal{Y} . Therefore,

$$\sum_{x \in \mathcal{Y}} |x_1| = \frac{p|\mathcal{Y}|}{2}.$$

However, since p is a multiple of 4, the right-hand side of this equality is even. As $|\mathcal{Y}|$ is odd, there must exist a point x in \mathcal{Y} such that x_1 is even. However, since the 1-norm of x is even, the coordinates of x must both be even. It follows that x cannot be primitive, a contradiction. ■

4. An expression for $\delta_z(d, k)$ when $d \geq 3$

In this section, we build a subset of \mathbb{P}_\circ^d that achieves the bound on $\delta_z(d, k)$ provided by Lemmas 3.1 and 3.2 when $d > 2$ and for a number of values of k when $d = 2$. We will distinguish two cases depending on whether d is, or not, a divisor of the smallest integer p such that $k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. Throughout the section, we assume that k and d (and therefore p) are fixed.

Let us first address the case when d is not a proper divisor of p . Note that, in this case, our construction will be done for all $d \geq 2$. We introduce, for the purpose of the construction, d sets that we denote \mathcal{S}_1 to \mathcal{S}_d , made up of points of 1-norm p from \mathbb{P}_\circ^d . Denote by r the remainder of the integer division of p by d and recall that $\lceil p/d \rceil$ is the quotient of this division. As a consequence, the lattice point x such that $x_i = \lceil p/d \rceil$ when $i \leq r$ and $x_i = \lfloor p/d \rfloor$ otherwise has 1-norm p . Moreover, $\lceil p/d \rceil$ and $\lfloor p/d \rfloor$ are relatively prime as they differ by 1, and x is necessarily primitive. For any integer j such that $1 \leq j \leq d$, denote

$$\mathcal{S}_j = \{\tau^{ir}(x) : 1 \leq i \leq j\}.$$

As announced, \mathcal{S}_j is made up of j points of 1-norm p from \mathbb{P}_\circ^d . Moreover,

$$(11) \quad \kappa(\mathcal{S}_j) = \left\lceil \frac{jp}{d} \right\rceil.$$

Using the sets \mathcal{S}_1 to \mathcal{S}_d , we prove the following.

LEMMA 4.1: *If d is not a divisor of p , then there exists a subset \mathcal{X} of \mathbb{P}_\circ^d such that $\kappa(\mathcal{X})$ is at most k and $|\mathcal{X}|$ is equal to $\lfloor \lambda(d, k) \rfloor$.*

Proof. Assume that d is not a divisor of p and consider a point x of 1-norm p in \mathbb{P}_\circ^d . Since C has order d , $C \cdot x$ has cardinality at most d . In particular, the 1-norms of the elements of $C \cdot x$ sum to at most dp . Observe that $C \cdot x$ coincides with \mathcal{S}_d when x is the unique element of \mathcal{S}_1 , and that \mathcal{S}_d has cardinality exactly d . Further observe that the points of 1-norm p in \mathbb{P}_\circ^d are partitioned into the orbits of their elements under the action of C on \mathbb{R}^d . Hence, one can take the union of some of these orbits in order to build a set \mathcal{Y} of points of 1-norm p from \mathbb{P}_\circ^d disjoint from \mathcal{S}_d , invariant under the action of C on \mathbb{R}^d , and that satisfies

$$\frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} - d < \frac{1}{p} \sum_{x \in \mathcal{Y}} \|x\|_1 \leq \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d}.$$

In this case, the integer j defined as

$$(12) \quad j = \left\lfloor \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor - \frac{1}{p} \sum_{x \in \mathcal{Y}} \|x\|_1$$

is non-negative and less than d . Denote

$$\mathcal{X} = (B(d, p-1) \cap \mathbb{P}_\circ^d) \cup \mathcal{Y} \cup \mathcal{S}_j,$$

with the convention that \mathcal{S}_0 is the empty set. By construction, both \mathcal{Y} and the intersection of $B(d, p-1)$ with \mathbb{P}_\circ^d are invariant under the action of C on \mathbb{R}^d . In particular, according to Proposition 2.1,

$$(13) \quad \kappa(\mathcal{X}) = \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) + \frac{1}{d} \sum_{x \in \mathcal{Y}} \|x\|_1 + \kappa(\mathcal{S}_j).$$

However, it follows from (12) that

$$(14) \quad \frac{1}{d} \sum_{x \in \mathcal{Y}} \|x\|_1 \leq k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) - \frac{j p}{d}.$$

In addition, by (11),

$$(15) \quad \kappa(\mathcal{S}_j) < \frac{j p}{d} + 1,$$

As this inequality is strict, we obtain $\kappa(\mathcal{X}) \leq k$ by combining (13), (14), and (15). Now recall that all the points in \mathcal{Y} have 1-norm p and \mathcal{S}_j has cardinality j . As a consequence the cardinality of \mathcal{X} can be decomposed as

$$(16) \quad |\mathcal{X}| = |B(d, p-1) \cap \mathbb{P}_\circ^d| + \frac{1}{p} \sum_{x \in \mathcal{Y}} \|x\|_1 + j.$$

Combining (12) and (16) yields

$$|\mathcal{X}| = |B(d, p-1) \cap \mathbb{P}_\circ^d| + \left\lfloor \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor.$$

The right-hand side of this equality is $\lfloor \lambda(d, k) \rfloor$, as desired. \blacksquare

We now address the case when d is a divisor of p . In this case, the construction of subset of \mathbb{P}_\circ^d of the right cardinality will rely on the following lemma.

LEMMA 4.2: *Assume that d is a divisor of p and that*

$$(17) \quad \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) + \frac{2p}{d} \leq k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d) - \frac{p}{d}.$$

Let \mathcal{Y} be the union of the orbits under the action of C on \mathbb{R}^d of some points of 1-norm p from \mathbb{P}_\circ^d . If $|\mathcal{Y}|$ is at least $d + 3$ and, whenever $2 \leq j \leq |\mathcal{Y}| - 2$, there exists a subset \mathcal{S} of j elements of \mathcal{Y} satisfying

$$(18) \quad \kappa(\mathcal{S}) = \frac{j p}{d},$$

then there exists a subset \mathcal{X} of \mathbb{P}_\circ^d such that $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(d, k) \rfloor$.

