Lattice points on the boundary of the integer hull *

Imre Bárány and Károly Böröczky, Jr.

May 31, 2002

Abstract

Consider $P_r = \mathrm{conv}(rB^d \cap \mathbb{Z}^d)$ where B^d is the unit ball of R^d. It is known that the number of vertices of P_r is of order $r^{d(d-1)/(d+1)}$. We prove that, besides the vertices, the boundary of P_r contains many lattice points: their number is of order $r^{d(d-1)/(d+1)}$, as well.

1 Introduction

Define $P_r = \mathrm{conv}(rB^d \cap \mathbb{Z}^d)$ where B^d is the unit ball of R^d. P_r is clearly a lattice polytope. It follows from (more general) results of Andrews, Konyagin and Sevastyanov, Schmidt (*cf.* [1], [8]), and [13]) that the number k-dimensional faces, $f_k(P_r)$ of P_r satisfies

$$f_k(P_r) \ll r^{\frac{d(d-1)}{d+1}}.$$

Here, and in what follows, for functions f, g the notation $f \ll g$ means that $f \leq Cg$ for some constant C depending only on the dimension. In addition, $f \approx g$ means that $f \ll g \ll f$.

It is proved in Bárány and Larman [4] that the above inequality is sharp, apart from the implied constant:

$$f_k(P_r) \gg r^{\frac{d(d-1)}{d+1}}.$$

*The first named author is supported by OTKA T 032452 and T 029255, the second named author is supported by OTKA T 031984 and T 030012.

Further, it is shown in [4] (see Remark 1 on page 173) that the number of lattice points on the boundary of P_r is $\ll r^{d(d-1)/(d+1)}$. The aim of this paper is to show that there are many lattice points, namely $\gg r^{d(d-1)/(d+1)}$, on the boundary of P_r that are not vertices of P_r. More formally, we have

Theorem 1 $|\partial P_r \cap \mathbb{Z}^d| - f_0(P_r) \gg r^{d(d-1)/(d+1)}$.

Actually, we will prove the following slightly stronger statement. Call a facet of P_r *rich* if it contains a lattice point in its relative interior.

Theorem 2 *The number of rich facets of P_r is $\gg r^{d(d-1)/(d+1)}$.*

For $d \geq 3$ we first prove Theorem 2, which readily implies Theorem 1. The order is reversed for $d = 2$: we give a direct proof of Theorem 1. In addition, we show that Theorem 1 yields Theorem 2 in the planar case.

We now describe the ideas of the proofs. Let F be a facet of P_r, with outer normal $v = v_F$. We always choose v to be a primitive vector; that is, $v \in \mathbb{Z}^d$ such that the greatest common divisor of its components is 1. We will denote by $\mathbb{P}^d$ the set of primitive vectors. So F lies in some lattice hyperplane H, orthogonal to v, and the cap cut off from B^d by H is lattice point free. In case $d \geq 3$, the proof of Theorem 2 is based on the fact that for a positive fraction of the facets, the intersection $H \cap B^d$ is "relatively large"; which forces F to contain at least one lattice point in its relative interior. Here we need an argument from discrepancy theory saying, roughly, that there are $\gg m^{d-2}$ lattice points on the boundary of $\sqrt{m}B^d$ (when m is an integer and $d \geq 5$). This argument cannot be used when $d = 2$, in which case we have a different and more geometric proof of Theorem 1.

The paper is organized as follows. Section 2 contains the proof of Theorem 2 for $d \geq 3$ together with the statement of three auxiliary lemmas. They are provided in Sections 3, 4 and 5. The rest of the paper is devoted to the proof of Theorems 1 and 2 in the planar case.

We will often make use of the following well-known fact.

Fact *Let $f : [1, \infty) \to R^+$ be a increasing (decreasing) function, and let k be a fixed integer. If $p_1, ..., p_k$ are distinct primitive vectors then $\sum_1^k f(|p_i|)$ is minimal (maximal) if and only if the set $\{p_1, ..., p_k\}$ consists of the k shortest primitive vectors.*

When evaluating certain sums we will apply the following well–known formula, see for instance [9]. Given $t > -d$, if h tends to infinity then

$$\sum_{\substack{v\in\mathbb{Z}^d \text{ primitive} \\ \|v\|\le h}} \|v\|^t \sim \frac{1}{\zeta(d)} \int_{\|x\|\le h} \|x\|^t \, dx = \frac{d\kappa_d}{(t+d)\,\zeta(d)}\, h^{t+d} \tag{1}$$

where κ_d is the volume of the unit d–ball and $\zeta(d) = \sum_{i=1}^{\infty} \frac{1}{i^d}$ (and $\sim$ stands for asymptotic equality).

2 Proof of Theorem 2 when $d \geq 3$

We start by stating the auxiliary lemmas. Define first

$$R_d(m) = |\{u \in \mathbb{P}^d \ : \|u\| = \sqrt{m}\}|.$$

Lemma 3 *For every $d > 2$ there exist $c > 0$ and $\varepsilon_0 > 0$ depending on d such that for any large T, at least ε_0 percent of all m with $\frac{1}{2}T < \sqrt{m} < T$ satisfy*

$$R_d(m) > cT^{d-2}.$$

Given $v \in \mathbb{P}^d$, we denote by $L(v)$ the lattice $v^\perp \cap \mathbb{Z}^d$, and by $\mu(v)$ the covering radius of $L(v)$. The latter is, by definition (see [11]), the smallest $t > 0$ such that $tB + L(v)$ covers aff $L(v)$ where B is the unit ball in aff $L(v)$. Note that the determinant of $L(v)$ is $\|v\|$.

