arXiv:2301.02862v1 [math.MG] 7 Jan 2023

具有较小表面积的整数平行多胞体

ASSAF NAOR 和 ODED REGEV

摘要。我们证明，对于任意 $n \in \mathbb{N}$，存在一个凸体 $K \subseteq \mathbb{R}n$，其表面积至多为 $n\frac{1}{2}+o(1)$，然而，K在整数格 $\mathbb{Z}$ n的平移像将 $\mathbb{R}n$铺满。

1. 引言

给定 $n \in \mathbb{N}$和一个格 $\Lambda \subseteq \mathbb{R}^n$，如果凸体 $K \subseteq \mathbb{R}^n$是一个 Λ-平行多胞体（例如， [12]），即，K按 Λ的元素进行平移后能够铺满 $\mathbb{R}^n$，也就是说， $\mathbb{R}^n = \Lambda + K = \bigcup_{x\in\Lambda}(x+K)$，并且对于任意不同的 x、$y \in \Lambda$，集合（$x+K$）∩（$y+K$）的内部为空，则称 K为平行多胞体（当 $n = 2$时称为平行六边形，当 $n = 3$时称为平行多面体；有些文献将 $\mathbb{R}^n$中的平行多胞体称为 n维平行多面体；例如， [1, 11]）。如果它对于某个格 $\Lambda \subseteq \mathbb{R}^n$是一个 Λ-平行多胞体，则称其为平行多胞体。我们将 $\mathbb{Z}^n$-平行多胞体称为整数平行多胞体。

超立方体 $[-\frac{1}{2}, \frac{1}{2}]^n$是一个整数平行多胞体，其表面积等于 $2n$。根据 [16, 推论 A， 2],对于每个n {v8>，都存在一个整数平行多胞体$K \subseteq \mathbb{R}^n$，其表面积比 $2n$ 小一个普适常数因子。具体而言， [16] 中考虑的整数平行多胞体K的表面积满足 $\mathrm{vol}_{n-1}(\partial K) \leqslant \sigma(n + O(n^{2/3}))$, 其中 $\sigma = 2\sum_{s=1}^{\infty}(s/e)^s/(s^{3/2}s!) \leqslant 1.23721$。据我们所知，这是目前已知的整数平行多胞体可能具有的最小表面积的最佳上界。本文的主要结果是以下定理：

定理 1。对于每个 $n \in \mathbb{N}$，都存在一个表面积为 $n\frac{1}{2}+o(1)$的整数平行多胞体。

由于 $\mathbb{Z}^n$ 的余体积为 1，任意整数平行多胞体 $K \subseteq \mathbb{R}^n$的体积 $\mathrm{vol}_n(K) = 1$。因此，根据等周不等式，我们有[1]

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

其中 $B_n \stackrel{\mathrm{def}}{=} \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1^2 + \cdots + x_n^2 \leqslant 1\}$ 表示欧几里得球，且 $S^{n-1} \stackrel{\mathrm{def}}{=} \partial B_n$。

根据 (1)，定理 1 在相差隐含的低阶因子的意义下是最优的。这个低阶因子能否完全消去仍是一个未解问题，也就是说，以下问题尚待回答：

问题2。F 对于每个 $n \in \mathbb{N}$，是否存在一个整数平行多胞体 $K \subseteq \mathbb{R}^n$，使得 $\mathrm{vol}_{n-1}(\partial K) \asymp \sqrt{n}$?

问题2可追溯至 [24], ，不过早期研究（从晶体学的角度来看，这自然是如此）聚焦于$n = 3$，并试图求出平行多面体可能具有的最小表面积的精确值；参见 [5] 中的猜想 7.5，以及其前一段中的历史讨论。关于$n = 2$ 时如何精确确定最小周长的对应问题，已在 [7] 中得到解答（一般平行六边形而非整数平行六边形的情形由 [17]解决；另见 [22], ，其中讨论的铺砌块不必是凸的）。当$n = 3$ 时求出精确最小值的问题仍然

A.N. 得到了美国国家科学基金会 DMS-2054875 项目、BSF 201822 项目以及西蒙斯研究员奖的资助。O.R. 得到了美国国家科学基金会 CCF-1320188 项目以及西蒙斯研究员奖的资助。[1]除通常的 O(·)、o(·)、Ω(·)、Θ(·) 记号外，我们还采用以下渐近记号约定。对于 a,b > 0，记作 a . b 或 b ≳ a，表示对某个普适常数 C > 0，有 a 6 Cb；而 a ≍ b 表示 (a . b) ∧(b . a)。若需表示对参数的依赖，我们会用下标标明。例如，存在辅助参数 ε 时，记号 a $\lesssim_\varepsilon$ b 表示 a 6 C(ε)b，其中 C(ε) > 0 可能仅依赖于 ε；a $\gtrsim_\varepsilon$ b 和 a $\asymp_\varepsilon$ b 的含义类似。

悬而未决；我们不再回顾这一主题的大量文献，而是请读者参阅专著 [4]（另见 [28]，其中给出了平行多面体另一种等周型问题的精确解）。

问题2在高维情形下的渐近性质，与文献主要关注的低维情形下寻找精确极小值解有所不同，但它是后者的自然延伸；因此，有理由认为，过去几个世纪中研究这一主题的学者曾考虑过这个问题。然而，据我们所知，在近期人们因发现该问题与理论计算机科学的联系而重新关注它之前，并无已发表的文献提及问题2；这一联系见于 [16]，并在 [33, 25, 3, 26, 6]中得到进一步探讨；具体而言，问题2见于 [6, 第 6]节。

在 [25] 中，证明了如果去掉铺砌集必须是凸集这一要求，问题2便有肯定答案；也就是说，根据 [25, 定理 1，1] 对每个$n \in \mathbb{N}$，都存在一个紧集$\Omega \subseteq \mathbb{R}^n$，使得$\mathbb{R}^n = \mathbb{Z}^n + \Omega$，并且对于任意不同的$x$和$y \in \mathbb{Z}^n$，$(x+\Omega)\cap(y+\Omega)$的内部为空，且$\mathrm{vol}_{n-1}(\partial\Omega)$。 p$n$；另见 [3]中对此结果的证明。 Ω 不具凸性这一点，与 [16]中发现的计算复杂性应用无关。 [25, 3] 中的证明构造出了一个显然非凸的集合 Ω。我们的定理 1 证明采用了完全不同的途径，并给出一个平行otope，其表面积接近 [25] 所保证的上界（在 [25], 之前，紧 $\mathbb{Z}^n$-铺砌集可能达到的最小表面积的最佳已知上界，是 [16]所给出的上述1.23721n）。

虽然人们可能会想把上述紧集 Ω 视为存在表面积相近的整数平行多胞体的证据，但这种希望并不可靠，因为平行多胞体的凸性要求施加了严格限制。具体而言，根据 [30]，对于每个$n \in \mathbb{N}$，$\mathbb{R}^n$中的平行多胞体只有有限种组合类型。[2] 事实上，结合 [10, 第 6] 节与 [30, 36] 可知，$K \subseteq \mathbb{R}^n$ 是平行多胞体，当且仅当K是中心对称多胞体，K的所有（$n-1$）维面都中心对称，并且沿K的任意一个（$n-2$）维面作正交投影，所得图形要么是平行四边形，要么是中心对称六边形。

