COVERING LATTICE POINTS BY SUBSPACES

IMRE BÁRÁNY, GERGELY HARCOS, JÁNOS PACH, GÁBOR TARDOS

ABSTRACT. We find tight estimates for the minimum number of proper subspaces needed to cover all lattice points in an n-dimensional convex body $\mathcal{C}$, symmetric about the origin 0. This enables us to prove the following statement, which settles a problem of G. Halász. The maximum number of n-wise linearly independent lattice points in the n-dimensional ball $r\mathcal{B}^n$ of radius r around 0 is $O(r^{n/(n-1)})$. This bound cannot be improved. We also show that the order of magnitude of the number of different $(n-1)$-dimensional subspaces induced by the lattice points in $r\mathcal{B}^n$ is $r^{n(n-1)}$.

1. INTRODUCTION AND STATEMENT OF RESULTS

This paper was inspired by the following question of G. Halász. *What is the maximal cardinality of a subset S of $r\mathcal{B}^n \cap \mathbb{Z}^n$ such that all n-element subsets of S are linearly independent?* (Here $\mathcal{B}^n$ denotes the unit ball around the origin in $\mathbb{R}^n$.) As any system of proper subspaces that cover $r\mathcal{B}^n \cap \mathbb{Z}^n$ provides an upper bound on the above quantity, we would like to determine the size of the *smallest* such covering system. We look at these questions from a somewhat broader perspective.

We introduce the following notations. Let $\mathcal{C} \subseteq \mathbb{R}^n$ be a convex compact body symmetric with respect to the origin. For $1 \leq i \leq n$, let λ_i denote the i-th *successive minimum* of $\mathcal{C}$. That is,

$$\lambda_i = \min\{\lambda \mid \dim(\lambda\mathcal{C} \cap \mathbb{Z}^n) \geq i\}.$$

Let $g(\mathcal{C})$ denote the minimum number of proper subspaces covering $\mathcal{C} \cap \mathbb{Z}^n$, and let $h(\mathcal{C})$ denote the maximum number of points that can be chosen from $\mathcal{C} \cap \mathbb{Z}^n$ so that they are in *general position*, i.e., no n of them are linearly dependent. Clearly, we have $h(\mathcal{C}) \leq (n-1)g(\mathcal{C})$.

The following two theorems, providing a lower bound on $h(\mathcal{C})$ and an upper bound on $g(\mathcal{C})$, respectively, give fairly tight estimates for these quantities.

1991 *Mathematics Subject Classification.* Primary 11H06; Secondary 52C07.

Key words and phrases. lattices, convex bodies, successive minima, covering by subspaces.

First author supported by grant T020914 of the Hungarian National Foundation for Scientific Research (OTKA)

Second author supported by grant 220/1762 of Soros Foundation, Budapest

Third author supported by NSF grant CCR-9732101, a PSC-CUNY Research Award, and grant T020914 of the Hungarian National Foundation for Scientific Research (OTKA)

Fourth author supported by grants T029255 and T030059 of the Hungarian National Foundation for Scientific Research (OTKA), and grant FKFP 0607/1999 of the Hungarian Ministry of Education

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

Theorem 1. *If $\lambda_n \leq 1$ then*

$$h(\mathcal{C}) \geq \frac{1-\lambda_n}{16n^2} \min_{0<m<n} (\lambda_m \dots \lambda_n)^{-\frac{1}{n-m}}.$$

Theorem 2. *If $\lambda_n \leq 1$ then*

$$g(\mathcal{C}) \leq c 2^n n^2 \log n \min_{0<m<n} (\lambda_m \dots \lambda_n)^{-\frac{1}{n-m}},$$

where c is an absolute constant.

In Halász' question, $\mathcal{C}$ is the n-dimensional ball, $r\mathcal{B}^n$, of radius $r > 1$ around the origin, whose successive minima satisfy $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 1/r$. Thus, in this case, Theorems 1 and 2 immediately imply that the correct orders of magnitude of both $g(r\mathcal{B}^n)$ and $h(r\mathcal{B}^n)$ are $O(r^{n/(n-1)})$.