Proof. Assume that \mathcal{Y} has cardinality at least $d + 3$. Consider the set of the points of 1-norm p contained in \mathbb{P}_\circ^d . Observe that this set is partitioned into the orbits of its elements under the action of C on \mathbb{R}^d . Moreover, these orbits have cardinality at most d . As in addition, $|\mathcal{Y}| \geq d + 3$, one can take the union of some of these orbits in order to build a set \mathcal{Z} disjoint from \mathcal{Y} that is invariant under the action of C on \mathbb{R}^d and that satisfies the inequalities

$$\frac{k - \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d)}{p/d} - |\mathcal{Y}| + 1 < \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1 \leq \frac{k - \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d)}{p/d} - 2.$$

As an immediate consequence, the integer j defined as

$$(19) \quad j = \left\lfloor \frac{k - \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor - \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1$$

is such that $2 \leq j \leq |\mathcal{Y}| - 2$. Assume that there exists a subset \mathcal{S} of j elements of \mathcal{Y} that satisfies (18) and consider the set

$$\mathcal{X} = [B(d, p - 1) \cap \mathbb{P}_\circ^d] \cup \mathcal{Z} \cup \mathcal{S}.$$

From there on, the argument is the same as in the proof of Lemma 4.1. According to Proposition 2.1,

$$(20) \quad \kappa(\mathcal{X}) = \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d) + \frac{1}{d} \sum_{x \in \mathcal{Z}} \|x\|_1 + \kappa(\mathcal{S}).$$

Moreover, it follows from (19) that

$$(21) \quad \frac{1}{d} \sum_{x \in \mathcal{Z}} \|x\|_1 \leq k - \kappa(B(d, p - 1) \cap \mathbb{P}_\circ^d) - \frac{j p}{d}.$$

Hence, we obtain $\kappa(\mathcal{X}) \leq k$ by combining (18), (20), and (21). Now, since all the elements of \mathcal{Z} have 1-norm p , and since \mathcal{S} has cardinality j ,

$$(22) \quad |\mathcal{X}| = |B(d, p - 1) \cap \mathbb{P}_\circ^d| + \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1 + j.$$

Combining (19) with (22) provides the equality

$$|\mathcal{X}| = |B(d, p-1) \cap \mathbb{P}_\circ^d| + \left\lfloor \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor,$$

whose right-hand side is precisely $\lfloor \lambda(d, k) \rfloor$. \blacksquare

We now build a subset of \mathbb{P}_\circ^d that achieves, when d is greater than 2 and a divisor of p , the upper bound on $\delta_z(d, k)$ provided by Lemmas 3.1 and 3.2.

LEMMA 4.3: *Assume that d is greater than 2 and a divisor of p . If*

- (i) $k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$ is distinct from p/d ,
- (ii) $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k$ is distinct from p/d ,

then there exists a subset \mathcal{X} of \mathbb{P}_\circ^d satisfying $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(d, k) \rfloor$. Otherwise, there also exists a subset \mathcal{X} of \mathbb{P}_\circ^d such that $\kappa(\mathcal{X}) \leq k$, but whose cardinality is $\lfloor \lambda(d, k) \rfloor - 1$ instead of $\lfloor \lambda(d, k) \rfloor$.

Proof. Assume that d is a divisor of p . Consider the point a of \mathbb{Z}^d whose first coordinate is $p/d - 1$, whose second coordinate is $p/d + 1$, and whose all other coordinates are p/d . Further consider the point b obtained from a by exchanging the first two coordinates and the point c obtained from b by exchanging the second and third coordinates. As d is greater than 2, the three points a , b and c each admit two coordinates that are consecutive integers. Therefore, they are primitive. Note, in addition, that they have 1-norm p . Consider the set

$$\mathcal{Y} = (C \cdot a) \cup (C \cdot b) \cup (C \cdot c).$$

We are going to show that \mathcal{Y} satisfies the requirements of Lemma 4.2. Observe that the orbits of a , b , and c under the action of C on \mathbb{R}^d have cardinality d . Further observe that these orbits are pairwise disjoint if d is greater than 3. Therefore, in this case, \mathcal{Y} has cardinality $3d$. If, however, d is equal to 3, then \mathcal{Y} has cardinality only 6 because $C \cdot a$ coincides with $C \cdot b$. Further observe that all the points contained in \mathcal{Y} have non-negative coordinates. Now, consider an integer j such that $2 \leq j \leq |\mathcal{Y}| - 2$. If j is even and at most $|\mathcal{Y}|/2$, denote

$$\mathcal{S}_j = \left\{ \tau^i(a) : 1 \leq i \leq \frac{j}{2} \right\} \cup \left\{ \tau^i(b) : 1 \leq i \leq \frac{j}{2} \right\}.$$

By construction, \mathcal{S}_j is a subset of j elements of \mathcal{Y} . Observe that \mathcal{Y} is a subset of $[0, +\infty[^d$ and, therefore, so is \mathcal{S}_j . Further observe that all the coordinates

of $a + b$ are equal to $2p/d$. Hence, all the coordinates of the sum of the points contained in \mathcal{S}_j are equal to jp/d . As a consequence,

$$(23) \quad \kappa(\mathcal{S}_j) = \frac{jp}{d},$$

Now assume that j is odd and at most $|\mathcal{Y}|/2$. We will distinguish two cases depending on whether d is equal to 3 or greater than 3. If d is equal to 3, then j must be equal to 3, as this is the only odd number that is both greater than 2 and at most $|\mathcal{Y}|/2$. In this case, we denote

$$\mathcal{S}_j = \{a, \tau(a), \tau^2(a)\},$$

and if d is greater than 3, we denote

$$\mathcal{S}_j = \left\{ \tau^i(a) : 1 \leq i \leq \frac{j+1}{2} \right\} \cup \left\{ \tau^i(b) : 1 \leq i \leq \frac{j-3}{2} \right\} \cup \left\{ \tau^{(j-1)/2}(c) \right\}.$$

Again, \mathcal{S}_j is a subset of j elements of \mathcal{Y} . Moreover, all the coordinates of the sum of its elements are equal to jp/d . Hence \mathcal{S}_j satisfies (23).

In the case when j is greater than $|\mathcal{Y}|/2$, denote

$$\mathcal{S}_j = \mathcal{Y} \setminus \mathcal{S}_{|\mathcal{Y}|-j}.$$

By construction, all the coordinates of the sum of the points contained in \mathcal{Y} are equal to $|\mathcal{Y}|p/d$ and all the coordinates of the sum of the points contained in $\mathcal{S}_{|\mathcal{Y}|-j}$ to $(|\mathcal{Y}| - j)p/d$. Hence, \mathcal{S}_j satisfies (23) in this case as well. As a consequence, when (17) holds, it follows from Lemma 4.2 that there exists a subset of \mathbb{P}_\circ^d of the desired cardinality, whose image by κ is at most k .

In the remainder of the proof, we assume that (17) does not hold, and we review several cases depending on the values of p/d and k . In each of these cases, we exhibit a subset of \mathbb{P}_\circ^d with the desired properties. Recall that

$$\lambda(d, k) = |B(d, p-1) \cap \mathbb{P}_\circ^d| + \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d}.$$

Observe that, when the difference $k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$ is less than p/d or, when that difference is exactly p/d with $p > d$, then $B(d, p-1) \cap \mathcal{P}_\circ^d$ has the desired properties. Moreover, if p is equal to d and

$$\frac{p}{d} \leq k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) < \frac{2p}{d},$$

then the union of $B(d, p-1) \cap \mathbb{P}_\circ^d$ with the singleton that contains the point of \mathbb{R}^d whose all coordinates are equal to 1 has the desired cardinality, and its

image by κ is at most k . Similarly, if p is greater than d and

$$\frac{p}{d} < k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) < \frac{2p}{d},$$

then the set $(B(d, p-1) \cap \mathbb{P}_\circ^d) \cup \{a\}$, where a is the point defined at the beginning of the proof is a subset of \mathbb{P}_\circ^d with the desired properties.

