Journal of Functional Analysis 285 (2023) 110122

Contents lists available at ScienceDirect

Journal of Functional Analysis

journal homepage: www.elsevier.com/locate/jfa

Full Length Article

An integer parallelotope with small surface area ☆

Assaf Naor [a,*], Oded Regev [b]

[a] *Mathematics Department, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA*
[b] *Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY 10012, USA*

ARTICLE INFO

Article history:
Received 17 January 2023
Accepted 31 July 2023
Available online 9 August 2023
Communicated by E. Milman

Keywords:
Integer lattice
Surface area
Tiling bodies

ABSTRACT

We prove that for any $n \in \mathbb{N}$ there is a convex body $K \subseteq \mathbb{R}^n$ whose surface area is at most $n^{\frac{1}{2}+o(1)}$, yet the translates of K by the integer lattice $\mathbb{Z}^n$ tile $\mathbb{R}^n$.

1. Introduction

Given $n \in \mathbb{N}$ and a lattice $\Lambda \subseteq \mathbb{R}^n$, a convex body $K \subseteq \mathbb{R}^n$ is called a Λ-parallelotope (e.g., [12]) if the translates of K by elements of Λ tile $\mathbb{R}^n$, i.e., $\mathbb{R}^n = \Lambda + K = \bigcup_{x\in\Lambda}(x+K)$, and the interior of $(x+K)\cap(y+K)$ is empty for every distinct $x, y \in \Lambda$. One calls K a parallelotope (parallelogon if $n = 2$ and parallelohedron if $n = 3$; some of the literature calls a parallelotope in $\mathbb{R}^n$ an n-dimensional parallellohedron; e.g., [1,11]) if

☆ A.N. was supported by NSF grant DMS-2054875, BSF grant 201822, and a Simons Investigator award (882965). O.R. was supported by NSF grant CCF-1320188 and a Simons Investigator award (623489).
* Corresponding author.
E-mail addresses: naor@math.princeton.edu (A. Naor), regev@cims.nyu.edu (O. Regev).

https://doi.org/10.1016/j.jfa.2023.110122
0022-1236/

it is a Λ-parallelotope for some lattice $\Lambda \subseteq \mathbb{R}^n$. We call a $\mathbb{Z}^n$-parallelotope an integer parallelotope.

The hypercube $[-\frac{1}{2}, \frac{1}{2}]^n$ is an integer parallelotope whose surface area equals $2n$. By [16, Corollary A.2], for every $n \in \mathbb{N}$ there exists an integer parallelotope $K \subseteq \mathbb{R}^n$ whose surface area is smaller than $2n$ by a universal constant factor. Specifically, the surface area of the integer parallelotope K that was considered in [16] satisfies $\mathrm{vol}_{n-1}(\partial K) \leqslant \sigma(n + O(n^{2/3}))$, where $\sigma = 2\sum_{s=1}^{\infty}(s/e)^s/(s^{3/2}s!) \leqslant 1.23721$. To the best of our knowledge, this is the previously best known upper bound on the smallest possible surface area of an integer parallelotope. The main result of the present work is the following theorem:

Theorem 1. *For every $n \in \mathbb{N}$ there exists an integer parallelotope whose surface area is $n^{\frac{1}{2}+o(1)}$.*

Because the covolume of $\mathbb{Z}^n$ is 1, the volume of any integer parallelotope $K \subseteq \mathbb{R}^n$ satisfies $\mathrm{vol}_n(K) = 1$. Consequently, by the isoperimetric inequality we have[1]

$$\mathrm{vol}_{n-1}(\partial K) \geqslant \frac{\mathrm{vol}_{n-1}(S^{n-1})}{\mathrm{vol}_n(B^n)^{\frac{n-1}{n}}} \asymp \sqrt{n}, \tag{1}$$

where $B^n \stackrel{\mathrm{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{R}^n : \ x_1^2 + \cdots + x_n^2 \leqslant 1\}$ denotes the Euclidean ball and $S^{n-1} \stackrel{\mathrm{def}}{=} \partial B^n$.

Thanks to (1), Theorem 1 is optimal up to the implicit lower order factor. It remains open to determine whether this lower-order factor could be removed altogether, namely to answer the following question:

Question 2. *For every $n \in \mathbb{N}$, does there exist an integer parallelotope $K \subseteq \mathbb{R}^n$ with $\mathrm{vol}_{n-1}(\partial K) \asymp \sqrt{n}$?*

Early investigations in the context of Question 2 focused on exact minimizers in low dimensions. The smallest possible perimeter of a unit-area parallelogon in $\mathbb{R}^2$ was evaluated in [17] and the smallest possible perimeter of an integer parallelogon in $\mathbb{R}^2$ was evaluated in [7]. The corresponding questions for parallelohedra in $\mathbb{R}^3$ remain open (though see [28] for a recent exact solution of a different isoperimetric-type question for parallelohedra); for example, Conjecture 7.5 in [5] asks for the smallest possible surface area of a unit volume parallelohedron in $\mathbb{R}^3$ (and proposes a conjectural minimizer). A lot of effort has also been devoted to the analogous questions (exact minimizers when

[1] We use the following conventions for asymptotic notation, in addition to the usual $O(\cdot), o(\cdot), \Omega(\cdot), \Theta(\cdot)$ notation. For $a, b > 0$, by writing $a \lesssim b$ or $b \gtrsim a$ we mean that $a \leqslant Cb$ for a universal constant $C > 0$, and $a \asymp b$ stands for $(a \lesssim b) \wedge (b \lesssim a)$. If we need to allow for dependence on parameters, we indicate it by subscripts. For example, in the presence of an auxiliary parameter ε, the notation $a \lesssim_\varepsilon b$ means that $a \leqslant C(\varepsilon)b$, where $C(\varepsilon) > 0$ may depend only on ε, and analogously for $a \gtrsim_\varepsilon b$ and $a \asymp_\varepsilon b$.

$n \in \{2, 3\}$) for tiling bodies that need not be convex, see [22] for the exact solution in this setting when $n = 2$, whereas the corresponding question when $n = 3$ remains open; see [24,39,4].

While the higher dimensional asymptotic nature of Question 2 differs from the aforementioned classical search for the exact minimum in low dimensions, it is a natural outgrowth of it and a folklore question that became popular after interest in this direction arose due to its connection to theoretical computer science that was found in [16] and was pursued in [34,25,3,26,6] (we stress that we are not aware of algorithmic implications of Question 2 and our interest in it stems only from the perspective of pure mathematics). To the best of our knowledge, Question 2 appeared in print only in [6, Section 6], which asks for the smallest possible growth rate (as $n \to \infty$) of the surface area of an integer parallelotope in $\mathbb{R}^n$, albeit without specifying the $O(\sqrt{n})$ rate as Question 2 does.

In [25] it was proved that Question 2 has a positive answer if one drops the requirement that the tiling set is convex, i.e., by [25, Theorem 1.1] for every $n \in \mathbb{N}$ there is a compact set $\Omega \subseteq \mathbb{R}^n$ such that $\mathbb{R}^n = \mathbb{Z}^n + \Omega$, the interior of $(x + \Omega) \cap (y + \Omega)$ is empty for every distinct $x, y \in \mathbb{Z}^n$, and $\mathrm{vol}_{n-1}(\partial\Omega) \lesssim \sqrt{n}$; see also the proof of this result that was found in [3]. The lack of convexity of Ω is irrelevant for the applications to computational complexity that were found in [16]. The proofs in [25,3] produce a set Ω that is decidedly non-convex. Our proof of Theorem 1 proceeds via an entirely different route and provides a paralletotope whose surface area comes close to the guarantee of [25] (prior to [25], the best known upper bound on the smallest possible surface area of a compact $\mathbb{Z}^n$-tiling set was the aforementioned $1.23721n$ of [16]).

It could be tempting to view the existence of the aforementioned compact set Ω as evidence for the availability of an integer parallelotope with comparable surface area, but this is a tenuous hope because the convexity requirement from a parallelotope imposes severe restrictions. In particular, by [30] for every $n \in \mathbb{N}$ there are only finitely many combinatorial types of parallelotopes in $\mathbb{R}^n$.[2] In fact, by combining [10, Section 6] with [30,37] we see that $K \subseteq \mathbb{R}^n$ is a parallelotope if and only if K is a centrally symmetric polytope, all of the $(n-1)$-dimensional faces of K are centrally symmetric, and the orthogonal projection of K along any of its $(n-2)$-dimensional faces is either a parallelogram or a centrally symmetric hexagon.