当然，定理 1 必须给出这样一个受约束多胞体。要理解这是如何实现的，首先需要强调：如果只要求一个表面积较小的平行多胞体，而非表面积较小的整数平行多胞体，那么这项任务就很容易完成。具体来说，根据已有文献可轻易得知，对于每个 n $\in \mathbb{N}$，都存在一个余体积为 1 的秩为 n 的格 $\Lambda \subseteq \mathbb{R}^n$，以及一个 Λ-平行多胞体 K $\subseteq \mathbb{R}^n$，使得 $\mathrm{vol}_{n-1}(\partial \mathrm{K})$. pn。事实上，根据 [34]，存在一个余体积为 1 的秩为 n 的格 $\Lambda \subseteq \mathbb{R}^n$，其填充半径至少为 cpn，其中 c >0 是一个普适常数。令 K 为 Λ的沃罗诺伊胞，即 K 由 $\mathbb{R}^n$ 中到 Λ任意一点的（欧几里得）距离不小于其到原点的距离的点组成。于是，K 是一个 Λ-平行多胞体，$\mathrm{vol}_n(\mathrm{K}) = 1$，因为Λ 的余体积为 1；又由于 Λ 的填充半径至少为 cpn，故 K $\supseteq$ cpnB^n。因此，根据以下简单引理，K 的表面积至多为 c^{-1}pn；在定理 1 的证明中我们将多次用到该引理：

Lem理 3. 设 $n \in \mathbb{N}$ 和实数域 >0。假设凸体 $K \subseteq \mathbb{R}^n$ 满足 $K \supseteq RB^n$。那么 ，

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

引理 3 已为人所知（ 例如， [19, 引理 2。1]）；为完整起见，我们将在第 2 节给出其简短证明。

尽管 $\mathbb{Z}^n$ 的填充半径很小，但上述观察推动了我们对定理 1 的归纳证明，其思路如下。固定 $m \in \{1, \ldots, n-1\}$，并设 V 是 $\mathbb{R}^n$ 的一个 m 维子空间。如果格 $V^\perp \cap \mathbb{Z}^n$ 的秩为 $n-m$，且其填充半径较大，那么引理 3 就给出其沃罗诺伊胞边界的 $(n-m-1)$ 维体积的一个有意义的上界。随后，我们可以考虑格 $\Lambda \subseteq V$，它是 $\mathbb{Z}^n$ 在 V 上的正交投影，并通过归纳法得到一个 Λ 平行多胞体（位于 V 内），其边界的 $(m-1)$ 维体积很小。考虑这样得到的两个凸体的乘积（依据将 $\mathbb{R}^n$ 与 $V^\perp \times V$ 对应起来的识别），我们便有望得到所需的整数平行多胞体。

[2]因此，仅为具体说明（这对当前目的并不重要）：自古以来，人们就知道平行六边形有 2 种类型；根据 [13]，平行多面体有 5 种类型；根据 [8, 35]，四维平行多胞体有 52 种类型。

这一方案显然存在障碍。子空间V的选取必须使格 $V^{\perp}\cap\mathbb{Z}^n$ 足够丰富，同时又不含短的非零向量。此外， $\mathbb{Z}^n$ 在V上的正交投影 Λ 并非 $\mathbb{Z}^m$，因此我们必须假设一个更强的归纳假设，并对 Λ 作适当的“修正”，以便继续归纳。事实证明，$V^{\perp}\cap\mathbb{Z}^n$ 的填充半径可能达到多大、上述修正所造成的损失，以及迭代应用我们前面概述的过程所需的总成本，这三者之间存在相互制约。权衡这些约束后，我们将看到，维数 m 的 V 的最佳选择是 $m = n\exp(-\Theta(\sqrt{\log n}))$。接下来的内容将详述这一策略的具体实施。

2. 定理 1 的证明

下文中，对于每个$n\in\mathbb{N}$，赋范空间 $\ell_2^n=(\mathbb{R}^n,\mathrm{k}\cdot\mathrm{k}_{\ell_2^n})$ 表示标准欧几里得空间，即

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

x、y $\in\mathbb{R}^n$的标准标量积记作 〈x, y〉 def $=\mathrm{x}_1\mathrm{y}_1+\cdots+\mathrm{x}_n\mathrm{y}_n$。$\mathbb{R}^n$的坐标基记作 $\mathrm{e}_1,\ldots,\mathrm{e}_n$，也就是说，对于每个 i $\in\{1,\dots,\mathrm{n}\}$，$\mathrm{e}_i$的第 i 个分量为 1，其余分量均为 0。$\mathbb{R}^n$的原点记作 $\mathbf{0}=(0,\dots,0)$。对于 $0<\mathrm{s}\leq\mathrm{n}$，$\mathbb{R}^n$ 上由 ℓ_2^n度量诱导的 s 维豪斯多夫测度记作 $\mathrm{vol}_s(\cdot)$。特别地，如果 K $\subseteq\mathbb{R}^n$ 是一个凸体（紧致且内部非空），则下列恒等式成立（例如参见 [27]）：

$$\mathrm{vol}_{n-1}(\partial K)=\lim_{\delta\to0^+}\frac{\mathrm{vol}_n(K+\delta B^n)-\mathrm{vol}_n(K)}{\delta}. \tag{2}$$

如果V是 $\mathbb{R}^n$ 的一个子空间，那么其正交补（相对于 ℓ_2^n 欧几里得结构）记为 $V^{\perp}$，从 $\mathbb{R}^n$ 到 V 的正交投影记为Proj_V。讨论V的子集 Ω 时，我们会稍微宽泛地使用记号和术语，将 $\partial\Omega$ 视为 Ω 在V中的边界；类似地，讨论 Ω 的内部时，指的是其在V中的内部。按照这一约定，当$K\subseteq V$是凸体或平行多面体时（相对于V的一个格），相关概念便有了恰当的解释。对于凸体$K\subseteq V$，(2) 的变体为

$$\mathrm{vol}_{\dim(V)-1}(\partial K)=\lim_{\delta\to0^+}\frac{\mathrm{vol}_{\dim(V)}\big(K+\delta(V\cap B^n)\big)-\mathrm{vol}_{\dim(V)}(K)}{\delta}. \tag{3}$$

引理 3 的证明。 由于$K\supseteq RB^n$，对于每个 $\delta>0$，我们有

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

其中，(4) 的最后一步用到了K是凸集这一事实。因此，

$$\mathrm{vol}_{n-1}(\partial K)\overset{(2)}{=}\lim_{\delta\to0^+}\frac{\mathrm{vol}_n(K+\delta B^n)-\mathrm{vol}_n(K)}{\delta}\overset{(4)}{\leqslant}\lim_{\delta\to0^+}\frac{\big(1+\frac{\delta}{R}\big)^n-1}{\delta}\mathrm{vol}_n(K)=\frac{n}{R}\mathrm{vol}_n(K). \qquad\square$$

我们在以下定义中引入的序列 $\{Q(n)\}_{n=1}^{\infty}$ 将在接下来的推理中发挥重要作用：

记号 4。 对每个 $n\in\mathbb{N}$，令 $Q(n)$ 为满足以下条件的所有 $Q\geqslant0$ 的下确界：对于每个秩为 n 的格 $\Lambda\subseteq\mathbb{Z}^n$，都存在一个 Λ-平行多胞体 $K\subseteq\mathbb{R}^n$，使得

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

由于对于任意整数平行多胞体 $K\subseteq\mathbb{R}^n$，$\mathrm{vol}_n(K)=1$，定理 1 是以下结果的特例：

定理 5。 存在一个普适常数 $C\geqslant1$，使得对于每个 $n\in\mathbb{N}$，$Q(n)\lesssim n^{C\sqrt{\log n}}$。