Lemma 4 *For every $d > 2$ and every $\varepsilon > 0$ there exists $c(\varepsilon) > 0$ such that for large enough T, the number of $v \in \mathbb{P}^d$ with $\|v\| < T^{d-1}$ and $\mu(v) > c(\varepsilon)T$ is at most $\varepsilon T^{d(d-1)}$.*

We will use $\{x\}$ to denote the rational part of $x \in \mathbb{R}$: $\{x\} = x - \lfloor x \rfloor$.

Lemma 5 *For every $\varepsilon > 0$ there exists a $\delta > 0$ such that for any $\alpha > 0$ and for large S, among the $m \in \mathbf{Z}$ with $\frac{1}{2}S < \sqrt{m} < S$ all but ε percent satisfy*

$$\left\{\alpha S^{\frac{d+1}{d-1}} \sqrt{m}\right\} > \delta.$$

Proof of Theorem 2 for $d \geq 3$. The number of $v \in \mathbb{P}^d$ satisfying $\frac{1}{2} T^{d-1} \leq \|v\| \leq T^{d-1}$ is $\gg T^{d(d-1)}$ according to (1). By Lemma 4, very few of them have $\mu(v)$ much larger than T. Combining this with Lemma 5 with $S = T^{d-1}$ yields the existence of positive c_0, c_1 and δ depending on d such that the following holds. For any $\alpha > 0$ and for large T, there exist $c_0 T^{d(d-1)}$ primitive vectors $v \in \mathbb{P}^d$ such that

(i) $\frac{1}{2} T^{d-1} < \|v\| < T^{d-1}$;

(ii) $\mu(v) < c_1 T$;

(iii) $\left\{\alpha T^{d+1} \|v\|\right\} > \delta$.

Proposition 6 *Let B be a $(d-1)$-dimensional unit ball (centered at the origin) of* $\operatorname{aff} L(v)$*. If $\rho > 3\mu(v)$, and $x \in \operatorname{aff} L(v)$, then the polytope $K = \operatorname{conv}\{(x + \rho B) \cap L(v)\}$ contains a lattice point in its relative interior.*

Proof. By the definition of μ, $y + \mu(v) B$ contains a lattice point for every $y \in \operatorname{aff} L(v)$. In particular, there is a $z \in L(v) \cap (x + \mu(v) B)$. So it suffices to show that $x + \mu(v) B \subset K$ since then z is in the relative interior of K. Assume a point from the boundary of $x + \mu(v) B$ is not contained in K. Then a $(d-2)$-dimesional hyperplane separates it from K. This hyperplane splits $x + \rho B$ into two parts. By the choice of ρ, both parts contain a translated copy of $\mu(v) B$. Consequently, both parts contain a lattice point, even the one disjoint from K, a contradiction. So all boundary points of $x + \mu(v) B$ are in K, implying that $x + \mu(v) B \subset K$. $\square$

Choose $\beta > 0$ so that

$$\sqrt{\frac{\delta}{\beta^{d-1}}} > 3 c_1 \beta.$$

Set $T = \beta r^{\frac{1}{d+1}}$ and $\alpha = 1/\beta^{d+1}$, and consider the vectors $v_1, \ldots, v_N \in \mathbb{P}^d$, $N \geq c_0 T^{d(d-1)}$, satisfying (i), (ii) and (iii). Let H_i be the lattice hyperplane farthest in direction of v_i intersecting rB. The equation for H_i is $x v_i = \lfloor r \|v_i\| \rfloor$, and the cap cut off from rB^d by H_i has depth $h_i = \{r \|v_i\|\} / \|v_i\|$. Then the radius of $H_i \cap rB$ is

$$\begin{aligned} \sqrt{(2r - h_i) h_i} \quad &> \quad \sqrt{r h_i} > \sqrt{r\delta / \|v_i\|} > \sqrt{r\delta / T^{d-1}} \\ &= \quad \sqrt{(T/\beta)^{d+1} \delta / T^{d-1}} = \sqrt{\delta / \beta^{d+1}}\, T > 3 c_1 T > 3\mu(v_i). \end{aligned}$$

In view of Proposition 6, $F_i = \operatorname{conv}(H_i \cap rB \cap \mathbb{Z}^d)$ is a facet of P_r that contains a lattice point in its interior. $\square$

3 Proof of Lemma 3

First we prove that

$$\sum_{\frac{1}{2}T<\sqrt{m}<T} R_d(m)^2 \ll T^{2d-2}.$$

It is clearly sufficient to verify that the number of pairs $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$, $x, y \in \mathbb{Z}^d$ such that

$$x_1^2 + \ldots + x_d^2 = y_1^2 + \ldots + y_d^2$$

and $|x_i|, |y_i| < T$ is $\ll T^{2d-2}$. Setting $a_i = x_i - y_i$ and $b_i = x_i + y_i$, the problem is translated into the question about the number of solutions of $ab = 0$ under the condition $\|a\|, \|b\| < 2\sqrt{d}T$ where $a = (a_1, \ldots, a_d)$ and $b = (b_1, \ldots, b_d)$. Set $R = 2\sqrt{d}T$. Routine estimations show that the number of solution is

$$= \sum_{\|a\|\leq R\ ,a\in\mathbb{Z}^d} \sum_{\|b\|\leq R\ ,b\in\mathbb{Z}^d\ ,ab=0} 1 = \sum_{\|v\|\leq R\ ,v\in\mathbb{P}^d} \lfloor \frac{R}{\|v\|} \rfloor \sum_{\|b\|\leq R\ ,b\in\mathbb{Z}^d\ ,vb=0} 1$$

$$\ll \sum_{\|v\|\leq R\ ,v\in\mathbb{P}^d} \frac{R}{\|v\|}\frac{R^{d-1}}{\|v\|} \ll R^d \sum_{\|a\|\leq R\ ,a\in\mathbb{Z}^d} \|v\|^{-2} \ll R^{2d-2} \ll T^{2d-2},$$

proving what was promised.