Of course, Theorem 1 *must* produce such a constrained polytope. To understand how this is achieved, it is first important to stress that this becomes a straightforward task if one only asks for a parallelotope with small surface area rather than for an *integer* parallelotope with small surface area. Namely, it follows easily from the literature that for every $n \in \mathbb{N}$ there exist a rank n lattice $\Lambda \subseteq \mathbb{R}^n$ whose covolume is 1 and a Λ-parallelotope $K \subseteq \mathbb{R}^n$ that satisfies $\mathrm{vol}_{n-1}(\partial K) \lesssim \sqrt{n}$. Indeed, by [35] there is a rank

[2] Thus, just for the sake concreteness (not important for the present purposes): Since antiquity it was known that there are 2 types of parallelogons; by [13] there are 5 types of parallelohedra; by [8,36] there are 52 types of 4-dimensional parallelotopes.

n lattice $\Lambda \subseteq \mathbb{R}^n$ of covolume 1 whose packing radius is at least $c\sqrt{n}$, where $c > 0$ is a universal constant. Let K be the Voronoi cell of Λ, namely K consists of the points in $\mathbb{R}^n$ whose (Euclidean) distance to any point of Λ is not less than their distance to the origin. Then, K is a Λ-parallelotope, $\mathrm{vol}_n(K) = 1$ since the covolume of Λ is 1, and $K \supseteq c\sqrt{n}B^n$ since the packing radius of Λ is at least $c\sqrt{n}$. Consequently, the surface area of K is at most $c^{-1}\sqrt{n}$ by the following simple lemma that we will use multiple times in the proof of Theorem 1:

Lemma 3. *Fix $n \in \mathbb{N}$ and $R > 0$. Suppose that a convex body $K \subseteq \mathbb{R}^n$ satisfies $K \supseteq RB^n$. Then,*

$$\frac{\mathrm{vol}_{n-1}(\partial K)}{\mathrm{vol}_n(K)} \leqslant \frac{n}{R}.$$

Lemma 3 is known (e.g., [19, Lemma 2.1]); for completeness we will present its short proof in Section 2.

Even though the packing radius of $\mathbb{Z}^n$ is small, the above observation drives our inductive proof of Theorem 1, which proceeds along the following lines. Fix $m \in \{1, \ldots, n-1\}$ and let V be an m-dimensional subspace of $\mathbb{R}^n$. If the lattice $V^\perp \cap \mathbb{Z}^n$ has rank $n - m$ and its packing radius is large, then Lemma 3 yields a meaningful upper bound on the $(n - m - 1)$-dimensional volume of the boundary of the Voronoi cell of $V^\perp \cap \mathbb{Z}^n$. We could then consider the lattice $\Lambda \subseteq V$ which is the orthogonal projection of $\mathbb{Z}^n$ onto V, and inductively obtain a Λ-parallelotope (residing within V) for which the $(m - 1)$-dimensional volume of its boundary is small. By considering the product (with respect to the identification of $\mathbb{R}^n$ with $V^\perp \times V$) of the two convex bodies thus obtained, we could hope to get the desired integer parallelotope.

There are obvious obstructions to this plan. The subspace V must be chosen so that the lattice $V^\perp \cap \mathbb{Z}^n$ is sufficiently rich yet it contains no short nonzero vectors. Furthermore, the orthogonal projection Λ of $\mathbb{Z}^n$ onto V is not $\mathbb{Z}^m$, so we must assume a stronger inductive hypothesis and also apply a suitable "correction" to Λ so as to be able to continue the induction. It turns out that there is tension between how large the packing radius of $V^\perp \cap \mathbb{Z}^n$ could be, the loss that we incur due to the aforementioned correction, and the total cost of iteratively applying the procedure that we sketched above. Upon balancing these constraints, we will see that the best choice for the dimension m of V is $m = n\exp(-\Theta(\sqrt{\log n}))$. The rest of the ensuing text will present the details of the implementation of this strategy.

2. Proof of Theorem 1

Below, for each $n \in \mathbb{N}$ the normed space $\ell_2^n = (\mathbb{R}^n, \|\cdot\|_{\ell_2^n})$ will denote the standard Euclidean space, i.e.,

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{R}^n, \qquad \|x\|_{\ell_2^n} \stackrel{\mathrm{def}}{=} \sqrt{x_1^2 + \cdots + x_n^2}.$$

The standard scalar product of $x, y \in \mathbb{R}^n$ will be denoted $\langle x, y\rangle \stackrel{\mathrm{def}}{=} x_1y_1 + \cdots + x_ny_n$. The coordinate basis of $\mathbb{R}^n$ will be denoted $e_1, \ldots, e_n$, i.e., for each $i \in \{1, \ldots, n\}$ the ith entry of e_i is 1 and the rest of the coordinates of e_i vanish. We will denote the origin of $\mathbb{R}^n$ by $\mathbf{0} = (0, \ldots, 0)$. For $0 < s \leqslant n$, the s-dimensional Hausdorff measure on $\mathbb{R}^n$ that is induced by the ℓ_2^n metric will be denoted by $\mathrm{vol}_s(\cdot)$. In particular, if $K \subseteq \mathbb{R}^n$ is a convex body (compact and with nonempty interior), then the following identity holds (see, e.g., [27]):

$$\mathrm{vol}_{n-1}(\partial K) = \lim_{\delta\to 0^+} \frac{\mathrm{vol}_n(K + \delta B^n) - \mathrm{vol}_n(K)}{\delta}. \tag{2}$$

If V is a subspace of $\mathbb{R}^n$, then its orthogonal complement (with respect to the ℓ_2^n Euclidean structure) will be denoted $V^\perp$ and the orthogonal projection from $\mathbb{R}^n$ onto V will be denoted Proj_V. When treating a subset Ω of V we will slightly abuse notation/terminology by letting $\partial\Omega$ be the boundary of Ω within V, and similarly when we will discuss the interior of Ω we will mean its interior within V. This convention results in suitable interpretations of when $K \subseteq V$ is a convex body or a parallelohedron (with respect to a lattice of V). The variant of (2) for a convex body $K \subseteq V$ becomes

$$\mathrm{vol}_{\dim(V)-1}(\partial K) = \lim_{\delta\to 0^+} \frac{\mathrm{vol}_{\dim(V)}\big(K + \delta(V \cap B^n)\big) - \mathrm{vol}_{\dim(V)}(K)}{\delta}. \tag{3}$$

Proof of Lemma 3. Since $K \supseteq RB^n$, for every $\delta > 0$ we have

$$K + \delta B^n \subseteq K + \frac{\delta}{R}K = \Big(1 + \frac{\delta}{R}\Big)\Big(\frac{R}{R+\delta}K + \frac{\delta}{R+\delta}K\Big) = \Big(1 + \frac{\delta}{R}\Big)K, \tag{4}$$

where the last step of (4) uses the fact that K is convex. Consequently,

$$\mathrm{vol}_{n-1}(\partial K) \stackrel{(2)}{=} \lim_{\delta\to 0^+} \frac{\mathrm{vol}_n(K + \delta B^n) - \mathrm{vol}_n(K)}{\delta} \stackrel{(4)}{\leqslant} \lim_{\delta\to 0^+} \frac{\big(1 + \frac{\delta}{R}\big)^n - 1}{\delta}\mathrm{vol}_n(K) = \frac{n}{R}\mathrm{vol}_n(K). \qquad \square$$

The sequence $\{Q(n)\}_{n=1}^\infty$ that we introduce in the following definition will play an important role in the ensuing reasoning:

Notation 4. For each $n \in \mathbb{N}$ let $Q(n)$ be the infimum over those $Q \geqslant 0$ such that for every lattice $\Lambda \subseteq \mathbb{Z}^n$ of rank n there exists a Λ-parallelotope $K \subseteq \mathbb{R}^n$ that satisfies

$$\frac{\mathrm{vol}_{n-1}(\partial K)}{\mathrm{vol}_n(K)} \leqslant Q. \tag{5}$$

As $\mathrm{vol}_n(K) = 1$ for any integer parallelotope $K \subseteq \mathbb{R}^n$, Theorem 1 is a special case of the following result:

Theorem 5. *There exists a universal constant $C \geqslant 1$ such that $Q(n) \lesssim \sqrt{n}e^{C\sqrt{\log n}}$ for every $n \in \mathbb{N}$.*

The following key lemma is the inductive step in the ensuing proof of Theorem 5 by induction on n:

Lemma 6. *Fix $m, n, s \in \mathbb{N}$ with $s \leqslant m \leqslant n$. Suppose that $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ is an m-by-n matrix all of whose entries are integers such that B has rank m and any s of the columns of B are linearly independent. Then,*

$$Q(n) \leqslant \frac{2(n-m)}{\sqrt{s}} + Q(m)\|\mathsf{B}\|_{\ell_2^n \to \ell_2^m}, \tag{6}$$

where $\|\cdot\|_{\ell_2^n \to \ell_2^m}$ denotes the operator norm from ℓ_2^n to ℓ_2^m.