Remark 1. If $\lambda_n > 1$, then $g(\mathcal{C}) = 1$ and hence $h(\mathcal{C}) < n$. If $\lambda_n < 1-\epsilon$, by Theorems 1 and 2 the values of $g(\mathcal{C})$ and $h(\mathcal{C})$ are determined by the successive minima of $\mathcal{C}$ up to a constant factor depending on ϵ and the dimension n. For $\lambda_n = 1$ no such approximation is possible. For arbitrary large $x > 1$, consider the convex bodies

$$\mathcal{C}_x = [-x, x]^{n-1} \times [-1, 1]$$

and

$$\mathcal{C}'_x = \operatorname{conv}(\{-xe_i, xe_i | 1 \leq i < n\} \cup \{-e_n, e_n\}),$$

where $(e_1, \ldots, e_n)$ is the standard basis of $\mathbb{Z}^n$. Both bodies have the same sequence of successive minima: $\lambda_i = 1/x$ for $i < n$ and $\lambda_n = 1$. However, $g(\mathcal{C}_x) \geq 2x$ and $h(\mathcal{C}_x) \geq x/2$, while $g(\mathcal{C}'_x) = 2$ and $h(\mathcal{C}'_x) = n$.

Remark 2. The integer lattice $\mathbb{Z}^n$ plays no particular role in the above theorems. Our inequalities are preserved by affine transformations, therefore they hold for n-dimensional lattices in general.

For any $r > 1$, let $\mathcal{H}_r$ denote the set of all $(n-1)$-dimensional subspaces (hyperplanes through 0) which contain $n-1$ linearly independent lattice points from the ball of radius r centered at the origin.

Theorem 3. *There exist suitable positive constants c_1 and c_2, depending only on n, such that*

$$c_1 r^{n(n-1)} \leq |\mathcal{H}_r| \leq c_2 r^{n(n-1)},$$

provided that r is large enough.

Analyzing the dependence of c_1 and c_2 on n, one can deduce the following result on

$$s_r = \frac{1}{|\mathcal{H}_r|} \sum_{H \in \mathcal{H}_r} |H \cap r\mathcal{B}^n \cap \mathbb{Z}^n|,$$

the average number of lattice points in $r\mathcal{B}^n$ in the hyperplanes belonging to $\mathcal{H}_r$.

Corollary. *There is an absolute constant c_3 such that*

$$\overline{\lim}_{r\to\infty} s_r \leq 2^{n^2+c_3 n}.$$

In Section 2, we essentially show that within $\mathcal{C}\cap\mathbb{Z}^n$ one can represent a finite projective space over a relatively small prime (see Lemma). To establish Theorem 1, we combine this result with a well known construction of P. Erdős (see [11, Appendix]).

Section 3 contains the proof of Theorem 2. This proof is also constructive: in most cases, to cover $\mathcal{C}\cap\mathbb{Z}^n$ we take all subspaces perpendicular to an integer vector in a body homothetic to the polar of $\mathcal{C}$.

The proof of Theorem 3 is given in Section 4.

The related (but different) problem of covering the lattice points within a convex body by *affine* subspaces was first investigated by K. Bezdek and T. Hausel [2]. They only considered 1-codimensional subspaces, i.e. hyperplanes (as we do here). Their work was sharpened and extended to the general case by I. Talata [14]. The estimates in these two papers are given in terms of the dimension n and the lattice width of the convex body.

2. Proof of Theorem 1

The proof is based on the following

Lemma. *Let $\lambda_n < 1$ and suppose that p is an integer satisfying*

$$1 < p < \frac{1-\lambda_n}{8n^2} \min_{0<m<n} (\lambda_m \ldots \lambda_n)^{-\frac{1}{n-m}}.$$

Then, for any $v \in \mathbb{R}^n$, there exist an integer $1 \leq j < p$ and a lattice point $w \in \mathbb{Z}^n$ with $jv + pw \in \mathcal{C}$.