Now, if p is equal to d and $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k$ is at most p/d , then the set obtained from $B(d, p) \cap \mathbb{P}_\circ^d$ by removing the point whose all coordinates are equal to 1 has the desired cardinality and its image by κ is at most k . Similarly, if $p > d$ and $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k$ is less than p/d , then removing from $B(d, p) \cap \mathbb{P}_\circ^d$ the point a results in a subset of \mathbb{P}_\circ^d of the right cardinality and image by κ . Finally, assume that p is greater than d and that $\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - k$ is equal to p/d . In that case, p/d is a divisor of $k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$. Hence,

$$\left\lfloor \frac{k - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor - 1 = \left\lfloor \frac{k - 1 - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor.$$

Note in particular that $k - 1 - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)$ cannot be a multiple of p/d . Therefore the set that we have already built, of cardinality

$$|B(d, p-1) \cap \mathbb{P}_\circ^d| + \left\lfloor \frac{k - 1 - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)}{p/d} \right\rfloor$$

whose image by κ is at most $k - 1$ has the desired properties. \blacksquare

Assume that d is greater than 2 and consider the set

$$\mathbb{E} = \bigcup \left\{ \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) + \frac{p}{d}, \kappa(B(d, p) \cap \mathbb{P}_\circ^d) - \frac{p}{d} \right\},$$

where the union is over the positive integers p that admit d as a proper divisor. Note in particular that \mathbb{E} depends on the dimension. With this notation Theorem 1.2 is a consequence, for all dimensions above 2, of Lemmas 3.2, 4.1, and 4.3, except for the part on the density of \mathbb{E} within \mathbb{N} .

The following result completes the proof of Theorem 1.2 when $d > 2$.

LEMMA 4.4: *If $d > 2$, then $\lim_{k \rightarrow \infty} \frac{|\mathbb{E} \cap [1, k]|}{k^{1/(d+1)}} = \frac{[4(d+1)! \zeta(d)]^{1/(d+1)}}{d}$.*

Proof. Consider the smallest integer p such that $k < \kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ and observe that the cardinality of $\mathbb{E} \cap [1, k]$ is at most twice the number of multiples

of d less than or equal to p and at least that number minus 4. Therefore,

$$\frac{2p/d - 4}{[\kappa(B(d, p) \cap \mathbb{P}_\circ^d)]^{1/(d+1)}} \leq \frac{|\mathbb{E} \cap [1, k]|}{k^{1/(d+1)}} \leq \frac{2p/d}{[\kappa(B(d, p-1) \cap \mathbb{P}_\circ^d)]^{1/(d+1)}}.$$

However, according to Theorem 4.2 from [9],

$$\lim_{p \rightarrow \infty} \frac{[\kappa(B(d, p) \cap \mathbb{P}_\circ^d)]^{1/(d+1)}}{p} = \left(\frac{2^{d-1}}{(d+1)! \zeta(d)} \right)^{1/(d+1)},$$

and the desired result follows. \blacksquare

Note that the asymptotic estimate of the density of \mathbb{E} within \mathbb{N} provided by Lemma 4.4 is exact. This estimate is two orders lower than the upper bound in the statement of Theorem 1.2. Indeed, we shall see in the next section that \mathbb{E} is more dense in 2-dimensions. However, if the statement of Theorem 1.2 is restricted to dimensions above 2, the upper bound on the density of \mathbb{E} can be replaced by the exact estimate from Lemma 4.4.

5. An expression for $\delta_z(2, k)$

This section is devoted to proving the 2-dimensional case of Theorem 1.2. We will assume throughout the section that d is equal to 2, that k is fixed, and that p denotes the smallest integer such that k is less than $\kappa(B(2, p) \cap \mathbb{P}_\circ^2)$. Observe that, when p is odd, the value of $\delta_z(2, k)$ is provided by Lemmas 3.1 and 4.1. Therefore, we only have to treat the case when p is even. Moreover, note that Lemmas 3.1, 3.2, and 3.3 provide the desired upper bound on $\delta_z(2, k)$ for all k . Hence, we only need to build subsets of \mathbb{P}_\circ^2 that achieve that bound for even p . We first consider the case when p is a multiple of 4.

LEMMA 5.1: *Assume that p is a multiple of 4. If $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is not a multiple of $p/2$ by an odd integer, then there exists a subset \mathcal{X} of \mathbb{P}_\circ^2 satisfying $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(2, k) \rfloor$. Otherwise, there also exists such a subset of \mathbb{P}_\circ^2 , but whose cardinality is $\lfloor \lambda(2, k) \rfloor - 1$ instead of $\lfloor \lambda(2, k) \rfloor$.*

Proof. Consider the point a such that $a_1 = p/2 - 1$ and $a_2 = p/2 + 1$. Note that, since $p/2$ is even, a is primitive. Moreover, a has 1-norm p .

Observe that the set of the points of 1-norm p from \mathbb{P}_\circ^2 is partitioned by the orbits of its elements under the action of C on \mathbb{R}^2 . Moreover, since p is greater than 2 the orbit of any of these elements under the action of C on \mathbb{R}^2 has

cardinality exactly 2. Therefore, one can take the union of some of these orbits in order to build a set \mathcal{Z} of points of 1-norm p from \mathbb{P}_\circ^2 that is invariant under the action of C on \mathbb{R}^2 , that is disjoint from $C \cdot a$ and that satisfies

$$(24) \quad \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2} - 2 < \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1 \leq \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2}.$$

Consider the difference

$$(25) \quad g = \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2} - \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1.$$

It follows from (24) that $0 \leq g < 2$. If $g \leq 1$, consider the set

$$\mathcal{X} = (B(2, p-1) \cap \mathbb{P}_\circ^2) \cup \mathcal{Z}.$$

By construction, \mathcal{X} is invariant under the action of C on \mathbb{R}^2 . In addition, as the elements of \mathcal{Z} all have 1-norm p , it follows from Proposition 2.1 that

$$(26) \quad |\mathcal{X}| = \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{1}{2} \sum_{x \in \mathcal{Z}} \|x\|_1.$$

However, as $g \geq 0$, it follows from (25) that

$$\frac{1}{2} \sum_{x \in \mathcal{Z}} \|x\|_1 \leq k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2).$$

Combining this with (26) shows that $\kappa(\mathcal{X}) \leq k$. Now recall that

$$\lambda(2, k) = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2}.$$

Since all the elements of \mathcal{Z} all have 1-norm p ,

$$(27) \quad |\mathcal{X}| = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1.$$

As g is non-negative, combining (25) with (27) shows that $|\mathcal{X}| = \lfloor \lambda(d, k) \rfloor$. Moreover, when g is equal to 1, we obtain that \mathcal{X} has cardinality $\lfloor \lambda(d, k) \rfloor - 1$. As g is equal to 1 if and only if $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is an odd multiple of $p/2$, the lemma is proven in this case.