To finish the proof, we use a well–known version of the inequality between the arithmetic and quadratic means, which says the following: Assume $a_1, \ldots, a_n$ are non-negative numbers whose average is A and whose quadratic mean is Q. Then $A^2 \leq Q$, moreover, if $cA^2 > Q$ for some $c > 1$, then at least $n/(4c)$ of the a_i satisfy $a_i > A/2$.

Now the number of integers m with $\frac{1}{2}T < \sqrt{m} < T$ is approximately $\frac{3}{4}T^2$. Thus the quadratic mean of the $R_d(m)$ is $\ll T^{2d-4}$. The number of primitive vectors v with $T/2 < \|v\| < T$ is $\gg T^d$, so the average of the $R_d(m)$ is $\gg T^{d-2}$. So the inequality just cited implies the lemma. $\Box$

Remark: For $d \geq 4$, Lemma 3 is actually the consequence of the regular behavior of the number of lattice points on the spheres $\sqrt{m}S^{d-1}$ (see [6]). If $d \geq 5$ then $R_d(m) \approx \sqrt{m}^{d-2}$ holds for any m. Assume that $d = 4$. If m is odd then number $r_4(m)$ of $u \in \mathbf{Z}^4$ with $\|u\| = \sqrt{m}$ satisfies $r_4(m) = 8\sum_{k|m} k$. We deduce that if m is odd then $R_4(m) > 4m$.

If $d = 3$ then $R_3(m)$ can be less than $c\sqrt{m}$ for any $c > 0$ even if m is chosen from some arithmetic sequence, so we need arguments as above.

4 Proof of Lemma 4

Given a $(d-1)$-dimensional lattice $\mathbb{L}$, its successive minima are denoted by $\lambda_i(\mathbb{L})$ for $i = 1, \ldots, d-1$. Minkowski's second theorem says (see P.M. Gruber and C.G. Lekkerkerker [7], p. 124, Theorem 6, and also for the definition of the $\lambda_i(\mathbb{L})$) that

$$\lambda_1(\mathbb{L}) \ldots \lambda_{d-1}(\mathbb{L}) \leq 2^{d-1} \det \mathbb{L}.$$

It is easy to see that $\mu(\mathbb{L}) \leq \lambda_1(\mathbb{L}) + \ldots + \lambda_{d-1}(\mathbb{L}) \leq (d-1)\lambda_{d-1}(\mathbb{L})$. Since trivially $\lambda_1(\mathbb{L}) \leq \ldots \leq \lambda_{d-1}(\mathbb{L})$, Minkowski's second theorem implies that

$$\lambda_1(\mathbb{L})^{d-2} \mu(\mathbb{L}) \ll \det \mathbb{L}. \tag{2}$$

We are going to estimate the number of $v \in \mathbb{P}^d$ such that $\|v\| \leq T^{d-1}$ and $\mu(v) = \mu(L(v)) \geq \omega T$ where ω will be specified later. (Recall that $L(v) = v^\perp \cap \mathbb{Z}^d$.) Now (2) gives for $\mathbb{L} = L(v)$ that $\lambda_1(L(v)) < c\omega^{\frac{-1}{d-2}} T$ where c depends only on d. This means that for such a v there is a $u \in L(v)$ with $\|u\| < c\omega^{\frac{-1}{d-2}} T$.

It follows by (2) with $\mathbb{L} = L(u)$ that $\mu(L(u)) \ll T$ (since clearly $\lambda_1(L(u)) \geq 1$). Thus the number of $v \in L(u)$ satisfying $\|v\| \leq T^{d-1}$ is

$$\ll \frac{T^{(d-1)^2}}{\det(L(u))} = \frac{T^{(d-1)^2}}{\|u\|}.$$

This, in turn, shows by (1) that the total number of $v \in \mathbb{P}^d$ such that $\|v\| \leq T^{d-1}$ and $\mu(v) \geq \omega T$ is

$$\ll \sum_{\substack{u \in \mathbb{P}^d \\ \|u\| < c\omega^{\frac{-1}{d-2}} T}} \frac{T^{(d-1)^2}}{\|u\|} \ll \frac{T^{d(d-1)}}{\omega^{\frac{d-1}{d-2}}}.$$

So this is going to be less than εT if ω is chosen large enough. □

5 Proof of Lemma 5

Proof: Set $M = \left[\frac{1}{4} S^2\right]$ and let N be the largest integer such that $M + N$ is smaller than S^2. Then $\lim_{S \to \infty} N/M = 3$. Define $\tilde{\alpha}$ by

$$\tilde{\alpha} N^{\frac{d+1}{2(d-1)}} = \alpha S^{\frac{d+1}{d-1}}$$

where $\tilde{\alpha}/\alpha$ is bounded from 0 and ∞.

