11-1-1990

On the Convex Hull of the Integer Points

Antal Balog

Imre Bárány

COWLES FOUNDATION FOR RESEARCH IN ECONOMICS
AT YALE UNIVERSITY

Box 2125, Yale Station
New Haven, Connecticut 06520

COWLES FOUNDATION DISCUSSION PAPER NO. 962

ON THE CONVEX HULL OF THE INTEGER POINTS

Antal Balog and Imre Bárány

November 1990

ON THE CONVEX HULL OF THE INTEGER POINTS IN A DISC

by

Antal Balog[1] and Imre Bárány[2]

ABSTRACT: Let P_r denote the convex hull of the integer points in the disc of radius r. We prove that the number of vertices of P_r is essentially $r^{\frac{2}{3}}$ as $r \to \infty$.

[1]School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540. Supported by NSF grant DMS–8610730.

[2]Cowles Foundation, Yale University, New Haven, CT 06520 and Courant Institute of Mathematical Sciences, NYU, NY 10012. Supported by the Program in Discrete Mathematics and its Application at Yale and NSF Grant CCR–8901484.

[1,2]Both authors are on leave from the Mathematical Institute of the Hungarian Academy of Sciences, 1364 Budapest, Pf 127, Hungary.

1. INTRODUCTION

Take a disc of radius r in the plane and consider P_r, the convex hull of the integer points inside the disc. How many vertices will P_r have?

Motivation for this question comes from several sources. First, in integer programming, one wants to know the number of solutions, when c varies, to the problem $\max c \cdot x$ subject to $x \in K$ where K is a convex body in R^d. The answer is the number of vertices of $\operatorname{conv}(K \cap \mathbb{Z}^d)$. A relevant result in integer *linear* programming is the following. Let $P \subset R^d$ be a polyhedron given by the inequalities $a_i \cdot x \leqq \alpha_i$ $(i = 1, \ldots, m)$ with $a_i \in \mathbb{Z}^d$ and $\alpha_i \in \mathbb{Z}$. The *size* of P, size(P) is defined as the number of bits necessary to encode it as a binary string, i.e., $\operatorname{size}(P) = \sum_{i=1}^{m} \left[\sum_{j=1}^{d} \lceil \log(|a_{ij}| + 1) \rceil + \lceil \log(|\alpha_i| + 1) \rceil \right]$. Then, as it is shown in [5], the number of vertices of $\operatorname{conv}(\mathbb{Z}^d \cap P)$ is at most $2m^d[12d^2 \operatorname{size}(P)]^{d-1}$. A construction in [3] shows that this result is best possible.

A second motivation comes from classical results. Write B^d for the d–dimensional Euclidean ball. Van der Corput proved in 1922 [6] that

$$(1) \qquad |\mathbb{Z}^2 \cap rB^2| = r^2\pi + O\left[r^{\frac{2}{3} - \epsilon}\right]$$

with $\epsilon = 0.01$. Since then there have been a lot of (minor) improvements in ϵ, probably the last coming from Iwaniec and Mozzochi (see [8]), generalized by Huxley [8]. He proves that if D is a convex body in R^2 with $\mathcal{C}^3$ boundary and positive curvature at every point of the boundary, then

$$(2) \qquad |\mathbb{Z}^2 \cap rD| = r^2 \text{ Area } D + O\left[r^{\frac{7}{11} + \epsilon}\right].$$

Another classical result is due to Jarnik [9]. He showed that if Γ is a strictly convex curve in the plane whose length is s, then

$$(3) \qquad |\mathbb{Z}^2 \cap \Gamma| \leqq \frac{3}{\sqrt[3]{2\pi}} s^{\frac{2}{3}} + O\left[s^{\frac{1}{3}}\right].$$

If Γ is C^3, then the exponent $\frac{2}{3}$ can be reduced to $\frac{3}{5}$ in (3). This is a result due to Swinnerton–Dyer [13] and Schmidt [12]. Jarnik gave an example of a strictly convex curve Γ whose length is s and whose radius of curvature is less than $7s$ at every point such that

$$|\mathbb{Z}^2 \cap \Gamma| \geqq \frac{3}{\sqrt[3]{2\pi}} s^{\frac{2}{3}} + O\left[s^{\frac{1}{3}}\right] .$$

(1) has been extended to higher dimensions:

$$|\mathbb{Z}^3 \cap rB^3| = r^3 \operatorname{vol}(B^3) + O\left[r^{\frac{4}{3}}\right] ,$$

$$|\mathbb{Z}^4 \cap rB^4| = r^4 \operatorname{vol}(B^4) + O\left[r^2 \log r\right] ,$$

$$|\mathbb{Z}^d \cap rB^d| = r^d \operatorname{vol}(B^d) + O\left[r^{d-2}\right] , \text{ for } d > 4 .$$

Here the first equality is due to Vinogradov [15] and Chen [4], the other two to Walfisz [14]. What we will need here is the weaker

$$(4) \qquad |\mathbb{Z}^d \cap rB^d| = r^d \operatorname{vol}(B^d) + o\left[r^{\frac{d(d-1)}{d+1}}\right] ,$$

valid for all $d \geq 2$.