Proof of Lemma. Find linearly independent vectors $v_i \in \lambda_i\mathcal{C}\cap\mathbb{Z}^n$ for $i = 1, \ldots, n$. Any vector $x \in \mathbb{R}^n$ can be uniquely written in the form $x = \sum_{i=1}^n a_i v_i + \sum_{i=1}^n b_i v_i$ with $a_i \in \mathbb{Z}$ and $b_i \in (-1/2, 1/2]$. Here $\sum_{i=1}^n a_i v_i \in \mathbb{Z}^n$ and

$$\sum_{i=1}^n b_i v_i \in \operatorname{conv}\left\{ \frac{v_i}{2p\lambda_i}, -\frac{v_i}{2p\lambda_i} \middle| 1 \leq i \leq n \right\} \subseteq \frac{\mathcal{C}}{2p},$$

whenever $\sum_{i=1}^n \lambda_i |b_i| \leq 1/(2p)$. Thus, the density d of the periodic set

$$S = \frac{\mathcal{C}}{2p} + \mathbb{Z}^n$$

is at least the probability that for independent uniform random numbers $b_i \in [0, 1/2]$ we have $\sum_{i=1}^n \lambda_i b_i \leq 1/(2p)$. This inequality is satisfied if $\lambda_i b_i \leq \epsilon/(2pn)$ for all $i < n$ and $\lambda_n b_n < (1-\epsilon)/(2p)$, where $\epsilon = (1-\lambda_n)/2$. Thus, we have

$$d \geq \min\left(1, \frac{1-\epsilon}{p\lambda_n}\right) \prod_{i=1}^{n-1} \min\left(1, \frac{\epsilon}{pn\lambda_i}\right).$$

This lower bound on d takes the form

$$A_m = \prod_{m \le i < n} \frac{\epsilon}{pn\lambda_i}$$

or

$$B_m = \frac{1-\epsilon}{p\lambda_n} \prod_{m \le i < n} \frac{\epsilon}{pn\lambda_i} ,$$

where $1 \le m \le n$ is an appropriate integer (the product is empty in case $m = n$).

We claim that each of these values is larger than $1/p$, so we have $d > 1/p$. The inequality $B_m > 1/p$ is equivalent to

$$p^{n-m} < \frac{(1-\epsilon)\epsilon^{n-m}}{n^{n-m}\lambda_m \dots \lambda_n}.$$

This is true, by the choice of ϵ, for $m = n$, and, by our bound on p, otherwise. The inequality $A_m > 1/p$ is equivalent to

$$C_m = p^{n-m-1}\lambda_m \dots \lambda_{n-1} < \left(\frac{\epsilon}{n}\right)^{n-m}.$$

If $m = n$, this is true, because $p > 1$. Suppose $m < n$, and use our bound on p to get

$$C_m < \frac{1}{p\lambda_n}\left(\frac{\epsilon}{4n^2}\right)^{n-m}.$$

If $\lambda_n \ge 1/2$ then $p\lambda_n \ge 1$, hence the desired inequality follows. If $\lambda_n < 1/2$ then $\epsilon > 1/4$, hence the previous inequality yields

$$C_m < \frac{1}{p\lambda_n}\left(\frac{\epsilon}{n}\right)^{n-m+1}.$$

On the other hand, using the monotonicity of the sequence (λ_i), we obtain

$$C_m \le p^{n-m-1}\lambda_n^{n-m} < (p\lambda_n)^{n-m}.$$

Taking a weighted geometric mean of the last two bounds, we get

$$C_m < \left\{\frac{1}{p\lambda_n}\left(\frac{\epsilon}{n}\right)^{n-m+1}\right\}^{\frac{n-m}{n-m+1}} \left\{(p\lambda_n)^{n-m}\right\}^{\frac{1}{n-m+1}} = \left(\frac{\epsilon}{n}\right)^{n-m},$$

as required. This proves $A_m > 1/p$ and hence $d > 1/p$.

Consider the periodic sets $S + jv/p$ for $j = 0, \dots, p-1$. Each of these p sets have density $d > 1/p$ thus two of these sets must intersect. We have

$$\frac{j_1 v}{p} + \frac{u_1}{2p} + w_1 = \frac{j_2 v}{p} + \frac{u_2}{2p} + w_2,$$

for some $0 \le j_1 < j_2 < p$, some $u_1, u_2 \in \mathcal{C}$ and some $w_1, w_2 \in \mathbb{Z}^n$. For $1 \le j = j_2 - j_1 < p$ and $w = w_2 - w_1 \in \mathbb{Z}^n$, we have