Now assume that g is greater than 1 and denote

$$\mathcal{X} = (B(2, p-1) \cap \mathbb{P}_\circ^2) \cup \mathcal{Z} \cup \{a\},$$

According to Proposition 2.1,

$$(28) \quad \kappa(\mathcal{X}) = \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{1}{2} \sum_{x \in \mathcal{Z}} \|x\|_1 + \frac{p}{2} + 1.$$

As g is greater than 1, (25) yields

$$\frac{1}{2} \sum_{x \in \mathcal{X}} \|x\|_1 < k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) - \frac{p}{2}.$$

Since this inequality is strict, combining it with (28) shows that $\kappa(\mathcal{Z}) \leq k$. Finally, as all the elements of \mathcal{Z} have 1-norm p ,

$$|\mathcal{X}| = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \frac{1}{p} \sum_{x \in \mathcal{Z}} \|x\|_1 + 1.$$

As g greater than 1, combining this with (25) shows that $|\mathcal{X}| = \lfloor \lambda(d, k) \rfloor$. ■

Let us now treat the case when p is even and $p/2$ is odd. The sub-cases when

$$k \in \left\{ \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{p}{2} + 1, \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) - \frac{p}{2} + 1 \right\}$$

turn out to be particularly interesting. In these two sub-cases, the subsets \mathcal{X} of \mathbb{P}_\circ^2 such that $|\mathcal{X}| = \delta_z(2, k)$ and $\kappa(\mathcal{X}) \leq k$ cannot be between $B(2, p-1) \cap \mathbb{P}_\circ^2$ and $B(2, p) \cap \mathbb{P}_\circ^2$ in terms of inclusion. Let us begin with the case when k is equal to $\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + p/2 + 1$.

PROPOSITION 5.2: *If p is even, $p/2$ is odd, and $p > 2$, then there exists a subset \mathcal{X} of \mathbb{P}_\circ^2 of cardinality $|B(2, p-1) \cap \mathbb{P}_\circ^2| + 1$ such that*

$$\kappa(\mathcal{X}) \leq \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{p}{2} + 1.$$

In addition, for any such subset \mathcal{X} of \mathbb{P}_\circ^2 , either

- (i) *some point in $B(2, p-1) \cap \mathbb{P}_\circ^2$ is not contained in \mathcal{X} , or*
- (ii) *some point in \mathcal{X} is not contained in $B(2, p) \cap \mathbb{P}_\circ^2$.*

Proof. Let a be the point in \mathbb{Z}_\circ^2 such that $a_1 = p/2$ and $a_2 = p/2 + 1$. Note that a belongs to \mathbb{P}_\circ^2 and consider the set

$$\mathcal{X} = (B(2, p-1) \cap \mathbb{P}_\circ^2) \cup \{a\}.$$

Note that $|\mathcal{X}| = |B(2, p-1) \cap \mathbb{P}_\circ^2| + 1$. Recall that $B(2, p-1) \cap \mathbb{P}_\circ^2$ is invariant under the action of C on \mathbb{R}^2 . As in addition, $\max\{|a_1|, |a_2|\} = p/2 + 1$,

$$\kappa(\mathcal{X}) \leq \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{p}{2} + 1,$$

as desired. Now observe that, if a subset \mathcal{X} of \mathbb{P}_\circ^2 satisfies that inequality and admits $B(2, p-1) \cap \mathbb{P}_\circ^2$ as a subset then, by Proposition 2.1, the only point z of 1-norm p contained in \mathcal{X} must satisfy

$$(29) \quad \max\{|z_1|, |z_2|\} \leq \frac{p}{2} + 1.$$

If in addition, z has 1-norm p , the two coordinates of z cannot have the same absolute value because z is primitive and p is greater than 2. Hence, according to (29), the absolute value of the coordinates of z must be $p/2 - 1$ and $p/2 + 1$. However, as $p/2$ is odd, these numbers are both even. As a consequence, z cannot be primitive, a contradiction. ■

The argument, for the proof of the following proposition is similar to that in the proof of Proposition 5.2, and we only sketch it.

PROPOSITION 5.3: *If p is even, $p/2$ is odd, and $p > 2$, then there exists a subset \mathcal{X} of \mathbb{P}_\circ^2 of cardinality $|B(2, p) \cap \mathbb{P}_\circ^2| - 1$ such that*

$$\kappa(\mathcal{X}) \leq \kappa(B(2, p) \cap \mathbb{P}_\circ^2) - \frac{p}{2} + 1.$$

In addition, for any such subset \mathcal{X} of \mathbb{P}_\circ^2 , either

- (i) *some point in $B(2, p-1) \cap \mathbb{P}_\circ^2$ is not contained in \mathcal{X} , or*
- (ii) *some point in \mathcal{X} is not contained in $B(2, p) \cap \mathbb{P}_\circ^2$.*

Proof. Consider the set \mathcal{X} obtained by removing from the intersection of $B(2, p)$ and \mathbb{P}_\circ^2 the point whose first coordinate is $p/2 - 1$ and whose second coordinate is $p/2$. This set has cardinality $|B(2, p) \cap \mathbb{P}_\circ^2| - 1$ and satisfies

$$(30) \quad \kappa(\mathcal{X}) \leq \kappa(B(2, p) \cap \mathbb{P}_\circ^2) - \frac{p}{2} + 1,$$

as desired. Moreover, using an argument similar to that of the proof of Proposition 5.2, we show that any subset \mathcal{X} of $B(2, p) \cap \mathbb{P}_\circ^2$ that satisfies (30), has cardinality $|B(2, p) \cap \mathbb{P}_\circ^2| - 1$, and admits $B(2, p-1) \cap \mathbb{P}_\circ^2$ as a subset must miss a point from $B(2, p) \cap \mathbb{P}_\circ^2$ whose absolute value of the coordinates are $p/2 - 1$ and $p/2 + 1$. However, as $p/2$ is odd, this point cannot be primitive. ■

The following lemma is a consequence of the two above propositions.

LEMMA 5.4: *Assume that p is even and that $p/2$ is odd. Further assume that either $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) < p$ or $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k \leq p/2$. If*

- (i) *$k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is distinct from $p/2$,*

(ii) $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k$ is distinct from $p/2$,

then there exists a subset \mathcal{X} of \mathbb{P}_\circ^2 satisfying $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(2, k) \rfloor$. Otherwise, there also exists a subset \mathcal{X} of \mathbb{P}_\circ^2 such that $\kappa(\mathcal{X}) \leq k$, but whose cardinality is $\lfloor \lambda(2, k) \rfloor - 1$ instead of $\lfloor \lambda(2, k) \rfloor$.

Proof. Assume that p is even and $p/2$ is odd and recall that

$$\lambda(2, k) = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2}.$$

Let us first treat the case when

$$k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) < p.$$

Observe that, if k is less than $\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + p/2$ or k is equal to this quantity but p is greater than 2, then we can take $\mathcal{X} = B(2, p-1) \cap \mathbb{P}_\circ^2$.

If $p = 2$ and $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) \geq p/2$, observe that

$$(31) \quad \left\lfloor \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2} \right\rfloor = 1.$$

Let \mathcal{X} be the union of $B(2, p-1) \cap \mathbb{P}_\circ^2$ with the singleton that contains the point whose two coordinates are equal to 1. This set has cardinality $|B(2, p-1) \cap \mathbb{P}_\circ^2| + 1$ and satisfies $\kappa(\mathcal{X}) \leq \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + p/2$, as desired. Therefore, the lemma holds in this case.

If $p > 2$ and $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) > p/2$, then (31) also holds. Therefore, a set \mathcal{X} with the desired properties is provided by Proposition 5.2.

Now assume that

$$\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k \leq \frac{p}{2}.$$

If p is equal to 2, then consider the set \mathcal{X} obtained from $B(2, p) \cap \mathbb{P}_\circ^2$ by removing the point whose two coordinates are equal to 1. This set has cardinality $|B(2, p) \cap \mathbb{P}_\circ^2| - 1$, as desired, and satisfies $\kappa(\mathcal{X}) \leq \kappa(B(2, p) \cap \mathbb{P}_\circ^2) - p/2$. Therefore, the lemma holds in this case.

