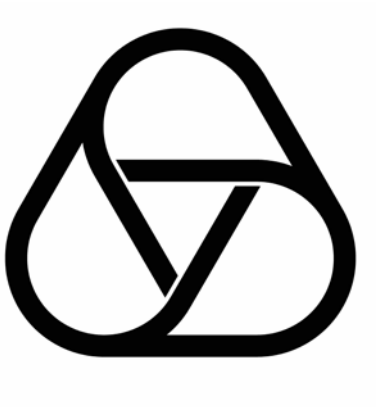
Oberwolfach Preprints



OWP 2014 - 17

BERNARDO GONZÁLEZ MERINO AND MATTHIAS HENZE

A Generalization of the Discrete Version of Minkowski's Fundamental Theorem

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

Starting in 2007, the MFO publishes a preprint series which mainly contains research results related to a longer stay in Oberwolfach. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 30 free hard copies (DIN A4, black and white copy) by surface mail.

Of course, the full copy right is left to the authors. The MFO only needs the right to publish it on its website *www.mfo.de* as a documentation of the research work done at the MFO, which you are accepting by sending us your file.

In case of interest, please send a **pdf file** of your preprint by email to *rip@mfo.de* or *owlf@mfo.de*, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX - XX).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

A GENERALIZATION OF THE DISCRETE VERSION OF MINKOWSKI'S FUNDAMENTAL THEOREM

BERNARDO GONZÁLEZ MERINO AND MATTHIAS HENZE

In memory of Hermann Minkowski on the occasion of his 150th birthday

Abstract. One of the most fruitful results from Minkowski's geometric viewpoint on number theory is his so called 1st Fundamental Theorem. It provides an optimal upper bound for the volume of an o-symmetric convex body whose only interior lattice point is the origin. Minkowski also obtained a discrete analog by proving optimal upper bounds on the number of lattice points in the boundary of such convex bodies. Whereas the volume inequality has been generalized to any number of interior lattice points already by van der Corput in the 1930s, a corresponding result for the discrete case remained to be proven. Our main contribution is a corresponding optimal relation between the number of boundary and interior lattice points of an o-symmetric convex body. The proof relies on a congruence argument and a difference set estimate from additive combinatorics.

1. Introduction

A *convex body* in the Euclidean vector space $\mathbb{R}^n$ is a compact convex set K whose set of interior points, denoted by $\operatorname{int} K$, is nonempty. The *convex hull* of a subset $S \subset \mathbb{R}^n$ is written as $\operatorname{conv} S$. We say that a convex body is *strictly convex* if its boundary does not contain a proper line segment, and we write $\mathcal{K}_o^n$ for the family of *o-symmetric* convex bodies in $\mathbb{R}^n$, that is, convex bodies K with $K = -K$, where $tK = \{tx : x \in K\}$, for any $t \in \mathbb{R}$.

Motivated by the fundamental inequalities of Minkowski and its various generalizations and extensions, we are interested in the relation of an o-symmetric convex body to the lattice $\mathbb{Z}^n$ consisting of all points in $\mathbb{R}^n$ with only integral coordinates. Such a point is shortly called *lattice point* in the sequel. Minkowski [7] proved that the cube $C_n = [-1, 1]^n$ has maximal *volume* (Lebesgue-measure) among all convex bodies in $\mathcal{K}_o^n$ with the property that the origin is their only interior lattice point. In symbols,

$$\text{(1)} \quad \operatorname{vol}(K) \le \operatorname{vol}(C_n) = 2^n, \quad \text{for every } K \in \mathcal{K}_o^n \text{ with } \operatorname{int} K \cap \mathbb{Z}^n = \{0\}.$$

2010 *Mathematics Subject Classification.* Primary 52C07; Secondary 11H06, 52A40, 11P70, 52A20.

Key words and phrases. Convex body, lattice point, Minkowski's fundamental theorem, discrete analog, difference set estimate, successive minimum.

This research was supported through the program "Research in Pairs" by the Mathematisches Forschungsinstitut Oberwolfach in 2014. The first author was partially supported by MINECO/FEDER project reference MTM2012-34037, Spain. The second author was supported by the ESF EUROCORES programme EuroGIGA-VORONOI, (DFG): RO 2338/5-1.

This inequality lies at the heart of Minkowski's geometric viewpoint on number theoretical questions. Its wide applicability, reaching beyond geometry and number theory, inspired the quest for generalizations and analogous relations ever since. Minkowski moreover obtained a discrete version of this fundamental inequality, saying that the cube also maximizes the total number of lattice points $\mathrm{G}(K) = \#(K \cap \mathbb{Z}^n)$ in o-symmetric convex bodies K obeying the above condition. More precisely,

$$\mathrm{G}(K) \leq \mathrm{G}(C_n) = 3^n, \quad \text{for every } K \in \mathcal{K}_o^n \text{ with } \operatorname{int} K \cap \mathbb{Z}^n = \{0\}, \tag{2}$$

and

$$\mathrm{G}(K) \leq 2^{n+1} - 1, \quad \text{if } K \text{ is moreover strictly convex.} \tag{3}$$

It has been shown in [3] that equality holds in (2) if and only if K is *unimodularly equivalent* to the cube, that is, there exists an invertible matrix $A \in \mathbb{Z}^{n\times n}$ with integer entries such that $K = AC_n$. A suitable smoothing of the convex hull of $[0,1]^n$ and $[-1,0]^n$ shows that the inequality (3) is also best possible. Besides Minkowski's original monograph [7], the book by Gruber & Lekkerkerker [6], in particular Sections 9.4, 26.2 and the Supplements to Chapter 4, is an excellent reference for the theory that developed out of these results. More recent developments are covered in [5].