下面的关键引理是在后续证明定理 5 时对n使用归纳法的归纳步骤：

引理 6. 设 $m,n,s \in \mathbb{N}$满足 $s \leqslant m \leqslant n$。假设$\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ 是一个 m 行 n 列矩阵，其所有元素均为整数，且 B 的秩为 m，并且B 的任意 s 列都线性无关。那么，

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

其中$\|\cdot\|_{\ell_2^n\to\ell_2^m}$表示从 ℓ_2^n到 ℓ_2^m的算子范数。

定理 5 讨论了 $\mathbb{Z}^n$中任意满秩子格（回想一下$Q(n)$的定义），而定理 1 中我们只关注 $\mathbb{Z}^n$ 本身；这一点强化了归纳假设，使得我们能够完成引理 6 的证明。如果 Λ 是$\mathbb{Z}^n$的任意满秩子格，那么一个 Λ-平行多胞体 $K \subseteq \mathbb{R}^n$ 不再必然满足 $\mathrm{vol}_n(K) = 1$，因此归纳假设必须纳入 $\mathrm{vol}_n(K)$ 的值，这正是我们在 (5) 中考虑 $\mathrm{vol}_{n-1}(\partial K)/\mathrm{vol}_n(K)$ 这一量的原因。注意，这一量不具有尺度不变性，因此研究它似乎有些不自然，但由于以下简单引理，它非常适用于前述归纳法：

引理 7. 固定 m，$n \in \mathbb{N}$以及一个 m 维子空间 V，它是 $\mathbb{R}^n$ 的子空间。设 $O \subseteq V^{\perp}$ 是 $V^{\perp}$ 的一个开子集，并设 $G \subseteq V$ 是 V 的一个开子集。那么，对于 $\Omega = O + G$，我们有

$$\frac{\mathrm{vol}_{n-1}(\partial\Omega)}{\mathrm{vol}_n(\Omega)} = \frac{\mathrm{vol}_{n-m-1}(\partial O)}{\mathrm{vol}_{n-m}(O)} + \frac{\mathrm{vol}_{m-1}(\partial G)}{\mathrm{vol}_m(G)}. \tag{6}$$

此外，如果 $T:\ \mathbb{R}^m \to V$ 是一个线性同构，且 $K \subseteq \mathbb{R}^m$ 是一个凸体，那么

$$\frac{\mathrm{vol}_{m-1}(\partial TK)}{\mathrm{vol}_m(TK)} \leqslant \frac{\mathrm{vol}_{m-1}(\partial K)}{\mathrm{vol}_m(K)}\|T^{-1}\|_{(V,\|\cdot\|_{\ell_2^n})\to\ell_2^m}, \tag{7}$$

其中 $\|\cdot\|_{(V,\|\cdot\|_{\ell_2^n})\to\ell_2^m}$ 是从赋予由 ℓ_2^n 继承的范数的 V 到 ℓ_2^m 的算子范数。

证明。对于 (6)，注意到由于 $O \perp G$，我们有 $\mathrm{vol}_n(\Omega) = \mathrm{vol}_{n-m}(O)\mathrm{vol}_m(G)$，并且 $\partial\Omega = (\partial O + G)\cup(O + \partial G)$，其中 $\mathrm{vol}_{n-1}((\partial O + G)\cap(O + \partial G)) = 0$，因此 $\mathrm{vol}_{n-1}(\partial\Omega) = \mathrm{vol}_{n-m-1}(\partial O)\mathrm{vol}_m(G) + \mathrm{vol}_{n-m}(O)\mathrm{vol}_{m-1}(\partial G)$。

对于 (7)，记 $\rho = \|T^{-1}\|_{(V,\|\cdot\|_{\ell_2^n})\to\ell_2^m}$，使得 $T^{-1}(V\cap B^n) \subseteq \rho B^m$。因此，

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

将这一包含关系与 (3) 结合起来，我们可知

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

注 8. 我们在陈述引理 7 时令 K 为凸体，因为这正是本文所需的。然而，证明并未实质性地依赖其凸性；所需的仅仅是 K 为 $\mathbb{R}^m$ 中的一个体，且其边界足够正则，从而恒等式 (2) 成立（将 n 替换为 m）。

引理 6 中的任意矩阵 B 都必须有一行至少包含 n/m 个非零项。事实上，否则 B 中非零项的总数将小于 m(n/m) = n，因此 B 的 n 列中至少有一列必定为零，这与假设的线性无关性矛盾（因为 s ⩾ 1）。因此，存在 j ∈{1, . . . , m}，使得 B*e j ∈ $\mathbb{R}^n$中的至少 ⌈n/m⌉ 个元素不为零。这些元素都是整数，因此 kB*e j k ℓ_2^n ⩾ p⌈n/m⌉。由此，(6) 中的量 kBk$_{\ell_2^n\to\ell_2^m}$ = kB*k$_{\ell_2^m\to\ell_2^n}$不可能小于 p⌈n/m⌉。

问题 9. 给定 m，$n \in \mathbb{N}$和 $C > 1$，满足什么条件时，最大 $s = s(m, n, C) \in \mathbb{N}$的数量级是多少？存在 $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ 使得 B 的任意 s 列都线性无关，并且

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

下面的引理是解决问题 9 的一个步骤，我们将在引理 6 的证明中用到：

引理 10. 设 $m,n \in \mathbb{N}$满足 $4 \leqslant m \leqslant n$，且 $n \geqslant (m \log m)/4$。存在 $s \in \mathbb{N}$满足 $s \gtrsim m^2/n$ 的情形，以及秩为 m 的 $\mathrm{B} \in \mathrm{M}_{m\times n}(\mathbb{Z})$，使得 B 的任意 s 列都线性无关，并且

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

引理 10 足以满足我们的需要，但它并非最佳。事实上，我们将在下文证明，在引理 10 的情形下，对于每个 $0 < \varepsilon \leqslant 1$，都存在 $s \in \mathbb{N}$，使得 $s \gtrsim m^{1+\varepsilon}/n^{\varepsilon} = m(m/n)^{\varepsilon} \geqslant m^2/n$，且存在秩为 m 的 $\mathrm{B} \in \mathrm{M}_{m\times n}(\mathbb{Z})$，其任意 s 列B 均线性无关，并且 $\mathrm{kBk}_{\ell_2^n \to \ell_2^m} \lesssim_{\varepsilon} \mathrm{p}n/m$。

虽然问题 9 自然地源自引理 6，而且本身也很有趣，但即使彻底回答问题 9，也无法完全消除定理 1 中的 $o(1)$ 项；后续推理中的瓶颈在别处，它使我们无法对问题2给出这样的答案（若答案确实存在）。

假设引理 *6* 和引理 *10* 成立时定理 *5* 的证明。我们将对 n 使用归纳法。为准备归纳法的基础情形，我们先记录下面这个估计（当格为 $\mathbb{Z}^n$ 时该估计是最佳的）。秩为 n 的 Λ 在 $\mathbb{Z}^n$ 中的子格的沃罗诺伊胞，即集合

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

是一个满足 $K \supseteq \frac{1}{2}B^n$ 的 Λ-平行多胞体。事实上，若 $y \in \Lambda \setminus \{0\}$，则 $\mathrm{kyk}_{\ell_2^n} \geqslant 1$，因为 $y \in \mathbb{Z}^n \setminus \{0\}$。因此，

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

由引理 3 可得，$\mathrm{vol}_{n-1}(\partial K)/\mathrm{vol}_n(K) \leqslant 2n$。这给出了先验界（较弱）：$Q(n) \leqslant 2n$。