As natural in this context, we use the notion of discrepancy. The discrepancy of the sequence $x_1, \ldots, x_N$ with $x_i \in (0,1]$ is, by definition,

$$D_N = \sup_{0<t<1} \left\{ \frac{\#(\{x_1, \ldots, x_N\} \cap [0,t])}{N} - t \right\}.$$

By a theorem of Erdős and Turán (see [12], Chap. 2 (2.42)), the discrepancy of the sequence $x_n = \{y_n\}$ $(n = 1, \ldots, N)$, satisfies

$$D_N \leq C \cdot \left(\frac{1}{\ln N} + \frac{1}{N} \sum_{h=1}^{[\ln N]} \left| \sum_{n=1}^{N} e^{2\pi i h y_n} \right| \right)$$

where C is an absolute constant. For $1 \leq h \leq \ln N$ and $1 \leq t \leq N$, define

$$f(t) = \tilde{\alpha} h N^{\frac{d+1}{2(d-1)}} \sqrt{M+t}.$$

Setting $y_n = f(n) = \tilde{\alpha}\sqrt{N}^{\frac{d+1}{2(d-1)}}\sqrt{M+n}$ we see that $\{x_n \ : n = 1, \ldots, N\}$ is the same as the set of numbers $\{\alpha S^{\frac{d-1}{d+1}}\sqrt{m}\}$ with $m \in \mathbb{Z}$ and $S/2 < \sqrt{m} < S$.

We can apply now Theorem 2.7 from Chap. 1 of [12], stating that

$$\left| \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i f(n)} \right| \ll \frac{f'(1)}{N} \frac{1}{\sqrt{f''(N)}} \ll \sqrt{\tilde{\alpha}} \ln N \frac{1}{N^{\frac{1}{2}(1-\frac{1}{d-1})}}.$$

Consequently, D_N tends to 0. $\square$

6 Rich edges

In this section $d = 2$ and so $P_r = \text{conv}(\mathbb{Z}^2 \cap rB^2)$. We write N_r to denote $f_0(P_r) = f_1(P_r)$, and hence Theorem 1 says that

$$|\partial P_r \cap \mathbb{Z}^2| - N_r \gg r^{2/3}. \tag{3}$$

Now we start the long process of proving Theorem 1, or, what is the same, (3). Assume, on the contrary, that there is a sequence $r_n \to \infty$ such that $|\partial P_{r_n} \cap \mathbb{Z}^2| - N_{r_n} = o(r_n^{2/3})$. To have simpler writing we will say that along the sequence $r = r_n$

$$|\partial P_r \cap \mathbb{Z}^2| - N_r = o(r^{2/3}). \tag{4}$$

As $N_r \approx r^{2/3}$ (see [2]), (4) means that all but a very small fraction of $\partial P_r \cap \mathbb{Z}^2$ are vertices of P_r.

Set now $A(r) = \text{Area}(rB^2 \setminus P_r)$. Using Pick's theorem and the error term in the circle problem [6] we get

$$\begin{aligned}\text{Area } P_r &= r^2\pi - A(r) = |P_r \cap \mathbb{Z}^2| - \frac{1}{2}|\partial P_r \cap \mathbb{Z}^2| - 1 \\ &= r^2\pi + o(r^{2/3}) - \frac{1}{2}|\partial P_r \cap \mathbb{Z}^2|.\end{aligned}$$

Thus (4) says that, along the sequence $r = r_n$,

$$N_r = 2A(r) + o(r^{2/3}). \tag{5}$$

Jarník's theorem [10] gives $N_r \le \sqrt[3]{2\pi}(1 + o(1))r^{2/3} \le 5.536r^{2/3}$. P_r is an inscribed (in rB^2) polygon on N_r vertices so it cannot approximate rB^2 too well: according to the well-known estimate (see [5] for instance)

$$A(r) \ge \frac{2\pi^3}{3}(1 + o(1))\frac{r^2}{N_r} \ge 0.675r^{2/3}.$$

These inequalities do not contradict (5). We will show that, under condition (4) and along the sequence r_n

$$N_r \le 5.1803r^{2/3}, \text{ and} \tag{6}$$

$$A(r) \ge 2.6744r^{2/3}. \tag{7}$$

This suffices to contradict (5). The improvement comes from considering short edges of P_r.

At this point we have to introduce some notation. Write $\mathbb{P} = \mathbb{P}^2$ for the set of primitive vectors from $\mathbb{Z}^2$ and let $p \in \mathbb{P}$. The line with equation $px = \|p\|r$ is tangent to rB^2. Define $\alpha = \alpha(p)$ as the fractional part of $\|p\|r$, that is $\alpha(p) = \{\|p\|r\}$. Let $L_k(p)$ denote the lattice line with equation $px = \|p\|r - \alpha - k + 1$ $(k = 1, 2, ...)$. Clearly, $\max\{px : x \in P_r\}$ is reached on one of these lattice lines and is reached on a segment $[a, b]$ $(a, b \in \mathbb{Z}^2)$ where $b - a = \lambda(p)p^{\perp}$ with $\lambda(p) \in \{0, 1, 2, ...\}$. Here $p^{\perp}$ is the rotated (by 90°, counterclockwise) copy of p. Of course, $a = b$ is possible and then $\lambda(p) = 0$. We will write $C_k(p)$ for the chord $L_k(p) \cap rB^2$. Its length is

$$|C_k(p)| \;=\; 2\sqrt{\left(2r - \frac{k + \alpha - 1}{\|p\|}\right)\frac{k + \alpha - 1}{\|p\|}} \tag{8}$$

$$
\begin{aligned}
&= 2\sqrt{\frac{2r(k+\alpha-1)}{\|p\|}} \cdot \sqrt{\left(1-\frac{k+\alpha-1}{2r\|p\|}\right)} \\
&= 2\sqrt{\frac{2r(k+\alpha-1)}{\|p\|}}(1+o(1))
\end{aligned}
$$

as $r \to \infty$ and k is bounded. (k will be 1 or 2 in most cases).