Another way of saying that $K \in \mathcal{K}_o^n$ contains only the origin as an interior lattice point is that its *first successive minimum*

$$\lambda_1(K) = \min\{\lambda > 0 : \lambda K \cap \mathbb{Z}^n \neq \{0\}\}$$

is at least one. Clearly, $\lambda_1(tK) = \frac{1}{t}\lambda_1(K)$, for every $t > 0$. Together with the relation $\mathrm{vol}(K) = \lim_{t\to\infty} \mathrm{G}(tK)/t^n$, this shows that the following result by Betke, Henk & Wills [2] is a common generalization of Minkowski's inequalities above. They proved that for $K \in \mathcal{K}_o^n$, we have

$$\mathrm{G}(K) \leq \left\lfloor \frac{2}{\lambda_1(K)} + 1 \right\rfloor^n, \tag{4}$$

and if K is strictly convex, then

$$\mathrm{G}(K) \leq 2 \left\lceil \frac{2}{\lambda_1(K)} \right\rceil^n - 1. \tag{5}$$

Here, the floor function $\lfloor x \rfloor$ and the ceiling function $\lceil x \rceil$ of a real number x denote, as usual, the largest integer smaller than or equal to x, and the smallest integer bigger than or equal to x, respectively.

Another perspective on extending Minkowski's volume inequality has already been taken by van der Corput [14], who showed that for every $K \in \mathcal{K}_o^n$ holds

$$\mathrm{vol}(K) \leq 2^{n-1}\left(\mathrm{G}(\operatorname{int} K) + 1\right), \tag{6}$$

with equality for the stretched cube $C_{n-1} \times [-\ell, \ell]$, where $\ell \in \mathbb{N}$. This is related to the results of Betke, Henk & Wills because for any o-symmetric convex body K, and any of its lattice points $z \in K \cap \mathbb{Z}^n$, we find that the open line segment $(-z, z)$ contains at most $\mathrm{G}(\operatorname{int} K)$ lattice points. That is, $\#([0, z) \cap \mathbb{Z}^n) \leq (\mathrm{G}(\operatorname{int} K) + 1)/2$ and therefore

$$\frac{2}{\lambda_1(K)} \leq \mathrm{G}(\operatorname{int} K) + 1, \quad \text{for any } K \in \mathcal{K}_o^n.$$

A combination of this observation with the bounds (4) and (5) shows that, analogous to van der Corput's inequality, there is also an upper bound on $\mathrm{G}(K)$ in terms of the number of interior lattice points of K. The best possible such upper bound is a linear function in $\mathrm{G}(\operatorname{int} K)$. This follows from a series of investigations for the general, not necessarily o-symmetric case, that culminated in the work of Pikhurko [8]. He proved that

$$\operatorname{vol}(P) \leq (8n)^n 15^{n2^{2n+1}} \mathrm{G}(\operatorname{int} P), \tag{7}$$

and

$$\mathrm{G}(P) \leq n!(8n)^n 15^{n2^{2n+1}} \mathrm{G}(\operatorname{int} P) + n, \tag{8}$$

whenever $\operatorname{int} P \cap \mathbb{Z}^n \neq \emptyset$ and P is a *lattice polytope* in $\mathbb{R}^n$, that is, the convex hull of finitely many lattice points. Although the minimal factor in front of $\mathrm{G}(\operatorname{int} P)$ admitting inequalities of this type is known to be doubly exponential in n, the above bounds are assumed to be far from tight. The determination of the exact bound is only solved for (7) in the case of lattice simplices with exactly one interior lattice point [1] (see [8] for more information and references).

Therefore, it is desirable to understand the special yet important case of o-symmetric convex bodies more thoroughly. As an exact analog to van der Corput's inequality (6) and an extension of (2) and (3), our main result is the following.

Theorem 1.1. *Let $K \in \mathcal{K}_o^n$.*

i) We have

$$\mathrm{G}(K) \leq 3^{n-1} \left(\mathrm{G}(\operatorname{int} K) + 2\right),$$

and equality holds if and only if K is unimodularly equivalent to the parallelepiped $C_{n-1} \times [-\ell, \ell]$, for some $\ell \in \mathbb{N}$.

ii) If K is strictly convex, then

$$\mathrm{G}(K) \leq 2^n \left(\mathrm{G}(\operatorname{int} K) + 1\right) - 1.$$

Note that Scott [10] obtained an inequality that implies the first result above in the case $n = 2$.

Our proof of Theorem 1.1 is based on two main ingredients. The first is an extension of an elegant congruence argument, for which we say that two lattice points $x, y \in \mathbb{Z}^n$ are *congruent modulo* $m \in \mathbb{Z}$, if $x - y \in m\mathbb{Z}^n$. Observe that the points of $\mathbb{Z}^n$ are partitioned into precisely m^n congruence classes, also often called *residue classes*. In order to illustrate the method, we recall Minkowski's proof of (2): Assume that for some $K \in \mathcal{K}_o^n$, we have $\mathrm{G}(K) > 3^n$. Then there are $x, y \in K \cap \mathbb{Z}^n$, $x \neq y$, that are congruent modulo 3. By symmetry and convexity of K, this shows that $(x - y)/3$ is a non-zero interior lattice point of K, contradicting the assumptions on the body. The second ingredient is an estimate on the size of difference sets of non-collinear finite point sets to which the next section is devoted. The details for Theorem 1.1 are then carried out in Section 3.