If $p > 2$ and $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k < p/2$, a set \mathcal{X} with the desired properties is provided by Proposition 5.3, and if $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k = p/2$, then consider any point x of 1-norm p in $B(2, p) \cap \mathbb{P}_\circ^2$. Any set obtained by removing the two elements of $C \cdot x$ from $B(2, p) \cap \mathbb{P}_\circ^2$ will have the desired properties. \blacksquare

We are ready to build the announced subsets of \mathbb{P}_\circ^2 . The construction relies on Lemma 5.4 when k is close to $\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ or to $\kappa(B(2, p) \cap \mathbb{P}_\circ^2)$, and

on Lemma 4.2 otherwise. We also use the property that, if n is an odd integer and m a positive integer, then $n - 2^m$ and $n + 2^m$ are relatively prime.

LEMMA 5.5: *Assume that p is even and that $p/2$ is odd. If*

- (i) $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is distinct from $p/2$,
- (ii) $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k$ is distinct from $p/2$,

then there exists a subset \mathcal{X} of \mathbb{P}_\circ^2 satisfying $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(2, k) \rfloor$. Otherwise, there also exists a subset \mathcal{X} of \mathbb{P}_\circ^2 such that $\kappa(\mathcal{X}) \leq k$, but whose cardinality is $\lfloor \lambda(2, k) \rfloor - 1$ instead of $\lfloor \lambda(2, k) \rfloor$.

Proof. Assume that p is even and that $p/2$ is odd. We will split the proof into three cases. The first case, when $k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ is less than p or $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) - k$ is at most $p/2$, is taken care of by Lemma 5.4.

Now assume that

$$(32) \quad \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + p \leq k < \kappa(B(2, p) \cap \mathbb{P}_\circ^2) - \frac{p}{2},$$

and that p is at least 10. In this case, we are going to use Lemma 4.2. Consider the point a of \mathbb{R}^2 whose first coordinate is $p/2 - 2$ and whose second coordinate is $p/2 + 2$. Further consider the point b obtained from a by negating the second coordinate and the point c whose first coordinate is $p/2 + 4$ and whose second coordinate is $p/2 - 4$. These points all have 1-norm p and, as $p/2$ is odd, they are primitive. Since the orbits of these points under the action of C on \mathbb{R}^2 have cardinality 2, and since these orbits are pairwise disjoint, the set

$$\mathcal{Y} = (C \cdot a) \cup (C \cdot b) \cup (C \cdot c).$$

has cardinality 6. Let us consider an integer j such that $2 \leq j \leq 4$. We will exhibit a subset of j elements of \mathcal{S} that satisfies (18), as required by Lemma 4.2. If j is equal to 2 we take for \mathcal{S} the set $\{a, \tau(a)\}$. If j is equal to 3, we take $\mathcal{S} = \{a, b, c\}$, and if j is equal to 4, we take $\mathcal{S} = \{a, \tau(a), b, \tau(b)\}$. By the choice of a , b , and c , \mathcal{S} satisfies (18). Therefore, according to Lemma 4.2, there exists a subset \mathbb{P}_\circ^2 such that $\kappa(\mathcal{X}) \leq k$ and $|\mathcal{X}| = \lfloor \lambda(2, k) \rfloor$, as desired.

Now assume that (32) still holds, but that $p = 6$. Recall that

$$\lambda(2, k) = |B(2, p-1) \cap \mathbb{P}_\circ^2| + \frac{k - \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)}{p/2}.$$

It follows from Theorem 1.1 that

$$\kappa(B(2, 6) \cap \mathbb{P}_\circ^2) - \kappa(B(2, 5) \cap \mathbb{P}_\circ^2) = 12.$$

Hence, according to (32), $6 \leq k - \kappa(B(2, 5) \cap \mathbb{P}_\circ^2) \leq 8$. In this range,

$$\left\lfloor \frac{k - \kappa(B(2, 5) \cap \mathbb{P}_\circ^2)}{6/2} \right\rfloor = 2.$$

Therefore, the subset \mathcal{X} of \mathbb{P}_\circ^2 made up of the points from $B(2, 5) \cap \mathbb{P}_\circ^2$ together with the two primitive points of 1-norm 6 whose coordinates are 1 and 5 satisfies the desired properties as it has cardinality $|B(2, 5) \cap \mathbb{P}_\circ^2| + 2$ and

$$\kappa(\mathcal{X}) \leq \kappa(B(2, 5) \cap \mathbb{P}_\circ^2) + 6.$$

Finally, note that no other case needs to be treated. In particular, when p is equal to 2, it follows from Theorem 1.1 that $\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) = 1$ and $\kappa(B(2, p) \cap \mathbb{P}_\circ^2) = 3$. Therefore, in this case, (32) is never satisfied. \blacksquare

For any positive integer p , let I_p be the set of the odd multiples of $p/2$ that lie between $\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)$ and $\kappa(B(2, p) \cap \mathbb{P}_\circ^2)$. Denote

$$\mathbb{E}_e = \bigcup_{p=1}^{\infty} I_{4p}.$$

Further consider the set

$$\mathbb{E}_o = \bigcup \left\{ \kappa(B(2, p-1) \cap \mathbb{P}_\circ^2) + \frac{p}{2}, \kappa(B(2, p) \cap \mathbb{P}_\circ^2) - \frac{p}{2} \right\},$$

where the union ranges over the even numbers p greater than 2 such that $p/2$ is odd. Denote $\mathbb{E} = \mathbb{E}_e \cup \mathbb{E}_o$. With this notation, the expression for $\delta_z(2, k)$ provided by Theorem 1.2 is a consequence of Lemmas 3.1, 3.2, 3.3, 4.1, 5.1, and 5.5. We now estimate the density of \mathbb{E} within \mathbb{N} in the 2-dimensional case, which completes the proof of Theorem 1.2.

LEMMA 5.6: *If d is equal to 2, then $\lim_{k \rightarrow \infty} \frac{|\mathbb{E} \cap [1, k]|}{k} = 0$.*

Proof. Observe that there are exactly

$$\frac{\kappa(B(2, i) \cap \mathbb{P}_\circ^2) - \kappa(B(2, i-1) \cap \mathbb{P}_\circ^2)}{i}$$

odd multiples of $i/2$ between $\kappa(B(2, i-1) \cap \mathbb{P}_\circ^2)$ and $\kappa(B(2, i) \cap \mathbb{P}_\circ^2)$. According to Theorem 1.1, this quantity is precisely $J_1(i)$. Hence, when $d = 2$,

$$|\mathbb{E} \cap [1, k]| \leq \sum_{i=1}^p J_1(i),$$

where p is the smallest integer such that $k < \kappa(B(2, p) \cap \mathbb{P}_\circ^2)$. Therefore,

$$(33) \quad \frac{|\mathbb{E} \cap [1, k]|}{k} \leq \frac{1}{\kappa(B(2, p-1) \cap \mathbb{P}_\circ^2)} \sum_{i=1}^p J_1(i).$$

Now recall that $J_1(i)$ is Euler's totient function (see, for instance [13]). In particular, we have the following estimate.

$$\lim_{p \rightarrow \infty} \frac{1}{p^2} \sum_{i=1}^p J_1(i) = \frac{3}{\pi^2}.$$

In addition, according to Theorem 4.2 from [9],

$$\lim_{p \rightarrow \infty} \frac{\kappa(B(2, p) \cap \mathbb{P}_\circ^2)}{p^3} = \frac{1}{3\zeta(2)}.$$

Hence letting k go to infinity in (33) proves the lemma. \blacksquare

6. The geometry of packed primitive point sets

In this section, we gather results on which sets of primitive points solve our packing problem. The first one is Theorem 1.3, announced in the introduction, that we prove using the constructions in the previous two sections.