The fact that Theorem 5 treats any sublattice of $\mathbb{Z}^n$ of full rank (recall how $Q(n)$ is defined), even though in Theorem 1 we are interested only in $\mathbb{Z}^n$ itself, provides a strengthening of the inductive hypothesis that makes it possible for our proof of Lemma 6 to go through. If Λ is an arbitrary full rank sublattice of $\mathbb{Z}^n$, then a Λ-parallelotope $K \subseteq \mathbb{R}^n$ need no longer satisfy $\mathrm{vol}_n(K) = 1$, so the inductive hypothesis must incorporate the value of $\mathrm{vol}_n(K)$, which is the reason why we consider the quantity $\mathrm{vol}_{n-1}(\partial K)/\mathrm{vol}_n(K)$ in (5). Observe that this quantity is not scale-invariant, so it might seem somewhat unnatural to study it, but it is well-suited to the aforementioned induction thanks to the following simple lemma:

Lemma 7. *Fix $m, n \in \mathbb{N}$ and an m-dimensional subspace V of $\mathbb{R}^n$. Let $O \subseteq V^\perp$ be an open subset of $V^\perp$ and let $G \subseteq V$ be an open subset of V. Then, for $\Omega = O + G$ we have*

$$\frac{\mathrm{vol}_{n-1}(\partial\Omega)}{\mathrm{vol}_n(\Omega)} = \frac{\mathrm{vol}_{n-m-1}(\partial O)}{\mathrm{vol}_{n-m}(O)} + \frac{\mathrm{vol}_{m-1}(\partial G)}{\mathrm{vol}_m(G)}. \tag{7}$$

Furthermore, if $T : \mathbb{R}^m \to V$ is a linear isomorphism and $K \subseteq \mathbb{R}^m$ is a convex body, then

$$\frac{\mathrm{vol}_{m-1}(\partial TK)}{\mathrm{vol}_m(TK)} \leqslant \frac{\mathrm{vol}_{m-1}(\partial K)}{\mathrm{vol}_m(K)} \|T^{-1}\|_{(V,\|\cdot\|_{\ell_2^n})\to \ell_2^m}, \tag{8}$$

where $\|\cdot\|_{(V,\|\cdot\|_{\ell_2^n})\to \ell_2^m}$ is the operator norm from V, equipped with the norm inherited from ℓ_2^n, to ℓ_2^m.

Proof. For (7), note that since $O \perp G$ we have $\mathrm{vol}_n(\Omega) = \mathrm{vol}_{n-m}(O)\mathrm{vol}_m(G)$, and $\partial\Omega = (\partial O + G) \cup (O + \partial G)$ where $\mathrm{vol}_{n-1}((\partial O + G) \cap (O + \partial G)) = 0$, so $\mathrm{vol}_{n-1}(\partial\Omega) = \mathrm{vol}_{n-m-1}(\partial O)\mathrm{vol}_m(G) + \mathrm{vol}_{n-m}(O)\mathrm{vol}_{m-1}(\partial G)$.

For (8), denote $\rho = \|T^{-1}\|_{(V,\|\cdot\|_{\ell_2^n})\to\ell_2^m}$, so that $T^{-1}(V\cap B^n)\subseteq \rho B^m$. Consequently,

$$\forall \delta\in\mathbb{R},\qquad TK+\delta(V\cap B^n)=T\big(K+\delta T^{-1}(V\cap B^n)\big)\subseteq T(K+\delta\rho B^m).$$

By combining this inclusion with (3), we see that

$$\begin{aligned}\mathrm{vol}_{m-1}(\partial TK) &\leqslant \lim_{\delta\to 0^+}\frac{\mathrm{vol}_m\big(T(K+\delta\rho B^m)\big)-\mathrm{vol}_m(TK)}{\delta}\\ &= \det(T)\lim_{\delta\to 0^+}\frac{\mathrm{vol}_m(K+\delta\rho B^m)-\mathrm{vol}_m(K)}{\delta}\stackrel{(2)}{=}\det(T)\mathrm{vol}_{m-1}(\partial K)\rho\\ &=\frac{\mathrm{vol}_m(TK)}{\mathrm{vol}_m(K)}\mathrm{vol}_{m-1}(\partial K)\rho.\qquad\square\end{aligned}$$

Remark 8. We stated Lemma 7 with K being a convex body since that is all that we need herein. However, the proof does not rely on its convexity in an essential way; all that is needed is that K is a body in $\mathbb{R}^m$ whose boundary is sufficiently regular so that the identity (2) holds (with n replaced by m).

Any matrix B as in Lemma 6 must have a row with at least n/m nonzero entries. Indeed, otherwise the total number of nonzero entries of B would be less than $m(n/m)=n$, so at least one of the n columns B would have to vanish, in contradiction to the assumed linear independence (as $s\geqslant 1$). Thus, there exists $j\in\{1,\ldots,m\}$ such that at least $\lceil n/m\rceil$ of the entries of $\mathsf{B}^*e_j\in\mathbb{R}^n$ do not vanish. Those entries are integers, so $\|\mathsf{B}^*e_j\|_{\ell_2^n}\geqslant\sqrt{\lceil n/m\rceil}$. Hence, the quantity $\|\mathsf{B}\|_{\ell_2^n\to\ell_2^m}=\|\mathsf{B}^*\|_{\ell_2^m\to\ell_2^n}$ in (6) cannot be less than $\sqrt{\lceil n/m\rceil}$.

Question 9. *Given $m,n\in\mathbb{N}$ and $C>1$, what is the order of magnitude of the largest $s=s(m,n,C)\in\mathbb{N}$ for which there exists $\mathsf{B}\in\mathsf{M}_{m\times n}(\mathbb{Z})$ such that any s of the columns of B are linearly independent and*

$$\|\mathsf{B}\|_{\ell_2^n\to\ell_2^m}\leqslant C\sqrt{\frac{n}{m}}.$$

The following lemma is a step towards Question 9 that we will use in the implementation of Lemma 6:

Lemma 10. *Suppose that $m,n\in\mathbb{N}$ satisfy $4\leqslant m\leqslant n$ and $n\geqslant (m\log m)/4$. There exist $s\in\mathbb{N}$ with $s\gtrsim m^2/n$ and $\mathsf{B}\in\mathsf{M}_{m\times n}(\mathbb{Z})$ of rank m such that any s of the columns of B are linearly independent and*

$$\|\mathsf{B}\|_{\ell_2^n\to\ell_2^m}\lesssim\sqrt{\frac{n}{m}}.$$

Lemma 10 suffices for our purposes, but it is not sharp. We will actually prove below that in the setting of Lemma 10 for every $0 < \varepsilon \leqslant 1$ there exist $s \in \mathbb{N}$ with $s \gtrsim m^{1+\varepsilon}/n^{\varepsilon} = m(m/n)^{\varepsilon} \geqslant m^2/n$ and $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ of rank m such that any s of the columns of B are linearly independent and $\|\mathsf{B}\|_{\ell_2^n \to \ell_2^m} \lesssim_{\varepsilon} \sqrt{n/m}$.

While Question 9 arises naturally from Lemma 6 and it is interesting in its own right, fully answering Question 9 will not lead to removing the $o(1)$ term in Theorem 1 altogether; the bottleneck in the ensuing reasoning that precludes obtaining such an answer to Question 2 (if true) is elsewhere.