2. The equality case in a planar difference set estimate

In this section, we discuss a combinatorial result on the minimal number of difference vectors generated by a non-collinear point set. To this end, we let $U - U = \{u - v : u, v \in U\}$ be the *difference set* of a subset $U \subset \mathbb{R}^n$. It is easy to see that, if U is finite and $\#U = k$, we have

$$\#(U - U) \geq 2k - 1.$$

This is best possible if U is an *arithmetic progression* which means that there exist $u, s \in \mathbb{R}^n$ such that $U = \{u, u+s, \ldots, u+(k-1)s\}$. Freiman, Heppes & Uhrin [4] showed that if we assume that U has affine dimension d, then one can improve this bound to

$$\#(U - U) \geq (d+1)k - \binom{d+1}{2}. \tag{9}$$

Note that the authors of [4] apply this inequality to sharpen a classic result of Blichfeldt on the number of lattice points in the difference set of an arbitrary Lebesgue-measurable set. For $d = 1, 2$, the estimate above cannot be further improved, but it is conjectured that for any $d \geq 3$ there is a better bound. In fact, revising a conjecture of Freiman, Stanchescu [12] claims that, for every $d \geq 2$, the maximal factor in front of k in an inequality of the type (9) is given by $2(d-1) + 1/(d-1)$ and proves this for the case $d = 3$. Such difference set estimates embed in the currently very active field of additive combinatorics, where people study more generally the structure of subsets A of some abelian group whose sum-sets or difference-sets $A \pm A$ have either very small or very large cardinality. For instance, generalizing an earlier result by Freiman, Ruzsa found an optimal lower bound on $\#(A + B)$, for two given subsets A and B, which includes (9) as a special case (see [9] for a survey on this and related problems). The interested reader may also consult the book of Tao & Vu [13] that covers the recent developments and their various applications in many branches of mathematics.

For our purposes, we need to investigate the case $d = 2$ of the inequality (9) more closely. We have seen that Freiman, Heppes & Uhrin obtained the optimal lower bound on the size of the difference set in this case. Moreover, for the case that $\#U$ is even, Stanchescu [11] characterized the point sets U attaining equality. However, in order to be able to prove Theorem 1.1, we also need to characterize the point sets of odd size with minimal value of $\#(U - U)$. To the best of our knowledge this has not been worked out before, and thus we give the complete proof of all three statements for the readers convenience. Before we can state the result, we need to introduce a notion of a generalized arithmetic progression. We say that a point set $U \subset \mathbb{R}^n$ is an *arithmetic progression of type* (k, l) if there exists an anchor point $u \in \mathbb{R}^n$ and two linearly independent vectors $s, t \in \mathbb{R}^n$ such that $U = V \cup (V+t) \cup \ldots \cup (V+(l-1)t)$, where $V = \{u, u+s, \ldots, u+(k-1)s\}$. Moreover, we say that a point set $U \subset \mathbb{R}^n$ is an *incomplete arithmetic progression of type* (k, l), if there is some $x \in \mathbb{R}^n$ such that $U \cup \{x\}$ is an arithmetic progression of type (k, l) and x is a vertex of $\operatorname{conv}\{U \cup \{x\}\}$.

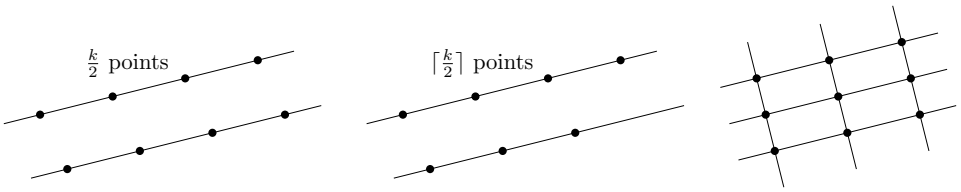


FIGURE 1. The equality cases in Theorem 2.1, for k even (left) and k odd (middle and right).

Theorem 2.1. *For any set $U \subset \mathbb{R}^n$ of k non-collinear points, we have*

$$\#(U-U) \geq \begin{cases} 3k-3 & \text{if } k \text{ is even,} \\ 3k-2 & \text{if } k \text{ is odd.} \end{cases}$$

Equality holds for even k if and only if U is an arithmetic progression of type $(k/2, 2)$, and for odd k if and only if U is either an incomplete arithmetic progression of type $(\lceil k/2 \rceil, 2)$ or an arithmetic progression of type $(3, 3)$.

Proof. First of all, we can reduce the problem to subsets U of $\mathbb{R}^2$. Indeed, since U is finite, we can always find a two-dimensional subspace S of $\mathbb{R}^n$ such that the projection $U|S$ of U onto S is a non-collinear point set with $\#(U|S) = \#U$. Clearly, $\#(U-U) \geq \#(U|S - U|S)$ and hence it suffices to prove the bound and also the equality characterization for $U|S$. Therefore, in the following we assume that $U \subset \mathbb{R}^2$.

Consider a set $V \subset \mathbb{R}^2$ of ℓ points lying on a common line. It is easy to see that $\#(V-V) \geq 2\ell - 1$ with equality if and only if the points in V are equally spaced on the line.

Consider now two parallel lines L and L' containing ℓ and m points, respectively, where $\ell \geq m \geq 1$ and $\ell \geq 2$. Then, the number of vectors $\pm(v-w)$, where v is one of the points in L and w is one of the points in L', is at least $2(\ell + m - 1)$. This is at least $4m - 2 \geq 3m$, for $m \geq 2$, and at least $2\ell \geq 4 > 3m$, for $m = 1$. We find exactly $3m$ such difference vectors if and only if $\ell = m = 2$, and the two points on L have the same distance as the two points on L'.