Proof of Theorem 1.3. First observe that all the subsets \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$ constructed in the proofs of Lemmas 4.1, 4.2, and 4.3 satisfy the double inequality

$$(34) \quad B(d, p-1) \cap \mathbb{P}_\circ^d \subset \mathcal{X} \subset B(d, p) \cap \mathbb{P}_\circ^d,$$

where p is the smallest integer such that k is less than $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. Hence, the theorem holds when $d > 2$, and when $d = 2$ while p is odd.

Now assume that $d = 2$ and that p is even. Observe that the subset \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$ constructed in the proof of Lemma 5.1 also satisfies (34). The same holds for the construction given in the proof of Lemma 5.5 except when $p/2$ is odd, p is greater than 2 and either

$$k = \kappa(B(2, p-1) \cap \mathbb{P}_\circ^d) + \frac{p}{2} + 1,$$

or

$$k = \kappa(B(2, p) \cap \mathbb{P}_\circ^d) - \frac{p}{2} + 1,$$

the cases treated by Propositions 5.2 and 5.3. According to these propositions, a subset \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$ cannot satisfy (34) in these cases, and the theorem follows. ■

Let us turn our attention to the unicity of the subsets of \mathbb{P}_\circ^d that solve our primitive point packing problem. Recall that we need to prove that unicity is not achieved apart for the cases already identified in [9]. It is noteworthy that this will not require any knowledge on the value of $\delta_z(d, k)$. Indeed, the general idea in order to prove that several subsets of \mathbb{P}_\circ^d solve our packing problem, is to consider such a subset, and to replace some of the points it contains without affecting its cardinality or increasing its image by κ .

We will do this by means of the following proposition.

PROPOSITION 6.1: *For any point z in \mathbb{P}_\circ^d , there exist a set \mathcal{K} of d points from \mathbb{P}_\circ^d , all of 1-norm $\|z\|_1$, and a partition of \mathcal{K} into $d/|C \cdot z|$ subsets, each of cardinality $|C \cdot z|$ such that, if \mathcal{L} is any of these subsets, then*

$$\kappa(C \cdot z) = \sum_{x \in \mathcal{L}} |x_i|$$

for every integer i satisfying $1 \leq i \leq d$. In addition, there exists a point of \mathbb{P}_\circ^d whose orbit under the action of C on \mathbb{R}^d admits \mathcal{L} as a subset.

Proof. Consider a point z in \mathbb{P}_\circ^d and note that when $C \cdot z$ has cardinality d then, we can take $\mathcal{K} = C \cdot z$. Assume that $|C \cdot z|$ is less than d . We can require without loss of generality that the first coordinate of z is non-zero by exchanging it for a point from $C \cdot z$ with that property. Pick an integer j such that

$$2 \leq j \leq \frac{d}{|C \cdot z|}.$$

Consider the point y such that $y_i = -z_i$ when i is equal to $(j - 1)|C \cdot z|$ and $y_i = z_i$ otherwise. Denote

$$\mathcal{L}_j = \{\tau^i(y) : 0 \leq i < |C \cdot z|\}.$$

By construction,

$$\kappa(C \cdot z) = \sum_{x \in \mathcal{L}_j} |x_i|.$$

Further denote $\mathcal{L}_1 = C \cdot z$ and call \mathcal{K} the union of \mathcal{L}_1 to $\mathcal{L}_{d/|C \cdot z|}$. By construction, \mathcal{K} , and its partition into the sets \mathcal{L}_i have the desired properties. ■

We now prove Theorem 1.4. Recall that, according to this theorem, there is a unique subset of \mathbb{P}_\circ^d that solves our primitive point packing problem if and only if k coincides with $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ for some integer p .

Proof of Theorem 1.4. When k coincides with $\kappa(B_1(d, p) \cap \mathbb{P}_\circ^d)$ for some integer p , the result is provided by Corollary 3.2 from [9]. Assume that

$$k \neq \kappa(B_1(d, p) \cap \mathbb{P}_\circ^d)$$

for all p and consider a subsets \mathcal{X} of \mathbb{P}_\circ^d such that $|\mathcal{X}| = \delta_z(d, k)$ and $\kappa(\mathcal{X}) \leq k$. Let us prove there is another such subset of \mathbb{P}_\circ^d .

If \mathcal{X} is not invariant under the action of C on \mathbb{R}^d , then there exists a integer i such that $\tau^i(\mathcal{X}) \neq \mathcal{X}$. However, $\tau^i(\mathcal{X})$ and \mathcal{X} have the same cardinality and the same image by κ . Therefore, the lemma holds in this case, and we assume from now on that \mathcal{X} is invariant under the action of C on \mathbb{R}^d .

We review two cases. Assume first that \mathcal{X} is equal to $B(d, p) \cap \mathbb{P}_\circ^d$ for some integer p . By assumption, k must then be greater than $\kappa(\mathcal{X})$. Consider the point a in \mathcal{X} whose first coordinate is equal to $p - 1$, whose second coordinate is equal to 1, and whose all other coordinates, if any, are equal to 0. Observe that adding 1 to any of the coordinates of a other than the second one results in a primitive point b of 1-norm $p + 1$. In addition, since \mathcal{X} is invariant under the action of C on \mathbb{R}^d , the equality

$$\sum_{x \in \mathcal{X}} |x_i| = \kappa(\mathcal{X})$$

holds for every integer i such that $1 \leq i \leq d$. Hence,

$$\mathcal{Y} = (\mathcal{X} \setminus \{a\}) \cup \{b\}$$

satisfies $\kappa(\mathcal{Y}) = \kappa(\mathcal{X}) + 1$. Now recall that k is greater than $\kappa(\mathcal{X})$. Therefore, \mathcal{Y} is a subset of \mathbb{P}_\circ^d distinct from \mathcal{X} such that $|\mathcal{Y}| = \delta_z(d, k)$ and $\kappa(\mathcal{Y}) \leq k$, as desired. Now assume that \mathcal{X} is distinct from $B(d, p) \cap \mathbb{P}_\circ^d$ for every integer p . In this case, there exists a point y in \mathcal{X} and a point z in $\mathbb{P}_\circ^d \setminus \mathcal{X}$ such that $\|z\|_1 \leq \|y\|_1$. As \mathcal{X} is invariant under the action of C on \mathbb{R}^d , it must admit $C \cdot y$ as a subset and be disjoint from $C \cdot z$. Hence, if the orbits of y and z under the action of C on \mathbb{R}^d have the same cardinality, the set

$$\mathcal{Y} = (\mathcal{X} \setminus C \cdot y) \cup C \cdot z$$

is a subset of \mathbb{P}_\circ^d distinct from \mathcal{X} such that $|\mathcal{Y}| = \delta_z(d, k)$ and $\kappa(\mathcal{Y}) \leq k$, as desired. Assume that $C \cdot y$ and $C \cdot z$ do not have the same cardinality.