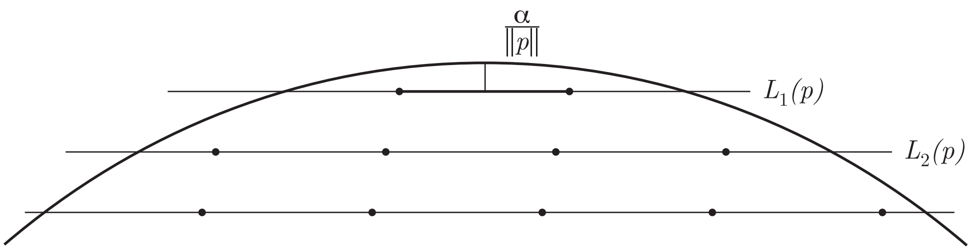

Figure 1

For $t > -2$, formula (1) states that if $h \to \infty$ then

$$\sum_{\substack{p\in\mathbb{P} \\ \|p\|\le h}} \|p\|^t = \frac{12}{\pi(t+2)}(1+o(1))h^{t+2}. \tag{9}$$

With the notation just introduced $\sum_{p\in\mathbb{P}} \lambda(p) = |\partial P_r \cap \mathbb{Z}^2|$, and $\sum_{p\in\mathbb{P}\,,\lambda(p)\ge 1} 1 = N_r$. Thus (4) is equivalent to saying that, along the sequence r_n

$$\sum_{p\in\mathbb{P}} \lambda(p) - \sum_{\substack{p\in\mathbb{P} \\ \lambda(p)\ge 1}} 1 = o(r^{2/3}). \tag{10}$$

Define $E_r = \{p \in \mathbb{P} : \lambda(p) \ge 2\}$: this is the set of directions of rich edges. Clearly, by (10),

$$|E_r| \le \sum_{p\in E_r} (\lambda(p)-1) = \sum_{p\in\mathbb{P}} \lambda(p) - \sum_{\substack{p\in\mathbb{P} \\ \lambda(p)\ge 1}} 1 = o(r^{2/3}), \tag{11}$$

Set $\rho = \sqrt[3]{r/10}$, $B_\rho = \rho B^2$, and

$$S_r = \mathbb{P} \cap B_\rho \setminus E_r.$$

This is the set of "short" minus "rich" directions. It follows from (9) and (11) that, along the sequence r_n,

$$|S_r| = \frac{6}{\pi}\left(\frac{r}{10}\right)^{2/3}(1+o(1)).$$

7 Digression: proof of Theorem 2

We show now, with a short digression, how (3) implies Theorem 2 in case $d = 2$. So we want to prove that $|E_r| \gg r^{2/3}$. Assume the contrary: $|E_r| = \varepsilon r^{2/3}$ for some $\varepsilon(r)$ tending to zero (along a sequence r_n). Let $[a, b] \subset C_k(p)$ be the edge corresponding to $p \in E_r$. Then $k \leq 2$ as otherwise $|C_{k-1}(p)| \geq \|p\|$ and then $C_{k-1}(p)$ would contain a lattice point and $[a, b]$ cannot be an edge of P_r. So

$$\lambda(p)\|p\| \leq |C_k(p)| \leq 2\sqrt{2r\frac{2}{\|p\|}} = 4\sqrt{\frac{r}{\|p\|}} \tag{12}$$

and $\lambda(p) \leq 4\sqrt{r}\|p\|^{-3/2}$.

Define h by $|\mathbb{P} \cap hB^2| = |E_r| = \varepsilon r^{2/3}$, so $h = \sqrt{\varepsilon\pi/6}r^{1/3}(1 + o(1))$ by (9). We can now use the Fact:

$$\begin{aligned}\sum_{p\in E_r}(\lambda(p) - 1) &\leq \sum_{p\in E_r}(4\sqrt{r}\|p\|^{-3/2} - 1) \leq 4\sqrt{r}\sum_{\substack{p\in\mathbb{P}\\ \|p\|\leq h}}\|p\|^{-3/2} - |E_r| \\ &\leq 4\sqrt{r}\frac{24}{\pi}(1 + o(1))h^{1/2} - \varepsilon r^{2/3} \ll \varepsilon^{1/4}r^{2/3}.\end{aligned}$$

This indeed implies (4), or (10) via (11). □

We remark that for $p \in E_r$ (12) gives the estimate

$$\lambda(p) \leq 4\sqrt{r}\|p\|^{-3/2}. \tag{13}$$

8 Auxiliary lemmas

We need a few simple geometric facts.

Lemma 7 *Along the sequence r_n*

$$\sum_{p\in E_r}\lambda(p)\|p\| = o(r).$$

Proof. Using (12) and the Fact with $|E_r| = \varepsilon r^{2/3}$ (from (11)) we get

$$\sum_{p\in E_r} \lambda(p)||p|| \le 4\sqrt{r} \sum_{p\in E_r} ||p||^{-1/2} \le \text{const } \varepsilon^{3/4} r. \ \square$$