Another motivation is the following. Let $x_1, \dots, x_n$ be points chosen randomly, independently and uniformly from B^d. Then $K_n = \operatorname{conv}\{x_1, \dots, x_n\}$ is a random polytope. It is known (see, for instance, Schneider's survey paper [11]) that the expected number of vertices of K_n is $\operatorname{const}(d) n^{\frac{d-1}{d+1}}$. Now if one chooses r so that $r^d \operatorname{vol}(B^d) = n$, then in rB^d there will be essentially n integral points, and the number of vertices of $\operatorname{conv}(\mathbb{Z}^d \cap rB^d)$ must be around

$$n^{\frac{d-1}{d+1}} \approx r^{\frac{d(d-1)}{d+1}}$$

if the integer points "behave" like random points in rB^d. It turns out that this is indeed the case for $d = 2$, as Theorem 1 below shows.

Write $N(r,d)$ for the number of vertices of $\operatorname{conv}(\mathbb{Z}^d \cap rB^d)$ and set $N(r) = N(r,2)$.

THEOREM 1. For large enough r

$$c_1 r^{\frac{2}{3}} \leqq N(r) \leqq c_2 r^{\frac{2}{3}},$$

where c_1 and c_2 are absolute constants.

From the proof we will get $c_1 \approx 0.33$ and $c_2 \approx 5.54$. It is not clear for us whether the limit $\lim_{r\to\infty} N(r) r^{\frac{-2}{3}}$ exists or not.

The proof of the upper bound in Theorem 1 is easier and works in any dimension:

$$N(r,d) \leqq c_d\, r^{\frac{d(d-1)}{d+1}}. \tag{5}$$

We can extend Theorem 1 to smooth enough convex bodies in R^2, using Huxley's result (2).

THEOREM 2. If D is a plane convex body with C^3 boundary and positive curvature, then

$$c_1(D) r^{\frac{2}{3}} \leqq \#\text{ of vertices of } \operatorname{conv}(\mathbb{Z}^2 \cap rD) \leqq c_2(D) r^{\frac{2}{3}}$$

where the constants $c_1(D)$ and $c_2(D)$ depend on the upper and lower bounds for the curvature of D.

The proof is essentially the same, but more technical than that of Theorem 1 and will therefore be omitted.

In the proofs we will use Vinogradov's notation $<<$ and $<<_d$. All implied constants are effective.

2. PROOF OF THE UPPER BOUNDS

The upper bound in Theorem 1 is easier. It follows from Jarnik's result (3) but one has to make the boundary of P_r strictly convex. Actually, Jarnik's original proof applies as well giving $c_2 = 3(2\pi)^{\frac{1}{3}} = 5.5358\ldots$. Or one can use the following result of Andrews [1], cf. [2], [12], [10] as well. If $P \subset R^d$ is a convex polytope with integral vertices and nonempty interior, then

$$\#\text{ vertices of } P <<_d (\text{vol } P)^{\frac{d-1}{d+1}}.$$

This proves (5) immediately.

Now we give a simple direct proof of (5). Assume v is a vertex of $\text{conv}(\mathbb{Z}^d \cap rB^d)$ and consider $M(v) = rB^d \cap (v - rB^d)$.

CLAIM 1. $\text{vol } M(v) \leqq 2^d$.

Indeed, $M(v)$ is convex and centrally symmetric with respect to $v \in \mathbb{Z}^d$. By Minkowski's theorem, $\text{vol } M(v) > 2^d$ would imply the existence of a point $x \in \mathbb{Z}^d \cap M(v)$, $x \neq v$. Then both x and $2v-x$ are integral and lie in rB^d so $v = \frac{1}{2}[x + (2v-x)]$ cannot be a vertex. □

Assume now that v is at distance Δ from the boundary of rB^d. Clearly,

$$\text{vol } M(v) > 2\frac{\Delta}{d}(\sqrt{2r\Delta})^{d-1} \text{ vol } B^{d-1},$$

that gives, together with Claim 1 $\Delta <<_d r^{-\frac{d-1}{d+1}}$. Then, using (1) and (4)

$$N(r,d) \leqq |\mathbb{Z}^d \cap rB^d| - |\mathbb{Z}^d \cap (r-\Delta)B^d| <<_d r^{\frac{d(d-1)}{d+1}}. \ \square$$

3. THE LOWER BOUND

For the lower bound in Theorem 1 define

$$\Delta = 2^{-\frac{1}{3}} r^{-\frac{1}{3}},$$

and set $A = A(r,\Delta) = rB^2 \setminus (r-\Delta)B^2$.