固定 $n \in \mathbb{N}$，并假设存在满足 $4 \leqslant m \leqslant n$ 且 $n \geqslant (m \log m)/4$ 的 $m \in \mathbb{N}$。利用引理 6 和引理 10 中的矩阵 B，可知存在一个普适常数 $\kappa \geqslant 4$，使得

$$Q(n) \leqslant \kappa\left(\frac{n^{\frac{3}{2}}}{m} + Q(m)\sqrt{\frac{n}{m}}\right). \tag{8}$$

我们将对 $n \in \mathbb{N}$ 使用归纳法，证明 $Q(n)$ 的以下上界，从而证明定理 5：

$$Q(n) \leqslant 4\kappa\sqrt{n}e^{\sqrt{2(\log n)\log(2\kappa)}}. \tag{9}$$

若 $n \leqslant 4\kappa^2$，则由上述讨论，n 时有 $Q(n) \leqslant 2n \leqslant 4\kappa \mathrm{p}n$，因此 (9) 成立。若 $n > 4\kappa^2$，则定义 e

$$m \overset{\text{def}}{=} \left\lfloor ne^{-\sqrt{2(\log n)\log(2\kappa)}} \right\rfloor. \tag{10}$$

容易验证，这样选取的m满足 $4 \leqslant m < n$且$n \geqslant (m \log m)/4$（并且有余量）。因此，(8)成立。利用归纳假设，可得

$$\begin{aligned} Q(m)\sqrt{\frac{n}{m}} &\leqslant 4\kappa\sqrt{n}e^{\sqrt{2(\log m)\log(2\kappa)}} \overset{(10)}{\leqslant} 4\kappa\sqrt{n}e^{\sqrt{2\left(\log n - \sqrt{2(\log n)\log(2\kappa)}\right)\log(2\kappa)}} \\ &\leqslant 4\kappa\sqrt{n}e^{\left(\sqrt{2\log n} - \sqrt{\log(2\kappa)}\right)\sqrt{\log(2\kappa)}} = 2\sqrt{n}e^{\sqrt{2(\log n)\log(2\kappa)}}, \end{aligned} \tag{11}$$

其中，(11)的倒数第二步用到了不等式 $\mathrm{p}a - b \leqslant \mathrm{p}a - b/(2\mathrm{p}a)$，该不等式对满足$a$、$b \in \mathbb{R}$且$a \geqslant b$的所有值都成立；在这里，$a = \log n$且$b = \sqrt{2(\log n)\log(2\kappa)}$，并且$a > b$，因为我们现在讨论的是$n > 4\kappa^2$的情形。将(11)代入(8)，并利用$m \geqslant \frac{1}{2}n\exp\left(-\sqrt{2(\log n)\log(2\kappa)}\right)$由(10)可知成立，得到(9)，从而完成定理 5 的证明。□

接下来我们将证明引理 6，这是定理 1 背后的关键递归步骤。

引理 6 的证明。为便于后续证明，我们先给出以下两个初等观察。将 B 的行空间记为 $\mathrm{V} = \mathrm{B}^*\mathbb{R}^m \subseteq \mathbb{R}^n$，并注意到由于假设 B 的秩为 m，故 $\dim(\mathrm{V}) = \mathrm{m}$。设 Λ 是一个秩为 n 且包含于 $\mathbb{Z}^n$的格。首先，我们断言格 $\mathrm{V}^{\perp} \cap \Lambda$的秩等于 $\mathrm{n} - \mathrm{m}$。事实上，我们可以写成 $\mathrm{V}^{\perp} \cap \Lambda = \mathrm{C}(\mathbb{Z}^n \cap \mathrm{C}^{-1}\mathrm{V}^{\perp})$，其中 C 是一个整数项可逆矩阵，即 $\mathrm{C} \in \mathrm{M}_n(\mathbb{Z}) \cap \mathrm{GL}_n(\mathbb{Q})$，使得 $\Lambda = \mathrm{C}\mathbb{Z}^n$。此外，$\mathrm{V}^{\perp} = \mathrm{B}$ 的核，因此

在 $\mathbb{Q}$ 上的维数， $\mathbb{Q}^n \cap V^\perp$ 等于 $n-m$。由于 $C^{-1} \in GL_n(\mathbb{Q})$，可知 $C^{-1}V^\perp$ 包含 $\mathbb{Z}^n$ 中的 $n-m$ 个线性无关元素。其次，我们断言 Λ 到 V 上的正交投影 $\mathrm{Proj}_V \Lambda$ 是 V 的一个离散子集，因此是一个格；由于我们假设 $\mathrm{span}(\Lambda) = \mathbb{R}^n$，其秩将为 $\dim(V) = m$，因此 $\mathrm{span}(\mathrm{Proj}_V \Lambda) = \mathrm{Proj}_V(\mathrm{span}(\Lambda)) = \mathrm{Proj}_V(\mathbb{R}^n) = V$。我们需要验证：对于任意满足 $\lim_{i\to\infty} \mathrm{Proj}_V x_i = \mathbf{0}$ 的 $\{x_1, x_2, \ldots\} \subseteq \Lambda$，存在 $i_0 \in \mathbb{N}$，使得当 $i \in \{i_0, i_0+1, \ldots\}$ 时，$\mathrm{Proj}_V x_i = \mathbf{0}$。事实上，由于 $V^\perp = B$ 的核，对每个 $x \in \mathbb{R}^n$ 都有 $Bx = B\mathrm{Proj}_V x$，因此 $\lim_{i\to\infty} Bx_i = \mathbf{0}$。但是，对每个 $i \in \mathbb{N}$ 都有 $Bx_i \in \mathbb{Z}^m$，因为 $B \in M_{m\times n}(\mathbb{Z})$ 且 $x_i \in \Lambda \subseteq \mathbb{Z}^n$。因此，存在 $i_0 \in \mathbb{N}$，使得对每个 $i \in \{i_0, i_0+1, \ldots\}$ 都有 $Bx_i = \mathbf{0}$，即 x_i 属于 B 的核 $= V^\perp$，故 $\mathrm{Proj}_V x_i = \mathbf{0}$。

令 $K_1 \subseteq V^\perp$ 为 $V^\perp \cap \Lambda$ 的沃罗诺伊胞，即 $K_1 = \{x \in V^\perp : \forall y \in V^\perp \cap \Lambda, \|x\|_{\ell_2^n} \leqslant \|x - y\|_{\ell_2^n}\}$。若 $y = (y_1, \ldots, y_n) \in V^\perp = \mathrm{Ker}(B)$，则 $y_1 Be_1 + \cdots + y_n Be_n = \mathbf{0}$。根据对 B 的假设，这意味着若还有 $y \neq \mathbf{0}$，则 $|\{i \in \{1, \ldots, n\} : y_i \neq 0\}| > s$。因此，由于 Λ 中元素的分量都是整数，

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

因此，若 $x \in \frac{\sqrt{s}}{2}(V^\perp \cap B^n)$，则

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

这意味着 $K_1 \supseteq \frac{\sqrt{s}}{2}(V^\perp \cap B^n)$，因此由引理 3 可得

$$\frac{\mathrm{vol}_{n-m-1}(\partial K_1)}{\mathrm{vol}_{n-m}(K_1)} \leqslant \frac{n-m}{\frac{1}{2}\sqrt{s}} = \frac{2(n-m)}{\sqrt{s}}. \tag{12}$$

接下来，固定 $i \in \{1, \ldots, m\}$。根据 V 的定义，i 的第 $B^* e_i$ 行属于 V，因此

$$\forall (x, i) \in \mathbb{R}^n \times \{1, \ldots, m\}, \qquad \langle x, B^* e_i \rangle = \langle \mathrm{Proj}_V x, B^* e_i \rangle. \tag{13}$$