According to Proposition 6.1, there exists a subset \mathcal{K}_y of d points from \mathbb{P}_\circ^d of the same 1-norm than y , and a partition \mathcal{P}_y of \mathcal{K}_y into $d/|C \cdot y|$ subsets, all of cardinality $C \cdot y$, such that any of these subsets \mathcal{L} satisfies $\kappa(C \cdot y) = \kappa(\mathcal{L})$. In addition, \mathcal{L} is contained in the orbit of some point from \mathbb{P}_\circ^d under the action of C on \mathbb{R}^d . Therefore, either \mathcal{L} is a subset of \mathcal{X} , or it is disjoint from it. If any of the sets \mathcal{L} in \mathcal{P}_y is disjoint from \mathcal{X} , then the set

$$\mathcal{Y} = (\mathcal{X} \setminus C \cdot y) \cup \mathcal{L}.$$

is distinct from \mathcal{X} . Yet, it satisfies $|\mathcal{Y}| = \delta_z(d, k)$ and, as $\kappa(C \cdot y)$ coincides with $\kappa(\mathcal{L})$, then so do $\kappa(\mathcal{Y})$ and $\kappa(\mathcal{X})$. Therefore, in this case the lemma holds.

Now assume that \mathcal{K}_y is a subset of \mathcal{X} . We proceed in the same way with $C \cdot z$. More precisely, by Proposition 6.1, there exists a set \mathcal{K}_z made up of d points from \mathbb{P}_\circ^d of the same 1-norm than z and a partition of it into $d/|C \cdot z|$ subsets of cardinality $C \cdot z$ such that, if \mathcal{L} is one of these subsets, then for every i ,

$$(35) \quad \kappa(C \cdot z) = \sum_{x \in \mathcal{L}} |x_i|.$$

Again, \mathcal{L} is either a subset of \mathcal{X} or disjoint from it. If any of the sets, say \mathcal{L} , in \mathcal{K}_z is a subset of \mathcal{X} , then the set

$$\mathcal{Y} = (\mathcal{X} \setminus \mathcal{L}) \cup C \cdot z.$$

is distinct from \mathcal{X} . Moreover by construction, it satisfies $|\mathcal{Y}| = \delta_z(d, k)$. Further note that, since, (35) holds for every i , $\kappa(\mathcal{Y})$ must be equal to $\kappa(\mathcal{X})$. As a consequence, the lemma also holds in this case.

Assume that \mathcal{K}_z is disjoint from \mathcal{X} . In this case the set

$$\mathcal{Y} = (\mathcal{X} \setminus \mathcal{K}_y) \cup \mathcal{K}_z$$

has cardinality $\delta_z(d, k)$. Moreover, by construction, for every i ,

$$\frac{d\kappa(C \cdot y)}{|C \cdot y|} = \sum_{x \in \mathcal{K}_y} |x_i|.$$

However, according to Proposition 2.1, the left-hand side of this equality is precisely the 1-norm of y . Similarly, for every i ,

$$\|z\|_1 = \sum_{x \in \mathcal{K}_z} |x_i|.$$

Now recall that $\|z\|_1 \leq \|y\|_1$. As a consequence, $\kappa(\mathcal{Y}) \leq \kappa(\mathcal{X})$. ■

7. Asymptotic estimates

In this section we provide sharp asymptotic estimates for some of the quantities we studied in the previous sections. We begin with the asymptotic behavior of $c_\psi(p, d)$ when d is fixed and p grows large. Recall that this quantity is the number of primitive points of 1-norm p contained in the positive orthant $]0, +\infty[^d$ or, in combinatorial terms, the number of compositions of p into d relatively prime integers. Let us first observe that there is no asymptotics in the 2-dimensional case. Indeed, according to Theorem 2.4, when $p \geq 2$,

$$c_\psi(p, 2) = J_1(p).$$

Recall that $J_1(p)$ is Euler's totient function. In particular, we have the following, where γ stands for Euler's constant (see for instance [13]).

PROPOSITION 7.1: *The following equalities hold.*

- (i) $\liminf_{p \rightarrow \infty} \frac{c_\psi(p, 2)}{p} \log \log p = e^{-\gamma},$
- (ii) $\limsup_{p \rightarrow \infty} \frac{c_\psi(p, 2)}{p} = 1.$

Let us now consider the case of the dimensions above 2. It is an immediate consequence of Theorem 1.1 that

$$(36) \quad |S(d, p) \cap \mathbb{P}_\circ^d| = \frac{1}{2} \sum_{j=1}^d 2^j \binom{d}{j} c_\psi(p, j).$$

Moreover, it follows from Theorem 2.2 from [9] that

$$(37) \quad \lim_{p \rightarrow \infty} \frac{|B(d, p) \cap \mathbb{P}_\circ^d|}{p^d} = \frac{2^{d-1}}{d! \zeta(d)},$$

where ζ stands for Riemann's zeta function. These two equalities provide the asymptotic behavior of $c_\psi(p, d)$ when d is fixed and p grows large.

THEOREM 7.2: *When $d \geq 3$, $\lim_{p \rightarrow \infty} \frac{c_\psi(p, d)}{p^{d-1}} = \frac{1}{(d-1)! \zeta(d)}$.*

Proof. Assume that $d \geq 3$. According to (36),

$$(38) \quad \frac{c_\psi(p, d)}{p^{d-1}} = \frac{|S(d, p) \cap \mathbb{P}_\circ^d|}{2^{d-1} p^{d-1}} - \sum_{j=1}^{d-1} \frac{1}{2^{d-j}} \binom{d}{j} \frac{c_\psi(p, j)}{p^{d-1}}.$$

Moreover, it follows from (37) that

$$(39) \quad \lim_{p \rightarrow \infty} \frac{|S(d, p) \cap \mathbb{P}_\circ^d|}{p^{d-1}} = \frac{2^{d-1}}{(d-1)! \zeta(d)}.$$

Using (38) and (39), the theorem can be established by induction on d . Indeed, recall that $c_\psi(p, 1) = 0$ when $p \geq 2$. In addition, by Proposition 7.1,

$$\lim_{p \rightarrow \infty} \frac{c_\psi(p, 2)}{p^2} = 0.$$

Hence, combining (38) and (39) proves the theorem when d is equal to 3. Now assume that d is greater than 3 and that the theorem holds for all dimensions less than d and greater than 2. In this case, by induction,

$$\lim_{p \rightarrow \infty} \frac{c_\psi(p, j)}{p^{d-1}} = 0$$

when $3 \leq j < d$, and according to Proposition 7.1,

$$\lim_{p \rightarrow \infty} \frac{c_\psi(p, 2)}{p^{d-1}} = 0.$$

As $c_\psi(p, 1) = 0$ when p is greater than 1, we just need to combine (38) and (39) in order to get the desired asymptotic estimate. \blacksquare

We also give the asymptotic behavior of $|B(d, p) \cap \mathbb{P}_\circ^d|$ and $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$ when p is fixed and d grows large. More precisely, we prove the following.