Based on these two basic observations, we set up an inductive argument as follows. Let L be a supporting line of an edge of $\operatorname{conv} U$ and let L' be the parallel supporting line to L on the other side of $\operatorname{conv} U$. Note, that $L \neq L'$ since U is non-collinear. Let us assume first, that every point of U is contained in either of those two parallel lines, and without loss of generality let $\ell = \#(U \cap L) \geq \#(U \cap L') = m \geq 1$. Then, we get that

$$\begin{aligned} \#(U-U) &\geq \#((U \cap L) - (U \cap L)) + 2(\ell + m - 1) \\ &\geq 2\ell - 1 + 2(\ell + m - 1) = 4\ell + 2m - 3. \end{aligned}$$

If $k = \#U$ is even, we thus get $\#(U-U) \geq 3(\ell + m) - 3 = 3k - 3$, with equality if and only if $\ell = m$, the points $U \cap L$ are equally spaced and the point set $U \cap L'$ is a translate of $U \cap L$. That is, U is an arithmetic progression of type $(k/2, 2)$. If k is odd, we have $\ell \geq m + 1$, and thus $\#(U-U) \geq 3(\ell + m) - 2 = 3k - 2$. Here, equality holds if and only if $\ell = m + 1$, the points $U \cap L$ are equally spaced and every difference vector generated by $U \cap L'$ can be generated by $U \cap L$. The latter condition holds if

and only if $U \cap L'$ is a translate of $(U \cap L) \setminus \{p\}$, for some endpoint $p \in U \cap L$, and thus, U is an incomplete arithmetic progression of type $(\lceil k/2 \rceil, 2)$.

Now, we study the case that $U \neq (U \cap L) \cup (U \cap L')$. Without loss of generality, we let $m = \#(U \cap L') \leq \#(U \cap L)$ and we write $U' = U \setminus (U \cap L')$. As we have seen before, we have at least $3m$ difference vectors of the form $\pm(v - w)$, where $v \in U \cap L$ and $w \in U \cap L'$. By construction, the projection of these difference vectors onto the orthogonal line to L is different from the projection of any difference vector generated by points of U', and thus they were different in the first place. Since the points in U' are non-collinear, we inductively get that

$$\#(U - U) \geq \#(U' - U') + 3m \geq 3(k - m) - 3 + 3m = 3k - 3. \tag{10}$$

As $\#(U - U)$ is always odd, we obtain the desired bound $\#(U - U) \geq 3k - 2$ in the case that $k = \#U$ is odd.

Characterization of equality.

We need to distinguish some cases.

Case 1: k is even and $\#(U - U) = 3k - 3$.

This holds precisely, if we have $\#(U' - U') = 3(k - m) - 3$ and there are exactly $3m$ difference vectors of the form $\pm(v - w)$, where $v \in U \cap L$ and $w \in U \cap L'$. By induction hypothesis, the first condition implies that $k - m$ is even and that U' is an arithmetic progression of type $((k - m)/2, 2)$. Moreover, from the second condition we get $m = \#(U \cap L) = 2$ and the distance of the two points $U \cap L$ is the same as the distance of the points $U \cap L'$. Let S and S' be the two parallel lines that contain the set U', and without loss of generality assume that these are horizontal lines, with S being the lower one. Since L supports an edge of $\operatorname{conv} U$ and $\#(U \cap L) = 2$, it supports one of the edges of $\operatorname{conv} U'$ that contain exactly two points of U. We claim that the two points $U \cap L'$ are distributed on S and S'. In order to see this, let us assume that $w \in U \cap L'$ does not lie on any of the lines S and S'. Since U is not completely contained on the lines L and L', there is another line L'' parallel to L that is different from these two and contains a point z of $U' \cap S$. But then the difference vector $w - z$ can neither be generated by U' nor by points from $U \cap L$ and $U \cap L'$, contradicting the equality assumption. Therefore, $w \in S \cup S'$, say $w \in S$, and moreover, it is easy to see that the distance from the closest point in $U' \cap S$ to w must be the same as the (equal) distance of any neighboring points in $U' \cap S$. Hence, U is an arithmetic progression of type $(k/2, 2)$.

Case 2: k is odd and $\#(U - U) = 3k - 2$.

Looking at (10), there are two options.

Case 2.1: $\#(U' - U') = 3(k - m) - 3$ and there are exactly $3m + 1$ difference vectors of the form $\pm(v - w)$, where $v \in U \cap L$ and $w \in U \cap L'$.

The first condition implies by induction that $k - m$ is even, thus m is odd, and that U' is an arithmetic progression of type $((k - m)/2, 2)$. As above, we assume that U' is equally distributed on the horizontal lines S and S'. In general, there are at least $2(\ell + m - 1)$ difference vectors $\pm(v - w)$, where $\ell = \#(U \cap L) \geq \#(U \cap L') = m$. This is exactly $3m + 1$ if either $\ell = m = 3$, or $\ell = 2$ and $m = 1$. Since L supports an edge of $\operatorname{conv} U'$, we see that in the first

case we have $L = S$ or $L = S'$, and thus $k - m = 6$. Therefore, U is a set of nine points equally distributed on three parallel lines and a similar argument as in Case 1 above shows that U must be an arithmetic progression of type $(3, 3)$ in order to avoid additional difference vectors besides those generated by two points in U' or one point each from $U \cap L$ and $U \cap L'$. In the second case, L intersects U' in exactly two points and thus supports a short edge of $\operatorname{conv} U'$. Again, we argue similarly as in Case 1 in order to see that the point $U \cap L'$ must lie on one of the horizontal lines S and S', say it lies on S, having the same distance from the closest point in $U' \cap S$ as the (equal) distance of any neighboring points in $U' \cap S$. Hence, U is an incomplete arithmetic progression of type $(\lceil k/2 \rceil, 2)$.