由于 B 的所有元素都是整数，因此可得

$$\forall (x, i) \in \mathbb{Z}^n \times \{1, \ldots, m\}, \qquad \langle B\mathrm{Proj}_V x, e_i \rangle = \langle \mathrm{Proj}_V x, B^* e_i \rangle \overset{(13)}{=} \langle x, B^* e_i \rangle \in \mathbb{Z}.$$

换言之，$B\mathrm{Proj}_V \mathbb{Z}^n \subseteq \mathbb{Z}^m$，因此格 $B\mathrm{Proj}_V \Lambda$ 是 $\mathbb{Z}^m$ 的子集。此外，由于 $\mathrm{Ker}(B) = V^\perp$，$B$ 在 V 上是单射的，所以 $B\mathrm{Proj}_V \mathbb{Z}^n$ 是 $\mathbb{Z}^m$ 的一个秩为 m 的子格。根据 $Q(m)$ 的定义，存在一个 $B\mathrm{Proj}_V \Lambda$-平行多胞体 $K_2^0 \subseteq \mathbb{R}^m$，使得

$$\frac{\mathrm{vol}_{m-1}(\partial K_2^0)}{\mathrm{vol}_m(K_2^0)} \leqslant Q(m). \tag{14}$$

由于 $V^\perp = \mathrm{Ker}(B)$，且 B 的秩为 $m = \dim(V)$，所以将 B 限制在 V 上所得的映射 $B|_V$ 是 V 与 $\mathbb{R}^m$ 之间的同构。令 $T: \mathbb{R}^m \to V$ 表示 $B|_V$ 的逆映射，定义 $K_2 = TK_2^0$。结合引理 7 的（第二部分）与（14），可得

$$\frac{\mathrm{vol}_{m-1}(\partial K_2)}{\mathrm{vol}_m(K_2)} \leqslant Q(m)\|B\|_{\ell_2^n \to \ell_2^m}. \tag{15}$$

令 $K = K_1 + K_2 \subseteq \mathbb{R}^n$。结合引理 7（第一部分）与 (12) 和 (15)，可得

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

因此，只需验证 K 是一个 Λ-平行多胞体，引理 6 的证明便告完成。我们的构造从设计上就保证了这一点，因为 K_1 是一个 $(V^\perp \cap \Lambda)$-平行多胞体，而 K_2 是一个 $\mathrm{Proj}_V \Lambda$-平行多胞体；验证这一事实只需展开定义，下面我们将为完整起见进行说明。

固定 $z \in \mathbb{R}^n$。由于 $\mathbb{R}^m = B\mathrm{Proj}_V \Lambda + K_2$，因此存在 $x \in \Lambda$，使得 $B\mathrm{Proj}_V z \in B\mathrm{Proj}_V x + K_2$。将 T 应用于这个包含关系，并利用 $TB|_V$ 是恒等映射，可得 $\mathrm{Proj}_V z \in \mathrm{Proj}_V x + K_2$。接下来，$V^\perp = K_1 + V^\perp \cap \Lambda$，因为 K_1 是 $V^\perp \cap \Lambda$ 的沃罗诺伊胞，所以存在 $y \in V^\perp \cap \Lambda$，使得 $\mathrm{Proj}_{V^\perp} z - \mathrm{Proj}_{V^\perp} x \in y + K_1$。因此，$z = \mathrm{Proj}_{V^\perp} z + \mathrm{Proj}_V z \in \mathrm{Proj}_{V^\perp} x + y + K_1 + \mathrm{Proj}_V x + K_2 = x + y + K \in \Lambda + K$。故，$\Lambda + K = \mathbb{R}^n$。

还需验证，对每个 $w \in \Lambda \setminus \{0\}$，$K$ 的内部都不与 $w + K$ 相交。事实上，根据 K 的定义，若 k 属于 K 的内部，则 $k = k_1 + k_2$，，其中 k_1 属于 K_1 的内部，且 k_2 属于 K_2 的内部。由于 B 在 $K_2 \subseteq V$ 上是单射，因此 Bk_2 属于 $BK_2 = K$ 02 的内部。若 $\mathrm{Proj}_V w \neq 0$，则 $B\mathrm{Proj}_V w \in B\mathrm{Proj}_V \Lambda \setminus \{0\}$，因此，由于 K 02 是一个 $B\mathrm{Proj}_V \Lambda$-平行多胞体，$Bk_2 \notin B\mathrm{Proj}_V w + K$ 02。将 T 应用于此包含关系可知，$k_2 \notin \mathrm{Proj}_V w + K_2$，，这意味着 $k \notin w + K$。另一方面，若 $\mathrm{Proj}_V w = 0$，则 $w \in (V^{\perp} \cap \Lambda) \setminus \{0\}$。由于 K_1 是一个 $V^{\perp} \cap \Lambda$-平行多胞体，因此 $k_1 \notin w + K_1$，，故 $k \notin w + K$。□

为了完成定理 5 的证明，还需证明引理 10。为便于后文引用，我们先记录以下简单的线性代数事实：

观察 11. 取 $m, n, s \in \mathbb{N}$，其中 $s \leqslant m \leqslant n$。假设存在 $A \in M_{m \times n}(\mathbb{Z})$，使得其任意 s 列都线性无关。那么，也存在 $B \in M_{m \times n}(\mathbb{Z})$，使得其任意 s 列都线性无关，且 B 的秩为 m，并且

$$\|B\|_{\ell_2^n \to \ell_2^m} \leqslant \sqrt{1 + \|A\|^2_{\ell_2^n \to \ell_2^m}}. \tag{16}$$

证明。令 $r \in \{1, \ldots, m\}$ 为 A 的秩。通过置换 A 的行，不妨设其前 r 行，即 $A^* e_1, \ldots, A^* e_r \in \mathbb{R}^n$，线性无关。此外，由于我们可以从 $\{e_1, \ldots, e_n\} \subseteq \mathbb{R}^n$ 中添加 $n - r$ 个向量，将 $A^* e_1, \ldots, A^* e_r$ 补成 $\mathbb{R}^n$ 的一组基，因此通过置换 A 的列，不妨设向量 $A^* e_1, \ldots, A^* e_r, e_{r+1}, \ldots, e_m \in \mathbb{R}^n$ 线性无关。令 $B \in M_{m \times n}(\mathbb{Z})$ 为行向量是 $A^* e_1, \ldots, A^* e_r, e_{r+1}, \ldots, e_m$ 的矩阵，因此按构造，B 的秩为 m。此外，

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

因此，(16) 成立。还需验证 B 的任意 s 列都线性无关。事实上，取 $S \subseteq \{1, \ldots, n\}$，满足 $|S| = s$，并令 $\{\alpha_j\}_{j \in S} \subseteq \mathbb{R}$，使得对每个 $i \in \{1, \ldots, m\}$，都有 $\sum_{j \in S} \alpha_j B_{ij} = 0$。特别地，对每个 $i \in \{1, \ldots, r\}$，都有 $\sum_{j \in S} \alpha_j A_{ij} = 0$。若 $k \in \{r + 1, \ldots, m\}$，由于 A 的第 k 行属于 A 的前 r 行的张成空间，存在 $\beta_{k1}, \ldots, \beta_{kr} \in \mathbb{R}$，使得对每个 $j \in \{1, \ldots, n\}$，都有 $A_{kj} = \sum_{i=1}^{r} \beta_{ki} A_{ij}$。因此，$\sum_{j \in S} \alpha_j A_{kj} = \sum_{i=1}^{r} \beta_{ki} \sum_{j \in S} \alpha_j A_{ij} = 0$。这表明，对每个 $i \in \{1, \ldots, m\}$，都有 $\sum_{j \in S} \alpha_j A_{ij} = 0$。根据 A 的假设性质，这意味着对每个 $j \in S$，$\alpha_j = 0$。□