$$jv + pw = \frac{u_1 - u_2}{2} \in \mathcal{C},$$

verifying the statement of the Lemma. □

Now it is easy to finish the proof of Theorem 1. Let p be the largest prime number satisfying the condition in the Lemma. If such a prime does not exist, then the statement of the theorem is trivial. The points of the *discrete moment curve* (used by Erdős in connection with Heilbronn's triangle problem [11]), $v_i = (1, i, i^2, \dots, i^{n-1})$ for integer values $0 \le i < p$ (and $v_\infty = (0, \dots, 0, 1) \in \mathbb{Z}^n$) are n-wise linearly independent over the p-element field. By the Lemma, we have integers $1 \le j_i < p$ and integer vectors w_i with $v_i' = j_i v_i + p w_i \in \mathcal{C}$. Clearly, the vectors v_i' are integer vectors, and they are n-wise linearly indepent over the p-element field, and hence over the reals. This shows $h(\mathcal{C}) > p$, and an application of Chebyshev's theorem concludes the proof.

3. Proof of Theorem 2

Let $\mathcal{C}^0$ denote the *polar body* of $\mathcal{C}$, i.e.,

$$\mathcal{C}^0 = \{x \in \mathbb{R}^n : ux \le 1 \text{ for all } u \in \mathcal{C}\}.$$

Denote by $\mu_1 \le \dots \le \mu_n$ the successive minima of $\mathcal{C}^0$. It is known that

$$1 \le \lambda_i \mu_{n-i+1} \le c_1 n \log n \quad (i = 1, \dots, n)$$

where c_1 is an absolute constant. The lower bound is a classical inequality of Mahler [10], the upper one has been recently proved by Banaszczyk [1].

Fix any integer $0 < m < n$, for the rest of the argument. It follows that

$$1 \le (\lambda_m \dots \lambda_n)(\mu_1 \dots \mu_{n-m+1}) \le (c_1 n \log n)^{n-m+1}. \tag{1}$$

For technical reasons, we will consider any increasing sequence

$$0 < \nu_1 < \dots < \nu_{n-m+1}$$

such that no ratio ν_i/ν_j $(i \ne j)$ is rational and

$$\mu_i \le \nu_i \quad (i = 1, \dots, n-m+1).$$

Let

$$w_i \in \mu_i \mathcal{C}^0 \cap \mathbb{Z}^n \quad (i = 1, \dots, n-m+1)$$

be linearly independent vectors, and consider some sets of integer vectors of the form

$$\mathcal{D}_\alpha^+ = \left\{ \sum_{i=1}^{n-m+1} a_i w_i : a_i \in [0, \alpha/\nu_i] \cap \mathbb{Z} \right\},$$

$$\mathcal{D}_\alpha = \left\{ \sum_{i=1}^{n-m+1} a_i w_i : a_i \in [-\alpha/\nu_i, \alpha/\nu_i] \cap \mathbb{Z} \right\},$$

where α is a non-negative parameter to be specified later. Clearly, $\mathcal{D}_\alpha$ is the union of 2^{n-m+1} isometric copies of $\mathcal{D}_\alpha^+$ satisfying

$$\mathcal{D}_\alpha \subseteq (n-m+1)\alpha \mathcal{C}^0 \cap \mathbb{Z}^n.$$

Also, the difference of any two vectors from $\mathcal{D}_\alpha^+$ lies in $\mathcal{D}_\alpha$. Let $f(\alpha)$ be the number of points in the first set, i.e.,

$$f(\alpha) = \left|\mathcal{D}_\alpha^+\right| = \prod_{i=1}^{n-m+1} \left(\left\lfloor \frac{\alpha}{\nu_i} \right\rfloor + 1 \right).$$