Proof of Theorem 5 assuming Lemma 6 and Lemma 10. We will proceed by induction on n. In preparations for the base of the induction, we will first record the following estimate (which is sharp when the lattice is $\mathbb{Z}^n$). The Voronoi cell of a rank n sublattice Λ of $\mathbb{Z}^n$, namely the set

$$K = \big\{x \in \mathbb{R}^n : \forall y \in \Lambda,\ \|x\|_{\ell_2^n} \leqslant \|x-y\|_{\ell_2^n}\big\},$$

is a Λ-parallelotope that satisfies $K \supseteq \frac{1}{2}B^n$. Indeed, if $y \in \Lambda \smallsetminus \{0\}$, then $\|y\|_{\ell_2^n} \geqslant 1$ since $y \in \mathbb{Z}^n \smallsetminus \{0\}$. Hence,

$$\forall x \in \frac{1}{2}B^n, \qquad \|x-y\|_{\ell_2^n} \geqslant \|y\|_{\ell_2^n} - \|x\|_{\ell_2^n} \geqslant \|x\|_{\ell_2^n}.$$

By Lemma 3, it follows that $\mathrm{vol}_{n-1}(\partial K)/\mathrm{vol}_n(K) \leqslant 2n$. This gives the (weak) a priori bound $Q(n) \leqslant 2n$.

Fix $n \in \mathbb{N}$ and suppose that there exists $m \in \mathbb{N}$ satisfying $4 \leqslant m \leqslant n$ and $n \geqslant (m\log m)/4$. By using Lemma 6 with the matrix B from Lemma 10 we see that there is a universal constant $\kappa \geqslant 4$ for which

$$Q(n) \leqslant \kappa\left(\frac{n^{\frac{3}{2}}}{m} + Q(m)\sqrt{\frac{n}{m}}\right). \tag{9}$$

We will prove by induction on $n \in \mathbb{N}$ the following upper bound on $Q(n)$, thus proving Theorem 5:

$$Q(n) \leqslant 4\kappa\sqrt{n}e^{\sqrt{2(\log n)\log(2\kappa)}}. \tag{10}$$

If $n \leqslant 4\kappa^2$, then by the above discussion $Q(n) \leqslant 2n \leqslant 4\kappa\sqrt{n}$, so that (10) holds. If $n > 4\kappa^2$, then define

$$m \stackrel{\mathrm{def}}{=} \left\lfloor ne^{-\sqrt{2(\log n)\log(2\kappa)}}\right\rfloor. \tag{11}$$

It is straightforward to verify that this choice of m satisfies $4 \leqslant m < n$ and $n \geqslant (m\log m)/4$ (with room to spare), i.e., the above conditions for (9) to hold are met. Using the induction hypothesis, it follows that

$$
\begin{aligned}
Q(m)\sqrt{\frac{n}{m}} &\leqslant 4\kappa\sqrt{n}e^{\sqrt{2(\log m)\log(2\kappa)}} \\
&\overset{(11)}{\leqslant} 4\kappa\sqrt{n}e^{\sqrt{2\left(\log n-\sqrt{2(\log n)\log(2\kappa)}\right)\log(2\kappa)}} \\
&\leqslant 4\kappa\sqrt{n}e^{\left(\sqrt{2\log n}-\sqrt{\log(2\kappa)}\right)\sqrt{\log(2\kappa)}} = 2\sqrt{n}e^{\sqrt{2(\log n)\log(2\kappa)}},
\end{aligned} \tag{12}
$$

where the penultimate step of (12) uses the inequality $\sqrt{a-b} \leqslant \sqrt{a} - b/(2\sqrt{a})$, which holds for every $a, b \in \mathbb{R}$ with $a \geqslant b$; in our setting $a = \log n$ and $b = \sqrt{2(\log n)\log(2\kappa)}$ and $a > b$ because we are now treating the case $n > 4\kappa^2$. A substitution of (12) into (9), while using that $m \geqslant \frac{1}{2}n\exp\left(-\sqrt{2(\log n)\log(2\kappa)}\right)$ holds thanks to (11), gives (10), thus completing the proof of Theorem 5. □

We will next prove Lemma 6, which is the key recursive step that underlies Theorem 1.

Proof of Lemma 6. We will start with the following two elementary observations to facilitate the ensuing proof. Denote the span of the rows of B by $V = \mathsf{B}^*\mathbb{R}^m \subseteq \mathbb{R}^n$ and notice that $\dim(V) = m$ as B is assumed to have rank m. Suppose that Λ is a lattice of rank n that is contained in $\mathbb{Z}^n$. Firstly, we claim that the rank of the lattice $V^\perp \cap \Lambda$ equals $n - m$. Indeed, we can write $V^\perp \cap \Lambda = \mathsf{C}(\mathbb{Z}^n \cap \mathsf{C}^{-1}V^\perp)$ where C is an invertible matrix with integer entries, i.e., $\mathsf{C} \in \mathsf{M}_n(\mathbb{Z}) \cap \mathsf{GL}_n(\mathbb{Q})$, such that $\Lambda = \mathsf{C}\mathbb{Z}^n$. Furthermore, $V^\perp = \mathrm{Ker}(\mathsf{B})$, so the dimension over $\mathbb{Q}$ of $\mathbb{Q}^n \cap V^\perp$ equals $n - m$. As $\mathsf{C}^{-1} \in \mathsf{GL}_n(\mathbb{Q})$, it follows that $\mathsf{C}^{-1}V^\perp$ contains $n - m$ linearly independent elements of $\mathbb{Z}^n$. Secondly, we claim that the orthogonal projection $\mathsf{Proj}_V\Lambda$ of Λ onto V is a discrete subset of V, and hence is a lattice; its rank will then be $\dim(V) = m$ because we are assuming that $\mathrm{span}(\Lambda) = \mathbb{R}^n$, so $\mathrm{span}(\mathsf{Proj}_V\Lambda) = \mathsf{Proj}_V(\mathrm{span}(\Lambda)) = \mathsf{Proj}_V(\mathbb{R}^n) = V$. We need to check that for any $\{x_1, x_2, \dots\} \subseteq \Lambda$ such that $\lim_{i\to\infty} \mathsf{Proj}_V x_i = \mathbf{0}$ there is $i_0 \in \mathbb{N}$ such that $\mathsf{Proj}_V x_i = \mathbf{0}$ whenever $i \in \{i_0, i_0 + 1, \dots\}$. Indeed, as $V^\perp = \mathrm{Ker}(\mathsf{B})$ we have $\mathsf{B}x = \mathsf{B}\mathsf{Proj}_V x$ for every $x \in \mathbb{R}^n$, so $\lim_{i\to\infty} \mathsf{B}x_i = \mathbf{0}$. But, $\mathsf{B}x_i \in \mathbb{Z}^m$ for every $i \in \mathbb{N}$ because $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ and $x_i \in \Lambda \subseteq \mathbb{Z}^n$. Consequently, there is $i_0 \in \mathbb{N}$ such that $\mathsf{B}x_i = \mathbf{0}$ for every $i \in \{i_0, i_0 + 1, \dots\}$, i.e., $x_i \in \mathrm{Ker}(\mathsf{B}) = V^\perp$ and hence $\mathsf{Proj}_V x_i = \mathbf{0}$.

Let $K_1 \subseteq V^\perp$ be the Voronoi cell of $V^\perp \cap \Lambda$, namely $K_1 = \{x \in V^\perp :\ \forall y \in V^\perp \cap \Lambda,\quad \|x\|_{\ell_2^n} \leqslant \|x - y\|_{\ell_2^n}\}$. If $y = (y_1, \dots, y_n) \in V^\perp = \mathrm{Ker}(\mathsf{B})$, then $y_1\mathsf{B}e_1 + \dots + y_n\mathsf{B}e_n = \mathbf{0}$. By the assumption on B, this implies that if also $y \neq \mathbf{0}$, then $|\{i \in \{1, \dots, n\} :\ y_i \neq 0\}| > s$. Consequently, as the entries of elements of Λ are integers,

$$
\forall y \in (V^\perp \cap \Lambda) \smallsetminus \{0\}, \qquad \|y\|_{\ell_2^n} > \sqrt{s}.
$$

Hence, if $x \in \frac{\sqrt{s}}{2}(V^\perp \cap B^n)$, then

$$
\forall y \in (V^\perp \cap \Lambda) \smallsetminus \{0\}, \qquad \|x - y\|_{\ell_2^n} \geqslant \|y\|_{\ell_2^n} - \|x\|_{\ell_2^n} > \sqrt{s} - \frac{\sqrt{s}}{2} = \frac{\sqrt{s}}{2} \geqslant \|x\|_{\ell_2^n}.
$$