Case 2.2: $\#(U' - U') = 3(k - m) - 2$ and there are exactly $3m$ difference vectors of the form $\pm(v - w)$, where $v \in U \cap L$ and $w \in U \cap L'$.

The first condition implies by induction that $k - m$ is odd and that U' is either an incomplete arithmetic progression of type $(\lceil (k - m)/2 \rceil, 2)$ or an arithmetic progression of type $(3, 3)$. From the second condition we infer that $m = \ell = \#(U \cap L) = 2$, and since L supports an edge of $\operatorname{conv} U'$ and contains exactly two points of U, the set U' cannot be an arithmetic progression of type $(3, 3)$. Hence, writing $k' = \lceil (k-m)/2 \rceil$, we have that $U' = V \cup (V' + t)$, where $V = \{u, u + s, \dots, u + (k' - 1)s\}$ and $V' = V \setminus \{u + (k' - 1)s\}$, for suitable $u, s, t \in \mathbb{R}^2$. Moreover, it is no restriction to assume that L intersects U' in the points $u, u + t$, and we let $U \cap L' = \{v, w\}$. Again by the same argumentation as in Case 1, we see that v and w must be contained on the lines spanned by V and V', respectively, and moreover $v = u + k's$ and $w = u + t + k's$, or vice versa. But now we find that the pair of difference vectors $\pm(w - (u + s)) = \pm(t + (k' - 1)s)$ can neither be generated by U' nor by points from $U \cap L$ and $U \cap L'$, contradicting that U is a point set attaining equality. Eventually, this shows that this last case cannot occur, finishing our proof. □

3. Proof of the general discrete Minkowski theorem

The case of strictly convex bodies is easier, so we shall prove it first.

Proof of Theorem 1.1 ii). Assume that $\mathrm{G}(K) \geq 2^{n+1}k$ for some $k \in \mathbb{N}$. Then, K contains, besides the origin, at least $2^n k$ pairs of lattice points $x, -x$. If at least k of these pairs are congruent to 0 modulo 2, then the points $\pm\frac{1}{2}x$ are interior lattice points of K and hence $\mathrm{G}(\operatorname{int} K) \geq 2k + 1$. Therefore, let us assume that at most $k - 1$ of these pairs are congruent to 0 modulo 2. By the pigeon hole principle this means that there is another congruence class modulo 2 containing at least $k + 1$ of these pairs. Let them be $v_1, \dots, v_{k+1} \in K \cap \mathbb{Z}^n$ in lexicographically increasing order, and note that $v_i \neq -v_j$ for every i, j. Since K is strictly convex, the points $\pm\frac{1}{2}(v_i - v_1)$ are pairwise different interior lattice points of K and hence again $\mathrm{G}(\operatorname{int} K) \geq 2k + 1$.

In summary, assuming that $\mathrm{G}(\operatorname{int} K) = 2k - 1$ implies that $\mathrm{G}(K) \leq 2^{n+1}k - 1 = 2^n\,(\mathrm{G}(\operatorname{int} K) + 1) - 1$, as desired. □

Proof of Theorem 1.1 i). The proof splits up into several cases.

Case 1: The interior lattice points of K are contained in a line L.

By the symmetry of K, the number of interior lattice points in K is always odd, hence $\mathrm{G}(\operatorname{int} K) = 2t-1$, for some $t \in \mathbb{N}$. Any two points $v, w \in K \cap \mathbb{Z}^n$ from the same residue class modulo three give rise to a lattice point $(v-w)/3$. Since K is convex and o-symmetric, this lattice point belongs to the interior of K and hence to L. This implies that all lattice points of K belonging to the same residue class modulo three are contained in a line parallel to L. Each lattice line contains lattice points from exactly three different residue classes. Now, let L' be such a parallel lattice line to L that contains two different lattice points $v, w \in K$ from the same residue class R_1. Then, the segment $[v, w]$ contains at least two lattice points in its interior and in fact one from each of the two other residue classes R_2 and R_3 that have points on L'. This shows that either there are at most three lattice points of K that fall into one of the classes R_1, R_2 and R_3, or all such lattice points are contained in the same line L'. Now, any such line can contain no more than $2t + 1 \geq 3$ lattice points, as we otherwise would get more than $2t - 1$ interior lattice points of K by its o-symmetry. There are 3^{n-1} groups of three residue classes with points in the same parallel line to L. By counting the lattice points in K by containment in these groups, we get $\mathrm{G}(K) \leq 3^{n-1}(2t + 1) = 3^{n-1}(\mathrm{G}(\operatorname{int} K) + 2)$ which is the inequality we want to prove.

Case 2: The interior lattice points of K are non-collinear.

Let us assume that $\mathrm{G}(K) > 3^n k$, for some $k \in \mathbb{N}$. Then, there exists a residue class modulo three that contains at least $k + 1$ different elements $u_0, u_1, \ldots, u_k \in K \cap \mathbb{Z}^n$. We show that this forces K to contain at least $3k+1$ interior lattice points. There are two different scenarios to consider.

Case 2.1: The points $u_0, \ldots, u_k$ are collinear.

We assume that the points $u_0, \ldots, u_k$ are labeled in increasing order on their common line L. Since they belong to the same residue class modulo three, there are at least two lattice points between any pair u_i and u_{i+1} on L, and hence the line segment $[u_0, u_k]$ contains at least $3k+1$ lattice points. By symmetry of K, we see that the central slice of K parallel to L contains at least $3k - 1$ interior lattice points. Because the interior lattice points of K are assumed not to be collinear, there must be an additional pair, and thus $\mathrm{G}(\operatorname{int} K) \geq 3k + 1$.

Case 2.2: The points $u_0, \ldots, u_k$ are non-collinear.