An integer point $x \in A$ is called a *vertex* if it is a vertex of P_r, and a *nonvertex* otherwise. The set of vertices will be denoted by V, the set of nonvertices by NV. For a nonvertex $x \in NV$ let $v \in V$ be the vertex nearest to x. This may not be unique, then choose any one of the nearest vertices. Draw an arrow from v to x and color this arrow green if it goes clockwise and blue if it goes counter–clockwise. We may assume that there are at least as many green arrows as blue ones, denote the set of green arrows by G. Clearly,

$$|NV| \leqq 2|G| .$$

Observe that, if $\overrightarrow{vx} \in G$, then $\|v-x\| \leqq \sqrt{2r\Delta}$. This is so because, as $x \in NV$, there must be a vertex of P_r in the cap (of rB^2) that has minimal area and contains x, and for any point y in that cap $\|x-y\| \leqq \sqrt{(2r-\Delta)\Delta} < \sqrt{2r\Delta}$.

CLAIM 2. If $\overrightarrow{vx} \in G$ and $\overrightarrow{vy} \in G$, then v, x, y are collinear.

PROOF. An easy computation shows that the triangle with vertices v, x, y has area less than $\frac{1}{2}$. (This is where $\Delta = 2^{-\frac{1}{3}} r^{-\frac{1}{3}}$ is needed.) But any lattice triangle has area at least $\frac{1}{2}$ so v, x, y must be collinear.

This means that for fixed $v \in V$ there is a longest green arrow $\overrightarrow{vx}$ (with $x = x(v)$, say) containing all other green arrows starting at v. Fix now a primitive vector $p \in \mathbb{Z}^2$ (i.e., a vector $p \neq 0$ with relative prime components) and consider $S(p)$, the sum of all vectors $x(v) - v$ coming from a longest green arrow $\overrightarrow{vx}(v)$ that is parallel to p and points in the same direction.

CLAIM 3. $\|S(p)\| << r^{\frac{1}{3}}$.

We postpone the proof to the end of this section.

Clearly, $\|S(p)\|/\|p\|$ is equal to the number of green arrows that are parallel to p and point the same direction. Now let $\{p_1, \ldots, p_m\}$ be the set of all primitive vectors with $S(p) \neq 0$. Evidently, $|V| \geq m$. On the other hand, by Claim 3

$$|G| = \sum_{i=1}^{m} \frac{\|S(p_i)\|}{\|p_i\|} << r^{\frac{1}{3}} \sum_{i=1}^{m} \frac{1}{\|p_i\|}.$$

Here $\sum_{i=1}^{m} \|p_i\|^{-1}$ will be the largest when $\{p_1, \ldots, p_m\}$ is the set of the m shortest primitive vectors in $\mathbb{Z}^2$. Then, as it is well–known [7] and actually easy to see

$$\sum_{i=1}^{m} \frac{1}{\|p_i\|} << \sqrt{m} \leqq \sqrt{|V|}.$$

Now by (1)

$$r^{\frac{2}{3}} << |A \cap \mathbb{Z}^2| = |V| + |NV| \leqq |V| + 2|G|$$
$$<< |V| + r^{\frac{1}{3}}\sqrt{|V|},$$

which clearly implies the lower bound.

It is perhaps worth stating separately what we used in the last part of the proof: In the disc ρB^2, $o(\rho^2)$ diameters contain only $o(\rho^2)$ of the integer points in ρB^2.

PROOF OF CLAIM 3. Consider the lattice lines

$$\ell_i = \left\{x \in R^2 : x = tp + i\frac{p^{\perp}}{\|p\|^2}, t \in R\right\}$$

where $i = 1, 2, \ldots$ and $p^{\perp}$ is the vector obtained from p by a 90° counter–clockwise rotation. (Here p is a primitive vector, again.) For each longest green arrow $\overrightarrow{vx}(v)$ where $x(v) = v + k(v)p$ $(k(v) = 1, 2, 3, \ldots)$ there is a line ℓ_i such that the segment connecting v and $x(v)$ is contained in $A \cap \ell_i$. This intersection consists of either one or two segments but in both cases we have

$$\|x(v) - v\| = k(v)\|p\| \leqq L_i := \text{half the length of } A \cap \ell_i .$$