This means that $K_1 \supseteq \frac{\sqrt{s}}{2}(V^\perp \cap B^n)$, and therefore by Lemma 3 we have

$$\frac{\mathrm{vol}_{n-m-1}(\partial K_1)}{\mathrm{vol}_{n-m}(K_1)} \leqslant \frac{n-m}{\frac{1}{2}\sqrt{s}} = \frac{2(n-m)}{\sqrt{s}}. \tag{13}$$

Next, fix $i \in \{1,\ldots,m\}$. By the definition of V, the i'th row $\mathsf{B}^* e_i$ of B belongs to V, so

$$\forall (x,i) \in \mathbb{R}^n \times \{1,\ldots,m\}, \qquad \langle x, \mathsf{B}^* e_i\rangle = \langle \mathsf{Proj}_V x, \mathsf{B}^* e_i\rangle. \tag{14}$$

Since all of the entries of B are integers, it follows that

$$\forall (x,i) \in \mathbb{Z}^n \times \{1,\ldots,m\}, \qquad \langle \mathsf{B}\mathsf{Proj}_V x, e_i\rangle = \langle \mathsf{Proj}_V x, \mathsf{B}^* e_i\rangle \overset{(14)}{=} \langle x, \mathsf{B}^* e_i\rangle \in \mathbb{Z}.$$

In other words, $\mathsf{B}\mathsf{Proj}_V \mathbb{Z}^n \subseteq \mathbb{Z}^m$, and hence the lattice $\mathsf{B}\mathsf{Proj}_V \Lambda$ is a subset of $\mathbb{Z}^m$. Furthermore, B is injective on V because $\mathrm{Ker}(\mathsf{B}) = V^\perp$, so $\mathsf{B}\mathsf{Proj}_V \mathbb{Z}^n$ is a rank m sublattice of $\mathbb{Z}^m$. By the definition of $Q(m)$, it follows that there exists a $\mathsf{B}\mathsf{Proj}_V\Lambda$-parallelotope $K_2^0 \subseteq \mathbb{R}^m$ such that

$$\frac{\mathrm{vol}_{m-1}(\partial K_2^0)}{\mathrm{vol}_m(K_2^0)} \leqslant Q(m). \tag{15}$$

Because $V^\perp = \mathrm{Ker}(\mathsf{B})$ and the rank of B is $m = \dim(V)$, the restriction $\mathsf{B}|_V$ of B to V is an isomorphism between V and $\mathbb{R}^m$. Letting $T : \mathbb{R}^m \to V$ denote the inverse of $\mathsf{B}|_V$, define $K_2 = TK_2^0$. By combining (the second part of) Lemma 7 with (15), we see that

$$\frac{\mathrm{vol}_{m-1}(\partial K_2)}{\mathrm{vol}_m(K_2)} \leqslant Q(m)\|\mathsf{B}\|_{\ell_2^n \to \ell_2^m}. \tag{16}$$

Let $K = K_1 + K_2 \subseteq \mathbb{R}^n$. By combining (the first part of) Lemma 7 with (13) and (16), we have

$$\frac{\mathrm{vol}_{n-1}(\partial K)}{\mathrm{vol}_n(K)} \leqslant \frac{2(n-m)}{\sqrt{s}} + Q(m)\|\mathsf{B}\|_{\ell_2^n \to \ell_2^m}.$$

Hence, the proof of Lemma 6 will be complete if we check that K is a Λ-parallelotope. Our construction ensures by design that this is so, as K_1 is a $(V^\perp \cap \Lambda)$-parallelotope and K_2 is a $\mathsf{Proj}_V\Lambda$-parallelotope; verifying this fact is merely an unraveling of the definitions, which we will next perform for completeness.

Fix $z \in \mathbb{R}^n$. As $\mathbb{R}^m = \mathsf{B}\mathsf{Proj}_V\Lambda + K_2^0$, there is $x \in \Lambda$ with $\mathsf{B}\mathsf{Proj}_V z \in \mathsf{B}\mathsf{Proj}_V x + K_2^0$. Apply T to this inclusion and use that $T\mathsf{B}|_V$ is the identity mapping to get $\mathsf{Proj}_V z \in \mathsf{Proj}_V x + K_2$. Next, $V^\perp = K_1 + V^\perp \cap \Lambda$ since K_1 is the Voronoi cell of $V^\perp \cap \Lambda$, so there is $y \in V^\perp \cap \Lambda$ such that $\mathsf{Proj}_{V^\perp} z - \mathsf{Proj}_{V^\perp} x \in y + K_1$. Consequently, $z = \mathsf{Proj}_{V^\perp} z + \mathsf{Proj}_V z \in \mathsf{Proj}_{V^\perp} x + y + K_1 + \mathsf{Proj}_V x + K_2 = x + y + K \in \Lambda + K$. Hence, $\Lambda + K = \mathbb{R}^n$.

It remains to check that for every $w \in \Lambda \setminus \{0\}$ the interior of K does not intersect $w + K$. Indeed, by the definition of K, if k belongs to the interior of K, then $k = k_1 + k_2$, where k_1 belongs to the interior of K_1 and k_2 belongs to the interior of K_2. Since B is injective on $K_2 \subseteq V$, it follows that $\mathsf{B}k_2$ belongs to the interior of $\mathsf{B}K_2 = K_2^0$. If $\mathsf{Proj}_V w \neq 0$, then $\mathsf{B}\mathsf{Proj}_V w \in \mathsf{B}\mathsf{Proj}_V \Lambda \smallsetminus \{0\}$, so because K_2^0 is a $\mathsf{B}\mathsf{Proj}_V\Lambda$-parallelotope, $\mathsf{B}k_2 \notin \mathsf{B}\mathsf{Proj}_V w + K_2^0$. By applying T to is inclusion, we see that $k_2 \notin \mathsf{Proj}_V w + K_2$, which implies that $k \notin w + K$. On the other hand, if $\mathsf{Proj}_V w = 0$, then $w \in (V^\perp \cap \Lambda) \smallsetminus \{0\}$. Since K_1 is a $V^\perp \cap \Lambda$-parallelotope, it follows that $k_1 \notin w + K_1$, so $k \notin w + K$. □

To complete the proof of Theorem 5, it remains to prove Lemma 10. For ease of later reference, we first record the following straightforward linear-algebraic fact:

Observation 11. *Fix $m, n, s \in \mathbb{N}$ with $s \leqslant m \leqslant n$. Suppose that there exists $\mathsf{A} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ such that any s of the columns of A are linearly independent. Then, there also exists $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ such that any s of the columns of B are linearly independent, B has rank m, and*

$$\|\mathsf{B}\|_{\ell_2^n \to \ell_2^m} \leqslant \sqrt{1 + \|\mathsf{A}\|^2_{\ell_2^n \to \ell_2^m}}. \tag{17}$$

Proof. Let $r \in \{1, \ldots, m\}$ be the rank of A. By permuting the rows of A, we may assume that its first r rows, namely $\mathsf{A}^* e_1, \ldots, \mathsf{A}^* e_r \in \mathbb{R}^n$ are linearly independent. Also, since we can complete $\mathsf{A}^* e_1, \ldots, \mathsf{A}^* e_r$ to a basis of $\mathbb{R}^n$ by adding $n - r$ vectors from $\{e_1, \ldots, e_n\} \subseteq \mathbb{R}^n$, by permuting the columns of A, we may assume that the vectors $\mathsf{A}^* e_1, \ldots, \mathsf{A}^* e_r, e_{r+1}, \ldots, e_m \in \mathbb{R}^n$ are linearly independent. Let $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ be the matrix whose rows are $\mathsf{A}^* e_1, \ldots, \mathsf{A}^* e_r, e_{r+1}, \ldots, e_m$, so that B has rank m by design. Also,

$$\forall x \in \mathbb{R}^n, \qquad \|\mathsf{B}x\|^2_{\ell_2^m} = \sum_{i=1}^r (\mathsf{A}x)_i^2 + \sum_{j=r+1}^m x_j^2 \leqslant \big(\|\mathsf{A}\|^2_{\ell_2^n \to \ell_2^m} + 1\big)\|x\|^2_{\ell_2^n}.$$