Notice that $f(\alpha)$ is an increasing, right continuous function which changes by a factor of at most 2 at its points of discontinuity, i.e., for any $\alpha > 0$,

$$f(\alpha) \leq 2f(\alpha-). \tag{2}$$

Also, $f(0) = 1$ and

$$f(\alpha) \geq \prod_{i=1}^{n-m+1} \frac{\alpha}{\nu_i}. \tag{3}$$

We claim that, whenever

$$f(\alpha) > 2(n-m+1)\alpha + 1 \tag{4}$$

holds, every lattice point in $\mathcal{C}$ is perpendicular to some non-zero element of $\mathcal{D}_\alpha$. To see this, fix any $u \in \mathcal{C} \cap \mathbb{Z}^n$ and consider all the scalar products uv where $v \in \mathcal{D}_\alpha^+$. These scalar products are integers, whose absolute values do not exceed $(n-m+1)\alpha$. Therefore, (4) implies the existence of two distinct $v_1, v_2 \in \mathcal{D}_\alpha^+$ with $uv_1 = uv_2$. Hence, the non-zero vector $v = v_1 - v_2 \in \mathcal{D}_\alpha$ is perpendicular to u. We established that (4) implies

$$g(\mathcal{C}) \leq |\mathcal{D}_\alpha| \leq 2^{n-m+1} f(\alpha). \tag{5}$$

By the right continuity of $f(\alpha)$, there is a minimum α such that

$$f(\alpha) \geq 16(n-m+1)^{\frac{n-m+1}{n-m}} (\nu_1 \dots \nu_{n-m+1})^{\frac{1}{n-m}}.$$

By (3), this α satisfies

$$\alpha \leq 4(n-m+1)^{\frac{1}{n-m}} (\nu_1 \dots \nu_{n-m+1})^{\frac{1}{n-m}}.$$

In particular, we have

$$4(n-m+1)\alpha \leq f(\alpha).$$

The inequality $0 < \lambda_m \leq \dots \leq \lambda_n \leq 1$ combined with (1) guarantees that

$$1 \leq \mu_1 \dots \mu_{n-m+1} \leq \nu_1 \dots \nu_{n-m+1},$$

whence also

$$32 \leq f(\alpha).$$

The last two estimates on $f(\alpha)$ show that (4) is satisfied. In particular, $\alpha > 0$, therefore (5) combined with (2) yields

$$g(\mathcal{C}) \leq 2^{n-m+2} f(\alpha-) < 2^{n-m+6} (n-m+1)^{\frac{n-m+1}{n-m}} (\nu_1 \dots \nu_{n-m+1})^{\frac{1}{n-m}}.$$

Taking the infimum of the right hand side over all admissible choices of the sequence $0 < \nu_1 < \cdots < \nu_{n-m+1}$, we get

$$\begin{aligned} g(\mathcal{C}) &\leq 2^{n-m+6}(n-m+1)^{\frac{n-m+1}{n-m}}(\mu_1 \ldots \mu_{n-m+1})^{\frac{1}{n-m}} \\ &\leq 2^{n-m+7} n(\mu_1 \ldots \mu_{n-m+1})^{\frac{1}{n-m}}. \end{aligned}$$

Combining this with (1), we obtain

$$\begin{aligned} g(\mathcal{C}) &\leq 2^{n-m+7} n(c_1 n \log n)^{\frac{n-m+1}{n-m}}(\lambda_m \ldots \lambda_n)^{\frac{1}{n-m}} \\ &\leq 2^{n+7} c_1^2 n^2 \log n \{2^{-m}(n \log n)^{\frac{1}{n-m}}\}(\lambda_m \ldots \lambda_n)^{\frac{1}{n-m}}. \end{aligned}$$

Here

$$2^{-m}(n \log n)^{\frac{1}{n-m}} \leq \max\{(n \log n)^{2/n}, 2^{-n/2} n \log n\}$$

is bounded from above by an absolute constant, hence we can see that

$$g(\mathcal{C}) \leq 2^n c n^2 \log n (\lambda_m \ldots \lambda_n)^{\frac{1}{n-m}},$$

where c is some absolute constant. Minimizing over all integers $0 < m < n$, Theorem 2 follows.