Lemma 8 *For all $p \in S_r$, $\alpha(p) \le 1/8$.*

Proof. If the chord $C_1(p)$ is longer than $3||p||$, then it contains at least 3 integers and $p \notin S_r$. Consequently, for $p \in S_r$, $3||p|| > |C_1(p)| = 2\sqrt{\left(2r - \frac{\alpha}{||p||}\right)\frac{\alpha}{||p||}}$ implying

$$\alpha < \frac{9||p||^3}{8r\left(1 - \frac{\alpha}{4r||p||}\right)} \le \frac{9}{8} \cdot \frac{||p||^3}{r} \cdot \frac{1}{1-\frac{1}{4r}} < \frac{9}{8} \cdot \frac{1}{10} \frac{1}{1-\frac{1}{4r}} < \frac{1}{8}. \ \square$$

Lemma 9 *For all $p \in S_r$, $C_1(p)$ contains an integer.*

Proof. Let $t||p|| = |C_2(p)| = 2\sqrt{\left(2r - \frac{\alpha+1}{||p||}\right)\frac{\alpha+1}{||p||}}$. Then

$$t \ge \sqrt{\frac{8r(\alpha+1)}{||p||^3}\left(1 - \frac{\alpha+1}{4r||p||}\right)} \ge \sqrt{8 \cdot 10\left(1 - \frac{2}{4r}\right)} > 8.$$

So if $C_1(p) \cap \mathbb{Z}^2 = \emptyset$, then $C_2(p)$ contains an edge of P_r with $\lambda(p) \ge 6$ and $p \notin S_r$. $\square$

Lemma 10 *If $p, q \in S_r$ and $p \ne q$, then $C_2(p)$ and $C_2(q)$ are disjoint.*

Proof. Write 2φ (resp. 2ψ) for the angle at which the chord $C_2(p)$ ($C_2(q)$) is seen from the origin. Evidently

$$\sin\varphi = \frac{1}{2r}|C_2(p)| < \sqrt{\frac{2(\alpha+1)}{r||p||}} < \frac{3}{2\sqrt{r||p||}},$$

since $\alpha \le 1/8$. Similarly for ψ. The area of the parallelogram 0, p, q, $p+q$ is at least one, so $1 \le ||p|| \cdot ||q|| \cdot \sin\gamma$ where γ is the angle between p and q. We want to show that $\varphi + \psi < \gamma$. This would follow from $\sin\varphi + \sin\psi < \sin\gamma$. Now

$$\sin\varphi + \sin\psi < \frac{3}{2\sqrt{r||p||}} + \frac{3}{2\sqrt{r|q|}} < \frac{1}{||p|| \cdot ||q||} \le \sin\gamma$$

where the inequality in the middle is equivalent to

$$\frac{3}{2}\left(\sqrt{p^2\|q\|}+\sqrt{q^2\|p\|}\right)<\sqrt{r}.$$

This follows from $\|p\|, \|q\| \le \rho = \sqrt[3]{r/10}$. $\square$

Lemma 11 *For all $p \in S_r$, $C_2(p) \cap \partial P_r \subset \mathbb{Z}^2$.*

Proof. By Lemma 10 the edge (or vertex) $[a,b]$ corresponding to $p \in S_r$ is contained in $C_1(p)$. Let c be the integer on ∂P_r immediately after b in anticlockwise order. Then $c \in L_k(p)$ for some $k > 1$. We will show $k = 2$. There are two cases.

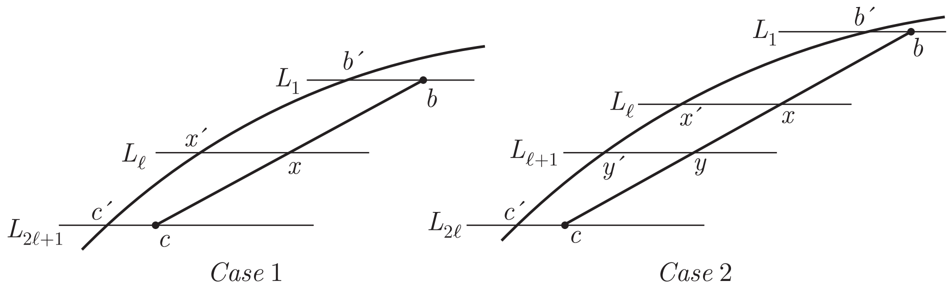

Figure 2

Case 1. k is odd, $k = 2\ell+1$ ($\ell \ge 1$). Set $x = \frac{1}{2}(b+c)$ and let b', x', c' denote the last points on the chords $C_i(p)$ ($i = 1,\ \ell+1,\ 2\ell+1$). As $x \pm \frac{1}{2}p \in \mathbb{Z}^2$, $|x'-x| < \frac{1}{2}\|p\|$ must hold. Then, a fortiori,

$$\frac{1}{2}\|p\| > |x'-x| \ge \left|x' - \frac{1}{2}(b'+c')\right| = \frac{1}{2}\left[|C_{\ell+1}(p)| - \frac{1}{2}(|C_1(p)| + |C_{2\ell+1}(p)|)\right].$$

It is easy to see geometrically that the last expression is minimal on the interval $\alpha \in [0, 1/8]$ at $\alpha = 1/8$, and when $\alpha = 1/8$, it is minimal for $\ell \ge 1$ if $\ell = 1$. Now with $\alpha = 1/8$ and $\ell = 1$

$$\begin{aligned}
\frac{1}{2}\|p\| &> \sqrt{\left(2r - \frac{9}{8\|p\|}\right)\frac{9}{8\|p\|}} - \\
&\quad -\frac{1}{2}\left(\sqrt{\left(2r-\frac{1}{8\|p\|}\right)\frac{1}{8\|p\|}} + \sqrt{\left(2r-\frac{17}{8\|p\|}\right)\frac{17}{8\|p\|}}\right) \\
&\ge \frac{1}{2}\sqrt{\frac{r}{\|p\|}}\left[\sqrt{9} - \frac{1}{2}(\sqrt{1}+\sqrt{17})\right](1+o(1)) \ge \frac{1}{2}\sqrt{\frac{r}{\|p\|}}0.438.
\end{aligned}$$

But this contradicts $\sqrt{\|p\|^3/r} \leq 1/\sqrt{10} < 0.3163$.