Therefore (17) holds. It remains to check that any s of the columns of B are linearly independent. Indeed, fix $S \subseteq \{1, \ldots, n\}$ with $|S| = s$ and $\{\alpha_j\}_{j\in S} \subseteq \mathbb{R}$ such that $\sum_{j\in S} \alpha_j \mathsf{B}_{ij} = 0$ for every $i \in \{1, \ldots, m\}$. In particular, $\sum_{j\in S} \alpha_j \mathsf{A}_{ij} = 0$ for every $i \in \{1, \ldots, r\}$. If $k \in \{r+1, \ldots, m\}$, then since the k'th row of A is in the span of the first r rows of A, there exist $\beta_{k1}, \ldots, \beta_{kr} \in \mathbb{R}$ such that $\mathsf{A}_{kj} = \sum_{i=1}^r \beta_{ki} \mathsf{A}_{ij}$ for every $j \in \{1, \ldots, n\}$. Consequently, $\sum_{j\in S} \alpha_j \mathsf{A}_{kj} = \sum_{i=1}^r \beta_{ki} \sum_{j\in S} \alpha_j \mathsf{A}_{ij} = 0$. This shows that $\sum_{j\in S} \alpha_j \mathsf{A}_{ij} = 0$ for every $i \in \{1, \ldots, m\}$. By the assumed property of A, this implies that $\alpha_j = 0$ for every $j \in S$. □

The following lemma is the main existential statement that underlies our justification of Lemma 10:

Lemma 12. *There exists a universal constant $c > 0$ with the following property. Let $d, m, n \geqslant 3$ be integers that satisfy $d \leqslant m \leqslant n$ and $n \geqslant (m \log m)/d$. Suppose also that $s \in \mathbb{N}$ satisfies*

$$s \leqslant \frac{c}{d}\left(\frac{m^d}{n^2}\right)^{\frac{1}{d-2}}. \tag{18}$$

Then, there exists an m-by-n matrix $\mathsf{A} \in M_{m\times n}(\{0,1\})$ *with the following properties:*

- *Any* s *of the columns of* A *are linearly independent over the field* $\mathbb{Z}/(2\mathbb{Z})$*;*
- *Every column of* A *has at most* d *nonzero entries;*
- *Every row of* A *has at most* $5dn/m$ *nonzero entries.*

The ensuing proof of Lemma 12 consists of probabilistic reasoning that is common in the literature on Low Density Parity Check (LDPC) codes; it essentially follows the seminal work [18]. While similar considerations appeared in many places, we could not locate a reference that states Lemma 12.[3] A peculiarity of the present work is that, for the reason that we have seen in the above deduction of Theorem 5 from Lemma 6 and Lemma 10, we need to choose a nonstandard dependence of m on n; recall (11).

In the course of the proof of Lemma 12 we will use the following probabilistic estimate:

Lemma 13. *Let* $\{W(t) = (W(t,1),\ldots,W(t,m))\}_{t=0}^{\infty}$ *be the standard random walk on the discrete hypercube* $\{0,1\}^m$*, starting at the origin. Thus,* $W(0) = \mathbf{0}$ *and for each* $t \in \mathbb{N}$ *the random vector* $W(t)$ *is obtained from the random vector* $W(t-1)$ *by choosing an index* $i \in \{1,\ldots,m\}$ *uniformly at random and setting*

$$W(t) = \big(W(t-1,1),\ldots,W(t-1,i-1),1-W(t-1,i),W(t-1,i+1),\ldots,W(t-1,m)\big).$$

Then, $\mathrm{Prob}[W(t) = \mathbf{0}] \leqslant 2(t/m)^{t/2}$ *for every* $t \in \mathbb{N}$*.*

Proof. If t is odd, then $\mathrm{Prob}[W(t) = \mathbf{0}] = 0$, so suppose from now that t is even. Let $\mathsf{P} \in \mathsf{M}_{\{0,1\}^m\times\{0,1\}^m}(\mathbb{R})$ denote the transition matrix of the random walk W, i.e.,

$$\forall f : \{0,1\}^m \to \mathbb{R},\ \forall x \in \{0,1\}^m, \qquad \mathsf{P}f(x) = \frac{1}{m}\sum_{i=1}^{m} f(x + e_i \bmod 2).$$

Then, $\mathrm{Prob}[W(t) = \mathbf{0}] = (\mathsf{P}^t)_{\mathbf{00}}$. By symmetry, all of the 2^m diagonal entries of P^t are equal to each other, so $(\mathsf{P}^t)_{\mathbf{00}} = \mathrm{Trace}(\mathsf{P}^t)/2^m$. For every $S \subseteq \{0,1\}^m$, the Walsh function $(x \in \{0,1\}^m) \mapsto (-1)^{\sum_{i\in S} x_i}$ is an eigenvector of P whose eigenvalue equals $1 - 2|S|/m$. Consequently,

$$\mathrm{Prob}[W(t) = \mathbf{0}] = \frac{1}{2^m}\,\mathrm{Trace}(\mathsf{P}^t) = \frac{1}{2^m}\sum_{k=0}^{m}\binom{m}{k}\left(1 - \frac{2k}{m}\right)^t. \tag{19}$$

[3] The standard range of parameters that is discussed in the LDPC literature is, using the notation of Lemma 12, either when $m \asymp n$, or when s, d are fixed and the pertinent question becomes how large n can be as $m \to \infty$; sharp bounds in the former case are due to [18] and sharp bounds in the latter case are due to [29,32]. Investigations of these issues when the parameters have intermediate asymptotic behaviors appear in [15,14,2,9,21,23].

Suppose that $\beta_1,\ldots,\beta_m$ are independent $\{0,1\}$-valued unbiased Bernoulli random variables, namely, $\mathrm{Prob}[\beta_i=0]=\mathrm{Prob}[\beta_i=1]=1/2$ for any $i\in\{1,\ldots,m\}$. By Hoeffding's inequality (e.g., [38, Theorem 2.2.6]),

$$\forall u\geqslant 0,\qquad \mathrm{Prob}\left[\left|\sum_{i=1}^m\Big(\beta_i-\frac12\Big)\right|\geqslant u\right]\leqslant 2e^{-\frac{2u^2}{m}}. \tag{20}$$

Observing that the right hand side of (19) is equal to the expectation of $\big(1-\frac{2}{m}\sum_{i=1}^m\beta_i\big)^t$, we see that

$$\begin{aligned}\mathrm{Prob}[W(t)=\mathbf{0}]&\overset{(19)}{=}\Big(-\frac{2}{m}\Big)^t\,\mathbb{E}\left[\left(\sum_{i=1}^m\Big(\beta_i-\frac12\Big)\right)^t\right]\\ &=\Big(\frac{2}{m}\Big)^t\int_0^\infty tu^{t-1}\mathrm{Prob}\left[\left|\sum_{i=1}^m\Big(\beta_i-\frac12\Big)\right|\geqslant u\right]\mathrm{d}u\\ &\overset{(20)}{\leqslant}2t\Big(\frac{2}{m}\Big)^t\int_0^\infty u^{t-1}e^{-\frac{2u^2}{m}}\,\mathrm{d}u=2\Big(\frac{2}{m}\Big)^{\frac t2}\Big(\frac t2\Big)!\leqslant 2\Big(\frac{2}{m}\Big)^{\frac t2}\Big(\frac t2\Big)^{\frac t2}=2\Big(\frac{t}{m}\Big)^{\frac t2}.\qquad\square\end{aligned}$$

With Lemma 13 at hand, we can now prove Lemma 12.