以下引理是支撑我们证明引理 10 的主要存在性结论：

引理 12。 存在一个普适常数 $c > 0$，具有以下性质。设 $d, m, n \geqslant 3$ 为整数，满足 $d \leqslant m \leqslant n$，且 $n \geqslant (m \log m)/d$。此外，假设 $s \in \mathbb{N}$ 满足

$$s \leqslant \frac{c}{d} \left(\frac{m^d}{n^2} \right)^{\frac{1}{d-2}}. \tag{17}$$

那么，存在一个 m 行 n 列的矩阵 $A \in M_{m \times n}(\{0,1\})$，具有以下性质：

- A 的任意 s 列在域 $\mathbb{Z}/(2\mathbb{Z})$ 上线性无关；
- A 的每一列至多有 d 个非零项；
- A 的每一行至多有 $5dn/m$ 个非零项。

接下来的引理 12 证明采用了低密度奇偶校验（LDPC）码文献中常见的概率推理；其基本遵循开创性工作 [18]。尽管类似的论述曾出现在许多地方，我们却未能找到明确陈述引理 12 的参考文献。[3] 本工作的一个特点是，出于我们在上述由引理 6 和引理 10 推导定理 5 的过程中所见的原因，我们需要选择 m 对 n 的一种非标准依赖关系；回顾式（10）。

[3] LDPC 文献中讨论的标准参数范围，采用引理 12 的记号时，要么是 $m \asymp n$ 的情形；要么是 s、d 固定，而相关问题变为当 $m \to \infty$ 时 n 能有多大；前一种情形的紧确界由 [18] 给出，后一种情形的紧确界由 [29, 32] 给出。关于参数具有中间渐近行为时这些问题的研究见 [15, 14, 2, 9, 21, 23]。

In t在引理 12 的证明过程中，我们将使用以下概率估计：

引理 13。 设 $\{W(t)=(W(t,1),\dots,W(t,m))\}_{t=0}^{\infty}$ 为从原点出发、在离散超立方体 $\{0,1\}^m$ 上的标准随机游走。因此，$W(0)=\mathbf{0}$，并且对每个 $t\in\mathbb{N}$，随机向量 $W(t)$ 由随机向量 $W(t-1)$ 通过均匀随机地选取一个指标 $i\in\{1,\dots,m\}$ 并令其为下式而得到

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

于是，对每个 $t\in\mathbb{N}$，都有概率 $[W(t)=\mathbf{0}]\leqslant 2(t/m)^{t/2}$。

证明。 若 t 为奇数，则概率 $[W(t)=\mathbf{0}]=0$，因此以下设 t 为偶数。令 $\mathsf{P}\in\mathsf{M}_{\{0,1\}^m\times\{0,1\}^m}(\mathbb{R})$ 表示随机游走 W 的转移矩阵，即，

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

那么，概率 $[W(t)=\mathbf{0}]=(\mathsf{P}^t)_{\mathbf{00}}$。由对称性，$\mathsf{P}^t$ 的所有 2^m 对角元素都相等，因此 $(\mathsf{P}^t)_{\mathbf{00}}=$ 等于 $\mathrm{Trace}(\mathsf{P}^t)/2^m$。对于每个 $S\subseteq\{0,1\}^m$，沃尔什函数 $(x\in\{0,1\}^m)\mapsto(-1)^{\sum_{i\in S}x^i}$ 是 P 的特征向量，其特征值等于 $1-2|S|/m$。因此，

$$\mathrm{Prob}[W(t)=\mathbf{0}]=\frac{1}{2^m}\mathrm{Trace}(\mathsf{P}^t)=\frac{1}{2^m}\sum_{k=0}^{m}\binom{m}{k}\left(1-\frac{2k}{m}\right)^t. \tag{18}$$

假设 $\beta_1,\ \dots,\ \beta_m$ 是相互独立、取值为 $\{0,1\}$ 且无偏的伯努利随机变量，也就是说，对于任意 $i\in\{1,\dots,m\}$，概率 $[\beta_i=0]=$ 概率 $[\beta_i=1]=1/2$。根据霍夫丁不等式（例如，[37, 定理 2.2.6]），

$$\forall u\geqslant 0,\qquad \mathrm{Prob}\left[\left|\sum_{i=1}^{m}\left(\beta_i-\frac{1}{2}\right)\right|\geqslant u\right]\leqslant 2e^{-\frac{2u^2}{m}}. \tag{19}$$

注意到（18）式右端等于 $\left(1-\frac{2}{m}\sum_{i=1}^{m}\beta_i\right)^t$ 的期望，我们得到

$$\begin{aligned}\mathrm{Prob}[W(t)=\mathbf{0}]&\overset{(18)}{=}\left(-\frac{2}{m}\right)^t\mathbb{E}\left[\left(\sum_{i=1}^{m}\left(\beta_i-\frac{1}{2}\right)\right)^t\right]=\left(\frac{2}{m}\right)^t\int_0^{\infty}tu^{t-1}\mathrm{Prob}\left[\left|\sum_{i=1}^{m}\left(\beta_i-\frac{1}{2}\right)\right|\geqslant u\right]\mathrm{d}u\\&\overset{(19)}{\leqslant}2t\left(\frac{2}{m}\right)^t\int_0^{\infty}u^{t-1}e^{-\frac{2u^2}{m}}\,\mathrm{d}u=2\left(\frac{2}{m}\right)^{\frac{t}{2}}\left(\frac{t}{2}\right)!\leqslant 2\left(\frac{2}{m}\right)^{\frac{t}{2}}\left(\frac{t}{2}\right)^{\frac{t}{2}}=2\left(\frac{t}{m}\right)^{\frac{t}{2}}.\end{aligned}$$

□

利用引理 13，我们现在可以证明引理 12。

引理 12 的证明。考虑随机矩阵 $\mathrm{A}\in\mathrm{M}_{m\times n}(\{0,1\})$，其列是 $\mathrm{W}_1(\mathrm{d})$、…、$\mathrm{W}_n(\mathrm{d})$ 的相互独立且同分布的副本，其中 $\mathrm{W}(0)=\mathbf{0}$、$\mathrm{W}(1)$、$\mathrm{W}(2)$、… 是定义在 $\{0,1\}^m$ 上、如引理 13 中所述的标准随机游走。根据构造，A 的每一列至多含有 d 个非零项。固定 $(\mathrm{i},\mathrm{j})\in\{1,\dots,\mathrm{m}\}\times\{1,\dots,\mathrm{n}\}$。如果 $\mathrm{W}j(\mathrm{d},\mathrm{i})=1$，那么生成 $\mathrm{W}j(\mathrm{d})$ 的随机游走的 d 步中至少有一步改变了第 i 个坐标。后一个事件的概率等于 $1-(1-1/\mathrm{m})^d$。因此，$\mathrm{Prob}[\mathrm{W}j(\mathrm{d},\mathrm{i})=1]\leqslant 1-(1-1/\mathrm{m})^d\leqslant \mathrm{d}/\mathrm{m}$，从而对于任意固定的 $\mathrm{S}\subseteq\{1,\dots,\mathrm{n}\}$，$\mathrm{W}j(\mathrm{d},\mathrm{i})=1$ 对每个 $\mathrm{j}\in\mathrm{S}$ 都成立的概率至多为 $(\mathrm{d}/\mathrm{m})^{|S|}$。 consequently，A 的所有行都至多含有 $\ell=\lceil 4\mathrm{d}\,\mathrm{n}/\mathrm{m}\rceil$ 个非零项的概率至少为

$$1-m\binom{n}{\ell}\left(\frac{d}{m}\right)^{\ell}\geqslant 1-m\left(\frac{en}{\ell}\right)^{\ell}\left(\frac{d}{m}\right)^{\ell}=1-m\left(\frac{edn}{m\ell}\right)^{\ell}\geqslant 1-m\left(\frac{e}{4}\right)^{4\log m}\geqslant\frac{1}{3},$$