Case 2. k is even, $k = 2\ell$ and $\ell \geq 2$. Write x (resp. y) for the intersection of the segment $[b, c]$ with $C_\ell(p)$, $C_{\ell+1}(p)$. The same way as above and with analogous notation $|x' - x| + |y' - y| < \|p\|$ as otherwise either $[x', x]$ or $[y', y]$ would contain an integer. Thus

$$\|p\| > |x' - x| + |y' - y| \geq |C_{\ell+1}(p)| + |C_\ell(p)| - |C_1(p)| - C_{2\ell}(p)|.$$

The right hand side is the smallest when $\alpha = 1/8$, again, and then when $\ell = 2$. A contradiction follows after a short computation. $\square$

According to Lemmas 10 and 12, $C_2(p) \cap \partial P_r = \{c, d\} \subset \mathbb{Z}^2$ for every $p \in S_r$. Assume c, b, a, d come in this order on ∂P_r. Define

$$T(p) = \{[d, a], [a, b], [b, c]\} \text{ and } T_r = \bigcup_{p \in S_r} T(p).$$

By Lemma 10, $T(p)$ and $T(q)$ are disjoint for distinct $p, q \in S_r$. The boundary of P_r consists of three parts: the first contains the segments in T_r, the second the edges corresponding to $p \in E_r$, and the third is the rest. This last group consists of edges $[a_i, b_i]$ corresponding to $q_i \in \mathbb{P}$ $(i = 1, ..., m)$ where $b_i - a_i = q_i^\perp$ and $\|q_i\| \geq \rho$. While the first and second group may have some overlap they are both disjoint from the third.

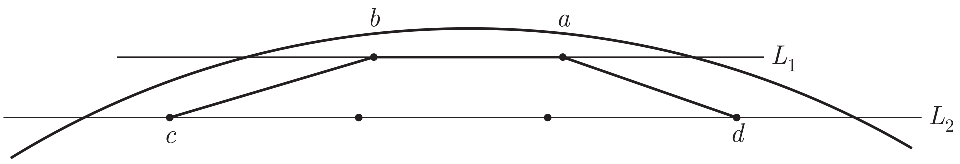

Figure 3

Lemma 12 *For large r (along the sequence r_n)*

$$3.8671r \leq \sum_1^m \|q_i\| \leq 4.2602r.$$

Proof. The perimeter of P_r is $2r\pi(1+o(1))$ and the second group contributes $o(r)$ to it (in view of Lemma 8). So it suffices to estimate $\sum_{x\in T_r}\|x\|$.

It is not hard to see that, for $p\in S_r$,

$$\begin{aligned}|d-a| &+ |a-b|+|c-b| \le \left(1+\frac{1}{r}\right)|C_2(p)| \\ &\le \left(1+\frac{1}{r}\right)\cdot 2\sqrt{\left(2r-\frac{\alpha+1}{\|p\|}\right)\frac{\alpha+1}{\|p\|}} \le 3\sqrt{\frac{r}{\|p\|}}\left(1+\frac{1}{r}\right)\end{aligned}$$

because $\alpha\le 1/8$. Then, by (9),

$$\begin{aligned}\sum_{x\in T_r}\|x\| &\le \sum_{p\in S_r}3\sqrt{\frac{r}{\|p\|}}\left(1+\frac{1}{r}\right)\le 3\sqrt{r}\left(1+\frac{1}{r}\right)\sum_{\substack{p\in\mathbb{P}\\ \|p\|\le\rho}}\|p\|^{-1/2} \\ &\le \frac{24}{\pi\sqrt{10}}\left(1+\frac{1}{r}\right)r\le 2.4158r.\end{aligned}$$

This proves the lower bound.

For the upper bound notice that when $p\in S_r$

$$\begin{aligned}|d-a| &+ |a-b|+|b-c|\ge |C_2(p)\cap P_r|>|C_2(p)|-2\|p\| \\ &\ge 2\sqrt{\frac{2r}{\|p\|}}\left(1-\frac{1}{r}\right)-2\|p\| =: \ell(p,r).\end{aligned}$$

Thus

$$\sum_{x\in T_r}\|x\|\ge\sum_{p\in S_r}\ell(p,r)=\sum_{\substack{p\in\mathbb{P}\\ \|p\|\le\rho}}\ell(p,r)-\sum_{p\in E_r}\ell(p,r)$$

The Fact shows the second sum that it is $o(r)$. So, again by (9),

$$\sum_{x\in T_r}\|x\|\ge\left(\frac{16}{\pi\sqrt{5}}-\frac{4}{5\pi}\right)(1+o(1))r\ge 2.0228r.\ \square$$

9 Proof of (6) and (7)

Next we prove (6). The number of edges (or segments) in the first group is at most

$$3|S_r|\le 3|\mathbb{P}\cap\rho B^2|\le\frac{18}{\pi}\left(\frac{r}{10}\right)^{2/3}(1+o(1))\le 1.2345r^{2/3}.$$

The contribution of the second group is $o(r^{2/3})$. Finally, in the third group,

$$\sum_1^m \|q_i\| \leq 4.2602r$$

and the q_i are distinct primitive vectors with $\|q_i\| \geq \rho$. Under these conditions m is maximal if the q_i are as short as possible. So choose the smallest $\bar\rho$ satisfying $m \leq |\mathbb{P} \cap (\bar\rho B^2 \backslash \rho B^2)|$. Then

$$4.2602r \geq \sum_{\substack{q\in\mathbb{P}\\ \rho\leq|q|\leq\bar\rho}} \|q\| = \frac{4}{\pi}(\bar\rho^3 - \rho^3)(1+o(1)).$$

We get $\bar\rho \leq \sqrt[3]{3.4460r}$ showing that

$$m \leq |\mathbb{P} \cap (\bar\rho B^2 \backslash \rho B^2)| = \frac{6}{\pi}(\bar\rho^2 - \rho^2)(1+o(1)) \leq 3.9458r^{2/3},$$

proving (6).