By Theorem 2.1 there are, depending on the parity of k, at least $3k$ or $3k + 1$ difference vectors of the form $u_i - u_j$, $i, j \in \{0, 1, \ldots, k\}$. Since the u_i belong to the same residue class modulo three, the points $(u_i - u_j)/3$ are interior lattice points of K. Hence, if k is even, we obtain $\mathrm{G}(\operatorname{int} K) \geq 3k+1$ as desired. If k is odd and Theorem 2.1 gives us exactly $3k$ difference vectors, then its equality characterization shows that $U = \{u_0, \ldots, u_k\}$ is an arithmetic progression of type $((k + 1)/2, 2)$. In order to show that also in this case K contains more than $3k$ interior lattice points we need to take more care.

Knowing that $\mathrm{G}(\operatorname{int} K) \geq 3k$, gives the desired estimate if K contains not too many more lattice points than $3^n k$. In fact, if $\mathrm{G}(K) \leq 3^n k + 2 \cdot 3^{n-1} - 1$, then $\mathrm{G}(K) \leq 3^{n-1} \mathrm{G}(\operatorname{int} K) + 2 \cdot 3^{n-1} - 1 < 3^{n-1} (\mathrm{G}(\operatorname{int} K) + 2)$. Hence, we now assume that $\mathrm{G}(K) > 3^n k + 2 \cdot 3^{n-1} - 1$, and moreover that no residue class contains $k+2$ lattice points of K, since otherwise we get $\mathrm{G}(\operatorname{int} K) \geq 3k+3$ from the considerations before. Let c be the number of residue classes with precisely $k+1$ elements in K. Then, $\mathrm{G}(K) \leq c(k+1) + (3^n - c)k = 3^n k + c$ and hence $c \geq 2 \cdot 3^{n-1}$. Let $U_1, \ldots, U_c$ be the sets of lattice points of K corresponding to these c residue classes. By assumption $\#(U_i - U_i) = 3k$, for all $i = 1, \ldots, c$, and hence they are all arithmetic progressions of type $((k+1)/2, 2)$. We now assume that $\mathrm{G}(\operatorname{int} K) = 3k$ and derive a contradiction.

We claim that under this condition the U_i need to be translates of each other. To this end, we write $U_i = \{u_0^i, \ldots, u_k^i\}$, for $i = 1, \ldots, c$, and up to a translation their anchor points lie at the origin. Thus, there are pairs of linearly independent vectors $s^i, t^i \in \mathbb{R}^n$ such that $u_l^i = l \cdot t^i$ and $u_{(k+1)/2+l}^i = s^i + l \cdot t^i$, for $l = 0, \ldots, (k-1)/2$. From this explicit description one derives $U_i - U_i = \left\{0, \pm t^i, \ldots, \pm \frac{k-1}{2} t^i\right\} \cup \left(\pm s^i + \left\{0, \pm t^i, \ldots, \pm \frac{k-1}{2} t^i\right\}\right)$, that is, the difference vectors in $U_i - U_i$ are equally distributed on three parallel lines. In order for all of them to generate the same set of interior lattice points of K, we need to have $U_i - U_i = U_j - U_j$, for $i, j = 1, \ldots, c$, which readily implies $s^i = s^j$ and $t^i = t^j$, for $i, j = 1, \ldots, c$, and hence our claim.

Every two-dimensional lattice plane contains lattice points from exactly nine different residue classes. For every U_i, its affine hull $S_i = \operatorname{aff} U_i$ is a lattice plane that actually contains at least one lattice point of K from each of the nine residue classes that are present in S_i. Since $c \geq 2 \cdot 3^{n-1}$, there must be one of them, say U_1 such that S_1 contains a lattice point from five of the other sets, say $U_2, \ldots, U_6$. Because $U_1, \ldots, U_6$ are translates of each other this means that there is a lattice line either parallel to $L_1 = \operatorname{aff}\{u_0^1, u_{(k+1)/2}^1\}$ containing at least 6 points of $U_1 \cup \ldots \cup U_6$, or parallel to $L_2 = \operatorname{aff}\{u_0^i, \ldots, u_{(k-1)/2}^i\}$ containing at least $3(k-1)/2+3$ lattice points of $U_1 \cup \ldots \cup U_6$. By symmetry of K, either the central slice C_1 of K parallel to L_1 contains at least 4 interior lattice points, or the central slice C_2 of K parallel to L_2 contains at least $3(k-1)/2+1$ interior lattice points. On the other hand, only 3 lattice points in C_1 and only k lattice points in C_2 are derived from $U_1 - U_1$. As $3(k-1)/2+1 > k$ for every $k \geq 3$, this contradicts our assumption that $\mathrm{G}(\operatorname{int} K) = 3k$.

Summarizing our investigations in Case 2, we have seen that under the assumption $\mathrm{G}(K) > 3^n k$, we find $\mathrm{G}(\operatorname{int} K) \geq 3k+1$. We know that $\mathrm{G}(\operatorname{int} K)$ is always some odd number. Every odd number can be written as either $3k$ for k odd, as $3k-1$ for k even, or as $3k-2$ for k odd. Therefore, we obtain $\mathrm{G}(K) \leq 3^n k = 3^{n-1} \mathrm{G}(\operatorname{int} K)$, or $\mathrm{G}(K) \leq 3^n k = 3^{n-1} (\mathrm{G}(\operatorname{int} K) + 1)$, or $\mathrm{G}(K) \leq 3^n k = 3^{n-1} (\mathrm{G}(\operatorname{int} K) + 2)$, depending on which of the three representations $\mathrm{G}(\operatorname{int} K)$ admits. This finishes the proof of the desired inequality for arbitrary $K \in \mathcal{K}_o^n$.