其中，第一步应用了斯特林公式，倒数第二步使用了 $\ell\geqslant 4dn/m$ 以及假设 $n\geqslant(m\log m)/d$，最后一步成立是因为 $m\geqslant 3$。

因此，只需证明：以大于 2/3 的概率，对于每个满足 $|S|\leqslant s$ 的 $\varnothing\neq S\subseteq\{1,\dots,n\}$，向量 $\{W_i(d)\}_{i\in S}\subseteq\{0,1\}^m$ 在 $\mathbb{Z}/(2\mathbb{Z})$ 上线性无关，其中 $s\in\mathbb{N}$ 满足（17），而（17）中出现的普适常数 $c>0$ 将在稍后指定；见（23）。因此，只需证明：以大于 2/3 的概率，对于每个满足 $|S|\leqslant s$ 的 $\varnothing\neq S\subseteq\{1,\dots,n\}$，都有 $\sum_{i\in S}W_i(d)\neq\mathbf{0}\bmod 2$。

因此，令 D 表示满足 $|S| \leqslant s$ 且满足 $\sum_{i\in S} W_i(d) \equiv \mathbf{0} \bmod 2$ 的 $\varnothing \neq S \subseteq \{1,\dots,n\}$ 的数量，则只需证明 $2/3 < \mathrm{Prob}[D=0] = 1 - \mathrm{Prob}[D \geqslant 1]$。根据马尔可夫不等式，如果我们证明 $\mathbb{E}[D] < 1/3$，则引理 12 的证明即告完成。

D 的期望值可以精确计算。事实上，

$$\mathbb{E}[D] = \mathbb{E}\left[\sum_{\substack{S\subseteq\{1,\dots,n\}\\ 1\leqslant|S|\leqslant s}} \mathbf{1}_{\{\sum_{i\in S} W_i(d)\equiv \mathbf{0} \bmod 2\}}\right] = \sum_{r=1}^{s}\binom{n}{r}\mathrm{Prob}[W(dr)=\mathbf{0}], \tag{20}$$

这里我们利用了以下事实：对于每个 $\varnothing \neq S \subseteq \{1,\dots,n\}$，$\sum_{i\in S} W_i(d) \bmod 2 \in \{0,1\}^m$ 与 $W(d|S|)$ 具有相同的分布。将引理 13 的结论代入（20），我们得到

$$\mathbb{E}[D] \leqslant 2\sum_{r=1}^{s}\binom{n}{r}\left(\frac{dr}{m}\right)^{\frac{dr}{2}} \leqslant 2\sum_{r=1}^{s}\left(\frac{ed^{\frac{d}{2}}r^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}}\right)^{r}, \tag{21}$$

其中在最后一步中，我们使用斯特林公式对二项式系数进行了界定。对于每个 $r \in \{1,\dots,s\}$，

$$\frac{ed^{\frac{d}{2}}r^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}} \leqslant \frac{ed^{\frac{d}{2}}s^{\frac{d}{2}-1}n}{m^{\frac{d}{2}}} \overset{(17)}{\leqslant} edc^{\frac{d}{2}-1} < \frac{1}{7}, \tag{22}$$

只要

$$c < \inf_{d\geqslant 3}\left(\frac{1}{7ed}\right)^{\frac{2}{d-2}} \in (0,1). \tag{23}$$

存在 因此，当 (23) 成立时，我们可以将 (22) 代入 (21)，得到 $\mathbb{E}[D] < 2\sum_{r=1}^{\infty}\frac{1}{7^r} = \frac{1}{3}$. □

现在我们可以证明引理 10，从而完成定理 5 的证明。

引理 *10* 的证明。 我们将证明以下更强的命题（引理 10 是其特例 $\varepsilon = 1$）。若 $0 < \varepsilon \leqslant 2$ 且 $m,n \in \mathbb{N}$ 满足 $2 + \lfloor 2/\varepsilon \rfloor \leqslant m \leqslant n$ 且 $n \geqslant (m\log m)/(2 + \lfloor 2/\varepsilon \rfloor)$，则存在 $s \in \mathbb{N}$，使得 $s \gtrsim \varepsilon m^{1+\varepsilon}/n^{\varepsilon}$，并且 $\mathsf{B} \in \mathsf{M}_{m\times n}(\mathbb{Z})$ 满足：B 的任意 s 列均线性无关，且 B 的行线性无关，并且

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

事实上，应用引理 12，取 $d = 2 + \lfloor 2/\varepsilon \rfloor \geqslant 3$（等价地，$d \geqslant 3$ 是满足 $2/(d-2) \geqslant \varepsilon$ 的最大整数），可推出存在一个整数 s 满足

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

以及一个矩阵 $\mathsf{A} \in \mathsf{M}_{m\times n}(\{0,1\}) \subseteq \mathsf{M}_{m\times n}(\mathbb{Z})$，满足 A 的任意 s 列在 $\mathbb{Z}/(2\mathbb{Z})$ 上线性无关，A 的每列至多有 d 个非零项，且 A 的每行至多有 $5dn/m$ 个非零项。如果一组向量 $\mathrm{v}_1,\dots,\mathrm{v}_s \in \{0,1\}^m$ 在 $\mathbb{Z}/(2\mathbb{Z})$ 上线性无关，那么它们在 $\mathbb{R}$ 上也线性无关（例如，令 $\mathsf{V} \in \mathsf{M}_{m\times s}(\{0,1\})$ 表示以 $\mathrm{v}_1,\dots,\mathrm{v}_s$ 为列的矩阵，则后一条件等价于 $\mathsf{V}^*\mathsf{V} \in \mathsf{M}_s(\{0,1\})$ 的行列式是一个奇整数，因此特别地它不为零）。因此，A 的任意 s 列在 $\mathbb{R}$ 上都线性无关。此外，

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

其中第一步是一个标准界，对任意 $m\times n$ 实矩阵均成立（例如，[20, 推论 2.3.2]）。因此，A 具备引理 10 中要求矩阵 B 满足的所有性质，只是我们尚不知道 A 的秩为 m；而观察 11 解决了这个（小）问题。□

最后，我们提出以下问题：

问题14. 固定 $n \in \mathbb{N}$。是否存在一个整数平行多胞体 $K \subseteq \mathbb{R}^n$，使得沿任意方向 $\theta \in S^{n-1}$ 对 K 作正交投影 $\mathrm{Proj}_{\theta^\perp} K$ 后，投影的（$n-1$）维面积至多为 $n^{o(1)}$?