Finally we prove (7). Given $[u,v] \subset rB^2$, the missed area, $A(u,v)$, beyond this segment is defined as

$$A(u,v) = \text{Area}\{x \in rB^2 : [0,x] \cap [u,v] \neq \emptyset\}.$$

It is easy to see that

$$A(u,v) \geq \frac{1}{12r}|u-v|^3(1+o(1))$$

where u, v are close to the boundary of rB^2 and u, v are almost orthogonal to $u-v$.

For $p \in S_r$ let $[d',c'] = C_2(p)$ with d', d, c, c' in this order. It is easy to see (we omit the proof) that $A(d',a) \leq A(d,a)$ and $A(b,c') \leq A(b,c)$. Then the missed area beyond the chord $C_2(p)$ is

$$\begin{aligned} & A(d,a) + A(a,b) + A(b,c) \geq A(d',a) + A(a,b) + A(b,c') \\ \geq\ & \frac{1}{12r}|C_2(p)|^3(1+o(1)) - \left(\frac{1}{2\|p\|}|C_2(p)| + \frac{1}{2}\right) \\ \geq\ & \frac{1}{3}\sqrt{\frac{2r}{\|p\|^3}}(1+o(1)) - \frac{1}{2} =: L(p,r) \end{aligned}$$

where $o(1)$ is uniform in p. Summing this for all $p \in S_r$ shows that the missed area beyond the segments in T_r is

$$\sum_{p \in S_r} L(p,r) = \sum_{\substack{p \in \mathbb{P} \\ \|p\| \le \rho}} L(p,r) - o(r^{2/3}) \ge 2.2478 r^{2/3}$$

as one can easily check. Finally, the missed area beyond the edges $[a_i, b_i]$ is

$$\ge \frac{1}{12r} \sum_{i=1}^{m} \|q_i\|^3.$$

The sum is minimal, under the condition that the q_i are distinct primitive vectors with $\|q_i\| \ge \rho$ and $\sum \|q_i\| \ge 3.8671r$, if the q_i are as short as possible. The by now routine computation reveals that

$$\frac{1}{12r} \sum_{i=1}^{m} \|q_i\|^3 \ge 0.4267 r^{2/3}. \ \square$$

Remark. This proof gives a very small value for the implied constants in Theorems 4 and 5. Computational experience (and [3] as well) shows

$$N_r \approx 3.45 r^{2/3} \text{ and } |\partial P_r \cap \mathbb{Z}^2| \approx 12 r^{2/3}.$$

References

[1] *G.E. Andrews:* A lower bound for the volumes of strictly convex bodies with many boundary points, Trans. Amer. Math. Soc. **106** (1965) 270–273.

[2] *A. Balog* and *I. Bárány:* On the convex hull of the integer points in a disk, DIMACS Series in Discrete Math. **6** (1991) 39–44.

[3] *A. Balog* and *J-M. Deshouliiers:* On some convex lattice polytopes, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), 591–606, de Gruyter, Berlin, 1999.

[4] *I. Bárány and D. Larman:* The convex hull of the integer points in a large ball, Math. Annalen, **312** (1998) 167–181.

[5] *L. Fejes Tóth:* Lagerungen in der Ebene, auf dem Kugel und im Raum, Springer, Berlin (1953).

[6] *E. Grosswald:* Representation of integers as sums of squares, Springer, 1985.

[7] *P.M. Gruber and C.G. Lekkerkerker:* Geometry of Numbers, North Holland, Amsterdam (1987).

[8] *S. B. Konyagin and K. A. Sevastyanov:* Estimation of the number of vertices of a convex integral polyhedron in terms of its volume, Funk. Anal. Pril., **18** (1984), no. 1, 13–15. (in Russian)

[9] *G.H. Hardy* and *E.M. Wright:* Introduction to the theory of numbers, Oxford, Clarendon (1954).

[10] *V. Jarnik:* Über Gitterpunkte und konvex Kurven, Math. Z. **24** (1925) 500–518.

[11] *R. Kannan* and *L. Lovász:* Covering minima and lattice point free bodies, Annals. Math. **128** (1988) 577–602.

[12] *L. Kuipers and H. Niederreiter:* Uniform Distribution of Sequences, New York, 1974.

[13] *W. Schmidt:* Integral points on surfaces and curves, Monats. Math. **99** (1985) 45–82.

I. Bárány
Alfréd Rényi Inst. of Math.
Budapest PO. Box 127.
1364 HUNGARY
e-mail: barany@renyi.hu
and
Department of Mathematics
University College London
Gower Street, London WC1E 6BT UK

K. Böröczky Jr.
Alfréd Rényi Inst. of Math.
Budapest PO. Box 127.
1364 HUNGARY
e-mail: carlos@renyi.hu