LEMMA 7.3: $\lim_{d \rightarrow \infty} \frac{|B(d, p) \cap \mathbb{P}_\circ^d|}{d^p} = \frac{2^{p-1}}{p!}$ and $\lim_{d \rightarrow \infty} \frac{\kappa(B(d, p) \cap \mathbb{P}_\circ^d)}{d^{p-1}} = \frac{2^{p-1}}{(p-1)!}$.

Proof. Observe that, when $d > p$, $c_\psi(p, d) = 0$. In this case, (36) yields

$$(40) \quad \frac{|B(d, p) \cap \mathbb{P}_\circ^d|}{d^p} = \frac{|B(d, p-1) \cap \mathbb{P}_\circ^d|}{d^p} + \frac{1}{2} \sum_{j=1}^p \frac{2^j}{d^p} \binom{d}{j} c_\psi(p, j).$$

The announced asymptotic behavior for $|B(d, p) \cap \mathbb{P}_\circ^d|$ can be obtained from this equality by induction on p . Indeed, as observed in [8] (see theorem 3.2 therein), $|B(d, 2) \cap \mathbb{P}_\circ^d| = d^2$, which provides the base case for the induction.

Now assume that p is greater than 2 and note that the limit

$$\lim_{d \rightarrow \infty} \frac{1}{d^p} \binom{d}{j}$$

is equal to 0 when $j < p$ and to $1/p!$ when $j = p$. Moreover, by induction,

$$\lim_{d \rightarrow \infty} \frac{|B(d, p-1) \cap \mathbb{P}_\circ^d|}{d^p} = 0.$$

As in addition, $c_\psi(p, p) = 1$, letting d grow large in (40) results in the desired asymptotic estimate for $|B(d, p) \cap \mathbb{P}_\circ^d|$ when d is fixed and p goes to infinity. Now recall that, as a consequence of Proposition 2.3,

$$\kappa(B(d, p) \cap \mathbb{P}_\circ^d) - \kappa(B(d, p-1) \cap \mathbb{P}_\circ^d) = \frac{p|S(d, p) \cap \mathbb{P}_\circ^d|}{d},$$

By another induction on p , this equality, together with our asymptotic estimate for $|B(d, p) \cap \mathbb{P}_\circ^d|$ provides the announced estimate for $\kappa(B(d, p) \cap \mathbb{P}_\circ^d)$. Note that the base case is given, again, by Theorem 3.2 from [8]. ■

The following estimate is an immediate consequence of Lemma 7.3.

THEOREM 7.4: $\lim_{d \rightarrow \infty} \frac{1}{d} \frac{|B(d, p) \cap \mathbb{P}_\circ^d|}{\kappa(B(d, p) \cap \mathbb{P}_\circ^d)} = \frac{1}{p}.$

References

- [1] Karim Adiprasito, June Huh and Eric Katz, *Hodge theory for combinatorial geometries*, Annals of Mathematics **188** (2018), 381–452.
- [2] George E. Andrews, *A lower bound for the volume of strictly convex bodies with many boundary lattice points*, Transactions of the American Mathematical Society **106** (1963), 270–279.
- [3] Manuel Aprile, Alfonso Cevallos and Yuri Faenza, *On 2-level polytopes arising in combinatorial settings*, SIAM Journal on Discrete Mathematics **32** (2018), no. 3, 1857–1886.
- [4] Matthias Beck and Sinai Robins, *Computing the continuous discretely*, Undergraduate Texts in Mathematics, Springer, 2015.
- [5] Tristram Bogart, Christian Haase, Milena Hering, Benjamin Lorenz, Benjamin Nill, Andreas Paffenholz, Günter Rote, Francisco Santos, and Hal Schenck, *Finitely many smooth d -polytopes with n lattice points*, Israel Journal of Mathematics **207** (2015), no. 1, 301–329.
- [6] Michel Brion and Michèle Vergne, *Lattice points in simple polytopes*, Journal of the American Mathematical Society **10** (1997), no. 2, 371–392.
- [7] Alberto Del Pia and Carla Michini, *On the diameter of lattice polytopes*, Discrete & Computational Geometry **55** (2016), 681–687.
- [8] Antoine Deza, George Manoussakis and Shmuel Onn, *Primitive zonotopes*, Discrete & Computational Geometry **60** (2018), 27–39.
- [9] Antoine Deza, Lionel Pournin and Noriyoshi Sukegawa, *The diameter of lattice zonotopes*, Proceedings of the American Mathematical Society **148** (2020), no. 8, 3507–3516.
- [10] Alicia Dickenstein, Sandra Di Rocco and Ragni Piene, *Classifying smooth lattice polytopes via toric fibrations*, Advances in Mathematics **222** (2009), 240–254.

- [11] Eugène Ehrhart, *Sur un problème de géométrie diophantienne linéaire. I. polyèdres et réseaux*, Journal für die reine und angewandte Mathematik **226** (1967), 1–29.
- [12] Eugène Ehrhart, *Sur un problème de géométrie diophantienne linéaire. II. systèmes diophantiens*, Journal für die reine und angewandte Mathematik **227** (1967), 25–49.
- [13] Godfrey H. Hardy and Edward M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1938.
- [14] June Huh, *Milnor numbers of projective hypersurfaces and the chromatic polynomial of graphs*, Journal of the American Mathematical Society **25** (2012), no. 3, 907–927.
- [15] Gil Kalai and Daniel Kleitman, *A quasi-polynomial bound for the diameter of graphs of polyhedra*, Bulletin of the American Mathematical Society **26** (1992), 315–316.
- [16] Victor Klee and David W. Walkup, *The d -step conjecture for polyhedra of dimension $d < 6$* , Acta Mathematica **117** (1967), 53–78.
- [17] Evangelos Kranakis and Michel Pocchiola, *Counting problems relating to a theorem of Dirichlet*, Computational Geometry **4** (1994), 309–325.
- [18] Percy A. MacMahon, *Memoir on the theory of the compositions of numbers*, Philosophical Transactions of the Royal Society of London A **184** (1893), 835–901.
- [19] Dennis Naddef, *The Hirsch conjecture is true for $(0, 1)$ -polytopes*, Mathematical Programming **45** (1989), 109–110.
- [20] Benjamin Nill and Günter M. Ziegler, *Projecting lattice polytopes without interior lattice points*, Mathematics of Operations Research **36** (2011), 462–467.
- [21] James E. Nymann, *On the probability that k positive integers are relatively prime*, Journal of Number Theory **4** (1972), 469–473.
- [22] Tadao Oda, *Convex bodies and algebraic geometry: An introduction to the theory of toric varieties*, Springer, 1988.
- [23] James E. Pommersheim, *Toric varieties, lattice points and Dedekind sums*, Mathematische Annalen **295** (1993), 1–24.
- [24] Francisco Santos, *A counterexample to the Hirsch conjecture*, Annals of Mathematics **176** (2012), 383–412.
- [25] Richard Stanley, *The number of faces of a simplicial convex polytope*, Advances in Mathematics **35** (1980), 236–238.
- [26] Noriyoshi Sukegawa, *An asymptotically improved upper bound on the diameter of polyhedra*, Discrete & Computational Geometry **62** (2019), 690–699.