More generally, let $\ell(h)$ denote the line parallel to p and at distance $r-h$ from the origin (so $0 < h < r$). Write $L(h)$ for the half–length of the intersection $A \cap \ell(h)$. Then

$$L(h) = \sqrt{(2r-h)h} - \sqrt{(2r-h-\Delta)\lceil h-\Delta \rceil_+}$$

where $|h-\Delta|_+ = h-\Delta$ if $h \geq \Delta$ and 0 otherwise. Clearly $\ell_i = \ell(h_i)$ with $h_i = r - \frac{i}{\|p\|}$. We must have

$$\|p\| \leq k(v)\|p\| \leqq L_i .$$

The inequality $\|p\| \leq L(h)$ implies an upper bound for h, namely,

$$h \leqq H := \left[1 + O(r^{-\frac{2}{3}})\right]\frac{2r\Delta^2}{\|p\|^2},$$

so that $H << r^{\frac{1}{3}}$. This shows that for $h \in [0,H]$

$$L(h) << \sqrt{2r}\left[\sqrt{h} - \sqrt{\lceil h-\Delta \rceil_+}\right] .$$

Now

$$\begin{aligned} \|S(p)\| &\leqq \Sigma\{L_i : 0 \leq h_i \leq H\} \\ &\leqq \|p\| + \|p\|\int_0^H L(h)dh + \max_{0 \leq h \leq H} L(h) , \end{aligned}$$

because the sum ΣL_i can be considered as an approximation to the integral $\int_0^H L(h)dh$. Evidently $\max L(h) \leq \sqrt{2r\Delta}$ and $\|p\| < \sqrt{2r\Delta}$. Then

$$\begin{aligned} \int_0^H L(h)dh &<< \sqrt{2r}\int_0^H\left[\sqrt{h} - \sqrt{\lceil h-\Delta \rceil_+}\right]dh \\ &= \sqrt{2r}\,\frac{2}{3}\left[H^{\frac{3}{2}} - |H-\Delta|^{\frac{3}{2}}\right] \\ &<< \frac{r\Delta^2}{\|p\|} . \end{aligned}$$

So indeed,

$$\|S(p)\| << \sqrt{2r\Delta} + r\Delta^2 + \sqrt{2r\Delta} << r^{\frac{1}{3}} . \square$$

REFERENCES

[1] G. E. Andrews, A lower bound for the volumes of strictly convex bodies with many boundary points, *Trans. Amer. Math. Soc.*, 106 (1963), 270–279.

[2] V. I. Arnold, Statistics of integral convex polytopes (in Russian), *Functional Anal. Appl.*, 14 (1980), 1–3.

[3] I. Bárány, R. Howe, L. Lovász, On integer points in polyhedra: A lower bound, to appear in *Combinatorica* (1991).

[4] J. R. Chen, The lattice points in a circle, *Sci. Sinica*, 12 (1963), 633–649.

[5] W. Cook, M. Hartman, R. Kannan, C. McDiarmid, On integer points in polyhedra, to appear in *Combinatorica* (1991).

[6] J. G. van der Corput, Verscharfung der Abschätzung beim Teilerproblem, *Math. Annalen*, 87 (1922), 39–65.

[7] F. Fricker, Einführung in die Gitterpunktlehre, Birkhäuser, Basel–Boston-Stuttgart, 1982.

[8] M. N. Huxley, Exponential sums and lattice points, *Proc. London Math. Soc.* (3), 60 (1990), 471–502.

[9] V. Jarnik, Über Gitterpunkte and konvex Kurven, *Math. Zeitschrift*, 24 (1925), 500–518.

[10] S. B. Konyagin, K. A. Sevastyanov, Estimation of the number of vertices of a convex integral polyhedron in terms of its volume (in Russian), *Funktional Anal. Appl.*, 18 (1984), 13–15.

[11] R. Schneider, Random approximation of convex sets, *Microscopy*, 151 (1988), 211–227.

[12] W. M. Schmidt, Integer points on curves and surfaces, *Monatshäfte für Math.*, 99 (1985), 45–72.

[13] H. P. F. Swinnerton–Dyer, The number of lattice points on a convex curve, *J. Number Theory*, 6 (1974), 128–135.

[14] I. M. Vinogradov, On the number of integer points in a sphere (in Russian), lzv. *Akad. Nauk SSSR, Ser. Mat.*, 27 (1963), 957–968.

[15] A. Walfisz, *Gitterpunkte in mehrdimensionalischen Kugeln*, *Panstwowe Wydawnictwo Naukowe*, Warszawa, 1957.