4. Proof of Theorem 3

The upper bound follows at once by noting that

$$|\mathcal{H}_r| \leq \binom{|r\mathcal{B}^n \cap \mathbb{Z}^n|}{n-1} = \binom{O(r^n)}{n-1} = O(r^{n(n-1)}).$$

For any primitive integer vector v, let $\mathcal{L}(v)$ stand for the $(n-1)$-dimensional lattice $\mathbb{Z}^n \cap v^\perp$ orthogonal to v, with determinant $\det \mathcal{L}(v) = |v|$. Write $\lambda_1(v) \leq \cdots \leq \lambda_{n-1}(v)$ for the successive minima of $\mathcal{L}(v)$, i.e.,

$$\lambda_i(v) = \min\{\lambda | \dim(\lambda\mathcal{B}^n \cap \mathcal{L}(v)) \geq i\}.$$

Denote by ω_n the volume of the unit ball $\mathcal{B}^n$. According to Minkowski's second fundamental theorem, we have

$$\lambda_1(v) \ldots \lambda_{n-1}(v) \leq 2^{n-1}\omega_{n-1}^{-1}|v|. \tag{6}$$

Define a set V by

$$V = \{v \in \mathbb{Z}^n \colon v \text{ is primitive and } |v| \leq \rho\},$$

where ρ will be specified later.

Claim. *If ρ is large enough, there are at least $\omega_n \rho^n/10$ elements $v \in V$ such that $\lambda_1(v) \geq D\rho^{\frac{1}{n-1}}$, where $D > 0$ is a suitable constant depending on n.*

Before proving the Claim, we show how it implies the lower bound in Theorem 3. By (6), whenever $\lambda_1(v) \geq D\rho^{\frac{1}{n-1}}$, we have

$$\lambda_{n-1}(v) \leq 2^{n-1}\omega_{n-1}^{-1}|v|(D\rho^{\frac{1}{n-1}})^{-(n-2)} \leq 2^{n-1}\omega_{n-1}^{-1}D^{-(n-2)}\rho^{\frac{1}{n-1}}.$$

So, for at least $\omega_n \rho^n/10$ elements $v \in V$, $\mathcal{L}(v)$ contains $n-1$ linearly independent lattice points from the ball of radius $r = 2^{n-1}\omega_{n-1}^{-1}D^{-(n-2)}\rho^{\frac{1}{n-1}}$. From here ρ can be expressed as a function of r, and the lower bound in Theorem 3 follows.

Proof of Claim. We shall assume throughout this argument that ρ is sufficiently large in terms of n. The inequality $\lambda_1(v) \leq D\rho^{\frac{1}{n-1}}$ is equivalent to the existence of a primitive $u \in \mathbb{Z}^n$ with $vu = 0$ and $|u| \leq D\rho^{\frac{1}{n-1}}$. In other words, $v \in \mathcal{L}(u)$ for some primitive u with $|u| \leq D\rho^{\frac{1}{n-1}}$. For any primitive u with $|u| \leq D\rho^{\frac{1}{n-1}}$, we estimate the number of corresponding vectors v.

Using (6) we can see that $\lambda_{n-1}(u) \leq 2^{n-1}\omega_{n-1}^{-1}D\rho^{\frac{1}{n-1}} = o(\rho)$ which implies that $\mathcal{L}(u)$ contains a lattice parallelotope of nonzero volume and of diameter $o(\rho)$. Therefore the number of corresponding vectors v is at most

$$|\mathcal{L}(u) \cap \rho\mathcal{B}^n| \leq 2\mathrm{vol}(\rho\mathcal{B}^{n-1})/\det\mathcal{L}(u) = 2\omega_{n-1}\rho^{n-1}/|u|.$$

Hence the total number of $v \in V$ with $\lambda_1(v) \leq D\rho^{\frac{1}{n-1}}$ is at most

$$2\omega_{n-1}\rho^{n-1} \sum_{|u| \leq D\rho^{\frac{1}{n-1}}} \frac{1}{|u|} \leq 4\omega_{n-1}\omega_n D^{n-1}\rho^n,$$

as can be shown by a straightforward calculation. The total number of points in V is at least $\frac{1}{2\zeta(n)}\omega_n\rho^n$. Thus, the number of $v \in V$ with $\lambda_1(v) \geq D\rho^{\frac{1}{n-1}}$ is at least

$$\left(\frac{1}{2\zeta(n)} - 4\omega_{n-1}D^{n-1}\right)\omega_n\rho^n,$$

which is larger than $\omega_n\rho^n/10$ if the constant D is chosen properly. $\square$