正如例如 [31, 第 1.6], 节 [27, 第 5.5]节中所述，应用柯西表面积公式可知，若问题14有肯定答案，则定理 1成立。相应地，若将问题14中$n^{o(1)}$ 替换为$O(1)$后仍有肯定答案，则问题2也有肯定答案。

除了问题14本身具有几何上的意义之外，若该问题有肯定答案，我们便可利用 [31] 推出：存在一个整数平行多胞体$K \subseteq \mathbb{R}^n$，使得以K为单位球的赋范空间$\mathbf{X}$ 具有某些理想的非线性性质；具体而言，我们将得到$\mathbf{X}$ 更优的随机聚类，以及$\mathbf{X}$子集上利普希茨函数更优的延拓定理。相关表述见 [31] ；若在此处列出，将大幅偏离主题。

参考文献

[1] A. D. Alexandrov，《凸多面体》，Springer 数学专著丛书，Springer-Verlag，柏林，2005年。由 N. S. Dairbekov、S. S. Kutateladze 和 A. B. Sossinsky 从1950年俄文版译出，附有 V. A. Zalgaller 的评注和参考文献，以及 L. A. Shor 和 Yu. A. Volkov 的附录。[2] Noga Alon 和 Uriel Feige，《论二探针、三探针和四探针的威力》，第二十届 ACM-SIAM 离散算法研讨会论文集，SIAM，费城，宾夕法尼亚州，2009年，第346–354页。[3] Noga Alon 和 Bo’az Klartag，《利用切格不等式构造经济的环面脊》，《拓扑分析杂志》1 (2009)，101–111。[4] Tomaso Aste 和 Denis Weaire，《追寻完美堆积》，第二版，泰勒与弗朗西斯出版社，纽约，2008年。[5] Károly Bezdek，《重新审视球堆积》，《欧洲组合学杂志》27 (2006)，864–883。[6] Mark Braverman 和 Dor Minzer，《利用置换对称体实现欧几里得空间的最优铺砌》，第36届计算复杂性会议，LIPIcs，《莱布尼茨信息学国际论文集》，第200卷，达格施图尔城堡：莱布尼茨信息学中心，瓦德恩，2021年，第5号论文，48页。[7] Jaigyoung Choe，《关于具有最小边界面积的基本域的存在性与正则性》，《微分几何杂志》29 (1989)，623–663。[8] B. Delaunay，《四维空间的正则划分 I、II》，《苏联科学院通报》2 (1929)，79–110（法文）。[9] D. Dellamonica, Jr.、P. Haxell、T. Łuczak、D. Mubayi、B. Nagle、Y. Person、V. Rödl、M. Schacht 和 J. Verstraëte，《线性超图的偶度子图》，《组合学、概率与计算》21 (2012)，113–127。[10] N. P. Dolbilin，《平行多面体的面的性质》，《斯捷克洛夫数学研究所论文集》266 (2009)，112–126。[11] N. P. Dolbilin，《平行多面体：回顾与新结果》，《莫斯科数学会汇刊》(2012)，207–220。[12] Peter Engel，《几何晶体学》，《凸几何手册》，A、B卷，北荷兰出版社，阿姆斯特丹，1993年，第989–1041页。[13] E. S. Fedorov，《图形学说原理》，苏联科学院出版社，莫斯科，1953年。[14] Uriel Feige，《低重量二进制向量的小线性相关》，《搭建桥梁》，Bolyai数学研究丛书，第19卷，Springer，柏林，2008年，第283–307页。[15] Uriel Feige、Jeong Han Kim 和 Eran Ofek，《稠密随机3-CNF公式不可满足性的见证》，第47届IEEE计算机科学基础年会（FOCS 2006），2006年10月21日至24日，美国加利福尼亚州伯克利，论文集，IEEE计算机学会，2006年，第497–508页。[16] Uriel Feige、Guy Kindler 和 Ryan O’Donnell，《理解平行重复需要理解泡沫》，第22届IEEE计算复杂性年会（CCC 2007），2007年6月13日至16日，美国加利福尼亚州圣迭戈，IEEE计算机学会，2007年，第179–192页。[17] László Fejes Tóth，《将球面划分为面积相等的凸区域的最短曲线网》，《匈牙利科学院数学与自然科学通报》62 (1943)，349–354。[18] R. G. Gallager，《低密度奇偶校验码》，《IRE信息论汇刊》8 (1962)，21–28。[19] Apostolos Giannopoulos、Alexander Koldobsky 和 Petros Valettas，《关于凸体投影表面积的不等式》，《加拿大数学杂志》70 (2018)，804–823。[20] Gene H. Golub 和 Charles F. Van Loan，《矩阵计算》，第四版，约翰斯·霍普金斯数学科学研究丛书，约翰斯·霍普金斯大学出版社，巴尔的摩，马里兰州，2013年。[21] Venkatesan Guruswami、Pravesh K. Kothari 和 Peter Manohar，《布尔约束满足问题反驳的算法与证书：平滑情形不比随机情形更难》，STOC ’22——第54届ACM SIGACT计算理论研讨会论文集，ACM，纽约，[2022] ©2022，第678–689页。[22] T. C. Hales，《蜂窝猜想》，《离散与计算几何》25 (2001)，1–22。[23] Jun-Ting Hsieh、Pravesh K. Kothari 和 Sidhanth Mohanty，《超图摩尔界的一个简洁而更精确的证明》，预印本见 https://arxiv.org/abs/2207.10850，2022年。[24] Lord Kelvin，《关于空间的均匀划分》，《伦敦皇家学会会刊》55 (1894)，1–16（英文）。

[25] Guy Kindler、Ryan O'Donnell、Anup Rao 和 Avi Wigderson，高维球面立方体与舍入，第49届IEEE计算机科学基础年会，FOCS 2008，2008年10月25日至28日，美国宾夕法尼亚州费城，IEEE计算机学会，2008年，第189–198页。[26] Guy Kindler、Anup Rao、Ryan O'Donnell 和 Avi Wigderson，球面立方体：由计算困难性放大得到的最优泡沫，《ACM通讯》**55** (2012)，90–97。[27] Daniel A. Klain 和 Gian-Carlo Rota，几何概率导论，Lezioni Lincee。 [林琴科学院讲座], 剑桥大学出版社，剑桥，1997年。[28] Zsolt Lángi，三维平行多面体的一个等周问题，《太平洋数学杂志》**316** (2022)，169–181。[29] Hanno Lefmann、Pavel Pudlák 和 Petr Savický，关于稀疏校验矩阵，《设计、编码与密码学》**12** (1997)，107–130。[30] H. Minkowski，关于凸多面体的一般定理。，《哥廷根科学学会通报》，数学—物理学部**1897** (1897)，198–219（德文）。[31] Assaf Naor，延拓、分离与同构反向等周不等式，预印本见`https://arxiv.org/abs/2112.11523`，2021年。[32] Assaf Naor 和 Jacques Verstraëte，校验矩阵与正方形的乘积表示，《组合数学》**28** (2008)，163–185。[33] Ran Raz，强平行重复的一个反例，《SIAM计算杂志》**40** (2011)，771–777。[34] C. A. Rogers，关于覆盖与堆积的一则短注，《伦敦数学学会杂志》**25** (1950)，327–331。[35] M. I. Shtogrin，第二三斜群的正则狄利克雷—沃罗诺 ˘ι 划分，Nauka出版社，莫斯科，1973年，《斯捷克洛夫数学研究所论文集》**1**23 (1973)。[36] B. A. Venkov，关于一类欧几里得多面体，《列宁格勒大学学报》，数学、物理与化学辑**9** (1954)，11–31。[37] Roman Vershynin，高维概率，剑桥统计与概率数学丛书，第47卷，剑桥大学出版社，剑桥，2018年。一本附有数据科学应用的导论，前言由 Sara van de Geer 撰写。

普林斯顿大学数学系，芬恩楼，华盛顿路，普林斯顿，新泽西州 08544-1000，美国 电子邮件地址：naor@math.princeton.edu 纽约大学库朗数学科学研究所计算机科学系，默瑟街251号，纽约，纽约州 10012，美国 电子邮件地址：regev@cims.nyu.edu