Characterization of the equality case.

For the characterization of the equality case, we henceforth assume that we consider some $K \in \mathcal{K}_o^n$ such that $\mathrm{G}(K) = 3^{n-1} (\mathrm{G}(\operatorname{int} K) + 2)$.

Case 1: The interior lattice points of K are non-collinear.

The previous paragraph shows that in order for equality to hold there needs to be some odd k such that $\mathrm{G}(\operatorname{int} K) = 3k-2$, and in particular $\mathrm{G}(K) = 3^n k$. Moreover, $k \geq 3$ due to the non-collinearity. If there exists a residue class modulo three that contains at least $k+1$ lattice points of K, then we have seen that $\mathrm{G}(\operatorname{int} K) \geq 3k+1$, clearly a contradiction. This means that each of the 3^n residue classes contains exactly k lattice points of K. Let U be the set of the k lattice points of K belonging to the residue class $3\mathbb{Z}^n$, and assume that the points in U are non-collinear. From the symmetry of K, we see that U must be an o-symmetric point set. By Theorem 2.1, we have $\#(U-U) \geq 3k-2$ and in fact we must have equality as $\mathrm{G}(\operatorname{int} K) = 3k-2$. Thus, the set U either is an incomplete arithmetic progression of type $(\lceil k/2 \rceil, 2)$, or an arithmetic progression of type $(3,3)$.

The first situation cannot occur, since no incomplete arithmetic progression of type $(\lceil k/2 \rceil, 2)$ is o-symmetric. In the latter situation, we have $k=9$, and the origin is the central point in U. The lattice points in the relative interior of $\operatorname{conv} U$ are interior lattice points of K, but it may happen that $\operatorname{conv} U$ contains exactly $3k-2 = 25$ relative interior lattice points. In this case, all of the eight other residue classes with a point in the plane $\operatorname{lin} U$ have less than k lattice points in $\operatorname{conv} U$. By assumption, fixing one of these residue classes R, there must be some lattice point in K, contained in the class R, which does not lie in $\operatorname{conv} U$. Then, either one of the eight points $U \setminus \{0\}$ is an interior lattice point of K, or the class R generates an interior lattice point that is not contained in $\operatorname{lin} U$. In both cases, we get more than the assumed $3k-2$ interior lattice points in K and thus a contradiction.

Now, assume that the points in U are contained in a line L. Let V be the k lattice points of K contained in one of the other two residue classes with points in L. Then, L contains at least $k-1$ lattice points of V. Indeed, it contains exactly $k-1$ such points, since otherwise $K \cap L$ contains at least $3k-2$ interior lattice points and hence the interior lattice points of K would be collinear which we assumed not to be the case. This means, that there is one point of V outside of L. Since $k-1 \geq 2$, there are at least three pairwise linearly independent vectors in the difference set $V-V$, hence implying the same structure for the set of interior lattice points of K. But this a contradiction again, because $K \cap L$ contains $3k-4$ interior lattice points of K and hence there is only one pair of opposite interior lattice points outside of L.

In conclusion, there is no equality case $K \in \mathcal{K}^n_o$ whose interior lattice points are non-collinear.

Case 2: The interior lattice points of K are collinear.

In the case $\mathrm{G}(\operatorname{int} K) = 1$ equality has been characterized in [3]. In fact, there is a unimodular transformation A such that $AK = C_n$. Therefore, we assume that $\ell = \mathrm{G}(\operatorname{int} K) \geq 3$, and we let L be the line containing the interior lattice points of K. The lattice points of K are distributed in 3^n sets each of which containing only lattice points of a fixed residue class modulo three. Let these sets be labeled R_{ij}, for $i = 1, \ldots, 3^{n-1}$ and $j = 1,2,3$, such that for every lattice line L' parallel to L there is some $i \in \{1, \ldots, 3^{n-1}\}$ so that L' contains only points of R_{ij}, for $j = 1,2,3$. As observed in the

beginning of the proof, each R_{ij} is contained in a line parallel to L. Moreover, if $\#R_{ij} \geq 2$, then between two consecutive points in R_{ij} there are another two lattice points corresponding to the other two residue classes present on the line containing R_{ij}. Hence, R_{i1}, R_{i2} and R_{i3} have to be contained in the same line which contains at most $\ell + 2 = \mathrm{G}(\operatorname{int} K) + 2$ lattice points of K in total. Note, that there cannot be some $i \in \{1, \dots, 3^{n-1}\}$ such that $\#R_{ij} \leq 1$, for all $j = 1, 2, 3$, because this would imply

$$\mathrm{G}(K) = \sum_{i=1}^{3^{n-1}} \sum_{j=1}^{3} \#R_{ij} \leq \sum_{i=1}^{3^{n-1}-1} (\ell + 2) + 3 < 3^{n-1}(\ell + 2) = \mathrm{G}(K),$$

a contradiction. Thus, for every $i \in \{1, \dots, 3^{n-1}\}$ there is a line L_i parallel to L containing all the points in R_{ij}, $j = 1, 2, 3$, and this line must contain exactly $\ell + 2$ lattice points of K in order for K to attain equality in Theorem 1.1 i). Since ℓ is odd, we can write $L_i = z_i + L$, where $z_i \in K \cap \mathbb{Z}^n$ is the midpoint of $L_i \cap K \cap \mathbb{Z}^n$. Without loss of generality, we let $z_1 = 0$, and hence $L_1 = L$.