Proof of Corollary. Let $c_3, c_4, \ldots$ denote absolute constants in this proof. We shall also assume that r is sufficiently large in terms of n. By looking at the proof of Theorem 3 we can see that an admissible choice for D is provided by

$$D^{n-1}\omega_{n-1} = \frac{1}{16\zeta(n)}.$$

Therefore

$$D \leq c_4 n^{1/2}$$

as follows from the explicit formula

$$\omega_{n-1} = \frac{\pi^{\frac{n-1}{2}}}{\Gamma\left(\frac{n+1}{2}\right)}.$$

Then ρ of the previous proof is defined by

$$r = 2^{n-1}\omega_{n-1}^{-1}D^{-(n-2)}\rho^{\frac{1}{n-1}} = 2^{n+3}\zeta(n)D\rho^{\frac{1}{n-1}}$$

which shows that

$$\rho \geq (c_5 2^{-n}n^{-1/2}r)^{n-1}.$$

Therefore

$$|\mathcal{H}_r| \geq \omega_n\rho^n/10 \geq c_6^n n^{-n/2}\rho^n \geq c_7^{n^2}2^{-n^3}n^{-n^2/2}r^{n(n-1)}. \tag{7}$$

Every $(n-1)$-element subset of $r\mathcal{B}^n \cap \mathbb{Z}^n$ is contained in a unique hyperplane $H \in \mathcal{H}_r$, i.e.,

$$\sum_{H\in\mathcal{H}_r} \binom{|H \cap r\mathcal{B}^n \cap \mathbb{Z}^n|}{n-1} = \binom{|r\mathcal{B}^n \cap \mathbb{Z}^n|}{n-1}.$$

By using the convexity of $x \mapsto \binom{x}{n-1}$ on $[n-2, \infty)$ we can deduce that

$$|\mathcal{H}_r|\binom{s_r}{n-1} \leq \binom{|r\mathcal{B}^n \cap \mathbb{Z}^n|}{n-1},$$

i.e., (7) combined with

$$|r\mathcal{B}^n \cap \mathbb{Z}^n| \leq 2\omega_n r^n \leq c_8^n n^{-n/2}r^n$$

shows that

$$c_7^{n^2}2^{-n^3}n^{-n^2/2}r^{n(n-1)}\binom{s_r}{n-1} \leq c_8^{n^2}n^{-n^2/2}r^{n(n-1)}.$$

In other words,

$$\binom{s_r}{n-1} \leq 2^{n^3}c_9^{n^2}$$

which implies

$$s_r \leq 2^{n^2+c_3 n}$$

as required. □

5. Epilogue

Halász' question studied in this paper is related to the following famous problem of Littlewood and Offord [9]. *Given k not necessarily distinct complex numbers, $v_1, v_2, \ldots, v_k$, whose absolute values are at least 1, at most how many of the 2^k subset sums $\sum_{i\in I} v_i$, $I \subseteq \{1, 2, \ldots, k\}$ can belong to the same open ball of unit diameter?*

Erdős [3] proved that for reals the best possible upper bound was $\binom{k}{\lfloor k/2\rfloor}$. G. O. H. Katona [6] and D. Kleitman [7] independently settled the original question by showing that the same bound is valid for complex numbers. Shortly after, Kleitman [8] managed to generalize this theorem to systems of vectors of absolute value at least 1 in any Euclidean space $\mathbb{R}^n$. In all cases, the upper bound is attained when all vectors (numbers) coincide.

Erdős and Moser considered the similar problem of haw many subset sums of k *distinct* numbers can coincide. A. Sárközy, E. Szemerédi [12] found the order of the magnitude of this number and later R. Stanley [13] found the exact answer. G. Halász [5] considered the similar problem of how many subset sums can coincide under various assumptions assuring that the k vectors are quite different. J. Griggs and G. Rote [4] investigated the following problem of this type. *Given k n-wise linearly independent vectors $v_1, v_2, \dots, v_k \in \mathbb{R}^n$, at most how many of the 2^k subset sums $\sum_{i\in I} v_i$, $I \subseteq \{1, 2, \dots, k\}$ can coincide?* Denoting this function by $f_n(k)$, they obtained that

$$f_n(k) > C_n \frac{2^k}{k^{3n/2-1}},$$

and it is implicit in Halász [5] that

$$f_n(k) < C'_n \frac{2^k}{k^{n/2+\lfloor n/2 \rfloor}}.$$

(Here C_n and C'_n are positive constants depending only on the dimension n.) The orders of magnitude of these two bounds differ already in 3-space ($n = 3$).