Proof of Lemma 12. Consider the random matrix $\mathsf{A}\in\mathsf{M}_{m\times n}(\{0,1\})$ whose columns are independent identically distributed copies $W_1(d),\ldots,W_n(d)$ of $W(d)$, where $W(0)=\mathbf{0},W(1),W(2),\ldots$ is the standard random walk on $\{0,1\}^m$ as in Lemma 13. By design, this means that each column of A has at most d nonzero entries. Fixing $(i,j)\in\{1,\ldots,m\}\times\{1,\ldots,n\}$, if $W_j(d,i)=1$, then in at least one of the d steps of the random walk that generated $W_j(d)$ the ith coordinate was changed. The probability of the latter event equals $1-(1-1/m)^d$. Hence, $\mathrm{Prob}[W_j(d,i)=1]\leqslant 1-(1-1/m)^d\leqslant d/m$ and therefore for every fixed $S\subseteq\{1,\ldots,n\}$, the probability that $W_j(d,i)=1$ for every $j\in S$ is at most $(d/m)^{|S|}$. Consequently, the probability that each one of the m rows of A has at most $\ell=\lceil 4dn/m\rceil$ nonzero entries is at least

$$1-m\binom{n}{\ell}\Big(\frac{d}{m}\Big)^\ell\geqslant 1-m\Big(\frac{en}{\ell}\Big)^\ell\Big(\frac{d}{m}\Big)^\ell=1-m\Big(\frac{edn}{m\ell}\Big)^\ell\geqslant 1-m\Big(\frac{e}{4}\Big)^{4\log m}\geqslant\frac13,$$

where the first step is the standard elementary bound $\binom{n}{\ell}\leqslant\big(\frac{en}{\ell}\big)^\ell$ (see, e.g., [33, Section 4]), the penultimate step uses $\ell\geqslant 4dn/m$ and the assumption $n\geqslant(m\log m)/d$, and the final step holds because $m\geqslant 3$.

It therefore suffices to prove that with probability greater than $2/3$ the vectors $\{W_i(d)\}_{i\in S}\subseteq\{0,1\}^m$ are linearly independent over $\mathbb{Z}/(2\mathbb{Z})$ for every $\varnothing\neq S\subseteq\{1,\ldots,n\}$ with $|S|\leqslant s$, where $s\in\mathbb{N}$ satisfies (18) and the universal constant $c>0$ that appears in (18) will be specified later; see (24). So, it suffices to prove that with probability greater than $2/3$ we have $\sum_{i\in S} W_i(d) \not\equiv \mathbf{0} \bmod 2$ for every $\varnothing \neq S \subseteq \{1,\ldots,n\}$ with $|S| \leqslant s$. Hence, letting D denote the number of $\varnothing \neq S \subseteq \{1,\ldots,n\}$ with $|S| \leqslant s$ that satisfy $\sum_{i\in S} W_i(d) \equiv \mathbf{0} \bmod 2$, it suffices to prove that $2/3 < \mathrm{Prob}[D=0] = 1 - \mathrm{Prob}[D \geqslant 1]$. Using Markov's inequality, it follows that the proof of Lemma 12 will be complete if we demonstrate that $\mathbb{E}[D] < 1/3$.

The expectation of D can be computed exactly. Indeed,

$$\mathbb{E}[D] = \mathbb{E}\Bigg[\sum_{\substack{S\subseteq\{1,\ldots,n\}\\ 1\leqslant|S|\leqslant s}} \mathbf{1}_{\{\sum_{i\in S} W_i(d)\equiv \mathbf{0} \bmod 2\}}\Bigg] = \sum_{r=1}^{s}\binom{n}{r}\mathrm{Prob}[W(dr)=\mathbf{0}], \tag{21}$$

where we used the fact that $\sum_{i\in S} W_i(d) \bmod 2 \in \{0,1\}^m$ has the same distribution as $W(d|S|)$ for every $\varnothing \neq S \subseteq \{1,\ldots,n\}$. By substituting the conclusion of Lemma 13 into (21) we see that

$$\mathbb{E}[D] \leqslant 2\sum_{r=1}^{s}\binom{n}{r}\left(\frac{dr}{m}\right)^{\frac{dr}{2}} \leqslant 2\sum_{r=1}^{s}\left(\frac{ed^{\frac{d}{2}}r^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}}\right)^{r}, \tag{22}$$

where in the last step we again used the standard bound $\binom{n}{r} \leqslant \left(\frac{en}{r}\right)^r$. For every $r \in \{1,\ldots,s\}$,

$$\frac{ed^{\frac{d}{2}}r^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}} \leqslant \frac{ed^{\frac{d}{2}}s^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}} \overset{(18)}{\leqslant} edc^{\frac{d}{2}-1} < \frac{1}{7}, \tag{23}$$

provided that

$$c < \inf_{d\geqslant 3}\left(\frac{1}{7ed}\right)^{\frac{2}{d-2}} \in (0,1). \tag{24}$$

Therefore, when (24) holds we may substitute (23) into (22) to get that $\mathbb{E}[D] < 2\sum_{r=1}^{\infty}\frac{1}{7^r} = \frac{1}{3}$. $\square$

We can now prove Lemma 10, thus concluding the proof of Theorem 5.

Proof of Lemma 10. We will prove the following stronger statement (Lemma 10 is its special case $\varepsilon = 1$). If $0 < \varepsilon \leqslant 2$ and $m,n \in \mathbb{N}$ satisfy $2 + \lfloor 2/\varepsilon \rfloor \leqslant m \leqslant n$ and $n \geqslant (m\log m)/(2+\lfloor 2/\varepsilon\rfloor)$, then there exist $s \in \mathbb{N}$ with $s \gtrsim \varepsilon m^{1+\varepsilon}/n^{\varepsilon}$, and $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ such that any s of the columns of B are linearly independent, the rows of B are linearly independent, and

$$\|\mathsf{B}\|_{\ell_2^n\to\ell_2^m} \lesssim \frac{1}{\varepsilon}\sqrt{\frac{n}{m}}.$$

Indeed, apply Lemma 12 with $d = 2 + \lfloor 2/\varepsilon \rfloor \geqslant \max\{3, 2/\varepsilon\}$ (equivalently, $d \geqslant 3$ is the largest integer such that $2/(d-2) \geqslant \varepsilon$) to deduce that there exist an integer s with

$$s \asymp \frac{1}{d}\left(\frac{m^d}{n^2}\right)^{\frac{1}{d-2}} = \frac{m}{d}\left(\frac{m}{n}\right)^{\frac{2}{d-2}} \leqslant \frac{\varepsilon}{2} m \left(\frac{m}{n}\right)^{\varepsilon} = \frac{\varepsilon m^{1+\varepsilon}}{2n^{\varepsilon}},$$

and a matrix $\mathsf{A} \in \mathsf{M}_{m\times n}(\{0,1\}) \subseteq \mathsf{M}_{m\times n}(\mathbb{Z})$ such that any s of the columns of A are linearly independent over $\mathbb{Z}/(2\mathbb{Z})$, every column of A has at most d nonzero entries, and every row of A has at most $5dn/m$ nonzero entries. If a set of vectors $v_1, \ldots, v_s \in \{0,1\}^m$ is linearly independent over $\mathbb{Z}/(2\mathbb{Z})$, then it is also linearly independent over $\mathbb{R}$ (e.g., letting $\mathsf{V} \in \mathsf{M}_{m\times s}(\{0,1\})$ denote the matrix whose columns are $v_1, \ldots, v_s$, the latter requirement is equivalent to the determinant of $\mathsf{V}^*\mathsf{V} \in \mathsf{M}_s(\{0,1\})$ being an odd integer, so in particular it does not vanish). Hence, any s of the columns of A are linearly independent over $\mathbb{R}$. Also,

$$\|\mathsf{A}\|_{\ell_2^n \to \ell_2^m} \leqslant \Big(\max_{i\in\{1,\ldots,m\}} \sum_{j=1}^{n} |\mathsf{A}_{ij}|\Big)^{\frac{1}{2}} \Big(\max_{j\in\{1,\ldots,n\}} \sum_{i=1}^{m} |\mathsf{A}_{ij}|\Big)^{\frac{1}{2}} \leqslant \sqrt{\frac{5dn}{m}} \cdot \sqrt{d} \asymp \frac{1}{\varepsilon}\sqrt{\frac{n}{m}},$$

where the first step is a standard bound which holds for any m-by-n real matrix (e.g., [20, Corollary 2.3.2]). Thus, A has all of the properties that we require from the matrix B in Lemma 10, except that we do not know that A has rank m, but Observation 11 remedies this (minor) issue. □

We end by asking the following question:

Question 14. *Fix $n \in \mathbb{N}$. Does there exist an integer parallelotope $K \subseteq \mathbb{R}^n$ such that the $(n-1)$-dimensional area of the orthogonal projection $\mathsf{Proj}_{\theta^\perp} K$ of K along any direction $\theta \in S^{n-1}$ is at most $n^{o(1)}$?*

An application of Cauchy's surface area formula (see [27, Section 5.5]), as noted in, e.g., [31, Section 1.6], shows that a positive answer to Question 14 would imply Theorem 1. Correspondingly, a positive answer to Question 14 with $n^{o(1)}$ replaced by $O(1)$ would imply a positive answer to Question 2.