We now claim that $H = \operatorname{lin}\{z_i : i = 1, \dots, 3^{n-1}\}$ is $(n-1)$-dimensional. To this end, we let $v \in L \cap \mathbb{Z}^n \setminus \{0\}$ be of minimal length and we relabel the z_i such that $z_2, \dots, z_n$ are linearly independent. This is always possible since $K \cap \mathbb{Z}^n$ is n-dimensional. The points $((\ell + 1)/2)v \pm z_i$, $i = 1, \dots, n$, are lattice points of K and $((\ell + 1)/2)v$ is contained in the relative interior of $\operatorname{conv}\{((\ell + 1)/2)v \pm z_i : i = 2, \dots, n\}$, but it is not an interior lattice point of K. Let $H' = \operatorname{lin}\{z_2, \dots, z_n\}$ and assume that there is some $k \in \{1, \dots, 3^{n-1}\}$ such that $z_k = u + \lambda v$, for some $u \in H'$ and, without loss of generality, some $\lambda > 0$. Then, $((\ell + 1)/2)v + z_k$ is strictly separated from the origin by the hyperplane $((\ell + 1)/2)v + H'$. As a consequence, we have

$$((\ell + 1)/2)v \in \operatorname{int} \operatorname{conv}\{((\ell + 1)/2)v \pm z_i : i \in \{1, \dots, n\} \cup \{k\}\} \subset \operatorname{int} K,$$

a contradiction. So we have $H' = H$, which proves the claim.

Since K is convex, $Q = \operatorname{conv}\{R_{ij} : i = 1, \dots, 3^{n-1}, j = 1, 2, 3\} \subseteq K$. Moreover, Q is a prism with basis parallel to H and height $(\ell + 1)\|v\|$ in the direction $L = \operatorname{lin}\{v\}$. Observe that none of the lines $z_i + L$, for $i > 1$, intersects K nor Q in the interior, because otherwise we would find interior lattice points of K outside L. In order to finish the proof, let us consider $Q' = \operatorname{conv}\{z_i \pm v : i = 1, \dots, 3^{n-1}\}$. We clearly have $\mathrm{G}(\operatorname{int} Q') = 1$ and $\mathrm{G}(Q') = 3^n$, and thus there exists a unimodular transformation A such that $AQ' = C_n$. Since A maps parallel lines to parallel lines, up to a suitable rotation, we have $AQ = C_{n-1} \times [-(\ell + 1)/2, (\ell + 1)/2]$. We finally remark that $Q = K$. If this would not be the case, then let $p \in K \setminus Q$ be strictly separated from Q by a hyperplane parallel to the facet of Q containing $A^{-1}e_1, \dots, A^{-1}e_{n-1}$, or $A^{-1}((\ell + 1)/2)e_n$ in its relative interior. Here, for $i = 1, \dots, n$, the ith coordinate unit vector is denoted by e_i, and it is the center of a suitable facet of C_n. In any of the cases above, $\operatorname{conv}\{p, Q\}$ and thus also K would contain the respective point in its interior, arriving again to a contradiction. Hence $Q = K$ as desired. □

References

1. Gennadiy Averkov, Jan Krümpelmann, and Benjamin Nill, *Largest integral simplices with one interior integral point: Solution of Hensley's conjecture and related results*, http://arxiv.org/abs/1309.7967, 2014.
2. Ulrich Betke, Martin Henk, and Jörg M. Wills, *Successive-minima-type inequalities*, Discrete Comput. Geom. **9** (1993), no. 2, 165–175.
3. Jan Draisma, Tyrrell B. McAllister, and Benjamin Nill, *Lattice-width directions and Minkowski's 3^d-theorem*, SIAM J. Discrete Math. **26** (2012), no. 3, 1104–1107.
4. Gregory A. Freiman, Aladár Heppes, and Béla Uhrin, *A lower estimation for the cardinality of finite difference sets in R^n*, Number theory, Vol. I (Budapest, 1987), Colloq. Math. Soc. János Bolyai, vol. 51, North-Holland, Amsterdam, 1990, pp. 125–139.
5. Peter M. Gruber, *Convex and Discrete Geometry*, Grundlehren der Mathematischen Wissenschaften, vol. 336, Springer-Verlag, Berlin, 2007.
6. Peter M. Gruber and Cornelis G. Lekkerkerker, *Geometry of Numbers*, second ed., North-Holland Mathematical Library, vol. 37, North-Holland Publishing Co., Amsterdam, 1987.
7. Hermann Minkowski, *Geometrie der Zahlen*, Bibliotheca Mathematica Teubneriana, Teubner, Leipzig-Berlin, 1896, reprinted by Johnson Reprint Corp., New York, 1968.
8. Oleg Pikhurko, *Lattice points in lattice polytopes*, Mathematika **48** (2001), no. 1–2, 15–24.
9. Imre Z. Ruzsa, *Additive combinatorics and geometry of numbers*, Proceedings of the International Congress of Mathematicians, vol. 3, 2006, pp. 911–930.
10. Paul R. Scott, *On convex lattice polygons*, Bulletin of the Australian Mathematical Society **15** (1976), no. 3, 395–399.
11. Yonutz V. Stanchescu, *On finite difference sets*, Acta Math. Hungar. **79** (1998), no. 1-2, 123–138.
12. ———, *An upper bound for d-dimensional difference sets*, Combinatorica **21** (2001), no. 4, 591–595.
13. Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.
14. Johannes G. van der Corput, *Verallgemeinerung einer Mordellschen Beweismethode in der Geometrie der Zahlen II*, Acta Arith. **2** (1936), 145–146.

Departamento de Matemáticas, Universidad de Murcia, Campus de Espinardo, 30100-Murcia, Spain

E-mail address: bgmerino@gmail.com

Institut für Informatik, Freie Universität Berlin, Takustrasse 9, 14195 Berlin, Germany

E-mail address: matthias.henze@fu-berlin.de