Note that the construction of Griggs and Rote [4] can be regarded as the special case of our construction at the end of Section 2, when $\mathcal{C}$ is a box of the form $[0, 1] \times [0, x]^{n-1}$.

Halász observed that the construction in [4] can be extended to give the following result. Let $h_n(r)$ denote the maximum number of n-wise linearly independent lattice points that can be chosen in $r\mathcal{B}^n$. Let $r(k)$ be the smallest r for which $h_n(r) \geq k$. Then

$$f_n(k) > C''_n \frac{2^k}{k^{n/2} r^n(k)}.$$

This would improve on the previous lower bound, provided that $r(k) = o(k^{(n-1)/n})$, or, equivalently,

$$\lim_{r\to\infty} \frac{h_n(r)}{r^{n/(n-1)}} = \infty.$$

However, the results in this paper show that this is not the case.

With the exception of Erdős, all Hungarian mathematicians mentioned in this section (Gábor Halász, Gyula Katona, András Sárközy, Endre Szemerédi) recently have turned or will turn *sixty*. We congratulate them with this note.

References

[1] Banaszczyk, W., *Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$. II. Application of K-convexity*, Discrete Comput. Geom. **16** (1996), 305–311.

[2] Bezdek, K. and Hausel, T., *On the number of lattice hyperplanes which are needed to cover the lattice points of a convex body*, Intuitive geometry (Szeged, 1991) (Colloq. Math. Soc. János Bolyai 63), North-Holland, Amsterdam, 1994, pp. 27–31.

[3] Erdős, P., *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.

[4] Griggs J. and Rote, G., *On the distribution of sums of vectors in general position*, DIMACS Series in Discrete Mathematics 49 (Contemporary Trends in Discrete Mathematics), Amer. Math. Soc., Providence, Rhode Island, 1999, pp. 139–142.

[5] Halász, G., *Estimates for the concentration function of combinatorial number theory and probability*, Period. Math. Hungar. **8** (1977), 197–211.

[6] Katona, G., *On a conjecture of Erdős and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar. **1** (1966), 59–63.

[7] Kleitman, D. J., *On a lemma of Littlewood and Offord on the distribution of certain sums*, Math. Z. **90** (1965), 251–259.

[8] Kleitman, D. J., *On a lemma of Littlewood and Offord on the distribution of linear combinations of vectors*, Adv. Math. **5** (1970), 155-157.

[9] Littlewood, J. and Offord, C., *On the number of real roots of a random algebraic equation. III*, Mat. Sb. **12** (1943), 277–285.

[10] Mahler, K., *Ein Übertragungsprinzip für konvexe Körper*, Časopis Pěst. Mat. Fys. **68** (1939), 93–102. (German)

[11] Roth, K. F., *On a problem of Heilbronn*, J. London Math. Soc. **26** (1951), 198–204.

[12] Sárközy, A. and Szemerédi, E., *Über ein Problem von Erdős und Moser*, Acta Arith. **11** (1965), 205–208.

[13] Stanley, R., *Weyl groups, the hard Lefschetz theorem, and the Sperner property*, SIAM J. Algebraic Discrete Methods **1** (1980), 168–184.

[14] Talata, I., *Covering the lattice points of a convex body with affine subspaces*, Intuitive geometry (Budapest, 1995) (Bolyai Soc. Math. Stud. 6), János Bolyai Math. Soc., Budapest, 1997, pp. 429–440.

Rényi Institute of the Hungarian Academy of Sciences, POB 127, H-1364 Budapest, Hungary and Department of Mathematics, University College London, Gower Street, London WC1E 6BT, England

E-mail address: `barany@math-inst.hu`

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544, USA

E-mail address: `gharcos@math.princeton.edu`

Rényi Institute of the Hungarian Academy of Sciences, POB 127, H-1364 Budapest, Hungary and Courant Institute, 251 Mercer Street, New York, NY 10012, USA

E-mail address: `pach@cims.nyu.edu`

Rényi Institute of the Hungarian Academy of Sciences, POB 127, H-1364 Budapest, Hungary

E-mail address: `tardos@math-inst.hu`