Apart from the intrinsic geometric interest of Question 14, if it had a positive answer, then we would deduce using [31] that there exists an integer parallelotope $K \subseteq \mathbb{R}^n$ such that the normed space $\mathbf{X}$ whose unit ball is K has certain desirable nonlinear properties, namely, we would obtain an improved randomized clustering of $\mathbf{X}$ and an improved extension theorem for Lipschitz functions on subsets of $\mathbf{X}$; we refer to [31] for the relevant formulations since including them here would result in a substantial digression.

Data availability

No data was used for the research described in the article.

Acknowledgments

We are grateful for helpful comments by Noga Alon, Károly Böröczky, Uriel Feige, Pravesh Kothari, Russell Lyons, Elchanan Mossel, Ashwin Sah, Laurent Saloff-Coste, Mehtaab Sawhney and Konstantin Tikhomirov.

References

[1] A.D. Alexandrov, Convex Polyhedra, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005, Translated from the 1950 Russian edition by N. S. Dairbekov, S. S. Kutateladze and A. B. Sossinsky, With comments and bibliography by V. A. Zalgaller and appendices by L. A. Shor and Yu. A. Volkov.

[2] Noga Alon, Uriel Feige, On the power of two, three and four probes, in: Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, Philadelphia, PA, 2009, pp. 346–354.

[3] Noga Alon, Bo'az Klartag, Economical toric spines via Cheeger's inequality, J. Topol. Anal. 1 (2009) 101–111.

[4] Tomaso Aste, Denis Weaire, The Pursuit of Perfect Packing, second ed., Taylor & Francis, New York, 2008.

[5] Károly Bezdek, Sphere packings revisited, Eur. J. Comb. 27 (2006) 864–883.

[6] Mark Braverman, Dor Minzer, Optimal tiling of the Euclidean space using permutation-symmetric bodies, in: 36th Computational Complexity Conference, LIPIcs, in: Leibniz Int. Proc. Inform., vol. 200, Schloss Dagstuhl. Leibniz-Zent. Inform, Wadern, 2021, 5.

[7] Jaigyoung Choe, On the existence and regularity of fundamental domains with least boundary area, J. Differ. Geom. 29 (1989) 623–663.

[8] B. Delaunay, Sur la partition régulière de l'espace à 4 dimensions. I, II, Bull. Acad. Sci. URSS 2 (1929) 79–110 (French).

[9] D. Dellamonica Jr., P. Haxell, T. Łuczak, D. Mubayi, B. Nagle, Y. Person, V. Rödl, M. Schacht, J. Verstraëte, On even-degree subgraphs of linear hypergraphs, Comb. Probab. Comput. 21 (2012) 113–127.

[10] N.P. Dolbilin, Properties of faces of parallelohedra, in: Geometriya, Topologiya i Matematicheskaya Fizika. II, in: Tr. Mat. Inst. Steklova, vol. 266, 2009, pp. 112–126.

[11] N.P. Dolbilin, Parallelohedra: a retrospective and new results, Trans. Mosc. Math. Soc. (2012) 207–220.

[12] Peter Engel, Geometric Crystallography, Handbook of Convex Geometry, vol. A, B, North-Holland, Amsterdam, 1993, pp. 989–1041.

[13] E.S. Fedorov, Načala učeniya o figurah, Izdat. Akad. Nauk SSSR, Moscow, 1953.

[14] Uriel Feige, Small linear dependencies for binary vectors of low weight, in: Building Bridges, in: Bolyai Soc. Math. Stud., vol. 19, Springer, Berlin, 2008, pp. 283–307.

[15] Uriel Feige, Jeong Han Kim, Eran Ofek, Witnesses for non-satisfiability of dense random 3CNF formulas, in: 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), 21-24 October 2006, Berkeley, California, USA, Proceedings, IEEE Computer Society, 2006, pp. 497–508.

[16] Uriel Feige, Guy Kindler, Ryan O'Donnell, Understanding parallel repetition requires understanding foams, in: 22nd Annual IEEE Conference on Computational Complexity, CCC 2007, 13-16 June 2007, San Diego, California, USA, IEEE Computer Society, 2007, pp. 179–192.

[17] László Fejes Tóth, Über das kürzeste Kurvennetz, das eine Kugeloberfläche in flächengleiche konvexe Teile zerlegt, Math. Naturwiss. Anz. Ungar. Akad. Wiss. 62 (1943) 349–354.

[18] R.G. Gallager, Low-density parity-check codes, IRE Trans. Inf. Theory 8 (1962) 21–28.

[19] Apostolos Giannopoulos, Alexander Koldobsky, Petros Valettas, Inequalities for the surface area of projections of convex bodies, Can. J. Math. 70 (2018) 804–823.

[20] Gene H. Golub, Charles F. Van Loan, Matrix Computations, fourth ed., Johns Hopkins Studies in the Mathematical Sciences, Johns Hopkins University Press, Baltimore, MD, 2013.
[21] Venkatesan Guruswami, Pravesh K. Kothari, Peter Manohar, Algorithms and certificates for Boolean CSP refutation: smoothed is no harder than random, in: STOC '22—Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, ACM, New York, 2022, pp. 678–689.
[22] T.C. Hales, The honeycomb conjecture, Discrete Comput. Geom. 25 (2001) 1–22.
[23] Jun-Ting Hsieh, Pravesh K. Kothari, Sidhanth Mohanty, A simple and sharper proof of the hypergraph Moore bound, Preprint, available at https://arxiv.org/abs/2207.10850, 2022.
[24] Lord Kelvin, On homogeneous division of space, Proc. R. Soc. Lond. 55 (1894) 1–16 (English).
[25] Guy Kindler, Ryan O'Donnell, Anup Rao, Avi Wigderson, Spherical cubes and rounding in high dimensions, in: 49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA, IEEE Computer Society, 2008, pp. 189–198.
[26] Guy Kindler, Anup Rao, Ryan O'Donnell, Avi Wigderson, Spherical cubes: optimal foams from computational hardness amplification, Commun. ACM 55 (2012) 90–97.
[27] Daniel A. Klain, Gian-Carlo Rota, Introduction to Geometric Probability, Lezioni Lincee. [Lincei Lectures], Cambridge University Press, Cambridge, 1997.
[28] Zsolt Lángi, An isoperimetric problem for three-dimensional parallelohedra, Pac. J. Math. 316 (2022) 169–181.
[29] Hanno Lefmann, Pavel Pudlák, Petr Savický, On sparse parity check matrices, Des. Codes Cryptogr. 12 (1997) 107–130.
[30] H. Minkowski, Allgemeine Lehrsätze über die convexen Polyeder, Nachr. Ges. Wiss. Gött., Math.-Phys. Kl. 1897 (1897) 198–219 (German).
[31] Assaf Naor, Extension, separation and isomorphic reverse isoperimetry, Preprint, available at https://arxiv.org/abs/2112.11523, 2021.
[32] Assaf Naor, Jacques Verstraëte, Parity check matrices and product representations of squares, Combinatorica 28 (2008) 163–185.
[33] A.M. Odlyzko, Asymptotic Enumeration Methods, Handbook of Combinatorics, vols. 1, 2, Elsevier Sci. B. V., Amsterdam, 1995, pp. 1063–1229.
[34] Ran Raz, A counterexample to strong parallel repetition, SIAM J. Comput. 40 (2011) 771–777.
[35] C.A. Rogers, A note on coverings and packings, J. Lond. Math. Soc. 25 (1950) 327–331.
[36] M.I. Shtogrin, Regular Dirichlet-Voronoĭ Partitions for the Second Triclinic Group, Trudy Mat. Inst. Steklov., vol. 1, Izdat. "Nauka", Moscow, 1973, p. 23.
[37] B.A. Venkov, On a class of Euclidean polyhedra, Vestn. Leningr. Univ., Ser. Mat. Fiz. Him. 9 (1954) 11–31.
[38] Roman Vershynin, An introduction with applications in data science, in: High-Dimensional Probability, in: Cambridge Series in Statistical and Probabilistic Mathematics, vol. 47, Cambridge University Press, Cambridge, 2018, With a foreword by Sara van de Geer.
[39] D. Weaire, R. Phelan, A counter-example to Kelvin's conjecture on minimal surfaces, Philos. Mag. Lett. 69 (1994) 107–110.